OPEN ACCESS

University of BRISTOL

This electronic thesis or dissertation has been downloaded from Explore Bristol Research, http://research-information.bristol.ac.uk

Author:
Hewlett, Emma M

Title:
Human Detection of Attacks Against Cyber-Physical Systems

General rights
Access to the thesis is subject to the Creative Commons Attribution - NonCommercial-No Derivatives 4.0 International Public License. A copy of this may be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode This license sets out your rights and the restrictions that apply to your access to the thesis so it is important you read this before proceeding.

Take down policy
Some pages of this thesis may have been removed for copyright restrictions prior to having it been deposited in Explore Bristol Research. However, if you have discovered material within the thesis that you consider to be unlawful e.g. breaches of copyright (either yours or that of a third party) or any other law, including but not limited to those relating to patent, trademark, confidentiality, data protection, obscenity, defamation, libel, then please contact collections-metadata@bristol.ac.uk and include the following information in your message:

• Your contact details
• Bibliographic details for the item, including a URL
• An outline nature of the complaint

Your claim will be investigated and, where appropriate, the item in question will be removed from public view as soon as possible.

Human Detection of Attacks Against Cyber-Physical Systems

By

EMMA M. HEWLETT

School of Engineering
UNIVERSITY OF BRISTOL

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of DOCTOR OF PHILOSOPHY in the Faculty of Engineering.

APRIL 2020

Word count: 42,212 (excluding appendices)

Abstract

Cyber attacks are a persistent threat that is continually evolving to match the technology landscape. This increasingly includes systems that incorporate physical components, including personal electronic devices, Internet of Things devices and large scale industrial systems that are increasingly being connected to the internet. Despite evidence that attacks are both directly targeting and inadvertently impacting such cyber-physical systems, to date very little research has sought to explore how good the human users of these systems are at observing and correctly identifying these attacks.

This thesis seeks to address this knowledge gap, exploring people's awareness of threats and whether the nature of cyber-physical systems means that attacks against them are detectable by human users. The main contributions from this work include: *(1)* A systematic study of how humans protect against, detect and respond to cyber attacks; *(2)* A detailed explanation of the devices that people use and their level of awareness of the sensors and components that these devices incorporate and how these could be targeted; *(3)* Information on how people detect attacks against physical devices versus more traditional attacks; *(4)* Information on the types of attacks that can be observed both directly from the behaviour of the physical components of an industrial control system and from the data outputs of the system; *(5)* Findings that show that, whilst attacks are often observed as anomalies, these errors are frequently attributed to technical error or failure; *(6)* Finally, this thesis explores whether findings relating to susceptibility and the ability to detect different attacks against physical systems can be generalised across different forms of attacks and systems.

Word Count: 264

Dedication and acknowledgements

This work was supported by the DYPOSIT: Dynamic Policies for Shared Cyber-Physical Infrastructures under Attack project through the Engineering and Physical Sciences Research Council (EPSRC reference- EP/N021657/2). My thesis has also been supported by both Lancaster University and the University of Bristol and thanks are given to both institutions.

Special thanks goes to Professor Awais Rashid, my main supervisor for all of your advice and guidance over the last four years and for supporting my future plans. Special thanks also to my supervisors Professor Utz Roedig and Professor Paul Taylor for all the support you have offered.

Recognition is also due to Dr Benjamin Green for the development of the Security Lancaster testbed that was used in Chapter 7, and to Kiran Caudrey-Joshi for adapting the attack scripts on the testbed for this study. Thanks also to Dominic Lindsay for writing the scripts for the study in Chapter 6. Without all of your support, these studies, and this thesis would not have been possible. Thanks also, to everyone who volunteered their time to participate in my studies.

On a personal note I would like to express my gratitude to my family for their support of my work, all of their encouragement and the constant belief that I would succeed. Finally thank you to all of my friends, office companions and work colleagues, who knowingly and unknowingly, have made the last few years an enjoyable experience.

Author's declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: E. M. Hewlett
DATE: 27.04.2020

TABLE OF CONTENTS

List of Tables

Table **Page**

List of Figures

Figure **Page**

List of Abbreviations

ACARS	Aircraft Communication Addressing and Reporting System
CDM	Critical Decision Making
COTS	Commercial off the Shelf
CPS	Cyber-Physical Systems
DDoS	Distributed Denial of Service
DoS	Denial of Service
EPPM	Extended Parallel Process Model
GNSS	Global Navigation Satellite System
GPWS	Ground Proximity Warning System
HMI	Human Machine Interface
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems- Cyber Emergency Response Teams
IDS	Intrusion Detection Systems
ILS	Instrument Landing System
IoT	Internet of Things
IP	Internet Protocols
MAC	Media Access Control
MCDU	Multipurpose Control and Display Unit
NFC	Near Field Communication
PLC	Programmable Logic Controllers
PMT	Protection Motivation Theory
SCADA	Supervisory Control and Data Acquisition
TCAS	Traffic Collision Avoidance System

TTAT	Technology Threat Avoidance Theory
VPN	Virtual Private Network

Part I

Thesis Introduction

CHAPTER 1

INTRODUCTION

1.1 Background

In 2010 we saw the emergence of Stuxnet. Whilst not the first documented attack against an Industrial Control System (ICS), this was the first discovered malware targeted solely at sabotaging these types of systems. This particular malware, which targeted Siemens Programmable Logic Controllers (PLC)s commonly used by Nuclear plants in Iran, resulted in the destruction of some of Iran's nuclear centrifuges [1]. This attack highlighted not only the potentially huge impacts of attacks against large scale industries and critical national infrastructure, but also the potential of cyber attacks to have an impact on physical systems.

Despite this increased awareness, ICS which were once often bespoke and completely isolated systems are still increasingly being connected to the internet. The increasing use of Commercial Off The Shelf (COTS) products and Internet Protocols (IP) within these systems also means that ICS increasingly resemble more traditional IT systems, and as such they are increasingly vulnerable to malicious interference. The vulnerability of critical national infrastructure to large scale attacks and the potential consequences of such an attack was again demonstrated in the 2015 and 2016 attacks against Ukranian power plants. These attacks again made use of malware, but in this case the malware was used to gain access to the machines controlling the power plant's circuit breakers. This allowed the attackers to switch off the power within the plant, with the 2015 attack causing a loss of power to over 200 thousand homes within the country [2].

Both of these attacks were large and well coordinated. However, attacks do not require this level of sophistication to have an impact on industrial or Cyber-Physical Systems (CPS). An example of an untargeted attack causing disruption against physical systems is the Slammer worm. In 2003 this malware was able to infect the Davis-Besse nuclear plant resulting in a

slowing down of the plant network, as well as crashing a computerised display panel which monitored the crucial safety indicators including temperature and radiation sensors [3]. Other examples include i) A software vulnerability being exploited in dynamic road message signs in San Francisco that allowed attackers to show the message 'Godzilla Attack! Turn back' [4, 5], and ii) In 2000 there was a publicly reported attack against a sewage facility in Maroochy Shire. This attack involved an individual using stolen radio equipment to issue commands to equipment he had helped to install and resulted in a pump station failure. The result of this attack was 800,000 litres of raw sewage being spilled out into local parks and rivers [6]. As these examples highlight, the impact of attacks against CPS can lead to especially pronounced real world consequences due to the impacts on physical components. The risks faced by large scale physical systems is also borne out in the numbers, with the Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) reporting that they responded to 295 cyber incidents in 2015, a 20% increase from the previous year [7].

However it is not only large scale physical systems that offer opportunities to attackers. Smartphones and laptops increasingly incorporate multiple physical sensors and physical components such as cameras, microphones, GPS and orientation sensors which could be compromised and used maliciously against the device owner. The proliferation of internet enabled toys and the internet of things (IoT) devices for home control further increases the number of potential targets for attackers. This can again be seen in analyses of the number of attacks that are occurring with a reported 249% increase in brute force attacks against IoT between 2016 and 2017 [8] and a 54% increase in the number of new mobile malwares identified between 2016 and 2017 [9].

Media reports also provide specific examples of attacks against physical devices. These include everything from smart printers being hacked to print unwanted messages, to baby monitors being used as spy cameras [10, 11]. Attacks against these devices can also impact more than just the device's owner. An example is the Mirai botnet where compromised IoT devices were used to launch a Distributed Denial of Service (DDoS) attack against the service provider Dyn, resulting in Twitter, Netflix and Reddit being temporarily unavailable to internet users [12, 13].

Research has explored methods for minimising the risk of attacks against cyber-physical devices. However, much of this work has focused on technological methods for identifying and managing cyber threats against cyber-physical systems. Measures to protect large-scale CPS have included research to adapt Intrusion Detection Systems (IDS) to CPS, exploring different methods to ensure that communications within these systems are kept secure, and methods for either augmenting legacy components [14] or of making newer, more secure, components that can replace these legacy components. However, whilst improving the technological aspects of security is an important activity, it is equally critical to consider the human users of these large-scale CPS. Focus only on the technology overlooks the fact that security is often made at an organisational level with the amount of effort and resources set aside for security dependent on the extent to which security is prioritised. It also overlooks the fact that many older systems will often have

been designed in isolation from other systems and networks and so will often not have considered security in their design, and as they have become more interconnected has resulted in unintended opportunities that could be exploited.

This focus on technological approaches has often come at the expense of exploring the human element and how the human system operators could offer potential security opportunities. This is despite the fact that previous attacks against CPS highlight that there are many cases of attacks that have been started by first attacking or exploiting the users, e.g., through spearphishing attacks against corporate networks in order to gain access to wider CPS. Perhaps more importantly, however, it also comes despite examples of the human users being able to observe security issues. In the case of detecting attacks against ICS there are at least two reported instances where the individuals working with these systems have observed malicious behaviour. Firstly, in 2016 Wired published anecdotal information that during the 2015 Ukraine power plant attack one of the system control operators observed their mouse tracker moving on screen, without their input, to manually manipulate the system's circuit breakers [2]. Whilst there is no evidence that this occurred, and if so how they responded is unknown, it does highlight a possible situation where had a user had an appropriate policy or plan of action for reporting suspicious behaviour then it could have potentially minimised the impact of the attack or aided in identifying the cause. In the case of the Maroochy Shire waste plant, whilst the attack was initially considered to be a technical failure when a worker started changing settings in one of the pumping stations and observed that these settings were being changed back it was identified as a malicious individual making the changes [15].

The human element of CPS is no less important when talking about smaller scale or personal CPS and yet many of the same research gaps remain. Research in this area has largely focused on attitudes towards different security mechanisms or to using IoT devices rather than looking at actual usage. Given that many IoT and smart devices which make use of cyber-physical components have many of the same issues around a lack of encryption as larger scale CPS, it is important to note the research gap regarding whether the users are aware of these security concerns. This knowledge gap also relates to whether individuals take any measures to protect their devices and whether they can detect different types of malicious behaviours against these systems. In particular studies of an individual's susceptibility to and their ability to detect specific attacks have instead focused on common attacks against traditional IT systems such as phishing emails and spoof webpages. In other words very little is understood about whether human users can help to identify potentially suspicious behaviours within a cyber-physical system.

Additionally, to date, there is no specific research seeking to answer whether the wealth of literature currently available into the detection of traditional attacks can be generalised across to different forms of attacks and types of systems. This is an important question across these two strands and which could help define our current level of knowledge in relation to the security of CPS.

1.2 Research Direction and Objectives

Considering several examples of attacks against physical devices highlights the potential benefits of exploring whether people can detect these attacks. Exploring the generalisability of these findings can also help to define our current level of knowledge and future research directions.

In the home environment individuals must usually rely on their own abilities to identify whether any of their, or their family's, devices have been compromised. A better understanding of how vulnerable home users are, and which types of attacks they are both aware of and can detect could aid in the development of security measures to help protect individuals from hard to observe attacks. Such understanding could also be used to inform the development of security advice to increase awareness of attacks.

On a larger scale the examples from the Ukranian attack and from the Maroochy Shire waste plant attack highlight that human users could help to add an additional layer of security to limit the progress of an attack or to mitigate its impacts. Understanding the types of attacks that people do, and don't, identify could also help organisations to make informed decisions about where to best invest security technology.

Research Direction: Against this context this thesis is organised around three key research questions.

1. Can human users identify attacks against cyber-physical systems?
2. Can we identify individuals who are better able to detect attacks against cyber-physical systems?
3. Are findings about the types of individuals who can detect attacks generalisable across different systems and attacks?

Objectives: Whilst in an ideal world all systems would have adequate security measures to prevent them from being compromised, this is not always the case. In light of this, the thesis seeks to explore the ability of users to act as an additional security buffer. The specific objectives of this thesis are therefore:

1. To explore and detail the current literature on human factors in security of cyber-physical systems.
    - To review the current literature on what makes people susceptible to different forms of attack including how individual differences influence the use of different security measures and how they may help with the detection of different forms of attacks.
2. To explore how human users protect cyber-physical systems in the home

  - To explore the different types of devices that people currently own and their awareness of how they can be attacked;
  - To experimentally test whether people can detect attacks against home devices and what sort of behaviours are labelled as suspicious;
  - To experimentally test the impact of individual differences in the detection of attacks against home CPS.

3. To explore the detection of attacks against CPS within industry by human users
  - To experimentally test whether people can detect different forms of attacks against ICS;
  - To experimentally test the impact of individual differences on the detection of attacks against industrial CPS.

4. To explore the generalisability of security findings across different systems and forms of attack
  - To discuss how research findings across devices and different attacks are similar and how they differ;
  - To discuss how the findings of this thesis relate to earlier findings across the security literature.

1.3 Approach

This thesis researches the ability of human users to observe attacks against cyber-physical systems and explores whether they are then able to identify these as attacks.

The methodological approaches used in the studies include interviews and surveys to explore users knowledge of different attacks against cyber-physical systems and whether individuals seek to protect themselves against these attacks. This helped to better understand the type of attacks that individuals may be faced with. However, the main approach taken through this thesis is to expose individuals to a range of different attacks against different systems and ask them to identify what types of behaviours they detect as unusual. This allowed exploration of what sort of system behaviours may be observable and detectable to the individuals using these systems. Participants were then asked whether they could attribute the cause of any unusual behaviours to explore whether people consider cyber attacks as a possible cause of strange system behaviours, with the impacts of priming individuals to consider cyber security also considered. The impact of different demographic factors were then explored via regression analyses to identify if whether people could detect an attack could be predicted based on various factors.

A key aspect of this work however is that the thesis explores the detection of attacks against a range of different systems and contexts.

1.3.1 Why Study the Detection of Attacks at Home and in Industry

The main research portion of this thesis is split into two different sections- identifying attacks against CPS at home and identifying attacks against CPS within industry. Studying the detection of attacks across different contexts offers several benefits.

Exploring the detection of attacks in a home environment allows a detailed exploration of the level of knowledge and importance that individuals have in relation to cyber-security. This includes knowledge of different types of physical components and how they can be targeted or compromised, and how they can be protected. Understanding the background of security awareness and knowledge of participants and how this relates to the detection of different attacks then allows a more complete and holistic picture to be built up around how knowledge, risk perception and use of security measures influences attack detection.

However, context is important and so to understand attack detection in a work environment this needs to be explored to see if, and how, this differs. Research looking at the human detection of attacks against CPS within a work context still has many gaps however. Attempting to address these gaps can provide valuable insight into whether human users can help to aid in providing security for these systems and help to highlight the types of attacks that humans may be particularly vulnerable to and which should be a key focus of technical security measures.

However, the main advantage of studying these two contexts and investigating some of the same individual differences is that the findings across these two strands can be compared. This provides valuable insight into whether findings from cyber security in one context can be generalised to other contexts, situations and attacks. This can help inform researchers as to the generalisability of the current knowledge base to different attacks and to larger scale systems. This is especially the case since research within an industrial context can be challenging and so knowing how generalisable findings from home environments are to this context could help shape the extent to which these challenges can be addressed.

1.4 Novel Contributions

The main contribution of this thesis is to produce, what is to the best of the author's knowledge, the first structured systematic and multidisciplinary study into whether people can observe, and then identify, the causes of different types of attacks against cyber-physical systems. In particular in seeking to address the objectives identified above the novel contributions of this work are:

1.4.1 A Systematic Literature Review of Human Factors in Cyber Security:

This thesis provides a systematic and up to date literature review exploring susceptibility to and the protective measures that individuals take to prevent falling victim to different cyber attacks. Identifying IT knowledge, risk perceptions, threat avoidance, perceived efficacy at dealing with a

cyber incident as key indicators as to whether individuals use security measures with many of these same factors then linked to the detection of attacks.

1.4.2 To Explore How Human Users Protect Cyber-Physical Systems in the Home

This thesis provides detailed research into why people take different security approaches for different types of electronic devices, and the decision making approaches behind these decisions. It finds that a lack of knowledge about how to protect different devices and a desire to protect some types of information more than others are key reasons for taking different approaches. This work also explores the types of behaviours that individuals consider to be suspicious, highlighting that for many individuals, priming to consider cyber security only alerts them to issues that occur onscreen.

1.4.3 To Explore the Detection of Attacks Against Cyber-Physical Systems Within Industry by Human Users

This thesis provides one of the first explorations into whether different individuals can detect a variety of different attacks against a water plant based on different types of information. The work also highlights that some forms of attack, such as a Denial of Service attack, are more likely to be detected than others such as replay attacks whilst also exploring where people attribute the blame for different types of errors.

1.4.4 To Explore the Generalisability of Security Findings Across Different Systems and Forms of Attack

This thesis presents a detailed exploration and discussion of whether findings into whether people can identify different forms of attacks can be generalised across different systems and attacks. The work highlights that whilst some forms of attacks are more observable than others, individual differences cannot be used to predict who is more likely to detect a cyber attack.

1.5 Outline of Thesis

This thesis is comprised of several parts which are structured as follows:

Part I: Introduction and Literature Review. Part I consists of this chapter and the literature review, introducing the topics of this thesis in detail and exploring where gaps in the literature remain.

- *Chapter 2- Individual Differences in Susceptibility to and Ability to Detect Cyber Attacks:* starts with an overview of our current understanding of how individuals approach cyber

security. This chapter explores the methods that people take to protect various devices from cyber attacks and the impact of individual differences on what approaches they use. It also details the current research regarding how people detect attacks and whether certain individual differences can influence someone's susceptibility to different forms of attack.

– *Chapter 3- Detecting Attacks Against Cyber-Physical Systems:* defines the types of attacks that this thesis focuses on and gives a more detailed discussion of the literature that has explored attacks against CPS in regards to the human security aspects.

Part II: Cyber-Physical Systems in the Home Environment. Part II details the first experimental strand of this thesis and consists of three chapters that focus on 'smart' and 'IoT' devices that are commonly used and which may also be found in the home such as smart phones and tablet devices.

– *Chapter 4- Have Users' Security Awareness and Approaches Evolved with the Prevalence of 'Smart Devices'?* This chapter details a survey that explored the types of devices that people are currently using, and the level of awareness that people have regarding the different physical sensors and components incorporated into the devices they own. The survey also explores whether typical home users are aware of how these sensors could be maliciously targeted or compromised and whether or not they take any security precautions to try and reduce the chances of this occurring.

– *Chapter 5- To Secure or Not Secure: Exploring Why People Use Different Security Strategies Across Different Devices:* This chapter expands on the findings of chapter 4. Having identified that many individuals had a much greater awareness of security and security measures for computers and laptops than they did for newer devices and that they still protect laptops and computers more than any other devices, Chapter 5 details an interview study to explore people's rationale for protecting different devices differently.

– *Chapter 6- Detection of Attacks Against Home Systems:* explores whether people can identify a range of different attacks when primed to consider security, as well as exploring what sort of system behaviours are considered to be malicious. The attacks involved in this study included traditional attacks such as phishing emails as well as appearing to switch on a camera placed next to the computer screen.

Part III: Cyber-Physical Systems Within Industry. Part III details the second experimental strand of this thesis and consists of two chapters exploring whether people can detect attacks against a water control plant. Whilst it was initially planned that this part would follow a similar structure to Part II, the lack of access to suitably qualified individuals working with ICS alongside the need for organisations to keep some security aspects confidential meant that we were unable to look at current use of security within industry. Given these challenges the focus was, therefore,

on examining what types of behaviours within these systems were considered suspicious and/ or malicious.

- *Chapter 7- Detection of Attacks Against in an ICS Testbed* This chapter details a study using the Lancaster University water plant test bed looking to explore whether people were able to observe features of different attacks against a simulated water-plant. We describe the results showing that people can identify various attacks, however some are more easily observed that others and that blame for any errors is often assigned to technical rather than security issues.
- *Chapter 8- Detection of Attacks Against a Water Control Plant From System Data:* explores whether individuals can identify attacks from an ICS by observing the data, rather than observing the actual physical components. This chapter, therefore, details a study that was designed to look at whether attacks could be detected from the data output of Supervisory Control and Data Acquisition (SCADA) systems. This study also expands upon the earlier pieces of work by exploring how detection of attacks differs based upon whether or not an individual has been primed to consider security.

Part IV: Thesis Conclusions and Discussion. Part IV synthesises all the evidence and findings from the first three sections whilst discussing the implications of the two experimental sections.

- *Chapter 9- Final Conclusions and Discussions:* This chapter brings together the key findings from the two experimental sections to highlight how findings across different types of systems differ and how they are similar. It provides a summary of all the findings of this work conducted along with an in depth discussion of what these findings mean for human security of cyber-physical systems and where future work should take this work forward.

CHAPTER 2

INDIVIDUAL DIFFERENCES IN SUSCEPTIBILITY TO AND ABILITY TO DETECT CYBER ATTACKS

In order to explore whether the factors that can influence an individual's susceptibility to attacks and whether an individual can detect attacks can be generalised across different types of systems, we first need to review current academic perspectives on what makes an individual more able to identify an attack. This chapter, therefore, presents the results of a systematic literature review that explored several questions. i) what security approaches do people take in order to minimise the risk of experiencing a cyber attack? ii) individual differences in the security approaches that people use? iii) what do we currently understand about how people detect attacks? iv) what individual differences have an impact on whether someone is likely to detect or fall victim to an attack? and v) how do individuals respond in the event of an attack? This chapter, therefore, sets the scene of this thesis by identifying the types of attacks that people may be at greatest risk of and by identifying the factors that are currently understood to impact on attack detection so that these can be explored across a range of different attacks and systems.

2.1 How Do People Seek To Secure Their Devices?

A key part of understanding whether people are likely to fall victim to different types of attacks is to consider whether people are aware of these threats and whether individuals seek to prevent themselves from falling victim. Individuals can seek to maintain their security in various ways, from using passwords to secure devices and accounts, to the use of specific security software, to behaving securely when online. However, this literature review has demonstrated that even when people are aware of different security measures, they are not always employed, with the

use of security measures varying between individuals and across devices. It also highlights that research has focused on certain forms of security measures over others.

Passwords: One of the most studied approaches to maintaining security is the use of passwords. Evidence suggests that, despite a few misconceptions, people can typically identify what constitutes a strong password [16–18]. Yet despite this people report using similar password making strategies [19] and data sets of leaked passwords reveal that many real-life passwords could be classified as weak or using similar patterns [20, 21]. Additionally, people report engaging in numerous insecure practices such as reusing whole or part of passwords [16, 18, 19, 22–28] or using aids, such as writing passwords down [18, 19, 24, 26, 27]. Whilst much of the research focused on the passwords of English speakers work by Abbott and Garcia (2015) looked at the password creation and recall of both English and Spanish speakers when they were given different rules or prompts to follow. One key finding was that Spanish participants appeared to be less likely to use words within their passwords compared to the English speakers [29].

One explanation is password overload, people not only need increasing numbers of passwords but passwords are increasingly complex with password trends suggesting that the average length of password has been increasing over the years [18]. Studies show that people struggle to meet the criteria of strict policies [27, 28] and find the resulting passwords harder to remember [28, 30] with changes to password policies also causing annoyance [26]. They also fail to prevent people from using meaningful information [30]. People therefore report reusing strong, frequently needed passwords to make this task more manageable [25]. Password reuse can therefore be a rational choice with many people reporting that they reuse passwords for unimportant accounts or stronger passwords for more important accounts [16, 18, 19, 22, 24, 31, 32]. Work by Camp (2014) and Camp et al. (2016) has explored using random visuals to aid with password creation and recall, concluding that these can help to increase the entropy and length of passwords [33, 34]. This supports work by Abbott and Garcia (2015) who also found better recall when using image prompts [29] however this approach is not commonly used.

A second explanation for insecure password practices is that individuals may not understand how password hacking tools work with people believing that names and dates not directly related to them are safe to use [19].

Factors that can then increase the security level of a password include the perceived trustworthiness of a site [35], password meters [36], although in one study this only worked for high value accounts [37], and the use of fear appraisals [38, 39]. However password meters have previously been found to be inconsistent at assessing the security of Chinese passwords [40]. One study by Abbott et al. (2018) which explored leaked passwords from US universities found that policies requiring longer and more complicated passwords led to less chance of passwords being reused [41].

Account security on mobile devices has also been explored, with one study concluding that

only 64.4% of individuals used screen locks [42] and that many individuals have increased the time for the screen to lock [43]. Research by Harbach et al. (2014) involving a survey and interview design identified several reasons for and against using a code lock. Reasons for included a general protection motivation as well as a desire to protect information or specific individuals from gaining access. Reasons for not locking a screen then included not perceiving a threat as well as finding locking a phone inconvenient [44].

Passwords and PINs on mobile devices are also reused [43] with passwords on these devices often having fewer uppercase letters and special characters [45] highlighting the effects of poor usability. Although work by Yang et al. (2014) suggested that people may compensate for this by creating longer passwords [46]. This research therefore highlights how even simple security measures can be neglected by individuals, and that people appear to take different approaches for newer devices.

Table 2.1 presents the research that has been conducted on password security alongside an evaluation of the different study methodologies.

Table 2.1: Current Research on Password Security

Report	Methodology	Evaluation
Grawemeyer and Johnson [31]; Hayashi and Hong [23]; Duggan, Johnson, and Grawemeyer [32]; Inglesant and Sasse [28].	Diary Study	+ Not based on memory/ recall; + Gathers data over a longer period of time; - Based on self-reports; - Typically uses small samples; - Have only investigated password events on computers.
Wash, Rader, Berman et al. [25].	Data Analysis - Log Data	+ Real password information gathered; + Compared real password use to self-reported password use; + 134 participants (- all students); - Data collection couldn't differentiate between successful and failed log in attempts.
Veras, Thorpe, and Collins [21]; Li, Han, and Xu [47]; Wang, Cheng, Gu et al. [40]; Han, Yu, Li et al. [48]; Shen, Yu, Xu et al. [20].	Data Analysis- Leaked passwords	+ Real life passwords; + Large sample; - No control on account importance or ability to examine demographic factors; - Can't guarantee nationality or language of individuals.
Von Zezschwitz, De Luca, and Hussmann [18]; Egelman et al. [43]; Stobert and Biddle [24]; Ur, Noma, Bees et al [19]; Mylonas, Kastania and Gritzalis [42]	Interviews	+ In-depth data collection; + Allows exploration of new or interesting topics; - Small samples; - Based on self-reports.
Notoatmodjo and Thomborson [22]; Zhang and McDowell [39]; Tam, Glassman, and Vandenwauver [16]; Shay et al. [26]; Petrie and Merdenyan [49].	Survey	+ Typically large samples; + Typically refers to real password usage; - Self-Reported data; ? Lots of variability regarding whether account importance is examined.
Campbell, Kleeman, and Ma [30]; Komanduri et al. [27]; Ur et al. [36]; Jenkins, Grimes, Proudfoot et al. [38]; Melicher et al. [45]; Ur et al. [17].	Online Experiment	+ Large sample; + Participants are often required to memorize passwords (and re-log in) as well as create them; - Not real passwords or data; - Convenience samples; ? Lots of variability regarding whether an important account is used.
Egelman, Sotirakopoulos, Muslukhov et al. [37]; Grimes, Marquardson, and Nunamaker [35]; Yang, Lindqvist, and Oulasvirta [46].	Lab Experiment	+ Password strength assessed; + Variables controlled; - Typically small samples of students; ? Lots of variability regarding whether a real or roleplaying account is used.

Installing Security Software and Hardware: Research exploring the use of security software, has also identified that the use of security approaches varies across devices. Whilst studies find

very high uptake of antivirus software on personal computers (85.8% [42] or 95.5% [50]) the use of antivirus software on other devices lags behind, with Mylonas et al. (2013) finding that only 24.5% of individuals use security software on their smartphone [42].

Work exploring the use of other forms of security software is sparse (see Figure 2.2), and sometimes contradictory. Of two studies looking at firewalls the first by Vrana et al. (2012) reported high proportions of participants (84%) using a firewall [51], however an interview study by Raja et al. (2010) suggested that firewalls are poorly understood and utilised [52]. One explanation may be a knowledge gap with a study by Bidgoli et al (2016) reporting that people often hold misconceptions such as that Apple devices don't get viruses [50] and Sharma et al. (2017) concluding that 61% of individuals are unaware of phishing detection tools [53]. Finally, one third of users were found to want more interaction with their antivirus software [54], suggesting a need to better understand what users want from security software.

Table 2.2: Current Research on the Use of Security Software

Report	**Methodology**	**Evaluation**
Bidgoli, Knijnenburg and Grossklags [50]	Interviews/ Survey	- Small sample; - Self-reports.
Mylonas, Kastania and Gritzalis [42]	Interviews	- Convenience sample on street (may have been reluctant to open up); - Interviews were short with insufficient time to explore all the issues; -Self-reports.
Sharma, Meenakshi and Bhatia [53]	Survey	- Small sample (50) of all IT students; - Results may have reflected a desire not to use software rather than a lack of awareness about it
Vrana [51]	Survey	- Sample was all students; - Self-reported measures.
Raja, Hawkey, Jaferian et. al [52]	Interviews	- Small sample (30) - Self-reports.

Security Mindfulness: Security can also be maintained through vigilance. Researchers have therefore explored whether people consider security when downloading new software or applications, see Figure 2.3. Work by Felt et al. (2012) explored this area and demonstrated that only 17% of participants pay attention to application permissions, with only 3% able to demonstrate that they understood them [55]. One proposed explanation is that many individuals trusted application repositories despite many being unaware of whether these repositories tested the applications [42, 56] or that again they lack knowledge with one study concluding that people are willing to behave securely when shown how [57]. Alternative explanations suggest that peer recommendations and the perceived value of an application are the biggest factors in deciding whether to download it [58], although people avoid applications that want information on their friends [58].

Installing Security Updates: One simple approach to security is to regularly install security updates, yet many individuals neglect to do this [51, 60]. Tian et al. (2015) found that 59.3% of participants had chosen not to update at some point [61]. Reasons for this often relate back to usability and concern regarding how updates could disrupt current activities, uncertainty of

Table 2.3: Current Research on Security Mindfulness

Report	Methodology	Evaluation
Bidgoli, Knijnenburg and Grossklags [50]	Interviews/Survey	- Small sample and based on self-reports.
Felt, Ha, Egelman et. al [55]	Survey/ Experiment	- Small convenience sample; + Used multiple methodologies.
Krasnova, Eling, Schneider et. al [58]	Survey	- Student sample; - Based on self reports.
Rajivan and Camp [59]	Experiment	- Simulation, so no risk to participant's information; + Used a large sample.
Mylonas, Gritzalis and Tsoumas et. al [56]	Interviews	- Convenience sample on street (may have been reluctant to open up); - Interviews were short with insufficient time to explore all the issues; - based on self-reports; + Large sample.
Mylonas, Kastania and Gritzalis [42]	Interviews	- Convenience sample on street (may have been reluctant to open up); - Interviews were short with insufficient time to explore all the issues; - Based on self-reports.
Struse, Seifert, Ulenbeck et. al [57]	Survey/ Experiment	+ Used a large sample; + Collected real-life data; - No explanations of why users ignore the security app.

why they should [62], a lack of time and concern that the update may be harmful [60] or concerns about functionality changes, privacy invasion or not seeing a reason to update [61]. Studies exploring this topic can be seen in Table 2.4.

Table 2.4: Current Research on Installing Security Updates

Report	Methodology	Evaluation
Fagan, Khan and Buck [60]	Survey	- Self-reports; - Young sample.
Vrana [51]	Survey	- Sample was all students; - Self-reported measures.
Vaniea, Rader and Wash [62]	Interviews	- Small sample (37); - Self-reports.
Tian, Liu, Dai et. al [61]	Survey/ experiment	+ Large sample; multiple methodologies; + Real behaviours; - Experimental app was unimportant.

Organisational Security: Within work contexts, general computer users have been found to perceive that their employers and IT departments are responsible for providing cyber security [63, 64]. Decisions regarding security behaviour were then influenced by perceived susceptibility to attacks and confidence in their ability to behave securely [65] and experience of security breaches, and how security behaviours may impact job productivity (e.g. delaying security updates when busy) [64]. Research into organisational security can be seen in Table 2.5.

Table 2.5: Current Research on Organisational Security

Report	Methodology	Evaluation
Blythe, Coventry and Little [64]	Interviews	- Small number or individuals; - Self reports; + Repetition in themes suggests data saturation was achieved; + Use of vignettes to elicit responses.
Gross and Rosson [63]	Interviews	- Only 12 participants (all college educated); - Self-reports.
Ng, Kankanhalli and Xu [65]	Survey	- Small sample; - Self-reports; - Doesn't detail specific security behaviours; + Includes individuals from different demographics.
Line, Zand, Stringhini et. al [66]	Interviews	- Self reports from a small sample; - Interviews occurred online; - Non-disclosure agreements prevent full transcripts from being shared; + Population that is not often reported.
Lévesque, Chiasson, Somayaji et. al [54]	Field Study	- Low number of threats to draw data from; - No causal link; - Participants were aware it was a study; + Studied over four months; + Real month computer usage.

Summary: Current research has explored the use of a wide range of security measures. However, whilst several studies have identified that people appear to use fewer measures on mobile devices, there has been no concerted effort into studying whether people seek to protect a wide range of different devices. In addition there has been little exploration into whether people are aware of different types of attacks that could be targeted against these devices and what motivates individuals to use security measures.

2.2 Explaining Variation in Whether Individuals Use Security Measures

Given the variance in the use of protective measures, researchers have sought possible explanations to predict who does and doesn't use different security approaches.

Theoretical Models: One approach to explaining this variation is through theoretical models such as the Technology Threat Avoidance Theory (TTAT) [67] which has been used to investigate the use of anti-spyware [68], malware avoidance [69], security when shopping online [70] and phsihing avoidance [71]. Together these studies have highlighted the importance of perceived threat severity, motivation to avoid threats, self efficacy and safe guard costs. Secondly, the Protection Motivation Theory (PMT), also emphasises the importance of response efficacy and response costs in the context of phishing [72] and risky online behaviours [73]. A third model developed from interviews also highlighted the role of self-efficacy and fear of cybercrime [50]. Findings supporting these models suggest that people seek to protect themselves as security threat awareness increases [74, 75] whilst telling individuals they were at risk, increased both security intentions and behaviours [76]. Conversely however, work by Boehmer et al. (2015) and Mariani et al. (2014) has found that intentions to perform safety actions were not related to perceived susceptibility, the seriousness of threats [77] or perceived risk [78] suggesting that an awareness of the threats alone is not sufficient to promote security behaviour. A study by Nguyen et al. (2017) investigating the impact of security costs found that only 50% of participants were willing to pay $9-11 a month for better phishing filters or to wait 7-9 minutes for an anti-phishing filters to scan emails [79].

Individual Differences: Multiple individual differences have been studied in relation to whether individuals use security measures. One key factor, has been an individual's level of security knowledge with numerous studies highlighting that individuals with higher security knowledge are more likely to be aware of, and use, security measures [71, 78, 80, 81]. Computer scientists have then been found to have harder to guess passwords [82] and IT students show more concern for opening email attachments [83]. Work has also found that many people are only aware of a limited number of risks which limits their ability to make decisions around what security measures to adopt [84].

A second well studied factor is gender and studies such as Mazurek et al. (2013) have concluded that men have slightly stronger passwords [82] but also report greater difficulty remembering them [49]. Whether this is a true gender difference or can be explained by other factors however still needs exploring with Mazurek et al. (2013) identifying that other factors may help to partially explain these effects. For example the IT department (which typically have a greater male population) also had significantly more secure passwords [82]. Men have also been found to report significantly higher anti-phishing self-efficacy and anti-phishing behaviour [85], although again the sample was largely university based with participants coming mostly from science and engineering or humanities colleges although no gender break down between these departments is provided. Further exploration of the impacts of gender versus IT knowledge is therefore required.

Several studies have also explored the potential impacts of culture. Work by Dinev et al. (2009) found that Americans had greater knowledge of antispyware and greater intentions to use it than Koreans [86]. Work by Uhomoibhi et al. (2011) found that Qatari participants were less likely than British participants to use anti-phishing software and to be concerned about phishing [87]. However whilst several other studies have explored culture, very few countries have been examined, with many factors uncontrolled for and few attempts made to explain any differences that have been found.

Social Influence: The behaviours of our peer group can also influence the security measures that we take, with people often using stories to give computer advice which are then incorporated into how people perceive cyber threats [88]. Das and Kim et al. (2014) reported that 40% of security behaviour changes are implemented due to external social influences e.g. observing a friend's behaviour, discussing new threats or experiencing a security breach [89]. A study of 46,000 Facebook users, by Das and Kramer et al. (2014), found that when people were advised that their friends were using recommended security features 4% implemented one of the features within a week [90].

Mental Models: Mental models and the mental shortcuts these can introduce are beneficial in dealing with many situations, however, they can also introduce biases into thinking. Positively however, individuals who hold models regarding hackers and viruses reporting taking more precautions to protect themselves [91]. Technical knowledge has then been found to influence mental models changing perceptions of privacy threats and how information is handled [92]. Further research is needed to study if training to improve the accuracy of individuals' mental models can aid them in recognising and dealing with attacks.

Finally work by Herath et al. (2009) has suggested that both intrinsic and extrinsic motivations can increase secure behaviours [93].

Table 2.6 presents the range of factors that have been studied, alongside an evaluation of

these studies.

Table 2.6: Individual Differences in Utilising Cyber Security Measures

Study	Gender	Age	Personality	Computer Use	IT Knowledge	Culture	Risk perceptions	Self-efficacy	Threat Avoidance	Social Norms	Other	Evaluation
Petrie and Merdenyan [49]	X					X						- Small samples in each culture; - Chinese participants recruited in Turkey and UK; - Self-report.
Nguyen, Rosoff and John [79]											X- Cost	+ Large sample; - Experimental study, no real costs to participants; - Self-reports, not actual behaviours.
Singh, Cabral, Demosthenous et al. [94]											X- Disability	+ Mixed demographics; - Self-reported information.
van Schaik et al. [75]	X	X		X			X				X- Control and voluntariness	+large sample; + Multiple cultures - Self reports.
Dinev, Goo, Hu et al. [86]						X		X				- Convenience sample of students; - Technical knowledge was not controlled. for.
Milne, Labrecque, and Cromer [70]	X	X		X								+ Large sample; + Non-student population; - Self-reported data.
Davinson and Sillence [76]							X					- Small sample (students); - Few male participants; - Self-report data.
Uhomoibhi, Al-Hamar and Dawson et al. [87]						X						+ Large sample; - Self-reported knowledge.
Herath and Rao [93]											X- Motivations	+ Large sample from multiple organisations and age groups; - Self-reported behaviour.
Radar, Wash and Brooks [88]											X- Social influence	+ Large sample; - All students; - Assumed all people tell stories; - Only asked for one story.
Das, Kim, dabbish et al. [89]											X- Social norms	+ Small sample; - Self-reports; - Assessed inter-rater reliability.
Das, Kramer, Dabbish et al. [90]											X- Social norms	+ Large sample; + Real-life behaviours; - Only examined behaviour changes.
Wash and Radar [91]		X			X		X	X				+ Large sample; - Self-reported behaviours.
Kang, Dabbish , Fruchter et al.[92]					X							-Small sample; + Multiple methods to gather data; + Assessed technical knowledge.
Liang, and Xue [68]							X	X	X			- Convenience sample of students.
Blythe and Coventry [72]							X	X				+Large sample; - Self-reports.
Jansen, Jurjen and van Schaik [95]							X	X			X- Fear	+Large sample; - Self-reports.
Kaye [96]	X											- Self-reported data; - Some of the participants had personal relationship with the researcher.
Duggan, Johnson and Grawemeyer [32]											X- Occupation	+ Diary-study, (not based on recall);- Small sample (some groups consisted of only 6).
Aldossary and Zeki [97]					X	X						- Small sample with only students in each condition.
Mazurek, Komanduri, Vidas et al. [82]	X				X							+ Large sample of real passwords (25,000).
Arachchilage and Love [71]							X	X				- Only used individuals aged 18-25; - self-reports.
Chen, Paik and McCabe [98]						X	X					- Self-reports; - Convenience samples.
Aldossary and Zeki [83]	X			X		X						- All student sample; - Self-report.
Boehmer, LaRose, Rifon et al. [77]								X				+ Large sample; - All students; - Self-reports.
Egelman and Peer [99]			X									+ Large sample; + Multiple studies to investigate different areas in detail; -Self-reports.
Gratian et al. [100]	X		X				X				X- Decision Making	+ Large sample; + Multiple security measures investigated; -Self-reports.
Flores, Holm, Ekstedt et al. [101]						X			X			+ Large simulated study;- Cultural aspects may reflect organisational culture rather than the impacts of country's culture; - Whilst significant, differences between groups were weak.
Ion, Reeder and Consolvo [80]					X							- Self-reports; - Convenience sample; - IT expertise was self-defined.
Rinn, Summers, Rhodes et al. [102]							X					- Small sample; - Self-reports.
Whitty, Doodson, Creese et al. [103]			X		X							- Large sample; - Self-reports.
Forget, Pearman, Thomas et al. [104]					X							+ Gathered real-life data from individual's computers; + Individuals were aware that data was gathered; - Small sample especially for interviews.
Hanus and Wu [81]					X							- Sample was all students; - Limited to desktop security.
Petrie and Merdenyan [49]	X					X						- Small samples in each culture; - Chinese participants were recruited from Turkey and UK; - Self-reports.
Chou and Sun [73]	X							X			X- Social norm	+ Large novel sample group; +Follow up interviews; - Self-reports.
McCormac et al. [105]	X	X	X				X					+ Large sample; - Self-reports.
Anwar et al. [106]	X											+Large sample; - Self-reports.
White, Ekin and Visinescu [74]					X			X				+ Large sample; - Self-reports.
Young, Carpenter, and McLeod [69]							X	X				+ Large sample; - All students; - Self-reports.
Sun, Yu, Lin et al. [85]	X							X				+ Large sample; - Self-reports.
Bidgoli, Knijnenburg and Grossklags et al. [50]								X			X- Fear	- Small sample; - Based on self-reports.
Mariani and Zappala [78]								X				- Small sample; - Based on self-reports.

Summary: There has been significant interest in exploring whether different characteristics make it more or less likely that an individual will make use of different security measures. Factors that have been frequently studied include gender, IT knowledge, risk perceptions, threat avoidance, perceived efficacy at dealing with cyber incident, age and personality. Overall the research suggests that IT knowledge, perceived risk, threat avoidance and being male do predispose an individual towards using more security measures. Findings for age and personality are more equivocal.

2.3 How Do People Detect Attacks?

Whilst work has explored susceptibility to attacks, comparatively few pieces of work have explored how individuals actually recognise behaviours that may be suspicious or how they make decisions regarding where to attribute the blame for a system error.

Aids for Identifying Attacks One approach has been to look at whether people heed security warnings designed to aid users in identifying suspicious or malicious events. Telemetry data has suggested that adherence to warnings varies based on the browser and the reported threat. E.g. malware warnings were ignored only 7.2% of the time on Firefox, however SSL warnings are more frequently ignored [107, 108] with up to 70% of SSL warnings on Chrome disregarded [109]. Studies have found that using polymorphic warnings (warnings that change or vary over time) [110–113] or active warnings (requiring the user to take consuming actions to disregard them) [114–116] or warnings that are personalised to the individual or the threat [117, 118] are more likely to be observed and potentially heeded.

However ignoring warnings does not always imply unsafe behaviours as many computer users may be presented with warnings for legitimate sites. Explanations for click throughs include familiarity and low perceived risk, with people twice as likely to ignore warnings for sites already in their browser history [119] or report that site reputation is the main reason for continuing onto a site [107]. There is also conflicting information from eye tracking studies on whether warnings are read [120, 121].

Using Different Cues to Detect Attacks: A second approach to exploring whether individuals can detect attacks has explored the cues people use to determine the legitimacy of emails and websites. These cues are discussed in Table 2.7. Overall research suggests that many individuals consider security features, additionally individuals will sometimes use poor indicators of security e.g. email security.

Table 2.7: How Computer Users Evaluate Security and Identify Attacks

Features Examined	Finding
URLs	Eye tracking suggests small numbers of individuals examine URLs [122] or email links [123].
HTTPS and SSL Indicators	Eye tracking suggests small numbers of individuals examine these features [124] [125]. Studies manipulating HTTPS indicators find people don't notice their absence [126, 127] although users report using them [128, 129].
Email Quality	Increased attention to email content e.g. poor grammar has been found to reduce response rates to phishing emails [130, 131] and to be a poor approach [132, 133].
Emotional Cues / Personal Content	The presence of emotional cues increases the chances that an individual will respond to phishing emails. [133–137], as did urgency cues [123] scarcity was particularly effective against younger individuals [138].
Security Images	Individuals frequently enter banking details when security images are missing [139] but some research has suggested that they have some benefit [140].

Summary: Current research has identified ways of making security warnings more effective, as well as the cues that individuals frequently use to assess the legitimacy of webpages and emails. However, whether people can identify a wider range of attacks and what information they would use to do so remains a research gap that has been poorly explored.

2.4 Explaining Variation in the Detection of Attacks

Considerable work has begun to try and identify what makes individuals susceptible to cyber-attack and whilst some results are consistent many findings are equivocal. (A previous review into this topic was conducted by Williams et al. (2017) [141]).

Technical Knowledge: One of the more consistent findings is that greater knowledge of computer systems and the attacks they face has been shown to reduce the likelihood of victimisation. In particular IT knowledge and experience can help individuals to recognise phishing attacks [142–147], with individuals able to accurately define phishing found to be less likely to become victims [148]. Past experiences of phishing victimisation also reduce an individual's susceptibility [149, 150]. Computer literacy and familiarity with platforms has also been associated with greater abilities to detect semantic social engineering attacks [151].

Difficulties with this type of research however are that participants' knowledge and experience is hard to assess objectively and so is often self-reported. In addition many studies looking at detection of attacks have primed the participants to consider security or the type of attack being studied.

Gender: Many researchers have found that men are typically better at identifying phishing attacks [152, 153], malicious pages [144] and social engineering attacks [154]. Conversely, multiple researchers have also found no gender differences for susceptibility to phishing attacks or malware downloads [155–158] and Blythe et al. (2011) found that men were more accurate at correctly identifying malicious emails, but only in younger individuals [130]. One possible explanation for the equivocal results comes from Sheng et al. (2010), mediation analysis of their results found that womens' greater susceptibility to phishing attacks could be partially explained by gender differences in technical knowledge and training [159].

One interesting study by Vidas et al. (2013) looked at evolving threats and explored whether individuals would scan potential malicious QR codes, finding that men were much more likely to do so. However this study involved placing posters with QR codes on a campus and city area and asking individuals to complete a questionnaire, and may instead reflect the fact that campus had a largely male population or that women may have been less likely to complete the questionnaire [160].

Personality Differences: When exploring personality in relation to attack susceptibility researchers have utilised different personality models, making results hard to compare. The most

frequently studied of these however is the big five model, consisting of openness, extraversion, conscientiousness, neuroticism and agreeableness [161]. Results are again equivocal, showing that it is hard to predict who is most likely to be more vulnerable. For example extroversion has been associated with accurately detecting different types of phishing attacks [162, 163]. Additionally, a study by Halevi et al. (2013) found that neuroticism is strongly linked to getting phished in women, but with no correlation in men [164], with a second study by Halevi et al. (2015) finding that conscientiousness is correlated to following a phishing link and running the requested plug-in in women but not men [165], suggesting that any personality relationships may be mediated by other factors. Additional findings include that higher sensation seeking is related to greater chances of having malware installed [166] and impulsivity has then been associated with phishing susceptibility [167].

Trust has also been associated with increased susceptibility to phishing [167] and social engineering attacks [168]. Whilst individuals with higher levels of the trait generalised communicative suspicion were found to be more likely to have higher perceived efficacy in detecting phishing emails, and to take a more strategic approach about whether to trust an email, although the researchers don't report on which approach is more effective at preventing phishing victimisation [169]. Higher attention vigilance and better short-term memory also reduced phishing susceptibility [150].

Computer Use: Additional factors that have been identified as explaining whether an individual may be susceptible to attacks are computer user's behaviours with studies of computer viruses showing that visiting more pages [170] and having more applications [156, 157] downloading software and online gaming [171] expose individuals to more malware.

Additional Factors: Researchers have investigated if there are any links between susceptibility and age, culture, perceived risk or severity and mental models. Results for age differ with some finding no differences for age and phishing victimisation [155, 158] whilst others show that younger individuals were more likely to respond to a social engineering attack [154] and less likely to fall for phishing [155]. However the age ranges of individuals studied is narrow with the susceptibility of children and older adults rarely examined. Additionally it could be argued that age may also reflect experience of the internet and phishing as well as greater financial risk [159].

However whilst perceived risk was generally associated with taking greater efforts to protect themselves, its association with whether an individual will detect or fall victim to an attack is less certain with some studies suggesting that individuals who perceive more risk from phishing less likely to respond [165, 172] but others finding no relationship [78, 148].

As mentioned culture has also been investigated but again, few cultures have been explored and few attempts have been made to try and explain any differences. However findings from

Uhomoibhi et al. (2011) include that Qataris have reported being particularly susceptible to attacks offering incentives [87] and work by Tembe et al. (2013) concluded that 31% of Indian participants reported having previously fallen for a phishing attempt compared to only 14% for American participants. However, as the results were self-reports this may reflect greater awareness or honesty in the Indian sample rather than increased susceptibility [173].

Research by Wash et al. (2010) suggests that people hold 'folk models' of security threats for malware and hackers, however these are often non-specific and miss many other types of threats. The authors speculated that computer users only having models of malware and hackers can leave individuals vulnerable to other forms of attacks [174]. Mental models also differ between experts and novices, with experts seeing more connections between different aspects of phishing [175] and having different risk models [176].

Finally working memory and the ability to inhibit irrelevant information has also been reported as inversely related to phishing susceptibility [177].

Categorising Users: An alternative approach has been to attempt to identify what 'type' of individual is likely to fall victim to an attack. Some researchers have had some success with this approach, Abbasi et al. (2016) identified that young males who are overconfident in their abilities, and who have experienced phishing but report only minor losses, are poor at detecting phishing emails [178]. A study by Ovelgonne et al. (2017) then found that software developers were the most at risk category for malware exposure [179]. However not everyone will easily fit into identified categories and an analysis of 10,314 responses to a cybercrime survey suggested that there is no 'one type' of individual who becomes a victim [180].

A summary of the individual differences studied regarding an individual's susceptibility to detect or fall victim to cyber-attacks can be seen in Table 2.8. The table also highlights inconsistencies, for example reports indicating that gender is both a factor, and not a factor, in susceptibility highlighting the need for further research on this topic.

Summary: Numerous pieces of research have explored whether individual differences can explain why some people may be more susceptible to attacks than others. Many of the factors explored are the same as those investigated to explore who uses different security measures such as gender, IT knowledge and perceived risk, with similar factors having an impact. Whilst more emphasis has been placed on exploring the impact of personality, findings remain equivocal.

2.5 Cyber Security: How do People Respond to an Attack

A second key research gap that exists in the area of cyber security is how do people respond to an attack. Current research has typically not touched upon this subject or assumed that recognition of malicious pages will simply result in the user avoiding the attack. This section

Table 2.8: Factors Influencing Susceptibility to Cyber Attacks

Topic	No. of Studies	Finding
Gender	14	Being male reduces susceptibility to phishing and malicious pages [138, 144, 152, 153, 159] and social engineering attacks [154]; Being male reduced phishing susceptibility in younger individuals [130]; But no gender differences for phishing susceptibility found by [134, 156] [155, 157, 158] or malware [54, 158]; Males were more susceptible to QR phishing [160].
Age	7	Younger students are more susceptible to phishing attacks [159]; Younger individuals less susceptible to phishing [138, 155]. Younger individuals more susceptible to social engineering attacks [154]; No differences [156, 157] [155, 158] .
Extroversion	5	Greater susceptibility to phishing [146, 168]; reduced susceptibility to phishing [162, 163]; more likely to delete emails [153].
Openness/ Sensation Seeking (SS)	5	Greater susceptibility to phishing [146, 153]; reduced susceptibility to phishing [162]; SS linked to increased malware risk [166]. No effect [168].
Neuroticism	4	Greater susceptibility to phishing [181] in women [164];Reduced susceptibility to social engineering attacks [168]; Low emotional stability associated with more secure email habits. [182].
Conscientiousness	3	Associated with more secure email habits [182] and reduced susceptibility to social engineering attacks [168]; Greater susceptibility to phishing [165].
Openness	1	Reduces susceptibility to social engineering attacks [168].
Impulsivity	4	Greater susceptibility to phishing [162, 167] No differences [183, 184].
Submissiveness	1	Greater susceptibility to phishing [146].
Generalised Communicative Suspicion Vs Trust	4	Individuals high in this trait use more strategic decision making approaches, those low take a more heuristic approach [169]. Greater trust increases phishing susceptibility [153, 167, 168].
Computer Use	5	Individuals who visit more sites have higher risk of becoming a victim of an online attack [170] [156, 180]; greater time spent online increases chances of malware victimisation [171]. Having more applications increases malware risk [157].
IT Knowledge	13	Higher self-reported computer skills and safe internet practices reduces phishing susceptibility [142] [78, 85, 143–148, 151]. Computer experts are exposed to greater malware [54, 156, 157].
Culture	4	British Individuals more likely to to use anti-phishing software than Qataris [87]formal IS training reduced phishing susceptibility in US and Swedish samples but not Indian [185] Indian populations report more phishing victimisation [173]; differences between rural and urban populations [186].
Risk Perceptions	4	Reduced susceptibility to phishing [172]; No relationship [78, 148]. Increases phishing susceptibility [165].
Victimisation Experience	3	Reduces phishing susceptibility [149, 150]. / Increases phishing susceptibility [168].
Short-term memory	2	Better short-term memory reduces phishing susceptibility [150, 177].
Mental models	3	People have mental models for limited forms of attack [174], they also differ between experts [175, 176].

presents research that has started to explore human responses focusing on affective, behavioural and cognitive responses.

Affective Responses: Cyber attacks not only lead to tangible physical responses but can result in emotional responses. Studies have suggested that the victims of account hacking report harm in the form of lost data, money and reputation but that they also report reduced trust, shame and embarrassment [187] as well as anger and in some cases fear [188]. Frequent exposure to attacks has also resulted in some individuals reporting a degree of data breach anxiety [189].

Behavioural Responses: Given the prevalence of attacks and their costs to society it would be beneficial to understand how people respond, especially given that the computer user is in a perfect position to report or help mitigate the impact of attacks. Yet surprisingly little research has focused on this topic. One reason is that many attacks target or affect large organisations, and business constraints then allow little opportunity to study how, or why, these events occurred. A further complication is that in many cases individuals are unaware that they have been a victim, and so it is impossible to know how often people respond by simply taking no action. One interview study, by Bidgoli et al. (2016), that addressed this topic identified five individuals who reported taking action when faced with an attack. Actions included contacting the real companies to inform them about fraudulent sites, contacting computer manufacturers and restoring a

computer to factory settings [50]. However, a study by Stembert et al. (2015) found that levels of reporting of suspicious emails were low, with individuals believing that they lacked the necessary experience to report them or stating they did not read the message [190].

Vance et al. (2014) took the approach of asking individuals to classify images, during the activity however they were occasionally interrupted by warnings about the images from the system, before later being presented with an onscreen video with a 'hacker screen'. This study found higher perceived risk and threat susceptibility, as well as a reduced likelihood of ignoring warnings after the video [191].

Alternatively researchers have looked at whether people change their behaviours when they are aware that they are currently being attacked. In a game study by Ben et al. (2009) individuals were attacked to see if this changed their security behaviours, it was found that participants were willing to accept higher usability costs for smaller gains when faced with more frequent attacks [192]. In a second game Fechner et al. (2012) had individuals try and hide their location data while revealing others, people did actively seek to avoid sharing home and work location information [193]. Whilst these studies show that individuals actively adjust their behaviours when they perceive that they are the victim of a cyber-attack (e.g., to reduce loss of game points or information) these conclusions are drawn from simulated scenarios that do not represent behaviours in the real-world.

Whilst research has started to investigate how individuals respond when they are aware of a cyber attack, many of the 'attack scenarios' are very unrealistic and here remains a lack of understanding of how an undetected cyber-attack can influence behaviour.

Cognitive Responses: Attacks have also been shown to influence people's cognition, with attacks shown to increase reported workload [194]. Neural data also supports these findings suggesting that when processing security warnings or phishing websites individuals experience activation in brain areas associated with cognitive judgements [184] and working memory [195] suggesting that individuals are exhibiting greater neural effort [196].

Summary: Several pieces of research have started to explore how people respond in the event of a cyber attack. These suggest that attacks can cause people not only to take action but also to experience negative emotions and increased workload, however more research is still required.

2.6 Cyber Security: Explaining Responses to an Attack

Finally, despite the small amount of research that has looked at how individuals respond in the event of an attack, there have been a few attempts to look at whether responses to an attack differ dependent on the context.

The Context of the Decision: One factor that has appeared to influence an individual's response to an attack is whether there are financial implications to the decision. Seventeen

analysts asked to respond to a simulated cyber incident by quarantining affected computers found that potential financial losses (new quarantines) were actively avoided, however financial benefits (lifting quarantine) were a lower priority [197]. This suggests people may sacrifice security to avoid triggering financial loss and this also applied to normal computer users [198, 199]. One example is work by Goel et al. (2017) who found that phishing emails that either threaten losses (e.g. loss of course registration) or promise gains (e.g. gift cards) are especially likely to be effective [134]. Even non-financial incentives can have an effect with enticements such as access to interesting information making people more likely to be tricked into disseminating harmful links [200] and people sharing more personal information in reciprocity attacks [201].

Decision Making Processes: One explanation for the differences in detection of attacks is the type of decision making that people engage in, in particular whether people make use of heuristic or systematic processing of information. Research by Vishwanath et al. (2016) has suggested that systematic processing is positively related to greater suspicion; with more heuristic processing negatively related to suspicion regarding emails [202]. With heuristic processing of emails leading to a greater likelihood of victimisation of phishing emails [80, 203], and individuals more likely to engage in heuristic processing when emails contain richer information, such as images and a sense of social presence. It has also been found that security decision making processes differ across different demographics (security experts, computer scientists and managers) possibly explaining differences in susceptibility between these groups [204]. Engaged individuals, who wished to control and manage both their computer's functionality and security, were also more likely to actively seek out information to aid security decisions [104]. Additionally offering individuals incentives also reduced susceptibility to phishing attacks [205].

Findings from D'Amico and Whitley (2007) suggest that the decision making activities of network defence analysts align closely to the idea of Endsley's three stage situational awareness model, consisting of a perception phase, a comprehension or current situation assessment phase and a projection or threat assessment phase [206, 207]. Additionally, Villamarin et al. (2010) found that praising or rewarding individuals reinforces behaving securely when interacting with emails [208].

Summary: Few pieces of work have explored why people respond to attacks as they do, although this is unsurprising given the small amount of research exploring how people respond to attacks. Understanding the impacts of context on how people respond could however be beneficial, especially given that current research showing that people are influenced by financial implications.

2.7 Discussion

This review has identified several key gaps in the literature regarding how humans respond to cyber attacks. However, the majority of research has focused on individual computer-users using a single computer. Whilst this is beneficial for understanding what occurs in this circumstance, work needs to investigate if the current findings hold true for how individuals deal with security and attacks on personal networks, such as those in the home or based on IoT devices. Work should also explore attacks against large-scale workplace systems.

Another research question aspect that has been largely unexplored is how individuals respond to attacks in real-time. Do they report suspicious behaviours or try to hide evidence of the attack (e.g. due to blame cultures or feelings of shame)? Such an understanding can particularly help improve security incident reporting mechanisms and lay the foundations for more positive security cultures within organisations.

Work is also needed to understand how cyber attacks impact individuals, even if they are not aware that they have been a victim. This could include impacts on workload or situational awareness resulting in impacts on job and task performance. It could also include impacts on trust in technology or on the reputation of technology providers.

This thesis seeks to begin addressing these issues by exploring how people protect their devices and how they respond to attacks across a range of different devices.

CHAPTER 3

DETECTING ATTACKS AGAINST CYBER-PHYSICAL SYSTEMS

Of particular interest to this thesis is whether individuals could identify an attack against cyber-physical systems. Within the context of this thesis this term is used to apply to any form of computer controlled or internet enabled device that has a physical impact, as such within this thesis the term cyber-physical system is used to refer to many IoT devices and smart cameras as well as larger scale systems such as ICS. Given the focus of this thesis, this chapter takes a more detailed exploration of the studies that have focused specifically on whether people can identify attacks against these systems.

3.1 How are Human Users Affected by Attacks Against Cyber-Physical Systems

Research Into Attacks Against CPS in the Home: Previous work looking at user perceptions of smart devices in the home environment has found that many users seek to prioritise their convenience over their privacy, suggesting that people may choose to use insecure devices if it offers them benefits. Despite this very few studies have explored people's use of these devices and whether they would seek to protect them. Additionally, very few studies have explored people's experiences when presented with either an actual or simulated attack against these devices. One study that did just that was conducted by Portnoff et al. (2015), this study explored the effectiveness of LED light indicators at letting individuals know when webcams were switched on without their permission. It was found that in many cases less than half of individuals noticed when the cameras, and therefore the lights, were switched on even when they were using the computer. When simply performing tasks near the computer rather than actually working on the computer, detection rates were even lower at only 4%. Overall this suggested that people

are poor at detecting potentially malicious behaviours from physical components [209]. It is however worth noting that the cameras were only turned on for 10 seconds, whilst this could still reasonably be enough time for a hacker it is possible that this time frame was simply too short for participants to notice. A follow up study by the authors noted that a large on-screen indicator was more effective at warning users, suggesting that individuals could identify a web-cam attack occuring when given the right cues [209].

Research Into Attacks Against Large Scale CPS: One area where researchers have sought to explore the impacts of attacks against large scale cyber-physical systems is in the transport industry, where an attack could have severe consequences. In particular work has explored how pilots would potentially respond in the event of a cyber attack. Work by Gontar et al. (2018) focused on the aviation domain arguing that, within this context, a malicious attack is likely to progress differently to a technical failure [194]. One key difference is that in the event of a technical failure there will usually be checklist or procedure providing actions to take and allowing the pilots to predict how the aircraft is likely to behave. However, in the event of a cyber attack occurring then the feedback that the pilot or operator may receive could be anything from absent to misleading with either scenario potentially resulting in poor decisions or a bad or even dangerous outcome.

To explore this argument the researchers explored whether experiencing an attack increased a pilot's workload, and whether providing a warning about the possibility of an attack would mitigate any impact on workload. Twenty-two male pilots took part in a flight simulation involving five trials. Whilst all the groups received a warning about a possible attack in one of the trials, only half the pilots were actually presented with the simulated attack. The results of the study showed that experiencing an attack increased the pilot's workload, however providing them with a warning about an attack (when no attack was present) did not. In addition to increasing their workload; experiencing the simulated attack also led to the pilots having reduced trust in the system as well as poorer task performance and whilst the warning did reduce the negative effects it did not completely eradicate them [194].

A second piece of research into how an attack can impact the aviation industry was conducted by Smith et al. (2019), who explored how pilots would respond in the event of potential attacks against three safety-related systems. In this study the participants were briefed on the topic of the study, but were unaware of the type of attacks which were targeted against the Traffic Collision Avoidance System (TCAS), the Ground Proximity Warning System (GPWS) and the Instrument Landing System (ILS). For each attack, participants were then asked to rate their levels of confidence about making the right decision, their workload, their trust in the system, and the level of impact that the attack had on the flight. The results showed that experiencing attacks led to increased workloads for the pilots as well as increased levels of distrust regarding the system being attacked. In addition to these effects on the pilots the attacks also led to changes

in behaviour, with pilots taking diversions or missing the originally planned approach as they investigated the information that they were being given. Finally in two out three of the attacks most of the pilots reported that the attack had had an impact on the safety of the plane [210].

A follow up piece of research repeated attacks against these three systems, but invited 30 pilots to take part [211]. One of the key take aways from this work was that in the absence of procedures or training, the responses to attacks was highly variable, with safety systems being switched on in 38% of scenarios. In addition the pilots experienced increased workloads and distrust.

The European Aviation Safety Agency has also explored the effects of multiple attacks against navigation and flight management systems, investigating six specific potential threats and whether they were identified during the incident. In this study eight individuals took part in seven trials, with each flight exposed to three of the six attacks. During the departure and climb phase of the flight simulation all the trials were exposed to a falsified weight and balance update. This false information would cause the flight path to be unstable. During the cruise phase, the flight was exposed to one of three different attacks. 1. A Global Navigation Satellite System (GNSS) enroute spoofing event, this attack changes the GNSS position generated by the GNSS receivers, which would result in the pilots having an inaccurate awareness of the plane location and where it was in relation to obstacles and other aircrafts. 2. An Aircraft Communication Addressing and Reporting System (ACARS) flight-plan update. This attack would result in the plane following an alternative route to the planned route, which could lead to increased workload. 3. A Denial of Service (DoS) attack event, this results in the Multipurpose Control and Display Unit (MCDU) screen freezing and not reacting to the pilots inputs, this reduces navigation functions and means that there is no support to aid with flight planning. During the descent and approach phases, six of the simulations were presented with a corrupted database attack, where the information on the final approach is altered. In this simulation the attack resulted in the glide path that would lead into the ground before the plane reached the runway. The final simulation then involved a GNSS Required Navigation Performance spoof attack. This resulted in the GNSS position drifting away from the planes real position. In the simulation this meant that at the end of the approach phase the plane was outside the protected position. The results from exploring these attacks found that the ACARS flight plan update, the database hack and the DoS attack were typically identified, although rarely regarded as a cyber attack. The other three scenarios often went undetected. This work therefore highlights that attacks can influence a pilots behaviour or workload even where they go undetected [212].

A fourth piece of work looking to understand what happens when technical countermeasures to a cyber attack fail in a transportation network was conducted by Millot et al. (2018) looking at train and tram networks. Focusing on how an attack can impact on an operator's situational awareness, their study involved placing human drivers in a simulator and observing how they respond when different cyber attacks were introduced. Since the work looked to identify and

explore realistic cyber attacks only two of the tested situations are discussed due to confidentiality reasons. These scenarios, used with six drivers, were a simulated loss of control over the rear vision of a tram, with the second involving a loss of the tram's breaking system. From running these simulations, the researchers concluded that the operator's ability to detect a malfunction depended on the situation. However, they also proposed that new tools could be developed to aid in fault detection as well as a signal that could alert human drivers should an attack be detected so that they could increase vigilance if necessary [213].

Interviews with six power distribution system operators found that only one of the participants had any written procedures available on how to respond to a cyber incident, although some reported that their organisations were working on addressing this issue [66]. Another study then highlighted that social, structural and institutional factors, such as insufficient quality control, can all facilitate security misconfigurations suggesting that organisational constraints prevent security from being a top priority. Suggesting that organisational security within companies with large industrial systems is poorly defined and often lacking in evidence based protocols [214].

3.2 Discussion

This review highlights that there is currently limited research that has explored the impact of attacks against cyber-physical systems on the human users of these systems. Whilst the research in this area is scarce, the work that has been done is typically very detailed and several key conclusions can be drawn.

Work looking at attacks against physical devices in the home has identified that some cues are more likely to be observed than others, with on screen indicators more likely to be observed than those occurring just off the screen. However current understanding of whether individuals within a home context can detect attacks against various devices, including IoT devices is low.

Research into attacks against large scale industrial systems is also sparse, and has largely focused on attacks against different transport systems. The findings of these studies show that identification of attacks varies across different types of attacks. It also highlights that experiencing an attack also leads to decreased trust and increased workload although simply priming an individual to be aware that an attack may occur does not increase the workload. Whether earlier findings from human centred security research can be generalised to these attacks however is currently not known and is a key objective for this thesis.

Part II

Cyber-Physical Systems in Home Environments

CHAPTER 4

CPS IN THE HOME- HAVE USERS' SECURITY AWARENESS AND APPROACHES EVOLVED WITH THE PREVALENCE OF 'SMART DEVICES'?

'Smart' devices, such as smartphones, tablets, smart watches and fitness trackers, are increasingly common, yet the few studies that have explored whether users keep them secure suggest that people take less effort to protect them compared to traditional computer devices. This chapter seeks to expand on this finding to answer the thesis research questions exploring smart device ownership, knowledge of the different sensors and components that these devices incorporate and how these can be attacked, and what measures do people take to protect their devices. In addition this chapter begins to explore whether security findings can be generalised across different devices and whether we can predict which individuals will use security measures. The novel aspects of this work are exploring the use of different security methods across multiple devices in the same sample population and exploring whether the security findings from traditional computers can be applied to other devices. The key findings presented in this chapter are: (1) The factors found to be related to the use of traditional IT security measures, such as IT knowledge, gender and concern about attacks are also correlated with using more measures to protect smart devices; (2) People report only moderate levels of IT knowledge and being unaware of many of the sensors they incorporate and how they can be attacked; (3) People take fewer measures to protect their smart devices, with poor IT knowledge one possible explanation.

4.1 Introduction

This chapter utilises a survey study to answer the thesis question regarding the use of protective measures across different home devices.

4.1.1 Contributions and Key Findings:

The main findings from this chapter are as follows:

1. It supports earlier findings by Mylonas et al. (2013) [42] that people use different protective measures across different devices, such as installing antivirus on computers but not on smartphones. It then expands on this by exploring both multiple protective measures including passwords, anti-virus software, installing updates and encryption, and multiple types of devices including computers, smartphones, tablets and home IoT devices. Our findings suggest that users have a knowledge gap, or level of complacency, that potentially leaves them vulnerable to attacks against non-traditional computer devices.

2. It demonstrates the importance of IT knowledge in awareness of security risks, identifying that many individuals are unaware of all the types of data that devices can gather and how this can be exploited. Users then take no security precautions to limit the scope of gathered data, e.g., disabling Near Field Communication (NFC) sensors when not in use.

3. It validates previous findings from the Technology Threat Avoidance Theory (TTAT) [67] which states that the likelihood of using more security measures is correlated with levels of concern about and perceived likelihood of attack as well as confidence in detecting attacks. It then expands upon TTAT by identifying that although people use fewer security measures to protect their smartphones, TTAT factors still appear to influence the use of these security measures. This indicates that users' security behaviours continue to be shaped by legacy notions of securing desktop PCs – notions that may not readily apply to smart devices and the large variety of sensors and actuators therein.

4.2 Related Work

4.2.1 Individual Differences in Using Cyber Security Measures

As discussed in chapter 2 there have been numerous studies that have explored who is most likely to make use of different security measures, whilst much of the current work has only looked at traditional PC or laptop devices, several key factors have emerged. One factor consistently found to be linked to using cyber security measures is security or IT knowledge, with people who report greater levels of security knowledge or training taking more measures to protect their privacy when using email [83, 97]. Males have also sometimes been reported as using more security

measures as well as using stronger passwords [82]. There is also research suggesting that males may be less susceptible to a variety of cyber attacks such as phishing although this may represent differences in IT knowledge rather than an actual gender difference [144, 152, 159].

A third factor that has been studied is age, although findings are equivocal about whether age does actually influence an individual's susceptibility to cyber attacks. Sheng et al. (2010) found that younger students were more susceptible to phishing attacks [159], whilst Mohebzada et al. (2012) found that younger individuals were less susceptible [155]. Lalonde et al. (2013) and Levesque et al. (2014) found age had no impact on susceptibility [156, 157]. Our work seeks to validate these earlier findings across multiple devices.

4.2.2 Models of Protective Behaviours

Several theoretical models have also been developed to try and identify and explain factors that influence whether people seek to protect themselves from different security threats. These include the Protection Motivation Theory (PMT) and the Extended Parallel Process Model (EPPM) which identify perceived self efficacy, response efficacy, susceptibility and severity of attack [215–217] as key determinants of using more security. However, these works have typically only explored one threat at a time of focused on one type of device.

These factors have also been explored specifically in relation to the computer security context by Liang and Xue who developed the Technology Threat Avoidance Theory (TTAT). Research using this model has shown that perceived severity and susceptibility to attacks are linked to motivations to avoid cyber threats [68]. The TTAT has then been applied to malware avoidance [69], and whether users protect themselves when shopping online, with self-efficacy also found to be an important determinant of secure behaviours [50, 70]. This work is novel in seeking to validate whether these theories can explain general cyber security behaviours with respect to multiple threats.

4.2.3 Cyber Security for Smart Devices

Previous research into how users protect the diverse array of smart devices they use is limited, however they have revealed some interesting findings, suggesting that people take different approaches across different security devices. Looking at passwords Egelman et al. (2014) found that individuals using smart devices also reuse their passwords [43]. However, work also suggests that smartphone users use fewer uppercase letters and special symbols in their passwords, but that these passwords are also often longer than the passwords they use on laptops and tablets [46] suggesting that people adapt their behaviours across devices.

The use of anti-virus software has also been found to differ across devices. Mylonas et al. (2013) found that, whilst over 85% of people use anti-virus software on their computers, only 24.5% used some form of this on their smartphones with 27% of respondents not aware that security software for smartphones is even available [42].

Many smart devices, e.g., smartphones, tablets and smart TVs, allow users to download various applications however studies suggest that users pay little attention to the permissions that they allow these apps. Felt et al. (2012) concluded that only 17% of participants paid attention to permissions when installing applications, and only 3% were able to demonstrate that they understood all the permission statements they had read [55]. Mylonas et al. (2013) also reported that the majority of respondents only read security warnings some of the time [42].

The work listed above suggests that many individuals do not make use of available security measures for smart devices. One possible explanation is that people have a poor understanding of the sensors these devices incorporate, or how accessing their data could be of benefit to an attacker. This is supported by Mehrnezhad et al. (2017) who found that many people were unaware of some of the sensors in smartphones [218]. Similarly Crager et al. (2017) found that many people are unaware of different forms of motion-sensor based data attacks [219] and Balebako et al. (2013) found that users were frequently unaware and uncomfortable at the scope of data that can be shared with smartphone applications [220]. This chapter seeks to explore levels of awareness of a wide range of different attacks and security measures.

4.3 Study Overview

4.3.1 Research Questions

This study sought to explore what types of internet-enabled devices people own, levels of awareness of different forms of attacks and what measures they take to protect these devices. In addition, we seek to validate earlier research and models that have identified factors which influence decisions to apply security features. The specific research questions explored in this chapter are:

Q_1: What types of devices do people currently own?
Q_2: Are people aware of all the sensors that their smart devices incorporate?
Q_3: Are people aware of cyber attacks that can target these types of devices?
Q_4: What security precautions do people take to keep these devices secure?

4.3.2 Hypotheses.

Based on the previous research, nine hypotheses were developed looking at how IT knowledge, gender, age and awareness and perceived risk influence the use of security measures on both traditional desktops and smartphones. These nine hypotheses are presented below and in Figure 4.1.

H_1: Greater IT knowledge will be positively associated with greater awareness of different types of cyber attacks.
H_2: Greater awareness of cyber attacks will be positively correlated with being more confident

in ability to detect cyber attacks, level of concern over attacks and perceived likelihood of being attacked.

H3: Males will have a greater awareness of cyber attacks than females.

H4: Age will be correlated with awareness of cyber attacks.

H5: People who are aware of more types of attacks will take more security precautions to protect their cyber devices.

H6: Confidence in ability to detect cyber attacks, level of concern over attacks and perceived likelihood of being attacked will be correlated with taking more measures to protect devices.

H7: Greater IT knowledge will be positively associated with using more security measures to protect devices.

H8: Males will take more security precautions to protect their devices.

H9: Age will be correlated with the number of security measures an individual takes to protect their devices.

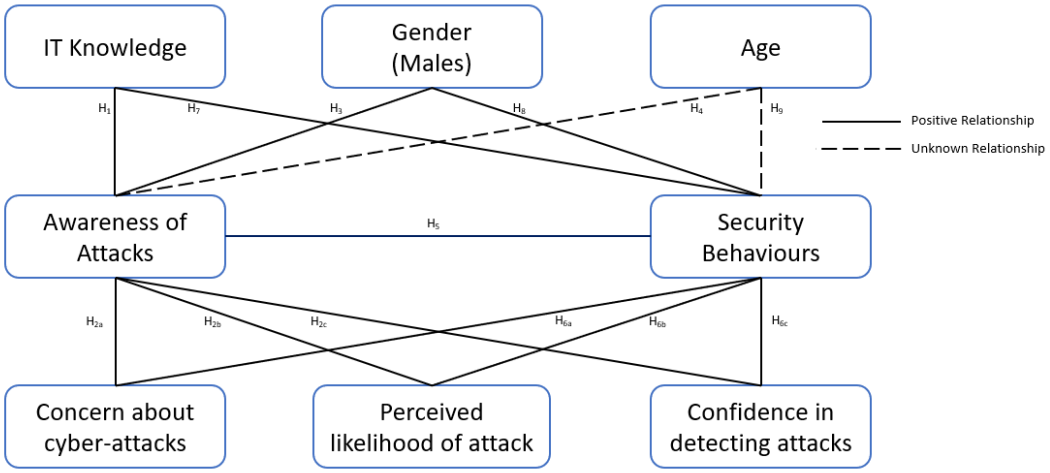


Figure 4.1: Hypotheses of Factors Influencing Attack Awareness and Security Measure Use in Smart Devices (shown by the lines)

4.4 Methodology

4.4.1 Recruitment and Procedure

This study was approved by the Lancaster University Research Ethical Committee[1] (See Appendix A) and was conducted as an online survey administered via Qualtrics from November to December 2017 (See Appendix B for the full survey and supporting material). Participants who took part in this study were entered into a prize draw to win one £20 Amazon voucher, with psychology students who took part also offered research credits.

[1]This research was initially conducted at Lancaster, before being moved to the University of Bristol.

Table 4.1: Demographic Breakdown of Participants

		Male	**Female**	**Total**
	Total	34 (28.1%)	87 (71.9%)	121 (100%)
Age	18-21	11 (9.1%)	50 (41.3%)	61 (50.4%)
	22-25	1 (0.8%)	5 (4.1%)	6 (5.0%)
	26-30	4 (3.3%)	7 (5.8%)	11 (9.1%)
	31-35	2 (1.7%)	5 (4.1%)	7 (5.8%)
	36-40	4 (3.3%)	2 (1.7%)	6 (5.0%)
	41-45	3 (2.5%)	1 (0.8%)	4 (3.3%)
	46-50	6 (5.0%)	3 (2.5%)	9 (7.4%)
	51-55	2 (1.7%)	9 (7.4%)	11 (9.1%)
	56-60	0 (0%)	4 (3.3%)	4 (3.3%)
	61+	0 (0%)	1 (0.8%)	1 (0.8%)
	Unknown	1 (0.8%)	0 (0%)	1 (0.8%)
Student?	Yes	12 (9.9%)	58 (47.9%)	70 (57.9%)
	No	20 (16.5%)	29 (24%)	49 (40.5%)
	Unspecified	2 (1.7%)	0 (0%)	2 (1.7%)
IT Knowledge	Very Low	0 (0%)	1 (0.8%)	1 (0.8%)
	Low	0 (0%)	9 (7.4%)	9 (7.4%)
	Moderate	20 (16.5%)	68 (56.2%)	88 (72.7%)
	High	7 (5.8%)	5 (4.1%)	12 (9.9%)
	Very High	7 (5.8%)	4 (3.3%)	11 (9.1%)

The survey was advertised on Lancaster university campus and via social networks and a total of 124 individuals responded, with 121 responses used in the analysis. Three responses were removed due to incomplete submissions. A breakdown of the participant demographics is presented in Table 4.1. Due to the majority of advertising happening around a university campus, and in particular through the psychology department's recruitment system (this system allows psychology students to volunteer for studies for research credits, although all students may access it for cash studies), a significant proportion of the sample population falls into the 18-21 years old female category. The sample does, however, include a wide range of individuals aged from 18 to 76 years and in a wide range of professions including retail, teaching, engineering and the police. IT knowledge in this case was self-reported by participants with defined examples provided, see Appendix D.

4.4.2 Data Analysis

Data was analysed using both descriptive statistics to explore the devices and security measures that people use. Statistical analyses including regression analysis and correlations were also performed. The full details of all the statistical tests that were run can be seen in Appendix C.

4.4.3 Threats to Validity

Given that many of the respondents were students this sample does not represent the typical age, education level or economic status of the population at large. Additionally this sample is known to move frequently and so they may be less likely than the general population to invest in smart devices for the home. The sample was also more than two-thirds female, which may have skewed any gender differences. Samples with skewed ages and genders are, however, common limitations in research conducted at universities (e.g., [16, 57]).

This work also relied on participants self-reporting information and it is possible that they may be reluctant to admit to not protecting their systems or being unaware of certain types of cyber attacks. To mitigate this all the options were available to select for all devices meaning that if participants selected using all protective measures for all devices then they would be stating that they were taking actions that were not possible, flagging that the individual was not being honest, or did not understand the options they were presented with. Participant levels of IT knowledge were also self-reported and whilst attempts were made to control for this by defining different levels of IT knowledge to try and help participants quantify this factor these definitions were defined by the researcher and future work should consider seeking to objectively measure participant's IT and security knowledge. One approach may be to use the Security SRK framework, developed by Rajivan et al. (2017). This framework consists of four variables (basic computer skills, advanced computer skills, security knowledge and advanced security skills) that could be used to assess IT security expertise and which were used to develop a questionnaire to assess this [221].

Lastly, one of the measures explored in detail is the number of protective mechanisms that people use to protect a device. Whilst this gives an indication of how much security that individual is applying, some mechanisms will offer greater levels of security than others (e.g., using anti-virus software compared to only covering up microphones) and so this is not a very reliable measure.

4.5 Results

4.5.1 Q1 What 'Smart' Devices Do People Own?

A breakdown of the personal computing devices owned by the participants can be seen in Figures 4.2 and 4.3.

All respondents reported owning at least one of the devices and as shown in Figure 4.2 the vast majority (>95%) owned smartphones and laptops with 60% reporting that they owned tablet devices such as iPads. The mean number of devices owned by individuals was 3.9, however most people reported owning 3. Interestingly less than a third of respondents (30.6%) reported owning desktop computers. This may be reflective of the largely student sample who don't want to move desktops around every year, but could also demonstrate that, as memory and processing power

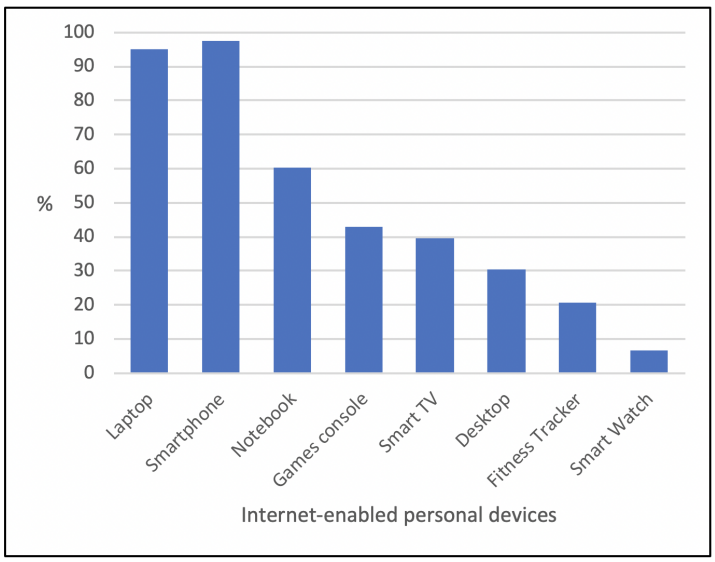


Figure 4.2: Percentage of Participants Owning Different Cyber Devices

has required less and less space, individuals are increasingly choosing portable devices. The survey has also highlighted that internet enabled devices such as smart TVs and games consoles are popular devices although uptake on the use of fitness trackers, and especially smart watches, is low.

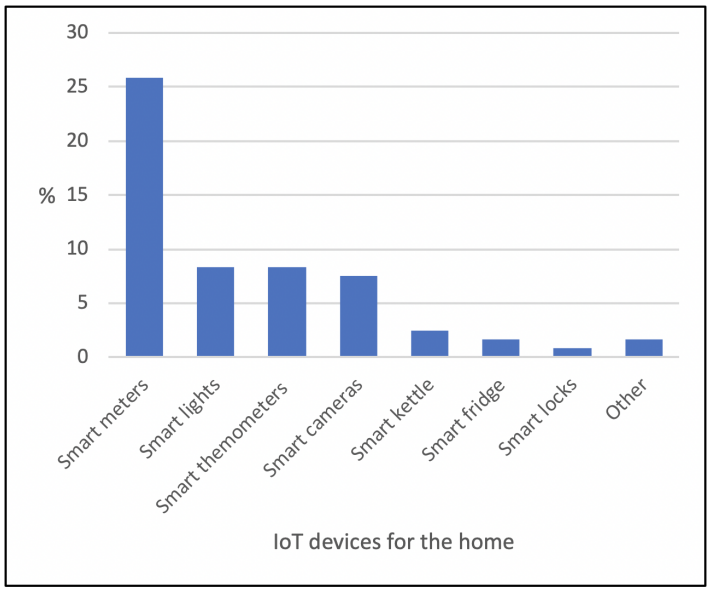


Figure 4.3: Percentage of Participants Owning Smart Devices for the Home

Figure 4.3 demonstrates that whilst individuals are increasingly using internet enabled devices, smart devices to control and monitor the home environment are a lot less utilised, likely

due to the student population who are unlikely to be focused on home improvement. The most commonly owned of these devices are smart meters, which automatically send meter readings to suppliers, with less than 10% of participants owning devices such as smart thermostats, lights and cameras.

4.5.2 Q2. Awareness of Smart Device Sensors

Participants were asked to specify what devices they owned and presented with a list of sensors to select those that they believed their device had in order to examine awareness. Many individuals only reported the manufacturer of their devices, rather than the model, and so it is not possible to explore in depth the accuracy of participant's beliefs regarding the sensors that their devices have, however several findings can be reported. Firstly, only 19.1% of individuals reported that their laptops had light sensors and only 4.1% reported that they had Near-Field Communication (NFC). Further only 26.3% were aware of smartphones having NFC. Additionally, 42.5% of people failed to report that their tablets had motion and orientation sensors although 60.2% of smartphone owners were aware that they are commonly used to orient screens. These findings suggest that many individuals are unaware of all of the information that their electronic device can gather and transmit. However greater knowledge regarding smartphones instead of tablets may suggest that people are more aware of sensors if they actively choose to use them, e.g., one possible explanation for people being more aware of NFC on smartphones may be that people may use it more, such as for Applepay and Android pay.

4.5.3 Q3. Awareness of How Sensors Can Be Compromised

Participants were also asked to specify whether or not they were aware of different types of cyber attacks from a list of options covering attacks that targeted a range of different sensors, to see if attacks against newer sensors and components were less likely to be known (See Figure 4.4). Findings from this question were generally positive with the vast majority of respondents aware of attacks such as theft of data, hacking of networks and ability to access cameras and sound recorders on devices. There were however four attacks for which more than half of the individuals were unaware. These included: network mapping, ransomware preventing access to cyber-physical systems, using NFC to steal financial information and using movement sensors to determine an individual's screen lock PIN.

4.5.4 Factors Influencing Awareness of Cyber Attacks

In order to explore the impact of these factors several Spearman Rank correlations were performed. This test measures the strength and direction of an association between two variables, Spearman's correlation was selected over Pearson correlation as it allows ordinal variables to be

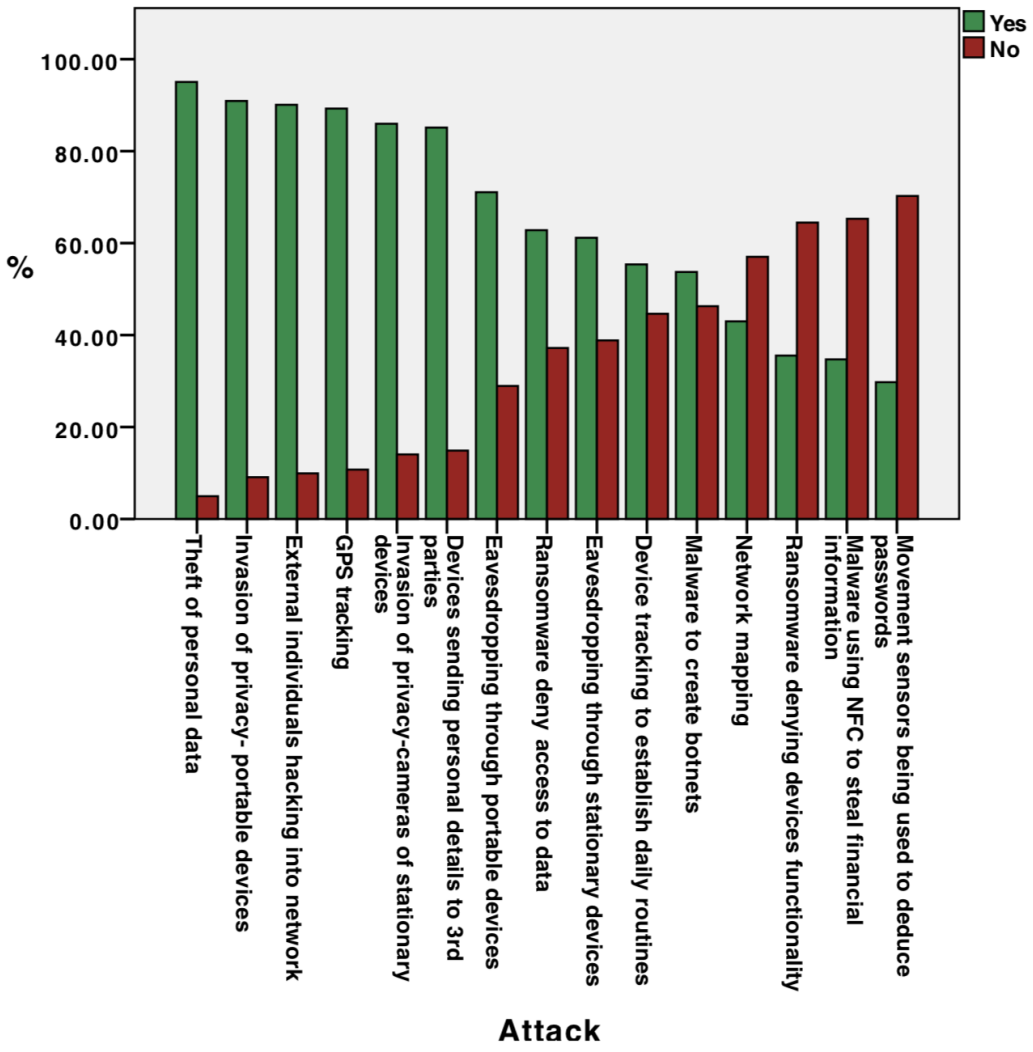


Figure 4.4: Number of Participants Aware and Unaware of Different Cyber Attacks

correlated against continuous variables. The results of these correlations can be seen in Figure 4.5, with more detail on the statistical analyses presented in Appendix C.

A moderate correlation was found between self-rated IT knowledge and the number of attacks that an individual was aware of with ($r_s(119) = .333$, $p = <.001$). This supports hypothesis 1 and suggests that people's self ratings for level of IT knowledge had some degree of accuracy.

Additionally, awareness of more types of cyber attacks was correlated with more confidence in their ability to detect cyber attacks ($r_s(119) = .306$, $p = .001$). The correlations between awareness of attacks with level of concern ($r_s(119) = .213$, $p = .019$) and perceived likelihood of being attacked ($r_s(119) = .180$, $p = .048$) were weak but significant. This supports hypothesis 2. However these correlations were not strong, especially for concern and perceived likelihood of attack suggesting

Correlations

			Age	IT_Knowledge	Likely	Concern	Confident	AttacksAware
Spearman's rho	Age	Correlation Coefficient	1.000	-.008	.005	.257**	-.043	-.089
		Sig. (2-tailed)	.	.930	.955	.005	.643	.336
		N	120	120	120	120	120	120
	IT_Knowledge	Correlation Coefficient	-.008	1.000	.064	-.025	.289**	.333**
		Sig. (2-tailed)	.930	.	.485	.790	.001	.000
		N	120	121	121	121	121	121
	Likely	Correlation Coefficient	.005	.064	1.000	.487**	.087	.180*
		Sig. (2-tailed)	.955	.485	.	.000	.344	.048
		N	120	121	121	121	121	121
	Concern	Correlation Coefficient	.257**	-.025	.487**	1.000	.118	.213*
		Sig. (2-tailed)	.005	.790	.000	.	.196	.019
		N	120	121	121	121	121	121
	Confident	Correlation Coefficient	-.043	.289**	.087	.118	1.000	.306**
		Sig. (2-tailed)	.643	.001	.344	.196	.	.001
		N	120	121	121	121	121	121
	AttacksAware	Correlation Coefficient	-.089	.333**	.180*	.213*	.306**	1.000
		Sig. (2-tailed)	.336	.000	.048	.019	.001	.
		N	120	121	121	121	121	121

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Figure 4.5: SPSS Output of Spearman Rank Correlations for Awareness of Different Cyber Attacks

other factors may play more of a role.

Hypothesis 3 predicted that there would be a relationship between gender and the number of attacks of which people are aware, to test this hypothesis a Mann Whitney U test was performed. The full details of this analysis can be seen in Appendix C Section C.1.2.

A Mann-Whitney U test was run to determine if there were differences in the number of attacks that people were aware of between males and females. Distributions of attack awareness for males (mean rank= 75.76) and females (mean rank= 55.23) were not similar, as assessed by visual inspection, and so the test compared differences in mean engagement scores. The results then showed a statistically significantly difference in mean engagement scores between males and females, U = 1,981, z = 2.908, p = .004.

No significant correlation for age and awareness of cyber attacks was found and so hypothesis 4 was not supported.

4.6 Q4. What Security Precautions Do People Take to Keep Devices Secure?

4.6.1 Protective Measures for Personal Devices

The measures that people use to protect these devices can be seen in Table 4.2. It shows that one of the most common measures that individuals take to protect their personal devices is

installing updates with this approach taken to protect all the devices examined. Passwords and anti-virus software were also reported as being frequently used on devices that allow these measures, although they were rarely reported as being used for devices such as smart TVs and fitness trackers. Precautions that were rarely used included covering microphones. Cameras were covered up on laptops by 41.74% of respondents, however they were frequently left uncovered on many other devices. The majority of people reported that they did not disable GPS, bluetooth or NFC sensors. However this survey did not examine whether measures were not taken because the respondent was unaware or unable to take the precaution, or because they actively decided that having sensor functionality was more important than the potential risks.

Participants were also given the opportunity to report any additional methods that they used to protect their devices, and some participants reported that they changed passwords at regular intervals with one participant also reporting that they generated passwords randomly and another reporting using password managers. Additional measures reported included two factor authentication, Virtual Private Networks (VPNs), hidden networks, IP masking, and separate email accounts or devices for different activities, e.g., gaming and banking.

Table 4.2: Protective Measures Employed by Participants to Protect Their Cyber Devices

Device	Password	Anti-virus	Read permissions	Install updates	Encryption	Firewall	Cover Camera	Cover microphone	Disable GPS	Disable Bluetooth	Disable NFC
Desktop	78%	91.89%	45.95	94.59%	37.84%	70.27%	18.92%	8.11%	10.81%	16.22%	0.00%
Laptop	79.13%	86.09%	40.00%	86.96%	26.09%	58.26%	41.74%	9.57%	18.26%	35.65%	11.30%
Tablet	68.49%	36.99%	30.14%	79.45%	17.81%	23.29%	9.59%	2.74%	23.29%	28.77%	6.85%
Smartphone	74.58%	31.36%	34.75%	83.05%	16.95%	13.56%	10.17%	4.24%	35.59%	44.92%	14.41%
Smart TV	18.75%	6.25%	0.00%	54.17%	4.17%	6.25%	2.08%	0.00%	4.17%	10.42%	2.08%
Games Console	46.15%	7.69%	15.38%	65.38%	0.00%	1.92%	3.85%	0.00%	3.85%	3.85%	1.92%
Smart Watch	75.00%	0.00%	0.00%	75.00%	0.00%	12.50%	0.00%	0.00%	0.00%	0.00%	0.00%
Fitness Tracker	17.39%	4.35%	4.35%	52.17%	0.00%	4.35%	0.00%	0.00%	4.35%	8.70%	4.35%

4.6.2 Protective Measures for IoT Devices

Given the small numbers of individuals who reported owning various smart devices for the home it is hard to draw any definitive conclusions on the actions that people take to protect these devices. It can be noted however that at least a third of individuals who owned any of these devices reported that they didn't know what security measures they used. Some individuals reported that they changed their default device passwords, used routers with passwords and password protected their networks, however these approaches were far from ubiquitous. Additionally, only two individuals reported that they keep these devices on a separate wifi network. Again participants were given the opportunity to report any additional measures that they use to protect smart devices within their home. Two individuals responded to this question with one individual reporting that they switch off security cameras when they get home via their Echo

and another stated that that they use media access control address filtering on their home WiFi network.

4.6.3 Factors Influencing the Use of Security Measures

This section explores whether individual differences influence the use of security features on laptops and smartphones. These devices were selected as the two most popular and because there are numerous security options available. The total number of protective measures included those selected from the options provided, as well as any additional measures that were reported in free text. To test these hypotheses several correlations and a Mann-Whitney U test were performed as can be seen in Figure 4.6 and Appendix C Sections C.2 and C.2.2.

Correlations

			Age	IT_Knowledge	Likely	Concern	Confident	AttacksAware	NoMeasuresLaptop	NoMeasuresSmartphone
Spearman's rho	Age	Correlation Coefficient	1.000	−.008	.005	.257**	−.043	−.089	−.055	.038
		Sig. (2-tailed)	.	.930	.955	.005	.643	.336	.560	.684
		N	120	120	120	120	120	120	114	117
	IT_Knowledge	Correlation Coefficient	−.008	1.000	.064	−.025	.289**	.333**	.361**	.272**
		Sig. (2-tailed)	.930	.	.485	.790	.001	.000	.000	.003
		N	120	121	121	121	121	121	115	118
	Likely	Correlation Coefficient	.005	.064	1.000	.487**	.087	.180*	.254**	.253**
		Sig. (2-tailed)	.955	.485	.	.000	.344	.048	.006	.006
		N	120	121	121	121	121	121	115	118
	Concern	Correlation Coefficient	.257**	−.025	.487**	1.000	.118	.213*	.248**	.280**
		Sig. (2-tailed)	.005	.790	.000	.	.196	.019	.008	.002
		N	120	121	121	121	121	121	115	118
	Confident	Correlation Coefficient	−.043	.289**	.087	.118	1.000	.306**	.194*	.173
		Sig. (2-tailed)	.643	.001	.344	.196	.	.001	.038	.061
		N	120	121	121	121	121	121	115	118
	AttacksAware	Correlation Coefficient	−.089	.333**	.180*	.213*	.306**	1.000	.458**	.294**
		Sig. (2-tailed)	.336	.000	.048	.019	.001	.	.000	.001
		N	120	121	121	121	121	121	115	118
	NoMeasuresLaptop	Correlation Coefficient	−.055	.361**	.254**	.248**	.194*	.458**	1.000	.741**
		Sig. (2-tailed)	.560	.000	.006	.008	.038	.000	.	.000
		N	114	115	115	115	115	115	115	112
	NoMeasuresSmartphone	Correlation Coefficient	.038	.272**	.253**	.280**	.173	.294**	.741**	1.000
		Sig. (2-tailed)	.684	.003	.006	.002	.061	.001	.000	.
		N	117	118	118	118	118	118	112	118

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Figure 4.6: Spearman Rank Correlations For Number of Laptop and Smartphone Security Measures Used

Awareness of Different Types of Attacks: Again unsurprisingly, individuals who report awareness of more attacks were found to use more protective measures. Correlation results for laptops was $r_s(113) = .458$, $p = <.001$. The correlation for smartphones was $r_s(116) = .294$, $p = .001$. This supports hypothesis 5.

Self-Rated IT Knowledge: For both laptops and smartphones there were positive correlations between the participant's self-reported level of IT knowledge and the number of security measures they used. For laptops there was a modest correlation, $r(113) = .361$, $p <.001$. The correlation for smart phones was slightly weaker, $r(116) = .272$, $p = .003$ but still significant and so hypothesis 7 was supported.

Perceived Likelihood of Being Attacked: The perceived likelihood of being attacked was positively, but weakly, correlated with taking more measures to protect both laptops ($r_s(113)$ = .254, p = .006) and smartphones ($r_s(116)$ = .253, p = .006).

Concern Over Being Attacked: Concern about being attacked was also significantly correlated with number of measures to protect laptops ($r_s(113)$ = .248, p = .008) and smartphones ($r_s(116)$ = .280, p = .004).

Confidence in Ability to Detect Cyber Attacks: However, whilst confidence in detecting cyber attacks against devices was weakly associated with an individual using more methods to protect their laptops ($r_s(113)$ = .194, p =.038), there was no significant relationship with the number of measures to protect smartphones ($r_s(116)$ = .173, p =.061).

Hypothesis 6 predicted that the perceived likelihood of being attacked, level of concern over being attacked and an individual's confidence in their ability to detect attacks would all be positively correlated with using more security measures to protect smartphones and laptops. This hypothesis was therefore only partially upheld.

Gender: To test hypothesis 8, two Mann-Whitney U tests were conducted. Distributions of number of protective measures for laptops were not similar. However the number of measures used by males (5.8) was statistically higher than the number reported by females (4.6), U= 1785.5, z= 2.829, p = .005.

Distributions of number of protective measures for smartphones were not similar. However the number of measures used by males (4.5) was statistically higher than the number reported by females (3.3), U= 1836.0, z= 2.626, p = .009. Hypothesis 8 was therefore supported.

Age: This piece of work did not find that age is implicated in using more or less measures to protect devices and so hypothesis 9 was rejected.

The findings from this work are presented in Figure 4.7. This figure shows that security behaviours continue to be influenced – as in the case of desktop PCs – by a participant's gender, IT knowledge, awareness of different attacks, concern about attacks and perceived likelihood of being attacked. This supports work showing that individuals with more knowledge of attacks and who perceive a greater level of risk are more likely to use security measures, as are males. In addition there are also relationships between IT knowledge, gender, concern about attacks, perceived likelihood of attacks and confidence in detecting attacks and an individual's awareness of attacks. This suggests that greater awareness of attacks may also increase concern and perceived likelihood of being a victim of an attack. The fact that confidence in detecting attacks was not linked to security behaviours suggests that people confident in detecting attacks may feel less need to protect themselves.

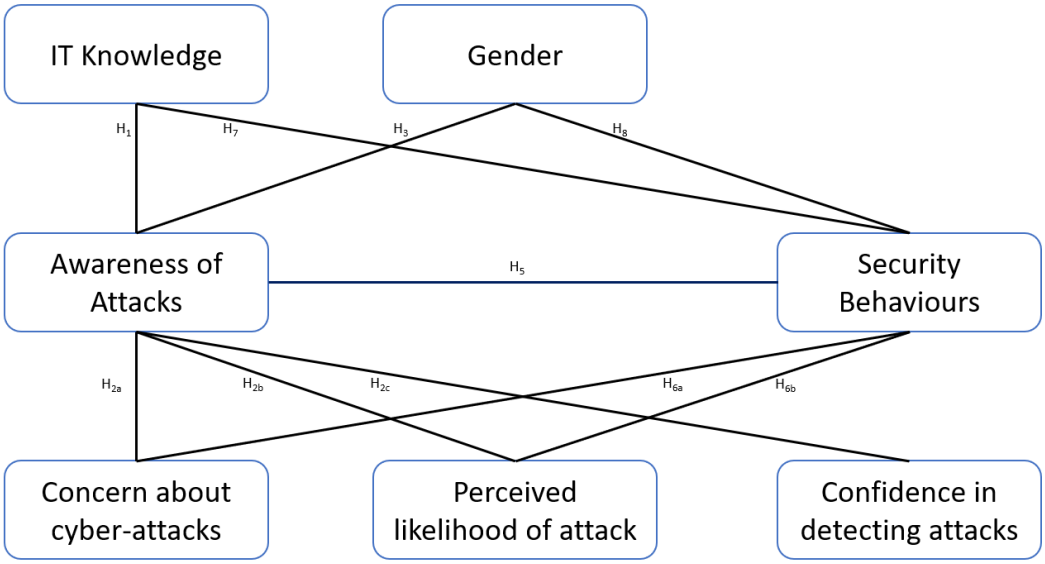


Figure 4.7: Factors Found to Influence the Use of Security for Smart Devices

4.7 Q5. Can We Predict If People Will Use Security Measures?

To answer this question multiple logistic regression analyses were run, exploring whether factors such as gender, self-rated IT knowledge, perceived likelihood of being attacked, concern about attacks and confidence in detecting attacks could be used to explain variance in the number if security measures used on laptops and smartphones. The full details of these analyses can be seen in Appendix C Section C.4.

The outputs of these models showed that in this sample, only a very small proportion of the dependent variable's variability (number of security measures used) was explained by the participant's demographics.

4.7.1 Predicting the Use of Security Measures on Laptops

The regression analysis for using security measures on laptops looked at IT knowledge, gender, awareness of different attacks, confidence in detecting attacks, perceived risks and concern about attacks. The results showed that the R^2 for this model was 28.9% with an adjusted R^2 of 24.9%. This means that using these independent demographic variables explained only 28.9% of the variability of the dependent variable (See Figure 4.8).

4.7.2 Predicting the Use of Security Measures on Smartphones

The regression analysis for using security measures on smartphones looked at IT knowledge, gender, awareness of different attacks, and perceived risks and concern about attacks. Note confidence was not included in this model as this was not significant for smartphones. The results

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin–Watson
1	.538[a]	.289	.249	1.99451	2.016

a. Predictors: (Constant), Concerned, ITKnowledge, Confident, Gender, NoAttacksAware, Likelihood

b. Dependent Variable: NoMeasuresLaptop

Figure 4.8: SPSS Model Output Summary for the Multiple Regression Analysis into the Number of Protective Measures Used for Laptops

showed that the R^2 for this model was 22.2% with an adjusted R^2 of 18.7%.This means that using these independent demographic variables explained only 28.9% of the variability of the dependent variable (See Figure 4.9).

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin–Watson
1	.471[a]	.222	.187	1.98336	1.967

a. Predictors: (Constant), Concerned, ITKnowledge, Gender, NoAttacksAware, Likelihood

b. Dependent Variable: NoMeasureSmartphone

Figure 4.9: SPSS Model Output Summary for the Multiple Regression Analysis into the Number of Protective Measures Used for Smartphones

An additional finding was that there was a strong correlation between the use of security measures on laptops with the use of security measures on smartphones $r_s(110) = .741$, $p < .001$. This suggests that if you know that someone protects one device that it is likely that they will take measures to protect other devices.

4.8 Additional Findings

4.8.1 IT Knowledge

An additional Mann Whitney U test revealed that males reported significantly greater levels of IT knowledge than females ($U = 2.018$, $z = 3.928$, $p < .001$) and so the gender difference may instead reflect the impact of IT knowledge on use of security measures, rather than a stand alone gender difference. IT knowledge could also help to explain the relationship between confidence in the ability to detect a malicious attack and greater use of security measures.

IT knowledge was also correlated with how confident an individual was that they could detect if their devices had been maliciously manipulated ($r_s(119) = .289$, $p = .001$, Figure 4.6). Confidence was then found to have a small correlation with number of measures to protect laptops, IT knowledge could then again explain this relationship.

4.8.2 Perceived Risk and Concern About Attacks

In addition to the findings discussed above, a positive correlation was seen between perceived likelihood of becoming a victim of a cyber attack and level of concern about becoming a victim ($r_s(119) = .487$, $p < .001$). This suggests that perceiving oneself as at risk may raise one's concern.

A final correlation that was found was a positive correlation between age and levels of concern about facing an attack ($r_s(118) = .257$, $p = .005$).

4.8.3 Previous Experiences of Security Issues

Finally participants were asked if they had ever personally experienced a security issue, with 34 (28%) participants reporting some form of incident. These included incidents such as detecting malware and viruses which was typically resolved by either deleting the malware or resetting the device or hard drive. One individual however bought a new computer in response to a security incident. Other individuals reported having email and accounts hacked, and having to change passwords. Four individuals explicitly reported that they had suffered from security incidents at work.

4.9 Discussion

This chapter has explored how users deal with increasing security threats across a range of different devices. A key finding is that early models and findings about cyber security do appear to be generalisable across devices, with IT knowledge, awareness of attacks, concern about attacks and increased perceived likelihood of being attacked all linked to greater use of security mechanisms. Whilst these results help to build our understanding of how users apply security mechanisms across devices, these findings actually represent a rather negative picture. Whilst attacks are evolving in order to exploit new devices or gain access to more information, people's awareness of security threats appears to be based on the threats that would target a desktop PC, with many individuals unaware of the different sensors that their devices incorporate and how these could be exploited. This lack of knowledge about their devices and how they could be maliciously targeted then leaves users potentially vulnerable.

This chapter, therefore, highlights a need to evolve users' understanding and awareness of the threats and countermeasures that can be applied to different devices. This may be best achieved by emphasising the importance of different forms of information stored on these devices including information that users may be unaware is being gathered by the various sensors and actuators

that these devices incorporate and how this could be used against them, e.g., how movement sensors could be used to learn passwords [219].

4.10 Interim Conclusions

Several conclusions can be drawn from this work. Firstly, factors that have previously been found to be related to the use of traditional IT security mechanisms, such as an individual's level of IT knowledge, awareness of attacks, gender and level of concern and perceived likelihood of being attacked are also correlated with using more measures to protect smart device.

Secondly, many individuals were found to be unaware of the different sensors that smart devices incorporate, or that these devices could even be targeted or protected. This shows how, for many users, understanding of security threats remains firmly rooted in the features of traditional desktop PCs and has not kept pace with the rapid evolution of technology. This highlights a need to increase awareness among users about the variety of sensors and actuators that are incorporated into smart devices and how these gather and communicate different forms of information.

Thirdly, whilst this chapter supports earlier research that certain factors are related to the use of different security measures it also highlights that these factors explain only a small amount of variance in the use of these measures. This suggests that other factors may also be influencing individuals decisions of whether to protect different devices.

CHAPTER 5

CPS IN THE HOME- TO SECURE OR NOT TO SECURE?

Chapter 4 identified that people take measures to protect the security of their devices. It also highlighted that factors such as IT knowledge, gender, concern and perceived likelihood of attack influence the use of security across different devices. However the work also revealed that a large proportion of variance between individuals remained unexplained. Further people appear to use fewer security measures on newer devices, compared to traditional computer devices, even when the same measures are available.

This chapter therefore details work that sought to *(1)* investigate the factors which motivate an individual to secure their devices, or which may prevent an individual from doing so and *(2)* explore why decision making varies across different devices. To do this interviews were conducted using a critical decision method approach with twenty individuals who owned at least two computer devices. These interviews support findings from Chapter 4 that knowledge, or a lack thereof, influences the use of security on smart devices, however the study also reveals that other factors, such as the costs of security and only a desire to protect important information also play a key role in individual's security decisions.

5.1 Introduction

This chapter builds on the previous chapter and seeks to answer the thesis research question regarding the motivations and barriers to using security measures. It also explores the research question regarding how the use of security measures differs across different devices.

5.1.1 Contributions and Key Findings:

The main findings from this chapter are as follows:

1. It supports earlier findings from chapter 4 that people take different security approaches across different devices.

2. It demonstrates the importance of IT knowledge in whether or not an individual uses security measures, with a lack of knowledge regarding security a key barrier to the use of security mechanisms.

3. It identifies additional motivations for using security mechanisms including to protect privacy and previous experiences of security issues.

4. It identifies barriers to the use of security features such as poor usability of security mechanisms, perceiving the costs to be too high, and a belief that the information contained on a device is unimportant.

5. This study also identified the main sources of information that individuals use to find out about security.

6. Finally, this work also identifies the key time points at which users are most likely to apply security measures and whether they are happy with the level of security they have achieved. We find that many users consider and apply security measures when they first set-up a new device. Opinions are then divided on overall security level. Whilst many participants expressed a desire for greater security, many also felt that the fact that they had experienced no adverse events meant that their security levels were sufficient.

5.2 Related Work

5.2.1 Security Methods Differ Across Devices

Several studies have identified that people take differing approaches to security across different devices, with Chapter 4 and work by Mylonas et al. (2013) [42] and Mcgill et al. (2017) [222] reporting that significantly more people use anti-virus software on their computers than on their smartphones. Interestingly this was despite Mcgill et al. (2017) finding that users reported similar levels of perceived vulnerability on smartphones as they do on computers [222]. A possible explanation for the findings of these researchers is that participants perceived the consequences of a security breach against their computers as likely to have worse consequences. Additionally, participants didn't believe they could protect mobile devices to the same level, and expressed a belief that other people were more likely to use more protective measures for their computers [222].

5.2.2 Motivations For Using Security

Alsaleh et al. (2017) [223] conducted thirty interviews to explore perceived risks and attitudes towards adopting smartphone security features. In relation to locking smartphones 57% reported that they did this due to privacy concerns related to the people they know, with only 29% locking phones in order to prevent strangers accessing their data. Of those who reported backing up their phone data the biggest reason was because they had experienced data loss, although this was not necessarily due to a malicious cyber incident. There were however low levels of concern regarding granting permissions to different applications or on sharing location information on social media.

5.3 Methodology

This study used an interview approach, based on the Critical Decision Making (CDM) method [224].

5.3.1 Ethical Considerations

This research was approved by the Lancaster University's Faculty of Science and Technology Research Ethics Committee (See Appendix D for the full interview script and supporting documents). All participants were informed about the interview topic and gave informed consent before the interviews.

5.3.2 Recruitment

The study was advertised via Lancaster University's Psychology Department research participation portal and took place between April and May 2018, with participants offered £5 for taking part. In total twenty individuals volunteered to participate, 16 (80%) female and 4 (20%) male. The age of participants ranged from 18-30 years.

5.3.3 Procedure

An initial pilot interview was conducted to assess the questions and this revealed that people struggled to list all of the security features they use. To counter this a list of various security approaches was incorporated into the questions to help prompt participants to consider and remember a wider variety of possible approaches.

Following the pilot interview, nineteen interviews were conducted. In each interview participants were asked to confirm that they owned a computer or laptop and at least one other smart or internet enabled devices (participants were required to own at least a computer and a smartphone or tablet to take part). They were then asked to confirm their age and gender.

The second part of the interview was then based upon a CDM approach, with questions aimed at detailing the point at which people make security decisions and what are the factors that lead them to take security approaches (or not to take security approaches).

Conducting a CDM typically involves asking participants to recall an incident and this incident is then explored in several phases, with each phase aimed at deepening understanding of the cognitive processing during the incident. In this study it is not one particular instance that is explored but the whole process of protecting a device, whether this occurred all at one time or over a longer period.

The phases used in this study were:

1. Identifying when security measures are used: Each participant had confirmed that they owned both a computer and smartphone prior to taking part in the study, however, each participants was also asked about any additional devices they owned that could connect to the internet. Where individuals did own any additional devices participants were encouraged to identify the one they perceived as posing the greatest risk to their privacy so that a third device could be explored. Once the devices to be discussed had been confirmed participants were asked to walk through from when they first started to consider the security of the device, up to the most recent time they made a security decision regarding the device.

2. Timeline verification: Once the participant had had the chance to describe the scenario from start to finish without interruption, the scenario was described back to the participant. The participant was then asked to identify any errors or to add any missing details that may occur to them. A time line was then drawn up by the researcher, with key decision points identified.

3. Deepening probes: During this stage participants were asked a series of questions for each decision point. These questions explored motivations, whether any other approaches were considered, what information was used to make the decision, the expected outcomes, and any barriers to implementing a decision (the full questionnaire can be seen in Appendix E).

4. 'What if' phase: Whilst the first three phases focus on what actually happened, this phase explores hypothetical scenarios, exploring if they would make different decisions in hindsight or what decisions they believe other people may have made.

After going through the CDM questionnaire participants were also asked several more questions in a semi-structured interview exploring reasons for not using any approaches that were not discussed and where they would seek any further information regarding cyber security.

5.3.4 Data Analysis

The aim of this research was to identify the common themes that were present in the data. In order to examine these thematic analysis was used. First the data sets were read and reread until

the researcher became familiar with the content of the transcriptions, with key or interesting passages being highlighted and commented on. Once an initial list of the key ideas had been produced effort was put into making a set of codes to describe the data, the transcripts were re-read to ensure that all of the data had been coded according to these definitions (a particular extract may belong to one code, multiple codes or none). Once all of the data had been coded the analysis was re-conducted at a higher level searching the codes for commonalities that allowed them to be classified under potential themes.

5.3.5 Threats to Validity

This work shares many of the of the same weaknesses as the work in Chapter 4 due to a student participant population which does not represent the typical age, education level or economic status make up of the population at large.

A second threat to validity is that the work, once again, relied on participants self-reporting which can be influenced by participants wishing to give socially acceptable answers or having a poor memory of the events. This is particularly an issue since many of the participants struggled to identify different security mechanisms, relying on the interview prompts. It is therefore possible that individuals used additional security measures but they were unable to recall these during the interview.

A final weakness is that whilst everyone reported having a laptop and a smartphone, very few participants reporting owning a third computer device, limiting the number and type of devices that were studied.

5.4 Key Findings

Five key topics were identified from the interviews: *(1)* People had different motivations for using security mechanisms; *(2)* There are numerous barriers that prevent individuals from using different security mechanisms; *(3)* There are several information sources that people utilise in order to learn more about security mechanisms; *(4)* People typically apply security mechanisms at certain time points and *(5)* People have numerous reasons for using different security mechanisms across different devices. These key findings are presented in Figure 5.1 and described in more detail below.

5.4.1 Motivations and Reasons for Using Security

The interviews revealed several key motivations that drive people to use different security approaches:

1. To protect important data stored on the device;
2. To protect the owner's privacy;

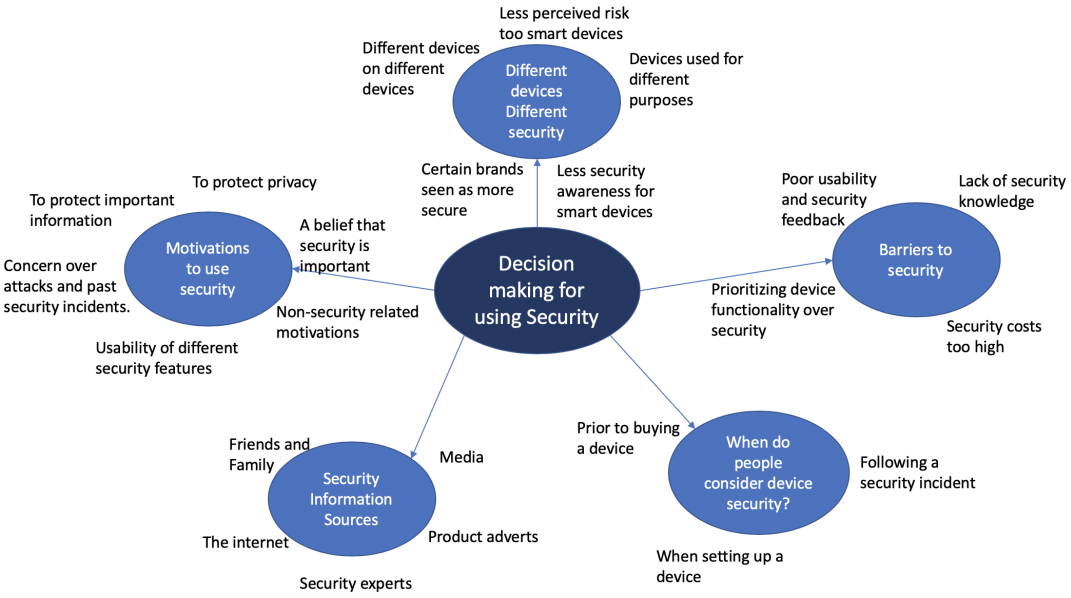


Figure 5.1: Themes Raised by Participants Regarding Why They Do and Don't Use Security Across Different Devices

3. Concern over attacks and past experiences of security issues;

4. The usability of different security features;

5. A general belief that security is important;

6. Non-security related motivations.

5.4.1.1 To Protect Important Data:

A common finding was that many participants reported a desire to ensure that information was not lost with participants using a variety of approaches such as passwords, antivirus software and encryption to achieve this. In particular they expressed concern about losing information that could impact their studies or work.

> 'Just cause erm I use my laptop for school work so I don't want anything that will probably like delete my files or um maybe like spoil my laptop cause the last laptop I had it had so much viruses on it so I couldn't use it anymore.' [Participant 4, female, 20 years]

Interestingly whilst some individuals like participant 15 did express a desire to take security measures to protect their memories, many others such as participant 8 did not consider their photos or music of particular importance.

> 'Well my motivation on my laptop is definitely just for my work and um that's got everything on it. I suppose on the tablet ipad as well its got all our photos on it from like the last three years so that's like a good reason to protect it I guess' [Participant 15, female, 19 years]

> 'I mean if someone stole my pictures it wouldn't really be the worst like its just my memories but its important information on my phone, money and stuff' [Participant 8, female, 21 years]

5.4.1.2 To Protect Their Privacy:

Linked to the idea of keeping data safe, many individuals reported that they felt a desire to maintain their privacy. This was distinct from the theme above where individuals wanted to protect particular file types from being lost, with individuals instead concerned about the fact that someone might be able to read their data or infer information about them that they wished to keep private.

> 'Because sometimes I leave my phone unattended I wanna be sure that nobody err sneaks into it and sees personal information.' [Participant 7, male, 21 years]

> 'Sometimes when you wanna like search for stuff and you don't want to leave a trace so then you use that [VPN]' [Participant 1, female 20 years]

Whilst people used a variety of security mechanisms, the desire to protect their privacy was a particular motivation for using passwords.

> 'Erm like everything has to have a password. I think its just if I lost it then it would be harder for someone to get into it erm even if I just left it for a few minutes then it will automatically password protect itself just against you know other people.' [Participant 1, female 20 years]

Whilst for many participants protecting their privacy was more of an abstract concern to do with making their data harder to access generally, for some, such as participants 12 and 14, there was also a desire to keep their information away from people they knew.

> 'I set it [password] a few years back when I had visitors in the house, I felt like now you know they might just open up the laptop to have a look and I don't like that'[Participant 12, female, 21 years]

> 'Er cause um before my friend used to just check up and read my messages I found it quite rude and intruding so I had to block my like um put in passwords' [Participant 14, female, 22 years]

5.4.1.3 Previous Experience of Security Issues:

Whilst only a few individuals reported that they had experienced an issue with security in the past, those individuals frequently reported that the experience had made them more wary and keen to ensure their security in the future.

> 'Antivirus, yeah cause I needed it after what happened back on my old laptop.' [Participant 4, female, 20 years]

> 'Long time ago when limewire existed I got a virus from there on my old laptop so since then I've been conscious of it' [Participant 8, female, 21 years]

For other participants like participant 11, this also appears to have had a large emotional impact, which they also discussed as being a key motivation for their desire to secure their devices.

> 'I've had problems in the past with somebody using my bank card online so it was just like iTunes transactions that I hadn't recognised so that's like caused me caused me to be like oh my god. I really need to do my antivirus like three times a week just to like see whether I think its a daily habit now its become like a part of life' [Participant 11, female, 25 years]

> 'I'm a bit scared because err I think one time erm I did get hacked and its a bit risky' [Participant 11, female, 25 years]

Whilst it is encouraging that individuals learn from past security incidents, understanding people's other motivations could remove the need for people to become a victim before securing their devices.

5.4.1.4 The Ease of Using Security Features:

Usability and the ease of using security features also increased participant's motivation for using them. A key example that was raised was that whenever a new device came with a security feature that was already enabled, participants reported that they would leave it running.

> 'Mine has like the laptop suggests that I use a Firewall so its something that you can turn on and off right so I just keep it on at all times. Cause I think that that's what it suggest so I don't turn it off.' [Participant 5, female, 19 years]

This suggests that participants do appreciate security but that difficulty installing security features or a lack of awareness of different security measures are the key barriers. This is also supported by the fact that participants reported that they would opt into getting security features that came with a new device.

> ‘So when I was looking for a laptop um it would tell you what security came with it and then you just sort of pay in and then have that come with the laptop so I was looking for those um because knowing me I don‘t really if if someone if the company like PC World hadn’t or you know suggested it then I wouldn’t have probably brought but it in the past I’d used that before’ [Participant 5, female, 19 years]

Ensuring that security is usable, and potentially exploring the option of having a wider array of security featured able to come pre-installed could be a way of increasing security across the general population. This could be especially true for devices where the option to buy features such as antimalware software at purchase is often not available or even discussed.

5.4.1.5 General Security:

When asked about their motivations for using security features, many participants reported simply ‘security’.

> ‘For the security reason of course’ [Participant 10, male, 26 years]

Whilst unspecific this is positive in that people are both recognising the importance of security and taking actions to maintain security, however it suggests that participants may struggle to articulate what it is they are trying to protect.

5.4.1.6 Non-Security Related Reasons:

Participants also engaged in several behaviours that can improve security for non-security reasons. This was especially the case with installing updates, with many participants suggesting that they did it more to avoid annoying pop-ups and reminders rather than because they felt that they offered any security benefits.

> ‘Well they’re kind of erm annoying that it just pops up every 10 or 20 twenty minutes its easy for me to just update it.’ [Pilot, female 20 years]

Whilst potentially effective at ensuring that people do install updates, research has suggested that people frequently feel frustrated with pop-ups [225]. Whether this approach is likely to be effective across the whole population is therefore uncertain, and again previous research has suggested that many people often neglect to install updates [60, 61].

Alternatively one participant reported that they install updates as soon as they are made available because failing to do so in the past had led to apps becoming slow or being unsupported, their motivation for doing so was therefore to ensure functionality rather than security.

> ‘I didn’t used to update my app as soon as like the update was available and er it tended tend to slow down my phone or you know even to an extent I couldn’t use

> my apps properly and all of that so after that I've always kind of sort of you know updated them immediately' [Participant 19, female, 21 years]

One individual who regularly changed their default passwords stated that they only did so to increase the memorability of the passwords rather than to make them secure.

> 'Just cause its easier to remember, I do something that's easier to remember' [Participant 3, female, 18 years]

This supports extensive literature that identifies that many people struggle to recall complex passwords [28] and are likely to reuse passwords [24, 26].

Finally one individual who used biometric security to lock their phone explicitly stated that it was nothing to do with security and that they only used it because they liked the feature.

> 'Its not about security its just you when I got this phone and it has er software and this fancy element its nothing to do with security' [Participant 19, female, 21 years]

Whilst these are all motivations specific to the individual, it is worth considering what other motivations may encourage secure behaviours.

5.4.2 Barriers to Using Security

The second theme that emerged from the research was barriers to using security and reasons for not using security. These included:

1. A lack of knowledge about different security behaviours;
2. Poor usability and a lack of feedback;
3. Considering the costs of security (financial, time, disk/memory storage) to be too high;
4. Prioritising device functionality over security.

5.4.2.1 A Lack of Knowledge About Security Behaviours:

A commonly occurring theme was that one of the key reasons for people not applying certain security approaches was that individuals were not sufficiently knowledgeable on how to use or acquire particular security mechanisms.

> 'I know that its [firewall] inbuilt in there somewhere but I don't know whether its active or inactive... I don't really know how to do it or what to do.' [Participant 2, male, 22 years]

In other cases individuals were just unaware that certain approaches existed. Participants had, therefore, never sought information about these approaches or had the knowledge about how to apply them.

> 'Well maybe erm not having knowledge of say VPN or encryption can limit me from using them and securing myself completely.' [Participant 2, male, 22 years]

Ensuring that information is readily available, or providing individuals with prompts to consider specific security features, rather than relying on individuals to actively seek out or research security methods may therefore be beneficial. This lack of knowledge was also present across different devices, with many individuals stating that they lacked knowledge about security features for smartphones. One example is participant 7 who reported that they were uncertain about how to install antivirus onto a phone.

> 'I'm not sure if how to install an antivirus on my smartphone' [Participant 7, male, 21 years]

This lack of knowledge regarding security for smartphones was highly prevalent with many individuals reporting that they had been unaware that security, beyond physical security, was even an issue for smartphones and that this was why they had never considered applying security software. Given that research shows many people are aware of antivirus software and that it is commonly used on computer devices this suggests that poor uptake could be largely due to a lack of knowledge or poor targeting of security information to the owners of smartphones.

5.4.2.2 Poor Usability and Feedback:

Supporting earlier research on the importance of usability, several participants reported that one of the barriers that prevented them from using security approaches that they had considered was doubt over whether it was actually working. This was especially the case with regards to antivirus software, with individuals having been found to want feedback and assurance that it is still protecting them [54].

> 'There is an app [antivirus] but I don't know that its working that's the problem... cause I like now that I've seen that app logo I do get notifications from it but maybe not as much as the computer would do it.' [Participant 7, female, 21 years]

One participant was then so concerned about downloading malicious software masquerading as an antivirus that she chose not to download any at all.

> 'I wasn't sure what um what kind I should get and um I know this sounds funny but really I'm um was afraid if I got the wrong one that it might cause me a problem' [Participant 16, female, 30 years]

One surprising finding however was that in some cases a high level of trust in the feedback actually meant that participants were actually less likely to take measures to protect themselves. This was particularly the case with web light camera indicators.

> 'I used to put Blue Tack over my webcam because I heard that you're supposed to do that again I just didn't feel that it was necessary because a light comes on when its in use' [Participant 6, male, 18 years]

> 'You do see a lot of people who have covered their cameras and ensured that their Bluetooth is off and all of that but I think its I've just gotten into the habit of not um seeing that as a huge threat because I know that when someone is using a camera there's automatically going to be a light next to the camera that warns me the camera is being used' [Participant 19, female, 21 years]

5.4.2.3 Time Costs:

Participants also noted the time costs associated with employing different security practices as one potential barrier to security. In particular several participants felt that using security could interrupt or delay the tasks they wanted to achieve

> 'Its a little bit annoying when you start scanning your laptop its a little bit annoying that it goes slower during this time its like half an hour or sometimes its a little bit too much.' [Participant 7, male, 21 years]

The time taken to install updates was also discussed and often reported as one of the reasons for delaying their installation, as it would interfere with the activities that they were trying to perform at the time.

> 'Sometimes because you'll be doing something and then if it takes long time its kind of a barrier to what you want to do and you never know how long its going to take' [Participant 5, female, 19 years]

Additionally, many individuals reported that they had an awareness that they lacked security knowledge but that they felt that acquiring the knowledge was not worth the amount time or effort required to gain it.

> 'You need to be willing to go out of your way, really understand what software you need and what's going on and how to protect yourselves and I'm just not prepared to do that' [Participant 12, female, 21 years]

> 'It was just one of those things that I felt like it that I've tried multiple times and every time it was like it it took considerable amounts of time like more than I was willing to invest and I've had other priorities' [Participant 16, female, 30 years]

Reducing the perceived costs e.g. by making access to security knowledge easier, could therefore once again help to reduce the perceived efforts.

5.4.2.4 Financial Costs:

A second cost that was discussed by several participants was financial. In particular, when asked about the potential barriers to security, several individuals reported that they considered the price of some anti-malware software to be too high or unreasonable.

> 'Umm maybe cost, I know that some of the products cost quite a lot of money either subscription or one off.' [Participant 6, male, 18 years]

There was also a belief that where free software was available, this was of inferior quality, with only the people who have the money to pay for the premium upgrades able to get good security.

> 'Usually all the ones you download [mobile anti-malware software] off the store are like free ones and they suck like literally they have full ads and all that kind of stuff and I used to work in a phone shop and I used to see all kinds of people with like thousands of antivirus stuff that like don't actually do anything' [Participant 1, female 20 years]

Whilst this barrier was only discussed in relation to antivirus it does highlight that users are unwilling to spend large amounts of money on security features. Future research should consider exploring the factors regarding whether an individual is likely to invest in security.

5.4.2.5 Disk/Memory Storage Costs:

A final cost barrier that was discussed was storage capacity and whether or not installing security would require deleting other apps in order to ensure that there was sufficient storage. This was more focused towards smart devices than traditional computers which have larger storage.

> 'Actually it means you have to have a certain amount of memory free, it might mean that you have to delete apps which can be a bit inconvenient. If it takes a while to update as well which can be inconvenient' [Participant 6, male, 18 years]

> 'Yeah, um not always I mean I don't always install the updates because it takes up loads of memory but if I do have memory then I do update it' [Participant 13, female, 22 years]

Whilst the costs did not always prevent an individual from employing a security approach they were still considered in relation to an internal final cost-benefit analysis, highlighting the need to ensure that the benefits of security are understood.

5.4.2.6 Prioritising Device Functionality Over Security:

Tying into the idea of individuals making decisions based on the costs and benefits, many individuals reported not using certain security approaches because they placed a greater priority on the device functioning as they wanted.

> 'I don't know I was thinking about it other people do it but I think I use Skype a lot like with my mummy and friends and family abroad so I suppose I covering my camera would be a bit would be kinda unconventional for me but I could do I mean now that I think about it I probably will do when I get back.' [Participant 5, female, 19 years]

This again supports the idea that people weigh up the personal costs and benefits about what they wish to prioritise.

5.4.3 Reasons for Using a Security Mechanism on One Device But Not Another

One of the key research questions that this work sought to identify was why individuals may take different approaches to securing different devices. When asking participants to explain these different security approaches, many of their explanations related back to their original motivations and barriers for using security and these can be summarised below:

1. Users store different information on different devices and only protect what they consider to be important information.
2. Users have far less awareness of security measures for smart devices compared to more traditional computer devices.
3. Users perceived smart devices to be at less risk of attack.
4. Users use devices for different purposes and so prioritise different functionality on different devices.

One additional and unexpected reason that emerged from the interviews was:

5 Users make decisions based not only on the type of device but also the brand of device, with several individuals reporting a belief that Apple devices could not get viruses.

5.4.3.1 Different devices have different information stored on them:

One of the main motivations for using security was because individuals perceived information as important. Therefore participants who stored different types of information on different devices, e.g., one device for university work and one device for gaming, often made different choices about how to secure them based on the information they contained.

> 'One reason would be that I don't have a lot information its more of a daily use and its a very basic superficial use of a mobile phone I don't use I mean I do use it extensively but not for anything extremely important' [Participant 19, female, 21 years]

In particular participants who reported not storing any important data on a device felt this justified not using anti-malware software.

5.4.3.2 Lack of Awareness of How to Protect Smart Devices:

Many individuals also reported that they were unaware that security software for smart devices existed. Participants who were unaware of the risks obviously then took no measures to defend against them and this was particularly the case for newer forms of devices.

> 'Well with a smartphone its not as complex as you know like a laptop because er I'm not really aware of like the antivirus or firewalls I could have on a smartphone because I don't have that knowledge' [Participant 11, female, 25 years]

For others they had never considered applying security features to these devices.

> 'I mean this might sound stupid but I never really thought of downloading that [antivirus] on the phone I guess I never saw it is a threat even though its probably the same or risk as a laptop I just never thought of that' [Participant 12, female, 21 years]

5.4.3.3 People Perceive Smart Devices to be Less At Risk:

Individuals reported putting differing levels of security on different devices because they perceived differing levels of risk. In one case because they were using a smartphone for different purposes to their laptop, e.g., not browsing the web, they believed that there was no need for antivirus software.

> 'I don't think that there's such a high chance of me getting a virus on a smartphone because I am not using it to browse on the web.' [Participant 7, male, 21 years]

Some participants then just thought that certain devices were less at risk because they were less likely to be targeted by attackers in the first place, or because these devices were more naturally secure.

> 'I've not done that I think that because its a smartphone its more secure' [Participant 14, female, 22 years]

One individual however reported that they felt passwords were more important for their portable devices as they felt that there would be more opportunity for people to access these devices.

> 'I think maybe a password on a phone would be a bit more important because you have it out and about... its much easier to misplace it than it is to misplace your laptop' [Participant 9, female, 20 years]

5.4.3.4 Prioritising Different Device Features:

Whilst many computers, laptops, smartphones and tablet devices have similar functionality, many individuals use these devices for different purposes and this impacts the security measures that they use. For example, participant 14 reported that they prioritised camera functionality over security on their phone because they used the camera frequently, however they covered it on their laptop because they hardly used it.

> 'Because I use my phone for selfies whatsapp videos many things I don't really use my laptop camera for many things' [Participant 14, female, 22 years]

5.4.3.5 Apple Devices Don't Need Antivirus:

One pervading belief that was held by a number of the participants was that Apple devices are protected against viruses and other forms of malware.

> '...cause when I was buying it I sort of thought of protection but most people were like Macs come pretty protected on their own anyway' [Participant 1, female, 20 years]

> 'I feel that its more security proofed than android devices and so I I prefer it for that reason' [Participant 16, female, 30 years]

There is, however, a growing number of malwares that can be harmful to Apple devices and it is unclear to what extent participants understood this risk with many choosing not to protect Apple devices, even if they would have if they had bought a Windows device.

5.4.4 Sources of Security Information

Participants identified several sources of information that they used for security, or which would be their first port of call if they wanted to search for more information on security.

5.4.4.1 Friends and Family:

A big source of security information was in the form of friends and family who offered both advice and helped individuals to set up their own security, frequently in the form of antivirus software.

> 'I think my dad's gotta antivirus already on there' [Participant 8, female, 21 years]

> 'To be honest my dad cause he knows a lot about computers just said to me its good to have something there to sort of keep checking your make sure you don't get any viruses' [Participant 8, female, 21 years]

Friends and social acquaintances then appeared to play a bigger role in whether an individual was likely to take physical approaches such as covering up their camera when not in use, with some individuals taking friend's advice to keep it covered and others observing acquaintances engaging in these behaviours.

> 'That was when my friend who does IT, an IT course debriefed me through the system so I thought oh its a new knowledge now so er I started doing that [to cover cameras] now cause he told me that' [Participant 11, female, 25 years]

Additionally one individual reported that whilst they have considered covering up their camera because people started talking about it they hadn't actually been motivated enough to do it yet.

> 'I have occurred to do it well I want to do my laptop one [cover camera] I just haven't got round to doing it I mean its not like that long everyone was like I'll do it so I haven't done it yet' [Participant 1, female, 20 years]

This suggests that whilst social influence may play a role, its effects are not always immediate and may be limited.

5.4.4.2 Internet:

The most commonly reported source of security information was the internet, with the majority of respondents reporting that they would simply Google the information they wanted.

> 'Err actually cause I don't really understand security I just Google it and just mostly are basic things that I do but I don't actually know if it works or not yeah' [Participant 10, male, 26 years]

> 'I think just online, any or my questions I'd just type into Google and see what comes up' [Participant 13, female, 22 years]

> 'I'd probably like just go straight to the internet just Google it' [Participant 17, female, 20 years]

Whilst it is perhaps obvious that many people would turn to the internet given the abundance of information available, previous research suggested that elderly individuals who generally trusted the internet did not like to use it for gathering security information [226]. This work suggests that this reluctance may not be present in younger populations. Whilst many individuals reported that they would use Google, rather than any particular sites or online resources that they trusted, some reported that they sought out videos or documentaries on the subject.

5.4.4.3 Media:

The media was also referenced as a source of security information with participants reporting that they undertook certain security behaviours after reading or watching the news about certain cyber issues.

> 'I guess if i usually if I like see anything on the news or if I see like with the er camera one I saw like um what was it like just talking about it and there was this video and it was talking about like Zuckerberg and he has it on his thing as well so I was like oh OK that could happen and I did more research.' [Participant 1, female 20 years]

> 'I also actually cover the top of my camera as well because er just in case er because I heard a bit of the articles and you know I read online stuff that its really risky because people could just look through the camera hole. So I don't know whether its true but its getting me a bit cautious...' [Participant 11, female, 25 years]

> 'I've seen er a couple of information videos where they talk about people hacking into computers access er accessing the webcam so there's a small sticker' [Participant 2, male 22 years]

Again this was especially the case for covering up webcams with many individuals reporting that this was a topic they had seen or heard in the news over the previous few years. One individual then reported that they started covering up their webcam after watching a fictional TV show that alerted them to the possibility of malicious individuals being able to access it.

> 'I covered up the webcam like with little dotty stickers and that's because I watched erm an episode of black mirror' [Participant 3, female, 18 years]

5.4.4.4 Security Experts:

A small proportion of the individuals reported that they had sought advice from security experts, suggesting that some people perhaps preferred to speak to a human being. However, the finding

may reflect the student population and their easy access to the university's IT support desk, which is a support option that many individuals would not have access to.

> 'Well when I got my new laptop I went to the *[IT help desk]* and then I um told them I wanted to get antivirus and they told me that the university offers one that's really good so I just got that one.' [Participant 4, female, 20 years]

Whilst the individual above went to the support desk with a specific question in mind, other participants did list it as a credible information source that they would use if they felt the need to seek out further information.

> 'To be honest because I"m a student um I actually tend to er have a habit of approaching *[IT help desk]* but I don't know whether they are skilled I think they must be because they are you know working at the university' [Participant 11, female, 25 years]

> 'There is a university help desk and maybe just have a little look on the internet' [Participant 15, females, 19 years]

5.4.4.5 Adverts:

Finally one individual reported that they had found out information regarding anti-malware protection directly from antivirus software adverts.

> 'Advertisements of antivirus softwares there they publicise all the advantages, disadvantages of having antivirus, not having antivirus' [Participant 2, male, 22 years]

Whilst adverts are obviously designed to sell a companies products, in this case they did give the individual the information they wanted to help come to a decision.

5.4.5 When Do People Apply Security Approaches?

This work also explored when people implemented different security approaches to identify what may prompt an individual to consider their security in the first place.

5.4.5.1 Device Setup:

For many individuals, security was only a particular consideration when they were buying and setting up a new device. For a small number of individuals who bought certain devices, e.g., Apple devices, security was a factor in what type of device that they bought. For others the buying process, especially when buying laptops, often came with the advice to buy some form of anti-malware software, and this advice often factored into their decisions. For other forms

of security such as setting passwords or firewalls, this was often performed during the setup process.

> 'I got it [antivirus] with the laptop its er because we the person who sold me it at [the store] told me that it would be credible to use it given my circumstances' [Participant 11, female, 25 years]

Whilst some are likely prompted by sales people as participant 12 above, many individuals reported that features such as passwords were also set up during setup, suggesting that the setup walkthroughs may be successful at encouraging individuals to set up passwords and biometric security features.

5.4.5.2 Maintaining Security:

Once a device was set up, participants reported that they sometimes maintained security through processes such as installing updates or conducting virus scans, however the activities different participants engaged in varied a lot. Whilst many individuals set up automatic updates, many others also reported that they often refused or delayed the installation of updates.

Additionally, people were also prompted to install security mechanisms outside of the initial set up process when they changed their activities, with participants also prompted to consider security when they are exposed either to online behaviour that they find irritating or possibly malicious.

> 'So as soon as I like when I used my computer computer to watch a movie like I like started ads so I put an adblocker up' [Participant 8, female, 21 years]

Overall, however, the findings suggest that security is not seen as an ongoing activity and so early set-ups should seek to maximise the number of security features that individuals incorporate.

5.4.5.3 When Encountering New Information:

Outside of this participants only reported actively seeking out security when they were faced with a security incident or when they happened to come across a new piece of advice, e.g. in the news.

> 'Usually if I like see anything on the news' [Participant 1, female, 20 years]

Ensuring that individuals are given knowledge about different security features early on, e.g. when first buying a device, could help to mitigate the risk of people only applying security after they become aware of a potential risk.

5.4.6 Happiness with Overall Level of Security

A final question that was explored in the interviews were whether or not participants were happy with the level of security they had achieved for their devices, this allowed exploration of whether people wanted higher levels of security but did not know how to achieve this.

Participants' opinions on whether or not they were happy with the level of security they achieved varied. Many individuals reported that they were content with their overall level of security, stating that they had not experienced any viruses or security issues as indicators that they have managed to keep their devices secure.

> 'Yeah I've not had any problems with viruses or anything before so I'd say I'm happy' [Participant 9, female, 20 years]

> 'Well yeah, I haven't really got any like hacked well I don't think I've got any like security issues so far.' [Participant 4, female, 20 years]

In contrast, several participants expressed doubt over their abilities to protect their devices, feeling that they didn't know or do enough.

> 'I don't honestly I don't feel I do enough when it comes to security for my laptop mostly because of ignorance and you know like if I knew I would do it but I'm also not willing to go out of my way to learn' [Participant 12, female, 21 years]

Despite stating that they were unhappy, individuals were not actively seeking to increase their security suggesting that whilst they had some concerns they were not excessively worried.

5.5 Discussion

This chapter highlights that IT security knowledge is a key determinant of whether or not an individual makes uses of different security mechanisms, with multiple participants reporting a lack of awareness about different security approaches as key reason for not using them. A lack of knowledge regarding security for non traditional computers was also one of the reasons people failed to take the same security precautions for smartphones and tablets as they do laptops. This supports some of the key findings from Chapter 4, however, the interviews in this chapter also identified several new motivations that lead people take different security approaches. Some of these motivations are unsurprising and have been found by previous researchers, such as that concerns about their security and privacy are motivators for using security features [223]. These findings also support early research models such as the PMT and TTAT [215–217]. This study did, however, identify that the usability of security features, as well as several non-security related factors can also encourage people to take measures to protect their devices. Many people highlighted that, when offered security features, e.g., firewalls during set-up, they would always

choose affirmatively, but that they wouldn't always seek out these features. This finding ties into the notion that many participants appeared to make security-related decisions based on a cost-benefit analysis, with many people using costs, including financial, time or disk or memory storage costs as reasons not to make use of certain security mechanisms. Likewise, participants also reported that they would sometimes prioritise a device's functionality over security features, e.g, whilst they might cover up a camera they rarely used, they would not cover a camera on a device where they used it frequently.

A final but important barrier was a lack of knowledge, with many individuals reporting being either entirely unaware of particular security mechanisms, or unaware of how to implement them. This was especially the case with regards to smartphone and tablet devices, with many individuals unaware that features that they frequently used on their laptop devices, e.g., antivirus software were even available for other forms of device. This highlights a need to evolve users' understanding and awareness of the threats and countermeasures that can be applied to different devices. However this in itself could be a challenge. Whilst some previous researchers have found training to be effective for increasing security knowledge [116], our interviews suggested that for many of the participants, the effort to learn about security for themselves was too much of a deterrent. This suggests a level of complacency or security fatigue that needs to be overcome.

Whilst differing levels of knowledge across different devices was a key explanation for why people use different methods for their different devices, there were also several alternative explanations. Positively these alternative explanations suggest that, in some instances, where individuals take different security approaches across different devices this is due to conscious choices, such as protecting devices with more sensitive information. This supports findings that people will often use more secure passwords for accounts they deem to be more important [18, 19, 24, 32]. However, whilst these may have been conscious decisions, these were still sometimes based upon non-factual assumptions, with some individuals reporting that these decisions were based upon beliefs that smartphones and Apple devices were not targeted by malware.

5.6 Interim Conclusions

There are several conclusions that can be drawn from this work.

Firstly this work provides further support that an individual's level of IT security knowledge and awareness of different security approaches is a key factor in whether an individual will use different security approaches. In particular poor knowledge about the different security software available on non-traditional computers was a key barrier to participants seeking to protect these devices and the information contained on them.

Secondly, people also report that other factors play a role in their decision making. In particular, they go to greater efforts to protect the information that is important to them whilst

balancing this against the various costs of different security approaches.

Thirdly, many participants, use different security approaches for different devices. This is often done to protect devices with more sensitive information, but is sometimes also the result of a perception that certain devices are more at risk of being compromised.

Fourth, this study highlights that individuals are most likely to apply security features when they first buy and set-up a device or following a security incident. Whether an individual seeks to behave securely throughout the life of a device varies, with many individuals often choosing to delay updates or failing to read application or software permissions.

CHAPTER 6

CPS IN THE HOME- DETECTION OF ATTACKS

The previous chapters have highlighted that whilst individuals report an awareness of many different types of attacks and multiple motivations for wanting to keep their devices secure, they remain unaware of some new forms of attacks. In addition the research showed that some security approaches were less likely to be applied to newer smart devices. There are a variety of reasons for this, but one key reason appears to be due to a lack of knowledge regarding how these devices may be vulnerable to attack, why someone might want to attack them, and how to protect these devices. This chapter seeks to take this work further by investigating whether this knowledge gap not only leads individuals to leave these devices more vulnerable, but whether it also makes it less likely that they will be able to detect attacks that target physical components.

6.1 Introduction

This chapter builds on from chapters 4 and 5 by looking at whether individuals can detect different forms of cyber attacks against home devices. In particular this chapter explores whether attacks against cameras and speakers are more or less likely to be identified compared to more traditional forms of attacks, such as phishing emails and whether individual differences can explain any differences in detection rates.

Finally, this work explores what types of behaviours individuals perceived as suspicious, when they had been primed to consider cyber security issues.

6.1.1 Contributions and Key Findings

The main findings from this chapter are as follows:

1. It identifies that some forms of cyber attack are easier to identify that others, with attacks against webcams placed besides monitors, particularly unlikely to be observed or recognised.
2. This chapter identifies that on-screen warning indicators may be more effective at gaining a user's attention than off-screen indicators.
3. This chapter identifies a mixed picture of individual differences being linked to attack detection. Gender, IT knowledge and confidence were all related to detection of one type of attack, with neuroticism having no significance for any attacks.

6.2 Related Work

As discussed in Chapter 2 there have been numerous studies exploring whether people are able to identify different forms of cyber attacks such as phishing emails and malicious web pages. This research has suggested that people use a range of strategies and cues to try and distinguish between legitimate and malicious pages, although not all of these strategies are effective [132].

One common approach taken by individuals has been to look for poor grammar or spelling. Research investigating the efficacy of looking at poor grammar has, however, been equivocal. Wang et al. (2012) [131] concluded that paying attention to phishing deception indicators (e.g. poor grammar) reduces the cognitive effort of considering a phishing email and reduces the likelihood that they will respond. However, Vishwanath et al. (2011) found that individuals who pay more attention to email source, grammar and spelling are less likely to identify phishing emails [133]. Phishing emails are however, increasingly sophisticated and designed to maximise the chances of getting a response. This includes utilising emotional cues such as inciting liking, reciprocity, social proof, scarcity [136], and urgency [133] as well making phishing emails more personal [134, 135]

An alternative approach for identifying suspicious emails and pages is to look for security icons, with work by Downs, Holbrook and Cranor (2007) asking individuals to role play as a 'Pat Jones' and respond to their emails, all of which contained a URL link. They found that individuals who understood the meaning of the lock symbols and who could interpret URLs were less likely to fall victim to phishing attacks [148]. Whilst focusing on these approaches may help to prevent individuals from falling victim to phishing attacks, research using eye-tracking studies has found that people frequently pay attention to the wrong features for making security decisions. Darwish et al. (2012) reported that users often focus on domain names to determine legitimacy rather than using security certificates. A second study by Alsharnouby (2015) found that very little time was spent examining security indicators and that even though participants did examine SSL and HTTPS identifiers they still frequently failed to identify suspicious pages [124].

Work looking at the detection of attacks against physical home devices has been much sparser however. Portnoff et al. (2015) however found that less than half of participants observed a webcam being turned, and this fell to just 4% when participants were not working on the

computer [209]. This chapter therefore seeks to expand on this work and compare detection of different forms of attacks against home devices.

6.3 Methodology

To investigate how detection of an attack against a physical device compared to detection of attacks against a traditional system, participants were invited to attend a lab study where they were asked to work their way through several webpages. These pages either contained several questions from a personality questionnaire or a link to an email account and participants were asked to keep in mind that they may be exposed to one or more cyber attacks throughout the experiment.

6.3.1 Ethical Considerations

This research was approved by Lancaster University's Faculty of Science and Technology research Ethics Committee (See Appendix F for approved ethics forms). All participants gave consent to participate and were informed that they may be observed throughout the study.

6.3.2 Recruitment

The study was advertised on a university campus using the Lancaster University psychology department recruitment system, posters and social media in December 2018 and January 2019. Participants were offered £3.50 for their participation. In total 69 individuals took part and a complete breakdown of the demographic breakdown can be seen in Table 6.1.

Table 6.1: Demographic Breakdown of Participants

		Male	Female	Other	Total
	Total	16 (23%)	52 (75%)	1 (1%)	69 (100%)
Age	18	1 (1%)	6 (9%)		7 (10%)
	19	1 (1%)	7 (10%)		8 (12%)
	20	5 (7%)	18 (26%)		23 (33%)
	21	3 (4%)	6 (9%)		9 (13%)
	22	2 (3%)	5 (7%)		7 (10%)
	23		3 (4%)		3 (4%)
	24		1 (1%)	1 (1%)	2 (3%)
	25		2 (3%)		2 (3%)
	26+	4 (6%)	4 (6%)		8 (12%)
IT Knowledge	Very Low				0 (0%)
	Low	1 (1%)	6 (9%)		7 (10%)
	Moderate	9 (13%)	34 (49%)	1 (1%)	44 (64%)
	High	5 (7%)	9 (13%)		14 (20%)
	Very High	1 (1%)	3 (4%)		4 (6%)

6.3.3 Procedure

All participants who volunteered were invited to attend a lab session where they were given the full instructions for the study, before being asked for their consent to take part in the study and to be observed throughout. Participants who consented were then sat at desk with two computer screens. The left hand-screen formed the main part of the experiment and the right-hand screen was for when participants were directed to specific email tasks. A camera was placed just in front of the bottom of left screen (if anyone asked they were informed that it was a camera and is sometimes used in eye tracking studies, this was to ensure that participants were able to clarify that this was a camera without priming everyone that this was an important element of the study, however this rarely occurred). The LED was a 5mm, blue, with a brightness of 9 candela and was designed to be clearly visible to the participants. It is worth noting that there was no actual camera behind the lens and so no recordings were made during this study. The speaker volume was maintained at a constant level and the blinds to the room were always closed to prevent any glare on the screens or on the LED. A diagram of the study layout can be seen in Figure 6.1.

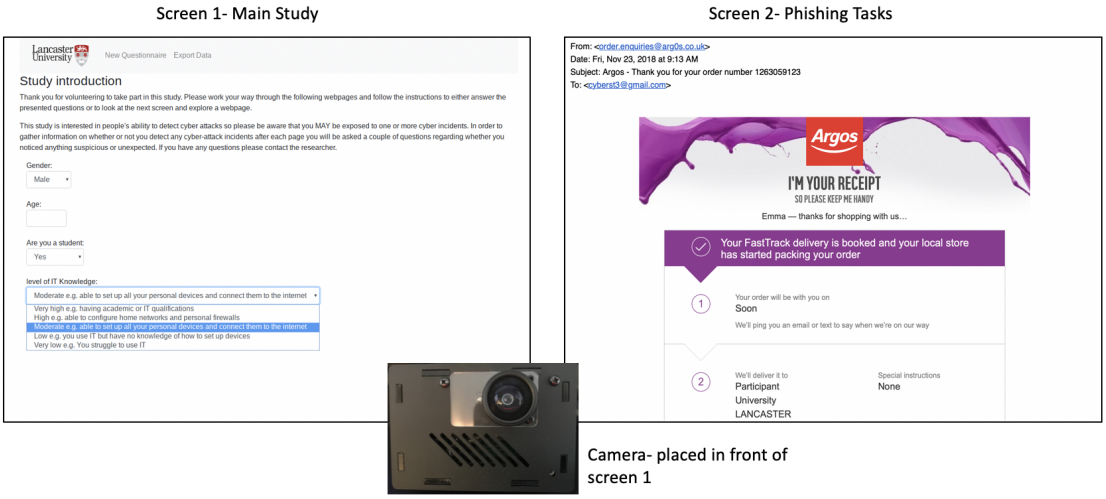


Figure 6.1: Equipment Layout For The Study

For the study, participants were presented with a series of webpages and the instructions to work through these individually. This involved either completing the questionnaire on the main screen or, if instructed to, looking at the phishing emails on the second screen, with the ordering of the webpages randomised for each participant. At the start of the study participants were also informed that they may be faced with one or more cyber attacks. Individuals were primed to consider security in order to explore participant's maximum ability to detect a range of different attacks. Each condition page was therefore followed by a short questionnaire page asking if on the last page they had seen anything strange, if they believed this was the result of a cyber attack, and how confident they were with their response. The pages and attacks that each

participant was presented with are described below and presented in Figure 6.2. The scripts were then run off of a raspberry pi and were written by another PhD student within the Lancaster computer science department.

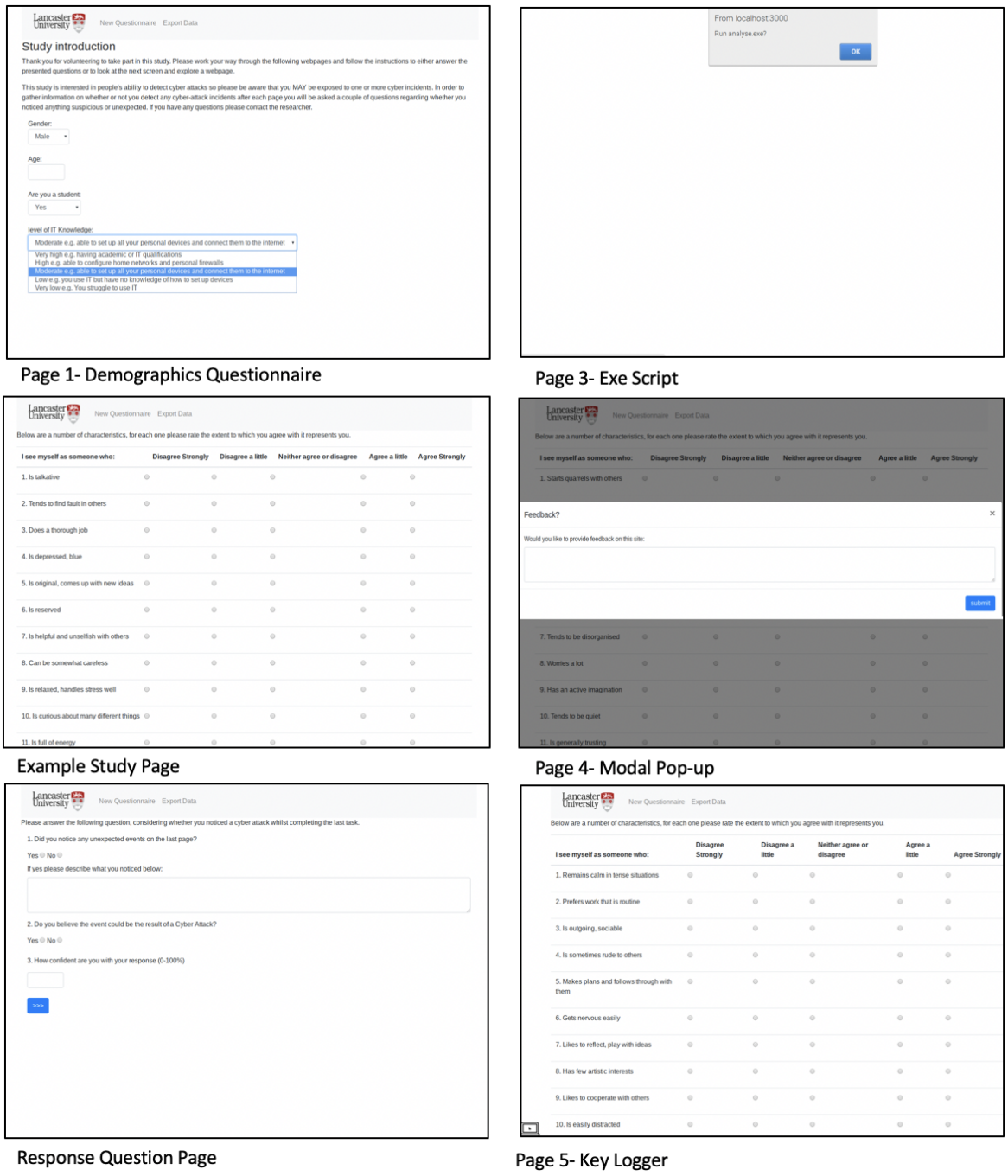


Figure 6.2: Examples of the Different Webpages Shown to Participants.

– Page 1 Demographic Questions Page- A basic demographic questionnaire (this page always

came first).

- Page 2 Email Account- Instruction to look at email account on screen 2 containing one phishing email (phishing condition) and two safe emails (email control 1 and 2). These can be seen in Figure 6.3.
- Page 3 Exe. Script- Questionnaire and a script that caused a pop-up asking to run an exe. file to appear before the page loaded (malicious pop-up).
- Page 4 Modal Pop-Up- Questionnaire and modal pop-up asking if they would like to provide feedback on the website (pop-up control).
- Page 5 Key Logger- Questionnaire and symbol in bottom left of screen that appeared when mouse was moved (On-screen warning condition).
- Page 6 LED Light- Questionnaire and script to switch on IoT camera LED (LED warning condition).
- Page 7 Audio File- Questionnaire and audio of Microsoft start-up sound (Audio warning condition).
- Pages 8 and 9 Controls- Questionnaires with no other events (control conditions).

The demographics collected involved age, gender and self-reported IT knowledge in order to explore the literature findings that these factors could be related to an individual's susceptibility to attacks. The questionnaires presented throughout the study used questions from standardised personality questionnaires including the big five trait taxonomy [161] so that personality traits could be explored in relation to ability to detect attacks.

One of the conditions involved asking the participants to view three emails (Figure 6.3) and make a judgment as to whether they posed a security risk. The three emails consisted of a fake email claiming to be from a well known store- Argos, but with the email using a zero in the sender address as well as a containing an unnecessary pdf attachment. The two safe emails consisted of a university newsletter and an email notification of an update to a privacy policy.

The task was designed to take approximately 20 minutes, and once participants had completed the experiment they were fully debriefed. This included being informed about the webcam light being switched on and reassured that their was no actual camera behind the lens.

6.3.4 Data Analysis

Data analysis involved descriptive and quantitative statistics to explore whether people are able to identify different types attacks. A Cochrans Q analysis was conducted to explore whether detection is higher across different conditions alongside some qualitative discussion about what types of system behaviour people found to be suspicious.

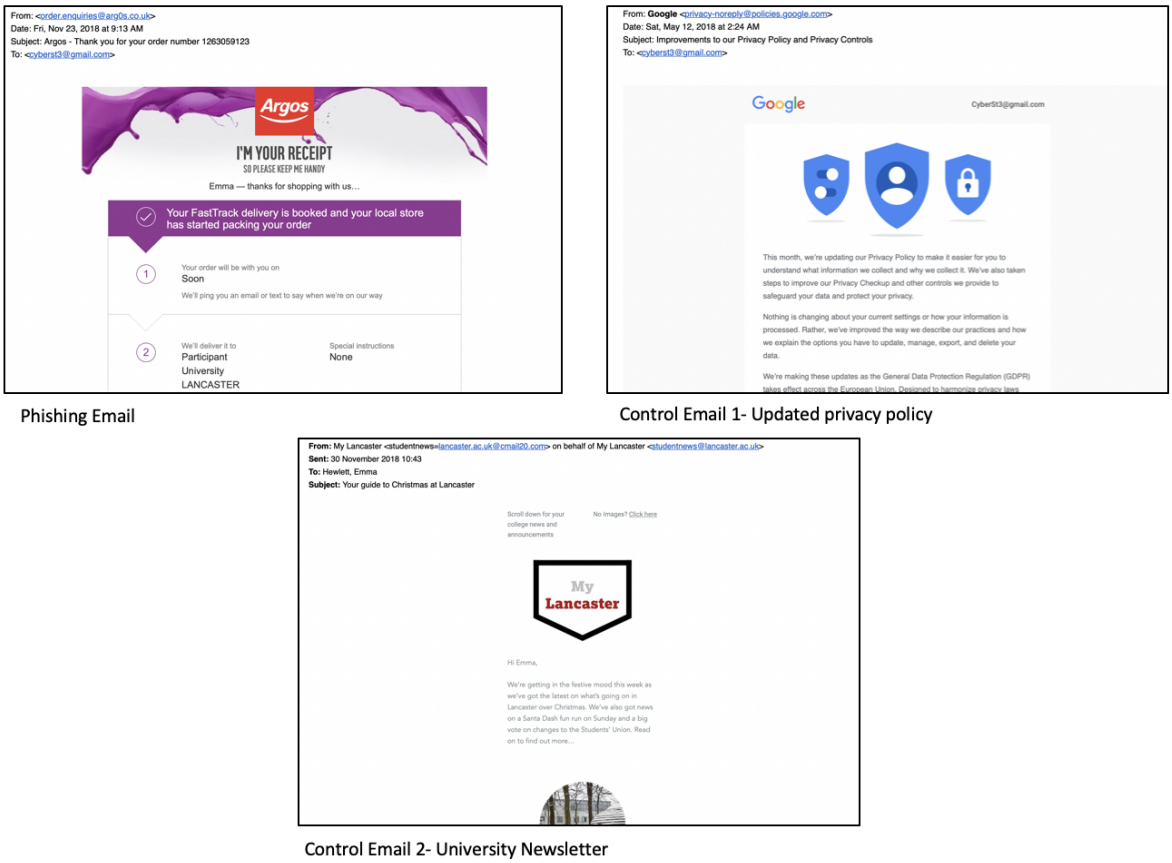


Figure 6.3: The Three Emails Presented to Participants

Additionally a regression analysis was used to explore whether factors that have been previously linked to susceptibility to cyber attacks could help to explain why some people detect attacks whilst others don't.

The full details on the statistical analyses that were conducted for this study can be found in Appendix G.

6.3.5 Threats to Validity

This work has several limitations. Firstly there was a small population sample, that consisted largely of students and whose self reported levels of IT knowledge had limited variance, limiting the generalisability of the findings. A second limitation is that the small number of participants restricted the number of variables that could be explored within this study meaning that only some aspects of personality could be explored. Thirdly, not all of the conditions that were explored represented realistic attacks against physical devices, although they still provided novel and useful information regarding the types of behaviours that are considered suspicious. A fourth limitation is that the physical representation of the different attacks differed in size (both the

key logger and LED light alerts were much smaller than both the pop-up condition events) and so the study may be exploring the participant's awareness of what was going on more than what system behaviours they considered to be suspicious. Finally, all the participants in this study were primed to consider security. Whilst this allowed an exploration of attribution of blame for security incidents, it doesn't allow for an exploration of whether people can detect attacks when they have not been primed to consider security issues.

6.4 Results

6.4.1 What Conditions Do Participants Consider to be Malicious Events?

Figure 6.4 shows the percentage of participants who labelled each condition as a cyber attack, highlighting a large degree of variance in whether an event was observed, and considered to be malicious, across these conditions. Notably, the exe. pop-up was the event most likely to be seen as a potential cyber attack. The mouse indicator was the second most likely to be considered an attack, although this may reflect unfamiliarity with this event. The webcam attack however was not identified as an attack any more than the control conditions.

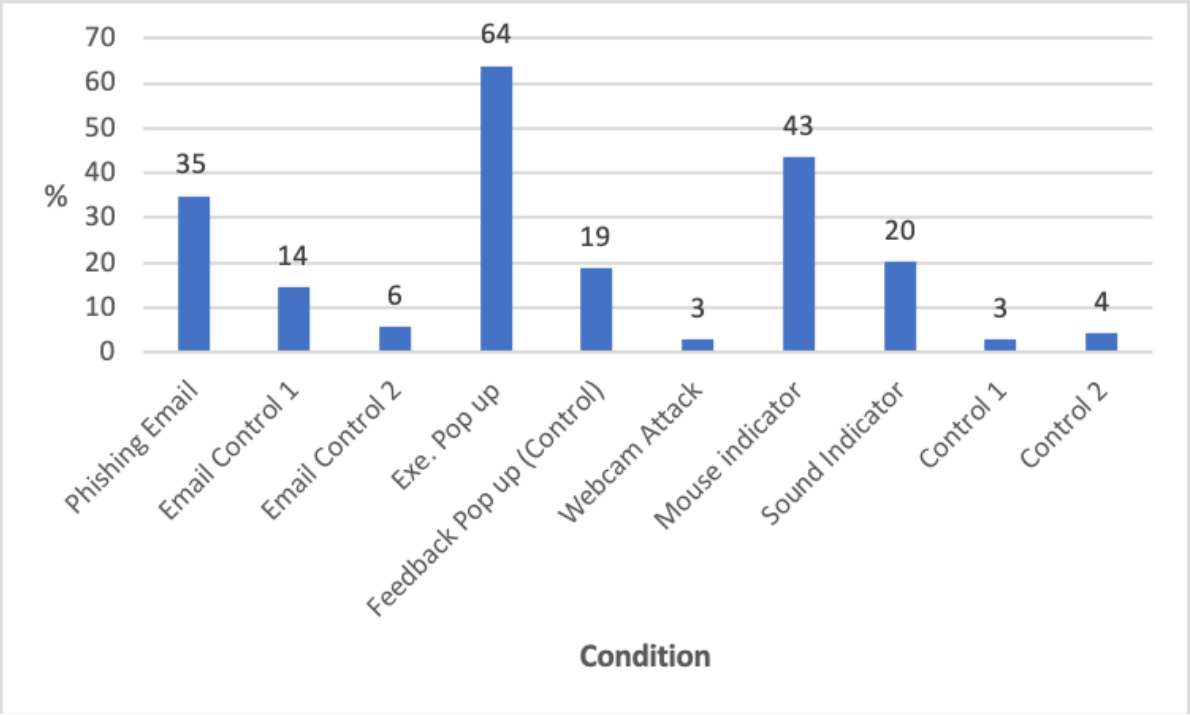


Figure 6.4: Percentage of Participants Reporting That Each Condition Represented a Cyber Attack

To explore these findings in more detail a Cochrans Q test was also run to explore if any of the differences in labelling a condition as suspicious were statistically significant. Note that false

positives for attacks (correctly believing that an attack had occurred for a particular condition, but describing the wrong incident) have been removed.

Figure 6.5 shows the outputs of this Cochrans Q test, with $X^2(9) = 157.846$, $p < .001$. This shows that the percentage of participants reporting that each condition was an attack was statistically significantly across the different conditions.

Test Statistics

N	69
Cochran's Q	157.846[a]
df	9
Asymp. Sig.	.000

a. 0 is treated as a success.

Figure 6.5: Results of the Cochrans Q Statistical Test

To explore which conditions had significant differences between them Dunn's post hoc tests were run. The outputs of these can be seen in Appendix G Section G.1.1, with all results interpreted with a Bonferroni adjustment to account for the fact that multiple tests were being run. The key results that emerged from this analysis are discussed in the sections below.

6.4.1.1 Identifying Phishing Emails

The first attack considered was phishing emails. Numerous campaigns have sought to raise awareness of this type of attack, with many large organisations and companies e.g. banks and government departments, running campaigns and placing warnings about fraudulent emails on their websites. Given these campaigns, as well as increasing research into training for improving phishing awareness [177, 227–230], phishing was deemed to be an attack with which many participants would potentially be very familiar. As can be seen in Figure 6.4, which shows how many people labelled each condition as a potential cyber attack, the phishing email was labelled as an attack much more frequently than the two control emails. Despite this less than half of the participants correctly identified it. Statistical analysis also revealed that, whilst there was a statistical difference between the number of people reporting the phishing email over email control 1 (p=.001), there was no statistical difference between the phishing email and email control 2 (p=.143). This suggests, that whilst people have some ability to detect some phishing emails, this ability is poor.

6.4.1.2 Identifying Malicious Pop-Ups

The second type of attack that was examined was a malicious pop-up that asked to run a .exe file. This was then compared to a modal feedback pop-up and to two control pages with no events, to

examine how well people were able to identify this as a potential attack. Figure 6.4, shows that this attack was by far the most recognised of those that were examined and that people were typically able to distinguish between a malicious pop-up and a harmless pop-up. However, nearly one-fifth of individuals did still consider the modal feedback pop-up as suspicious despite being common across many websites.

The statistical analysis revealed that the .exe pop-up was statistically more likely to be considered an attack compared to the modal feedback pop-up and compared to the two control conditions ($p<0.001$). The .exe pop-up attack was also statistically more likely to be identified as an attack compared to the phishing email suggesting that people are statistically more likely to recognise a malicious pop-up than phishing emails ($p=0.001$).

6.4.1.3 Identifying the Web Cam Attack

This study was especially interested in exploring whether individuals can detect attacks against physical devices, with one condition exploring whether individuals were able to identify a webcam light being switched on and recognise this as suspicious. In this particular study only 2 individuals (2.9%) correctly identified that this had occurred although both of these individuals did regard this as a malicious event. This was the same number of individuals who reported an attack in control condition 1 and slightly less than for control condition 2 and so there was no statistical difference between these conditions ($p=1.00$). It is worth noting however that whilst this work was interested in what participants considered to be a 'cyber attack', by giving them tasks to perform on the computer screen it may have resulted in a degree of inattentional blindness that could explain why this attack was so rarely observed. Future work should therefore explore this type of attack when attention is not directed so directly towards the screen or when the webcam is in a position that participants may be more familiar with.

6.4.1.4 Exploring Other Kinds of Indicators to Improve Security

Given that one earlier study had suggested that people are poor at observing web-cam lights, this study also included two additional conditions which did not mimic an explicit attack, but which used different potential warning indicators. These two conditions, page 5- key logger and page 7- audio file, were included to explore the types of security warnings to which people pay attention. Both of these conditions were viewed with suspicion. The mouse indicator was rated as an attack more frequently than the phishing email (although not significantly) and as more suspicious than both the control conditions (which was significant $p <.001$). One-fifth of participants also reported the sound indicator as suspicious. Although this was not significant compared to the control conditions.

Perhaps most interestingly, however, is that even more people noticed these occurrences, than reported them as suspicious with 62% of participants observing the mouse indicator and 55% reporting the sound indicator. These were, therefore, both significantly more likely to be noticed

than the LED indicator light switching on. This could provide valuable insights for the design of potential security alerts, highlighting that visual security indicators may be best placed on screen and that individuals should be given the option to have audio warnings. More research is needed however to examine the impact of familiarity and habituation effects for different warning types.

6.4.2 What Level of Variance in Detection of Attacks Can Be Explained By Looking at Participant's Demographic Factors?

In order to explore whether any of the independent variables could explain some of the variance in whether an individual detects an attack three binomial logistic regression analyses were run (one for each attack). Due to the relatively small number of participants only four independent variables could be tested. Here only gender, IT knowledge, level of confidence and neuroticism were used. Gender, IT knowledge and level of confidence were chosen as these variables had all been found to be significant in the use of more security measures (Chapter 4). Neuroticism was chosen as one of the personality traits that had more consistent findings in the security literature.

The full outputs and assumption testing from these tests can be seen in Appendix G, Section G.2.

6.4.2.1 Ascertaining the Impact of Gender, IT Knowledge, Confidence and Neuroticism on the Detection of Phishing Emails

A binomial logistic regression was performed to explore the effects of gender, IT knowledge, confidence in their decision as to whether their was an attack and neuroticism on the likelihood that participants would detect a phishing email. The logistic regression model was statistically significant $X^2(4)= 11.592$, p=.021. The model explained 21.7% (Nagelkerke R^2) of the variance in the detection of phishing emails (see Figure 6.6).

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	75.428[a]	.157	.217

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	11.592	4	.021
	Block	11.592	4	.021
	Model	11.592	4	.021

Figure 6.6: Outputs of the Binomial Regression Analysis for Detecting a Phishing Email

In addition this model correctly classified 75.0% of cases. Sensitivity or true positives (the percentage of cases where the model correctly identified that a participant would detect the attack) was 47.8%. Specificity or true negatives (the number of individuals who didn't detect the phishing email and who were predicted to not detect the attack) was 88.9% (See Appendix G).

Positive predictive value (the number of predicted detections of phishing emails that were correct) was 68.8% and the negative predictive value was 76.9%. Of the four predictor variables only one was statistically significant: gender, with males having an 8.07 times higher odds of successfully detect a phishing email (as shown in Table 6.2).

Table 6.2: Logistic Regression Predicting the Likelihood of Participants Detecting a Phishing Email Based on Gender, IT Knowledge, Confidence and Neuroticism

	B	SE	Wald	df	p	Odds Ratio
Gender	2.088	.771	7.334	1	.007	8.070
IT Knowledge	.282	.398	.500	1	.479	1.325
Confidence	-.002	.023	.011	1	.917	.998
Neuroticism	.017	.054	.105	1	.746	1.018
Constant	-2.382	2.598	.840	1	.359	.092

6.4.2.2 Ascertaining the Impact of Gender, IT Knowledge, Confidence and Neuroticism on the Detection of a Malicious .Exe Pop-Up

A binomial logistic regression was performed to explore the effects of gender, IT knowledge, confidence in their decision as to whether there was an attack, and neuroticism on the likelihood that participants would detect a malicious .exe pop-up. The logistic regression model was statistically significant $X^2(4)$= 9.808, p=.044. The model explained 24.8% (Nagelkerke R^2) of the variance in the detection of phishing emails (see Figure 6.7).

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	43.346[a]	.134	.248

a. Estimation terminated at iteration number 6 because parameter estimates changed by less than .001.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	9.808	4	.044
	Block	9.808	4	.044
	Model	9.808	4	.044

Figure 6.7: Outputs of the Binomial Regression Analysis for Detecting an .Exe Pop-Up

The model correctly classified 88.2% of cases. Sensitivity or true positives (the percentage of cases where the model correctly identified that a participant would detect the attack) was 22.2%. Specificity or true negatives (the number of individuals who didn't detect the phishing email and who were predicted to not detect the attack) was 98.3% (see Appendix G).

Positive predictive value (the number of predicted detections of phishing emails that were correct) was 66.7% and the negative predictive value was 89.2%. Of the four predictor variables only one was statistically significant: IT Knowledge (as shown in Table 6.3). For each level of increase in how high someone rated their IT knowledge there, was a 3.800 odds increase in the participant correctly labelling a malicious .exe pop-up.

Table 6.3: Logistic Regression Predicting the Likelihood of Participants Detecting a Malicious .Exe Pop-Up Based on Gender, IT Knowledge, Confidence and Neuroticism

	B	SE	Wald	df	p	Odds Ratio
Gender	.460	1.096	.176	1	.675	1.584
IT Knowledge	1.335	.559	5.712	1	.017	3.800
Confidence	.051	.037	1.926	1	.165	1.053
Neuroticism	.086	.074	1.345	1	.246	1.090
Constant	-12.959	4.780	7.349	1	.007	.000

6.4.2.3 Ascertaining the Impact of Gender, IT Knowledge, Confidence and Neuroticism on the Detection of a Webcam Attack

A binomial logistic regression was performed to explore the effects of gender, IT knowledge, confidence in their decision as to whether their was an attack and neuroticism on the likelihood that participants would detect a webcam attack. The logistic regression model was statistically significant $X^2(4)$= 10.613, p=.031. The model explained 40.1% (Nagelkerke R^2) of the variance in the detection of webcam attacks (see Figure 6.8).

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	19.813[a]	.145	.401

a. Estimation terminated at iteration number 20 because maximum iterations has been reached. Final solution cannot be found.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	10.613	4	.031
	Block	10.613	4	.031
	Model	10.613	4	.031

Figure 6.8: Outputs of the Binomial Regression Analysis for Detecting a Webcam Attack

The model also correctly classified 94.1% of cases. Sensitivity or true positives (the percentage of cases where the model correctly identified that a participant would detect the attack) was 25%. Specificity or true negatives (the number of individuals who didn't detect the webcam attack and who were predicted to not detect the attack) was 98.4% (see Appendix G).

Positive predictive value (the number of predicted detections of webcam attacks that were correct) was 50% and the negative predictive value was 95.5%. Of the four predictor variables only one was statistically significant: how confident the participant was that they could detect attacks (as shown in Table 6.4). This was, however, a negative relationship.

6.5 Discussion

The chapter had three purposes: i) to identify whether people are more likely to detect certain forms of attacks, in particular attacks against physical devices, ii) to look at whether individuals with certain characteristics are more likely to correctly identify these attacks, and iii) to explore

Table 6.4: Logistic Regression Predicting the Likelihood of Participants Detecting a Webcam Attack Based on Gender, IT Knowledge, Confidence and Neuroticism

	B	SE	Wald	df	p	Odds Ratio
Gender	-19.228	8203.523	.000	1	.998	.000
IT Knowledge	.247	1.029	.058	1	.810	1.281
Confidence	-.148	.064	5.309	1	.021	.862
Neuroticism	0.0965	.094	1.039	1	.308	1.101
Constant	4.981	5.363	.863	1	.353	145.659

the types of behaviours that individuals pay attention to and then deem to be potentially suspicious. The findings of this chapter suggest that some forms of attacks are more likely to be detected than others, with the attack against a physical camera especially hard to detect, and yet participants did observe other forms of potential security indicators. These insights have implications for understanding the threats to which people may be particularly vulnerable to. With regards to trying to predict whether someone will detect an attack, all of the predictive models were significant. Despite this, for each model, only one independent variable had a significant impact and this varied across attack type. The implications of these findings are discussed in more detail below.

Detecting Attacks Against Physical Devices: This thesis is particularly interested in whether people can detect attacks against physical devices, with this study exploring the detection of attacks against a webcam. This attack simulated a remote access trojan malware being used to turn on a camera (or specifically a camera LED light). The findings showed that detection for this particular attack was exceptionally low, with the same number of people viewing this as a malicious condition as for the control conditions. Worryingly more people actually viewed a control email and a safe pop-up as more suspicious than this attack. Rates of detection for this type of attack were especially low when compared to detection rates for more traditional attacks like phishing emails and malicious pop-up attacks. One possible explanation for this may be that participants are more familiar with these types of attacks and so these attacks were more likely to come to mind when primed to consider 'cyber security'. A second possible explanation is that by giving participants a task to do on the computer (personality test) this led to particular emphasis being placed on on-screen occurrences and so this should be explored further whilst participants do different activities. This seems particularly likely given that even small on-screen indicators were observed by participants.

On a positive note people did observe other visual indicators, with 62% of participants reporting that they observed a visual indicator on-screen for the mouse tracking condition. This could be due to a lack of awareness about this type of attack or could be due to people not recognising or observing LED lights. This supports findings by Portnoff et. al (2015) [209] which found that alerts presented onscreen were observed with much more frequency than webcam indicator lights. Whilst the Portnoff study used much more prominent on-screen alerts, this study

highlights that even subtle onscreen indicators may be an effective method of warning people that physical devices are currently in use. An alternative form of alert that could be used is a sound indicator, which was also observed with more frequency than the LED light and deemed as more suspicious.

Detecting Other Forms of Attack: Whilst this study was especially interested in the detection of attacks against physical components the methodology also involved looking at a range of different attacks. From exploring a multitude of attacks, we can also identify that people were poor at detecting phishing emails. Whilst the phishing email was statistically more likely to be considered malicious than the two control emails, the phishing email was still detected in less than 50% of cases (less than chance). The malicious .exe pop up, however, was detected more than half of the time (statistically more than the phishing email) highlighting that there are big differences in the detection of different attacks.

Can We Predict Individuals Who Are Better at Detecting Attacks? A key part of this study was to investigate whether gender, IT knowledge, confidence in decision regarding whether its an attack and neuroticism could be used to predict whether someone would detect an attack and whether this was the same across attacks. Whilst all of the models were significant, each model only had one significant factor and this varied across every attack. Neuroticism was never found to be significant. Whilst this study does provide some very limited support for factors such as gender, IT knowledge and confidence as relevant to detecting attacks, overall the findings show that we cannot predict who will detect an attack with any accuracy, or what factors may be predictive for that particular attack. In addition, the positive predictive values were low.

In addition this study's findings contradict earlier findings with a negative relationship between confidence and detection of webcam attacks.

6.6 Interim Conclusions

Chapters 4 and 5 explored how people protect their cyber devices from attacks. This chapter expanded on these earlier chapters, by looking at whether people can detect different attacks and draws the following conclusions:

- Firstly, some forms of attack are more likely to be detected than others. This suggests that just as there are differences in levels of awareness of different attacks, people have differing levels of awareness about how an attack may manifest. In particular attacks such as phishing emails and malicious .exe pop-ups were both statistically more likely to be considered cyber attacks than switching on a camera.

- Secondly, just as gender, IT knowledge and confidence in detecting attacks were all found to be statistically related to a greater awareness of different attacks and using more security measures they were also found to be related to the ability to detect attacks. Despite this

the attack each variable predicted varied, suggesting this is not a simple relationship and that findings are not generalisable across different types of attacks.

– Thirdly, this chapter has identified that different types of indicators may be more likely to be noticed and therefore may be more appropriate to be used as warnings. In particular on-screen or audio indicators were more likely to be observed than an off-screen LED suggesting that these may be more effective as security alerts.

– Fourthly, building on previous research into personality, this chapter explored whether neuroticism could also predict a person's ability to detect different attacks, finding no significance.

Part III

Cyber-Physical Systems Within Industry

CHAPTER 7

CPS IN INDUSTRY- DETECTION OF ATTACKS IN AN ICS TESTBED

Cyber threats against large scale industrial systems are increasing and have the potential for severe consequences, yet the majority of work on how to detect these attacks has focused on technology and neglected to consider the individuals who work alongside these systems. Due to the challenges of recruiting industry professionals and using real industry systems this study used a simplified water distribution plant testbed and novice users who were given instructions on how to use this simplified system. The study then investigated the extent to which these individuals could identify a range of attacks that produced physical malfunctions against the system. In total each individual was exposed to four attacks against the testbed system and one additional attack against a laptop, which was included as a control to explore whether familiarity had a large impact on detection of attacks. The results found that 74% of individuals identified at least one attack and 70% identified at least one attack against the ICS. However, no individuals identified more than three out of the five attacks. The work also identified that some attacks, such as Denial of Service attacks, were more likely to be identified than others such as replay attacks, however in the majority of cases participants attributed any malfunction to technical failure rather than malicious interference.

7.1 Introduction

Whilst attacks against ICS are not common, there are increasing numbers of examples of where these systems have been adversely affected by attacks. Large scale targeted attacks have included the Stuxnet virus which targeted nuclear facilities in Iran, and the 2015 and 2016 attacks against Ukranian power plants where attackers used malware to gain remote access to machines controlling the circuit breakers. Whilst both of these were malicious attacks targeted

directly at ICS, the Slammer worm highlights that non-targeted attacks that gain access to SCADA system can have negative consequences. An example of this being the Davis-Besse plant which reported that the Slammer worm resulted in slowing down the plant network and crashing a computerised display panel which monitored the crucial safety indicators including temperature and radiation sensors [3].

These attacks have highlighted the need to maintain cyber security within these systems. However, whilst a range of technologies exist to help protect these systems and to aid in the detection of malicious activities, the human operators have been comparatively under studied. No matter how much cyber security is automated there will always be a human in the loop at some point in the process, whether this is the human decision maker engaged in intrusion detection, the security system administrator who sets up the network and various security measures such as firewalls or the software engineer who designs the automated programs. However, for an attack to have been successful it needs to have evaded these technical measures. This work, therefore, investigates whether individuals asked to monitor an ICS testbed, in this case the Security Lancaster waterplant testbed, can aid in detecting or mitigating a cyber attack. This could be beneficial because operators have both a a good understanding of the system‘s capabilities and may be the first to notice any disruption that may result from it which would mean that they could potentially act as a final line of defence. Anecdotal evidence to support this idea comes from informal reports that a system controller observed the cursor on his screen being remotely operated right before the Ukraine power grid hack in 2015 [2].

7.1.1 Contributions and Key Findings

The novel contributions of this work are as follows:

- Provides evidence that individuals who work with ICS are able to observe system failures that may result from a cyber attack.
- Identifies that some forms of attacks are more visible to system operators than others.
- Demonstrates that whilst system failures from a cyber attack may be identified, the error is frequently attributed to technical error rather malicious interference.
- Concludes that individual differences such as personality and gender are not related to the ability to detect cyber attacks against an ICS.

7.2 Related Work

7.2.1 Expert Detection in ICS

Work looking at humans in the security context of ICS has often focused on security professionals whose job it is to prevent unwanted network incursions. This has included work utilising a

simplified Intrusion Detection System (IDS) which was given to both students and security professionals. These participants were then asked to monitor the alerts from the IDS and seek to identify whether these alerts represented a cyber attack. Whilst they found no differences between the experts and novices when the participants were looking at an entire sequence of events (such as whole attack process), when looking at the individual alerts the experts were able to detect a significantly greater proportion of the malicious events, whilst also reporting fewer false positives. The study suggested that whilst security expertise was undeniably beneficial to the detection of malicious events, knowledge of the system also aided the detection of network intrusions [231].

Supporting the notion that knowledge of the system, and the environment in which it is located, is essential for individuals to be involved in maintaining its security is work by Goodall [232]. This research involved interviewing nine individuals whose roles involved intrusion detection. It was concluded that understanding the 'normal' for a system can help security experts to identify alerts that simply represent normal traffic in one system, but which would be of concern in another system, emphasising the importance of situated knowledge.

7.2.2 Operator Responses to Cyber Attacks

Given that situational knowledge is so important in identifying when a system is behaving abnormally, and that there will always be the possibility of zero day attacks or those that are simply able to evade a systems defences, work is starting to consider whether the operators of cyber-physical systems would be able to identify an attack. This is a key topic for several reasons. Firstly the operators who work directly with the system are in a key position to identify abnormal behaviour. Being aware of the possibility that these systems could be targeted in this manner could enable the the operators to act as a final line of defence. Taking the anecdotal example of the cursor being remotely controlled in the Ukraine attacks, such behaviour from system could be readily identified as malicious, yet whether the individual involved would have any way of reporting such behaviour to the people best placed to respond to the attack would vary dependent on the organisation, its policies and training. Secondly, regardless of whether the operator can detect an attack, it is likely to have a physical consequence which the operator is likely to have to address. Understanding how operators seek to mitigate the impact of an attack or how an attack impacts on their workload and task performance could still be beneficial to organisations as they seek to determine the costs and benefits of investing in different levels of cyber security.

These ideas have started to be picked up, with researchers exploring them within the context of the transport industry. The European Aviation Safety Agency explored the effects of six attacks against aircraft navigation and flight management systems. The results from exploring these attacks found that three of the attacks, updating a flight plan, a DoS attack and hacking a database to change the threshold height of the landing approach were more likely to be observed than the rest of the attacks

A second piece of work looking to understand what happens when technical countermeasures to a cyber attack fail in a transportation network was conducted by Millot et al. (2018) looking at train and tram networks. Focusing on how an attack can impact on an operator's situational awareness, their study involved placing human drivers in a simulator and observing how they respond when different cyber attacks were introduced. Since the work looked to identify and explore realistic cyber attacks only two of the tested situations are discussed due to confidentiality reasons. These scenarios, used with six drivers, were a simulated loss of control over the rear vision of a tram with the second involving a loss of the tram's breaking system. From running these simulations, the researchers concluded that the operator's ability to detect a malfunction depended on the situation. However, they also proposed that new tools could be developed to aid in fault detection as well as a signal that could alert human drivers should an attack be detected so that they could increase vigilance if necessary [213].

These two studies are very specific instances of attacks, and were explored with only a small number of individuals but they do highlight the need to explore how an attack influences the individuals working with the targeted systems. This work therefore seeks to expand on the work by exploring whether people can detect a variety of different forms of attack on an ICS.

7.3 Methodology

To investigate whether individuals could detect malicious interference on a CPS a simulation study was conducted on the Security Lancaster water plant (Figure 7.1). Inside the testbed there are two water tanks with water pumping between the two of them in a cycle. Participants were then asked to monitor the water levels on one of the water tanks. This could be done via the Human Machine Interface (HMI) screen (screen in left of image) which was placed in front of them on a desk, or by physically getting up and checking on the water tanks directly. During the simulation participants were also asked to respond to any emails that came in on a laptop that was also placed on the desk. Throughout the simulation all participants were exposed to five cyber attacks, four on the testbed and one on the laptop.

7.3.1 Recruitment

This study was approved by the Lancaster Research Ethics Committee (the ethics forms can be seen Appendix H) and all participants consented to their data being used in this study.

This study was run from September to December 2017, with participants offered £6 for their participation. In total fifty students were recruited from around a UK university campus, however three individuals were excluded. The first two participants were excluded because two of the simulated attacks involve pumps and they therefore went from producing noise to complete silence. Since in real life the operator would likely not be in such proximity to all of the system components, the following experimental sessions were run with an audio recording of

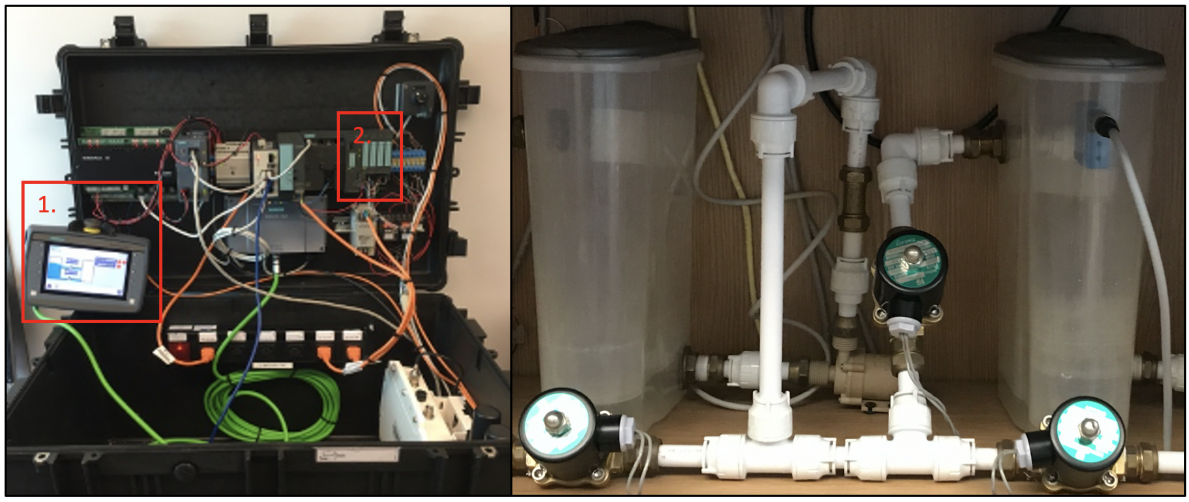


Figure 7.1: Diagram of the Portable Security Lancaster Water Distribution Plant Testbed and Water Tank Set Up. 1. Human Machine Interface, 2. Programmable Logic Controllers

Table 7.1: Demographic Breakdown of Participants

		Male	**Female**	**Total**
Age	18-21	11 (23%)	22 (47%)	33 (70%)
	22-25	2 (4%)	6 (13%)	8 (17%)
	26-30	1 (2%)	2 (4%)	3 (6%)
	31-35	2 (4%)	0 (0%)	2 (4%)
	46-50	0 (0%)	1 (2%)	1 (2%)
	Total	16 (34%)	31 (66%)	47 (100%)
Security Knowledge	Very Low	2 (4%)	6 (13%)	8 (17%)
	Low	6 (13%)	21 (45%)	27 (57%)
	Moderate	6 (13%)	2 (4%)	8 (17%)
	High	2 (4%)	2 (4%)	4 (9%)
	Total	16 (34%)	31 (66%)	47 (100%)

the simulation, so whilst a difference in noise was evident it wasn't so explicitly obvious unless the participants were paying particular attention. A third participant was excluded because the software controlling the webcam crashed and came up with a warning that was visible to the participant.

Table 7.1 shows the demographic information of the 47 participants who were involved in the final analysis.

7.3.2 Procedure

Participants who consented to take part in the experiment were given an introduction to the system where they were shown how the system was working and where to read the water levels using either the HMI or from the water tanks directly. A simplified diagram of the study setup

and different attacks can be seen in Figure 7.2.

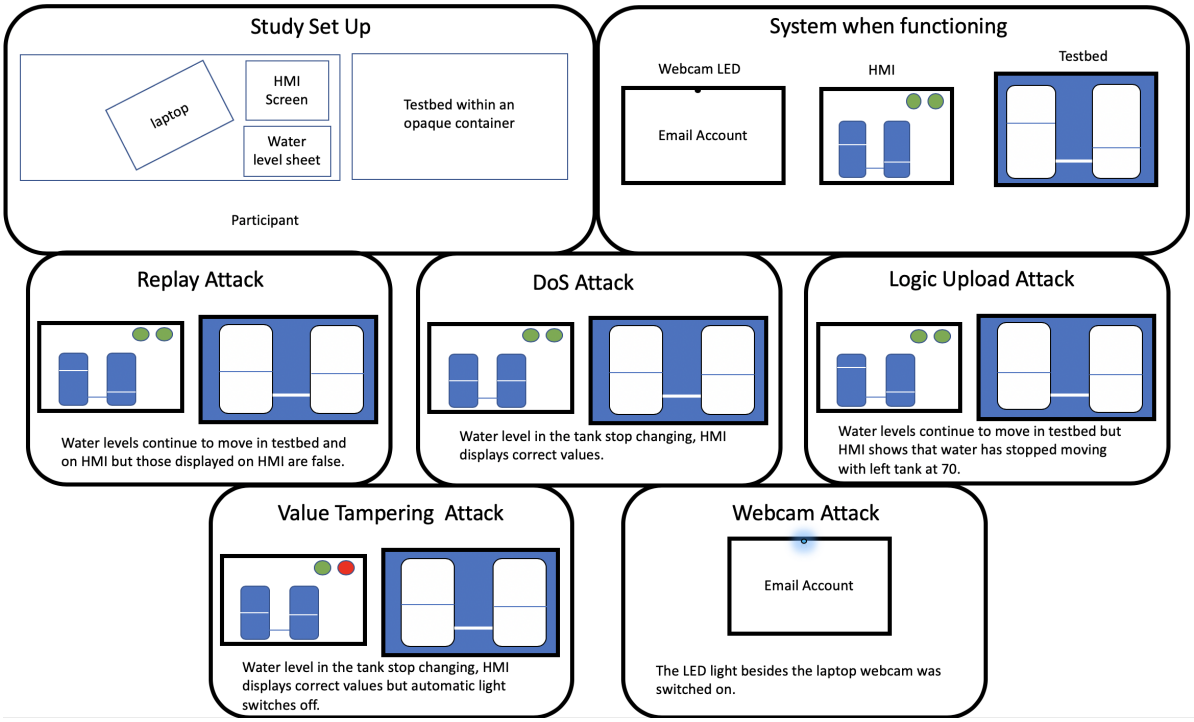


Figure 7.2: Simplified Diagram of the Study Set Up and Each of the Individual Attacks.

Once they were familiar with the system, participants were told that they were to play the role of the system operator, to monitor the water levels of the containers and report these by writing down the levels of the left-hand tank every 30 seconds (they were given a digital clock to aid in this task). Only one tank needed to be observed due to this being a closed system with water being pumped between the two tanks and so as levels rose in one tank they decreased in the other. Additionally participants were asked to respond to any emails that came through on a laptop placed besides the HMI. In a real world environment most control room operators would receive information from various field sites or parts of the system but not have direct line of sight over the whole system. Therefore, in this set up, participants were given easy access to a HMI but were required to get up if they wished to see the actual water levels directly, with the water tanks placed approximately 1.5m away from the HMI and laptop. Despite this 13 (28%) individuals got up to inspect the tanks at some point with two of these individuals doing so for approximately half of the experiment time. During the study a recording of the pumps at work was also played to muffle the sound abruptly stopping during the DoS attack as were interested in their observations of the system and HMI rather than their ability to detect changes in sound.

For the first eight minutes the system then behaved as it was supposed to, giving participants time to familiarise themselves with how the system performs when running correctly and they also received the first of the two task emails to allow them to understand the sort of questions

they would be asked. At eight minutes the first attack was run (each attack lasted forty seconds) against the testbed system. To prevent learning or fatigue effects the order of the four ICS attacks was counterbalanced (varied across participants to control for order effects) with the remaining three system attacks occurring at minutes 12, 14 and 18. Finally the webcam light was switched on at minute twenty. The webcam attack always occurred last as its purpose was to explore whether the participants could identify an attack against a system with which they were more familiar, and so we wished to ensure that the webcam did not prime participants as to the real nature of the study. In total the simulation lasted for 22 minutes. The different attacks are presented below and the order in which they were presented can be seen in Table 7.2 and these used scripts modified for use in this study by another PhD student within the Lancaster computer science department.

- **Replay Attack:** The Programmable Logic Controller (PLC) sends false values back to the HMI but these are based on previous values making them appear realistic. This attack therefore resulted in HMI values that appeared to jump up. They then followed the same pattern of always increasing and decreasing, however, they always reached peak and minimum values, unlike when it was working normally.

- **Denial of Service (DoS) attack:** This attack caused the PLC to crash, resulting in the water pump to stop working meaning that the water levels on the HMI would stop moving.

- **Logic Upload Attack:** This attack caused the logic on the PLC to spoof values back to the HMI. Whilst the pump continued to work and the water levels continued to rise and fall as normal the HMI showed that water level was holding at 70.

- **Value Tampering Attack:** This attack directly overwrote the PLC process causing it to hold the water levels static, so similar to the DoS attack the water levels in the tank and the HMI stopped moving, although the pump still worked at holding the levels steady. However, this attack also switched off the automatic mode lights on the HMI screen.

- **Webcam attack:** The webcam on the laptop was switched on (meaning the webcam light was also switched on).

Table 7.2: Counterbalancing of Attacks

	3 Mins	**8 Mins**	**12 Mins**	**13 Mins**	**14 Mins**	**18 Mins**	**20 Mins**
1	Email Request 1	Replay Attack	Logic Upload	Email Request 2	Value Tampering Script	Denial of Service Attack	Webcam Attack
2	Email Request 1	Logic Upload	Denial of Service Attack	Email Request 2	Replay Attack	Value Tampering Script	Webcam Attack
3	Email Request 1	Denial of Service Attack	Value Tampering Script	Email Request 2	Logic Upload	Replay Attack	Webcam Attack
4	Email Request 1	Value Tampering Script	Replay Attack	Email Request 2	Denial of Service Attack	Logic Upload	Webcam Attack

During the simulation, participants were given a sheet to record the water levels at each thirty second point, this sheet also provided a space where they could record any notes or issues. To identify whether participants identified the different attacks these sheets were consulted to see if they recorded any issues. In addition, following the simulation a small debriefing interview was conducted where individuals were asked whether they had any issues during the simulation, and if so to describe these. In addition to asking whether they identified any attacks, participants were asked to identify who they thought they would contact if this happened in a real world setting to explore where they were most likely to attribute the blame for any errors. Finally participants were given an online questionnaire with demographic and personality questions.

Using this methodology the following research questions are then explored:

1. Do people detect different attacks against an ICS system?
2. What level of variance in detection of attacks can be explained by looking at participant's demographic factors?
3. Where do individuals attribute blame for system errors?

7.3.3 Threats to Validity

This work was an exploratory study to provide a novel look at whether individuals could detect an attack against an ICS. It does have some limitations that should be addressed in future studies. Firstly the sample used in this study was composed of novices rather than individuals who are familiar with working with ICS. Therefore, the results may be reflective of new starters but may not apply to experts with years of experience. Additionally the sample consisted largely of young females which may have affected the analyses. This is particularly the case for gender where the Mann Whitney U test approached significance ($p = .061$). Future research may wish to explore this further. Difficulties in recruiting individuals with more security knowledge prevented the impact of security and IT knowledge on detection of attacks to be explored, and this may explain some of the difference between males and females.

Secondly, in order to prevent priming, participants could not be interrogated regarding whether they detected attacks throughout the study which meant that in six cases it was not clear exactly which attack was detected and so some of the data has had to be excluded.

Thirdly, the study used a simplified ICS, with the tasks involved not representative of the full range of activities that operators would usually be conducting. Therefore in more complex systems where cognitive load will be higher, detection rates may be even lower.

7.4 Results

This section presents the results of the three different research questions that were explored within this work. Full details of the statistical tests that were conducted can be found in Appendix

I.

7.4.1 Do people Detect Different Attacks Against an ICS?

Fig 7.3 shows the percentage of people who detected each of the different attacks. In six instances (13%), participants detected suspicious behaviour but were unsure at what time in the simulation this occurred and the possible attacks that they could relate to are represented by the error bars. From this figure it is possible to identify that some attacks were more likely to be detected than others with the DoS attack the most likely to be detected, while the replay attack, and, attacks against the webcam were the least likely to be detected.

In total 14 (30%) of participants failed to identify any of the attacks against the ICS, meaning that 70% were able to identify at least one attack. However, no single individual identified more than three of the four ICS attacks. In total three individuals identified the webcam attack against the laptop and two of these consisted of people who did not identify any of the ICS attacks. In total only 12 individuals (26%) did not identify any of the five attacks.

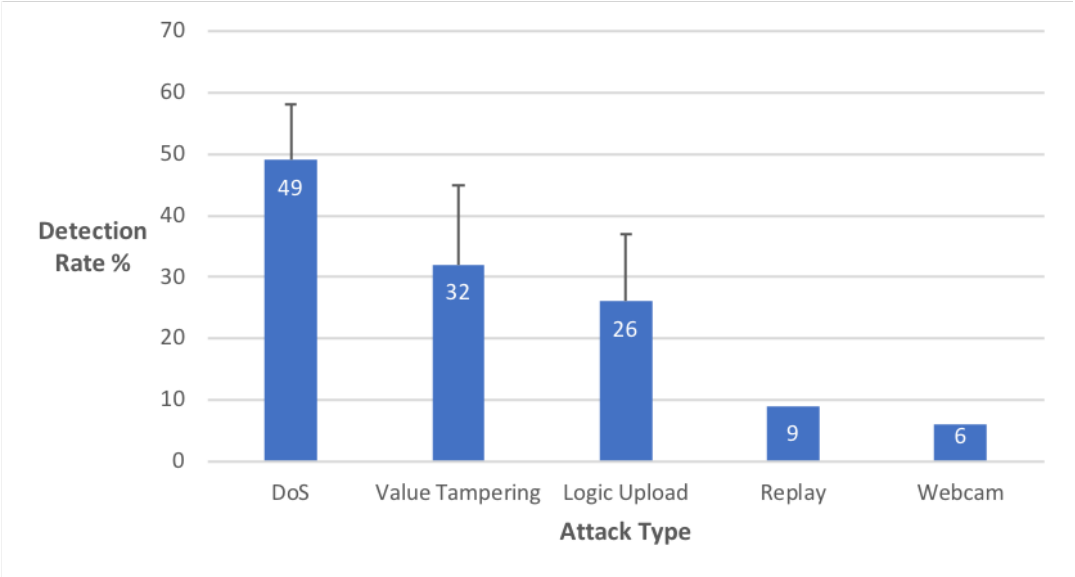


Figure 7.3: The Proportion of Individuals Who Detected Each Type of Attack. Error Bars Represent Maximum Possible Levels of Detection Where There is Uncertainty Regarding Which Attack was Identified

To investigate whether these findings are significant a Cochrans Q test was run. This test is suitable to use here as it is intended to be used with dichotomous variables and when participants have undergone multiple different trials. It involves looking at whether the number of people identifying an attack is the same between the different types of attacks. Instances where an attack was observed but the specific attack scenario could not be identified were removed from the analysis. The results of this test revealed that number of participants detecting attacks was

statistically significant across the different attack scenarios, $X^2(4)= 34.247$, p <.0001 (see Figure 7.4).

Test Statistics

N	41
Cochran's Q	34.247[a]
df	4
Asymp. Sig.	.000

a. 1 is treated as a success.

Figure 7.4: Outputs of the Cochrane Q Test Exploring Detection of Attacks Against an ICS

To explore this result in more detail, pairwise comparisons were performed using Dunn's post hoc analysis. This follow up procedure looks at all the individuals variables and compares them to each other. Adjusted p values using Bonferroni's correction were then used to account for the multiple comparisons. The results showed that the number of participants detecting the DoS attack (53.7%) was statistically significant compared to the number who identified the logic upload attack (26.8% detected) p= .040; replay attack (9.8% detected) p<.001 and the webcam attack (7.3% detected) p<0.001. There was also a statistical difference in the number of people detecting the value tampering and replay attacks p= 0.4 and between the number detecting the value tampering and webcam attacks p= .017 (see Figure 7.5).

7.4.2 What Level of Variance in Detection of Attacks Can Be Explained by Looking at Participant's Demographic Factors?

To explore whether we could predict who would be able to observe different attacks, and to explore whether this is the same across different types of attack, binomial logistic regression analyses were run for each of the different attacks. For each of these analyses the variables that were selected to be investigated were gender, extraversion and neuroticism. Gender was selected as a variable that previous research has been suggested plays a role in attack susceptibility. Extraversion and neuroticism were then chosen as personality traits which have shown the most consistent findings. In this study IT knowledge was excluded due to a lack of variance. The full analyses can be seen in Appendix I, Section I.2.

7.4.2.1 Predicting Who Will Observe a Logic Upload Attack:

The logistic regression model for this attack was not statistically significant, $X^2(3)= 3.171$, p=.366 and the model only explained 10.8% (Nagelkerke R^2) of the variance (see Figure 7.6). This

Pairwise Comparisons

Sample 1–Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
Webcam–Replay	–.024	.093	–.262	.794	1.000
Webcam–Logic_Upload	–.195	.093	–2.094	.036	.363
Webcam–Value_Tampering	–.293	.093	–3.141	.002	.017
Webcam–DoS	–.463	.093	–4.973	.000	.000
Replay–Logic_Upload	–.171	.093	–1.832	.067	.670
Replay–Value_Tampering	–.268	.093	–2.879	.004	.040
Replay–DoS	–.439	.093	–4.711	.000	.000
Logic_Upload–Value_Tampering	–.098	.093	–1.047	.295	1.000
Logic_Upload–DoS	.268	.093	2.879	.004	.040
Value_Tampering–DoS	.171	.093	1.832	.067	.670

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.
Asymptotic significances (2–sided tests) are displayed. The significance level is .05.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

Figure 7.5: Results of the Cochran Q Post-Hoc Tests for Detection of Attacks Against an ICS

suggests that gender, neuroticism and extraversion cannot predict who will detect a logic upload attack.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi–square	df	Sig.
Step 1	Step	3.171	3	.366
	Block	3.171	3	.366
	Model	3.171	3	.366

Model Summary

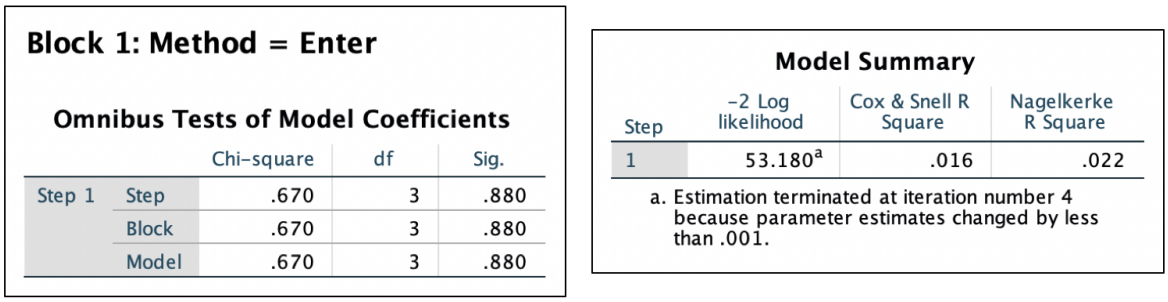
Step	–2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	44.517[a]	.074	.108

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Figure 7.6: Model Fit for Regression Analysis of Whether Individuals Detect Logic Upload Attacks

7.4.2.2 Predicting Who Will Observe a Value Tampering Attack:

The logistic regression model for this attack was not statistically significant, $X^2(3)= .670$, p=.880 and the model only explained 2.2% (Nagelkerke R^2) of the variance (see Figure 7.7). This suggests that gender, neuroticism and extraversion cannot predict who will detect a logic upload attack.



Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	.670	3	.880
	Block	.670	3	.880
	Model	.670	3	.880

Model Summary

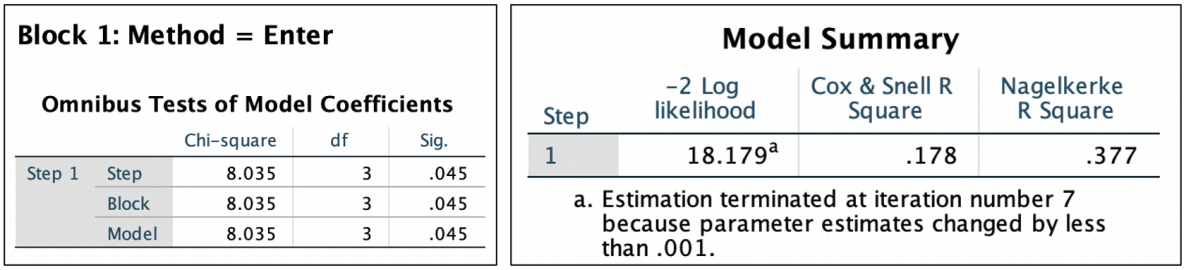
Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	53.180[a]	.016	.022

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Figure 7.7: Model Fit for Regression Analysis of Whether Individuals Detect a Values Tampering Attack

7.4.2.3 Predicting Who Will Observe a Replay Attack:

The logistic regression model for this attack was statistically significant, $X^2(3)= 8.035$, p=.045 and the model explained 37.7% (Nagelkerke R^2) of the variance (see Figure 7.8).



Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	8.035	3	.045
	Block	8.035	3	.045
	Model	8.035	3	.045

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	18.179[a]	.178	.377

a. Estimation terminated at iteration number 7 because parameter estimates changed by less than .001.

Figure 7.8: Model Fit for Regression Analysis of Whether Individuals Detect a Replay Attack

Whilst none of the individual variables was found to be significantly related to the detection of replay attacks the model correctly classified 92.7% of cases. However specificity/ true negatives was only 25% likely due to the low numbers of individuals who observed this particular attack (See Appendix I).

7.4.2.4 Predicting Who Will Observe a DoS Attack:

The logistic regression model for this attack was not statistically significant, $X^2(3)= 1.399$, p=.706 and the model only explained 4.5% (Nagelkerke R^2) of the variance (see Figure 7.9). This suggests that gender, neuroticism and extraversion cannot predict who will detect a logic upload attack.

7.4.2.5 Predicting Who Will Observe a Webcam Attack:

The logistic regression model for this attack was not statistically significant, $X^2(3)= 1.682$, p=.641 and the model only explained 9.9% (Nagelkerke R^2) of the variance (see Figure 7.10). This

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	1.399	3	.706
	Block	1.399	3	.706
	Model	1.399	3	.706

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	55.220[a]	.034	.045

a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.

Figure 7.9: Model Fit to Look at the Level of Variance Explained in Whether Individuals Detect a DoS Attack.

suggests that gender, neuroticism and extraversion cannot predict who will detect a logic upload attack.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	1.682	3	.641
	Block	1.682	3	.641
	Model	1.682	3	.641

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	19.782[a]	.040	.099

a. Estimation terminated at iteration number 6 because parameter estimates changed by less than .001.

Figure 7.10: Model Fit to Look at the Level of Variance Explained in Whether Individuals Detect an Attack Against a Webcam

7.4.2.6 Gender

A Mann-Whitney U test was run to explore in more detail if there were differences in detection of cyber attacks between males and females, due to observations from Figure 7.11 suggesting that this may be significant. However, distribution of number of observed attacks was not statistically significantly different between males and females, U = 167.5, z = -1.876, p>0.05 (see Figure 7.12).

7.4.3 Who Would Individuals Report Suspicious Behaviour Too?

Individuals who identified an attack were asked to whom they think they would report the issue to explore where they thought the error may lie. To help with this question, participants were given a list of possible contacts: peers, management, technicians, IT, security or head of department. The majority of respondents reported that they would report incidents to either technicians or management explaining that they thought they believed it was a technical issue. Additionally, many participants reported that they didn't know enough about the system and so would just go to management. Two individuals reported that they would report it to IT, highlighting that

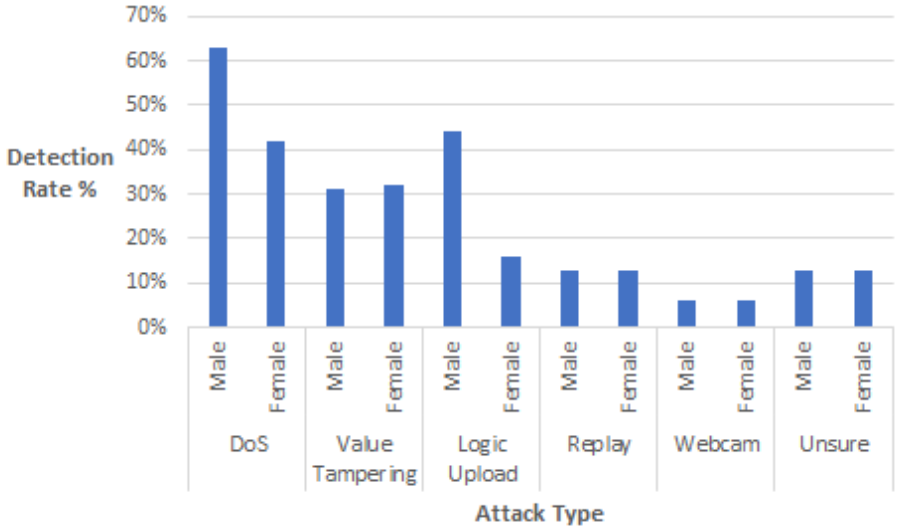


Figure 7.11: Figure Showing the Proportion of Individuals Who Detected Each Type of Attack Based on Gender

Total N	47
Mann-Whitney U	167.500
Wilcoxon W	663.500
Test Statistic	167.500
Standard Error	42.901
Standardized Test Statistic	-1.876
Asymptotic Sig. (2-sided test)	.061

Figure 7.12: Mann-Whitney U Outputs of Attack Observation Scores for Both Genders

the automation lights had switched off and that it seemed to be an issue with the HMI. Whilst one individual did ask whether the researcher was causing the issues during the simulation highlighting that they believed that the researcher was maliciously interfering with the system behaviour, this suggests that a small minority of participants had some level of awareness about possible issues in the system. However, none of the participants reported that they would have reported the issue to security, suggesting that few individuals considered that the issues were likely to pose a security threat.

7.5 Discussion

This study found that whilst individuals are poor at identifying when they have been a victim of a cyber attack, some individuals will be able to detect the abnormal behaviours that may result from such an event, with certain types of instances more likely to be identified than others. In particular incidents that cause a complete failure of a system (e.g. a DoS attack) were the most likely to be detected by participants using the system. One possible explanation for this is that the DoS attack caused the pumps to completely switch off and even with the audio recording this resulted in a noticeable change in sound and that this could have provided a noticeable clue that something was no longer running correctly. The second type of attack that was most likely to be detected was the value tampering attack. One explanation for this is that this attack not only disrupted the usual pattern of water levels changing but also caused the lights on the system to change. In fact several individuals, who did not notice the impact of this attack on the water levels instead only observed this change on the HMI. This suggests that attacks resulting in a visible change on the monitoring system may also be particularly likely to be identified by individuals who are familiar with monitoring the system. Whilst this is one possible explanation, the difference between detection of this attack compared to the logic upload attack, which only changed the water levels on the HMI was not significant, suggesting there may be another explanation for why these attacks were identified, such as that people were very quick to identify changes in the system's 'typical' behaviour.

The replay attack was the least likely to be noticed, this is perhaps unsurprising given that in this sort of attack an attacker is most likely seeking to provide plausible data in order to hide their actions. In addition the experimental study set-up meant that it may not have been obvious that that attack was repeating set values. This study does however provide further evidence to the fact that, should such an attack be successful against any technical counter measures, it will be particularly hard for novice individuals working with the system to identify that the system has been manipulated. One solution for this would be to not only protect the network but seek to ensure that the data within the system, e.g., typical readings, are encrypted. Many legacy devices and protocols often communicate in plain text and so encryption of this data would make it harder for an attacker to accurately spoof the system behaviour [14].

The webcam attack was initially added to compare how detection of attacks varied with familiarity with different systems, yet very few individuals (three (6%)) noticed this despite the camera turning on for a minute. This is perhaps due to the fact that the most attention was paid to the main task. Whilst not the main interest of this study, the fact that people are exceptionally poor at detecting when a camera in close proximity to them is turned on even when they are given visual cues highlights that people may be vulnerable to Remote Access Trojans attacks like this one. This finding supports earlier work by [209] who also found that detection of webcam lights was poor with 45% of participants noticing it when performing tasks on the computer and only 5% spotting it when performing paper-based tasks besides the computer. It also supports

the findings of Chapter 6. Given that many new computer devices often incorporate cameras, this finding has potential implications for people both in their home and work environments.

Whilst previous work into certain types of cyber attacks has suggested that some types of people may be more susceptible than others, with males found to be less likely to fall for phishing emails or malicious pages [144, 152, 153, 159] the evidence is equivocal. This particular research supports work that suggests that individual differences such as gender and age do not impact on susceptibility [155–158].

7.6 Interim Conclusions

To the author's knowledge this is the first work to look at human detection of cyber-attacks within a water plant environment and the work draws several key conclusions.

Firstly 74% of participants identified at least one of the five attacks and 70% identified at least one of the attacks against the ICS, suggesting that in some instances human operators may be able to provide a source of information against any attacks in the instance that they successfully bypass technical defences.

Secondly, there were statistical differences in the number of people who detected different forms of cyber attacks, suggesting that some forms of disruption may be more obvious than others. This supports findings from Part II suggesting that some types of system abnormalities are more observable both on home systems and industrial systems, and both when participants have, and haven't, been primed to consider security.

Thirdly, whilst people may detect issues that could result from a cyber attack these events are often attributed to technical failures, with only a small minority able to identify that the behaviours may be the result of malicious interference.

Finally, the outputs of this analysis revealed that factors such as personality and gender are not significantly related to the ability (or inability) to detect different forms of cyber attack. Again, this generally supports the findings from Part II that these variables are not consistently able to predict an individual's ability to actually detect different forms of cyber attacks.

This work is the first step towards providing evidence for the fact that people working in close proximity to an ICS are able to detect when these systems malfunction in a manner that might result from a cyber attack. Further it identifies that attacks are not equal and that some may in fact may be more likely than others to be noticed.

CHAPTER 8

CPS IN INDUSTRY- DETECTION OF ATTACKS FROM SYSTEM DATA

Chapter 7 identified that individuals can observe several different forms of attack against a CPS when given a task observing the actual physical system. However, whilst the attack scenarios were frequently observed they were commonly attributed to system errors. This study seeks to expand on this earlier work in two ways. Firstly, by exploring whether individual can detect attacks from the data outputs of a waterplant, this will allow exploration of whether individuals in a system operator role can detect a range of different attacks based on SCADA data. In particular whether a replay attack, which was often unobserved from watching the system directly, is more observable from looking at the data outputs from the system. Secondly, this study will also expand on Chapter 7 by looking at the impact of priming participants to consider security risks, to explore whether primed and unprimed individuals can correctly attribute the cause of an incident to a cyber attack.

8.1 Introduction

Attacks against an ICS can have a wide range of impacts against various parts of the system. It is, therefore, important to consider that different roles may have different information on which to base decisions. This chapter, therefore, serves as a follow on to Chapter 7. Whilst Chapter 7 explored whether attacks could potentially be observed by technicians working with the physical system, this chapter focuses on whether an attack could be observed by system operators observing SCADA system outputs. This allowed exploration of whether individuals in different roles may be best placed to identify attacks, whilst also exploring whether findings on individual differences and attack detection are generalisable across different contexts.

This study was also particularly interested in exploring whether individuals could observe a

replay attack. This attack involves repeating realistic but false values into a system in order to hide changes that an attacker may be causing. This attack appeared to be the hardest to detect when observing the physical system in Chapter 7. However, given that humans are typically skilled in pattern recognition, it was considered that this attack may be more observable when monitoring the system using numeric outputs.

8.1.1 Contributions and Key Findings

The novel contributions of this study are:

- An exploration of whether system operators can observe three different types of attacks (replay, Man in the Middle and DoS attack[1]) against a waterplant testbed SCADA system;
- An exploration of the effects of priming to consider security attacks, on whether participants could observe different attacks in an industrial setting;
- An exploration of whether knowing that there might be a cyber attack has an impact on a participant's workload when monitoring an ICS.

8.2 Related Work

Research has increasingly begun to study the effects of cyber attacks against ICS, with particular interest around the impact of attacks against the transportation industry. One study by the European Aviation Safety Agency [212] explored detection of 6 different types attacks, concluding that three of the six were commonly detected. A similar conclusion was drawn by [213] who found that train and tram drivers could detect some forms of attacks but not others.

Additionally, previous research has considered the other impacts of a cyber attack against large scale physical systems, exploring factors such as whether an attack can influence behaviour, workload or trust and confidence within the system [194, 210]. The findings from these studies suggest that experiencing an attack increases an individual's workload, however simply informing individuals (in this case pilots) that there may be a cyber attack did not result in a workload increase if there was no cyber attack. An attack was also found to lead to changes in behaviour and poorer task performance, reduced trust in the system and reduced confidence that they were making the right decision.

These studies were however conducted within the transport industry. To the best of our knowledge there has been no studies specifically looking at critical national infrastructure. This study therefore seeks to address this gap by exploring detection of and impacts on workload of a cyber attack in a waterplant.

[1]This study only used three attacks instead of the four in Chapter 7 as false values would appear the same on a SCADA system regardless of whether the water levels were moving or not.

8.3 Methodology

This study took an experimental approach, with participants asked to monitor and control a simplified SCADA system, observing the water pressure within the system and opening a pump whenever this became too high. Throughout the study the participants were then exposed to three different cyber attacks, whilst half of the participants were primed to consider cyber security the other participants were simply asked to be alert to any potential issues.

8.3.1 Ethical Considerations

This research was approved by the University of Bristol's Faculty of Engineering Research Ethics Committee. All participants then volunteered to take part and gave consent prior to the study beginning. All participants were properly debriefed, especially those who had not been informed regarding the security aspect of the research, and given the opportunity to ask any questions. The ethics form can be seen in Appendix J.

8.3.2 Recruitment

This study was advertised on Bristol university campus using posters and across social media. Participants were recruited from July- November 2019 and offered £3.50 for taking part. In total 50 individuals took part in this study and the full demographic breakdown can be seen in Table 8.1. Participants ranged from 18-63 years old with 62% female and 64% students.

Table 8.1: Demographic Breakdown of Participants in Chapter 8

		Security Condition			**Control Condition**			**All**
		Male	**Female**	**Total**	**Male**	**Female**	**Total**	**Total**
	Total	**8**	**17**	**25**	**11**	**14**	**25**	**50**
Age	18-21	2	1	**3**	4	4	**8**	**11**
	22-25	1	9	**10**	4	3	**7**	**17**
	26-30	3	4	**7**	2	2	**4**	**11**
	31-35	1	2	**3**	0	4	**4**	**7**
	36-40	1	0	**1**	0	1	**1**	**2**
	41-45	0	1	**1**	0	0	**0**	**1**
	60+	0	0	**0**	1	0	**1**	**1**
Student?	Yes	4	10	**14**	9	9	**18**	**32**
	No	4	6	**10**	2	5	**7**	**17**
	Unknown	0	1	**1**	0	0	**0**	**1**
IT Knowledge	Very Low	0	2	**2**	0	0	**0**	**2**
	Low	0	3	**3**	0	1	**1**	**4**
	Moderate	3	9	**12**	7	12	**19**	**31**
	High	2	3	**5**	2	1	**3**	**8**
	Very High	3	0	**3**	2	0	**2**	**5**

8.3.3 Procedure

All participants who volunteered to take part in this study were invited to attend a lab session where they were given the full instructions of the study and asked for their consent to take part. If participants agreed to take part they they were either assigned to the security group or assigned to the control condition where they were told that the study was looking at safety within ICS.

Participants were then seated in front of a computer with two screens, a mouse and keyboard. The first screen involved a simulation of a SCADA system that was made using PsychoPy3 (images based off of OpenScada software). Figure 8.1 shows what this simulation looked liked. Every two seconds the software presented a new image, which would have a new top line in the values table showing the new time and water pressure value. The second screen was then an empty email inbox, and they were informed that they would receive emails related to the system throughout the study.

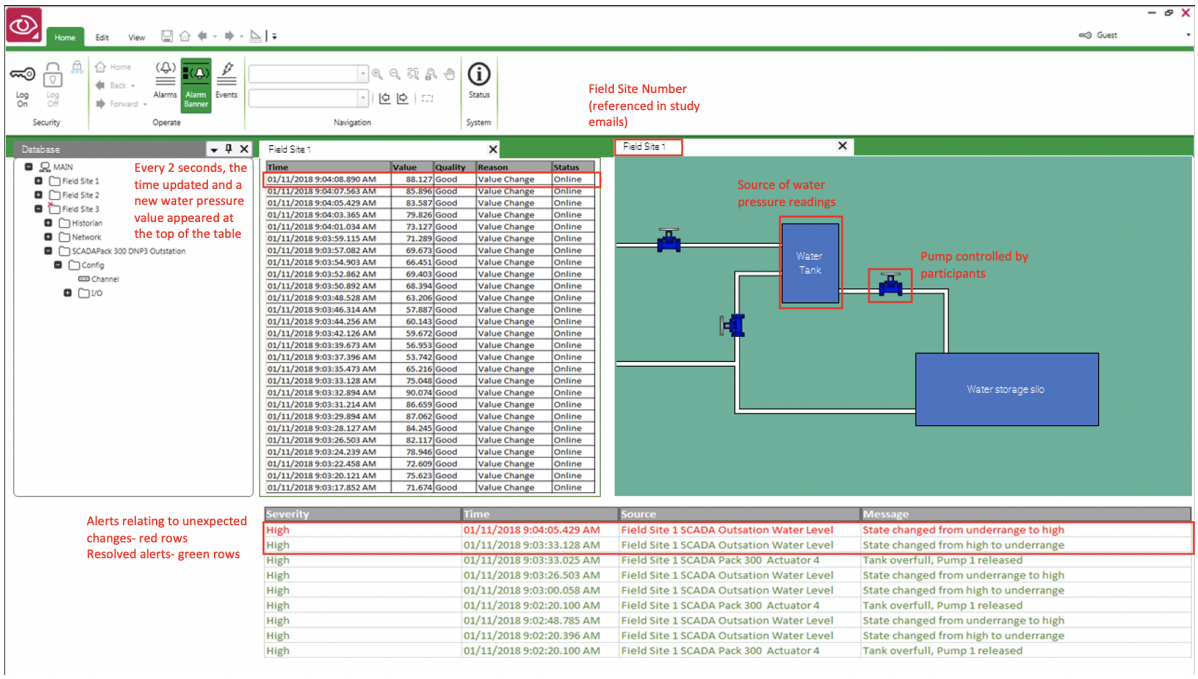


Figure 8.1: Labelled Example of the Study Screen

Prior to the study starting, participants were shown the system, and given the instructions both on paper and on screen (The on-screen instructions can be seen in Figure 8.2). They were then shown a short 10 second clip of the simulation so that they could see what this would look like to help put the instructions into context. Participants were then given the opportunity to ask any questions or to see the simulation again. If they were happy then they could press the space bar to begin.

Once the study started it would automatically present a new image every two seconds and at

approximately every 30-40 seconds the water pressure would go above 80. When this occurred participants were asked to press either the 'p' or 'space' button on the keyboard to simulate opening a pump in order for the water pressure to go down (if participants did not open the pump within 10 seconds then the simulation would automatically open it in order for the simulation to progress). Every time they opened the pump participants were asked to record their workload using the Bedford workload scale[2]. At the end of the study participants were given a questionnaire that covered demographics and the big 5 personality questionnaire.

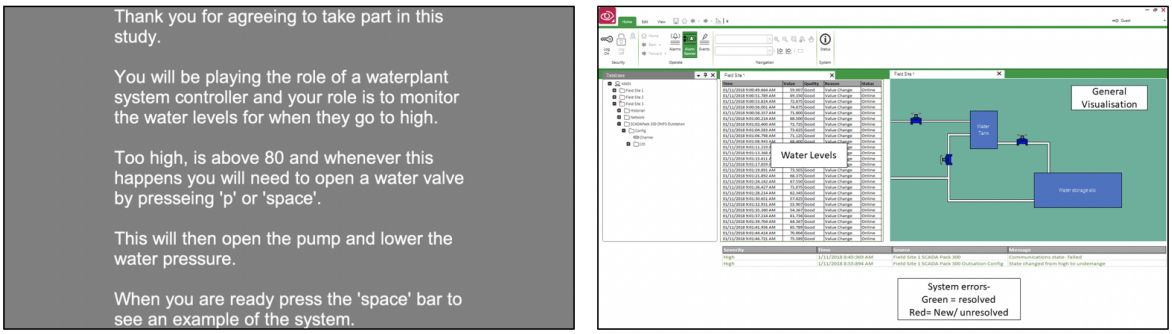


Figure 8.2: Demonstration of Study Instructions

Throughout the study participants were presented with three cyber attacks:

- **Replay Attack:** In this attack thirty seconds worth of values were repeated three times, although the time stamps continued to change as expected (see Figure 8.3, which shows these values being repeated). Such exact repetition of values would be exceptionally unlikely and could suggest that an attacker is sending 'spoof" realistic values to the system. This attack was of particular interest as it was especially hard for participants to identify in Chapter 7.

- **Man in the Middle Attack:** Over a period of a couple of minutes water levels reached above eighty (high water pressure) more frequently. At the same time participants also received emails stating that water pressure within the local infrastructure is decreasing and was too low, to see if people recognised the discordance between the two information sources (see Figure 8.4 which shows the emails).

- **DoS Attack:** Participants received a warning in the simulation stating that there was a PLC communication state failure, the next two times they tried to open the pump this then failed until the communication failure error was resolved (see Figure 8.5).

[2]This is a mental workload scale that is measured from 1 (low)- 10 (high) and has previously been used within the aviation industry.

Participants were asked to record any unusual system behaviours, with the security group also asked to record whether or not they believed that the incident could be the result of a cyber attack.

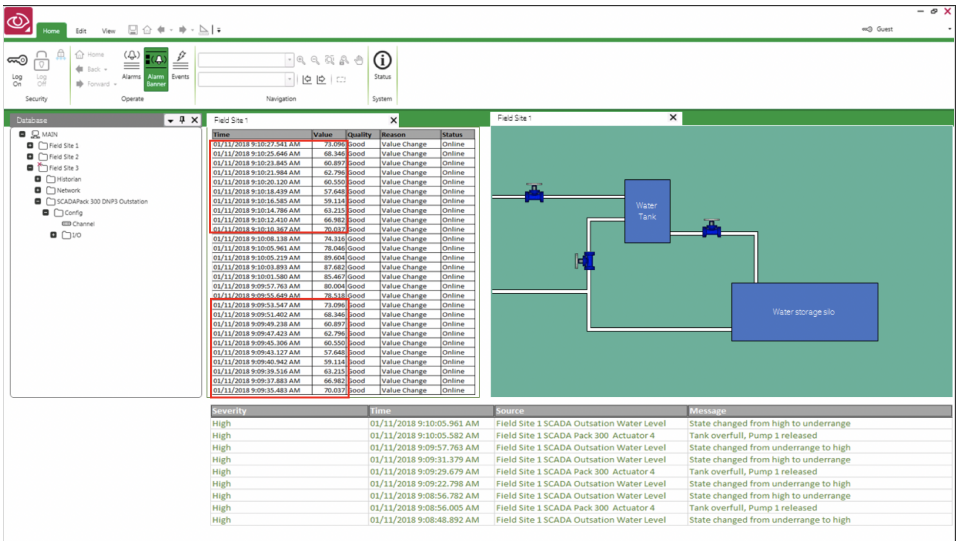


Figure 8.3: Image of the Replay Attack, Highlighting That the Water Pressure Levels are Being Repeated

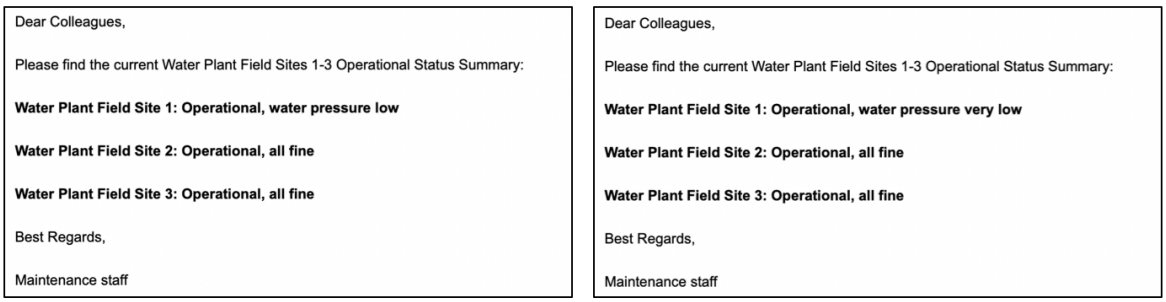


Figure 8.4: Image of the Emails Sent as Part of the Man in the Middle Attack

8.3.4 Analysis

Several statistical analyses were run as part of this study. These included a Cochrans Q test to see if some forms of attack are easier to observe than others. Chi-square tests to explore the effects of priming on observing attacks, a Mann-Whitney U test to explore the effects of priming on workload and binomial logistic regression analyses to explore the impacts of individual differences on the ability to observe different attacks. The full details of these analyses can be seen in Appendix K.

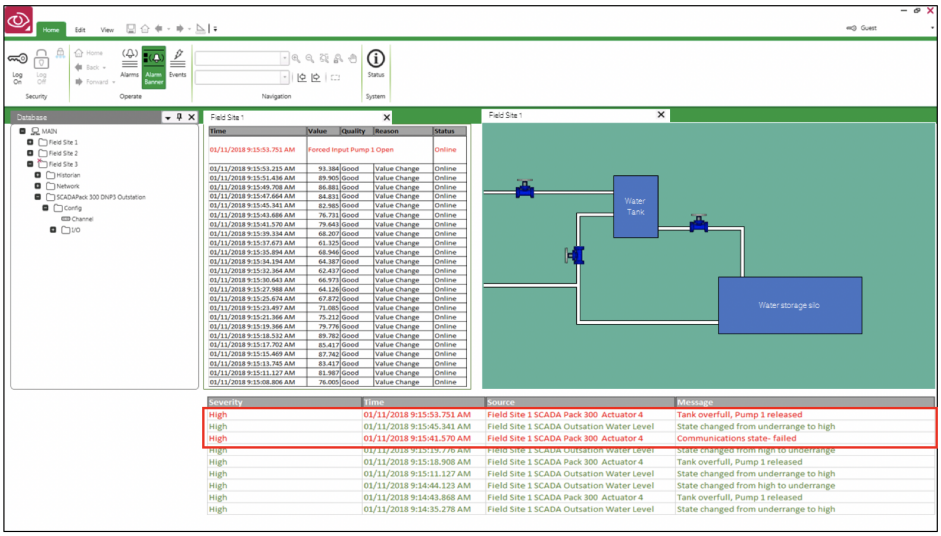


Figure 8.5: Image of the DoS Attack- Including Warnings of a Communication Failure and Pump Being Forced Open

8.3.5 Threats to Validity

This study has several limitations. Firstly this study used a simulated and simplified SCADA system that requires comparatively little input compared to a real system. Secondly, the individuals involved in this study were not technically experienced and so the results have limited generalisability to a real life situation. Additionally the small sample limits the ability to test multiple independent variables that may influence an individual's ability to detect these attacks.

8.4 Results

8.4.1 Can People Observe Attacks Against a Waterplant System?

The results of whether or not people can observe different attacks and how this differs between the two conditions can be seen in Figure 8.6. This figure demonstrates that more than half of the participants were able to observe the effects of the simulated man in the middle attack and the DoS attack. However only one participant (2% of the total sample) observed the replay attack. This supports the findings of Chapter 7 that replay attacks appear to be subtle and hard for humans operating a system to identify even when they have been primed to consider security. This does, however, disprove the idea that individuals may be better at detecting replay attacks when looking at specific data values rather than the physical system. Consideration should be given however to the idea that participant's inability to detect replay attacks may have been due to the experimental set-up such as having small values or a the lack of training on the system.

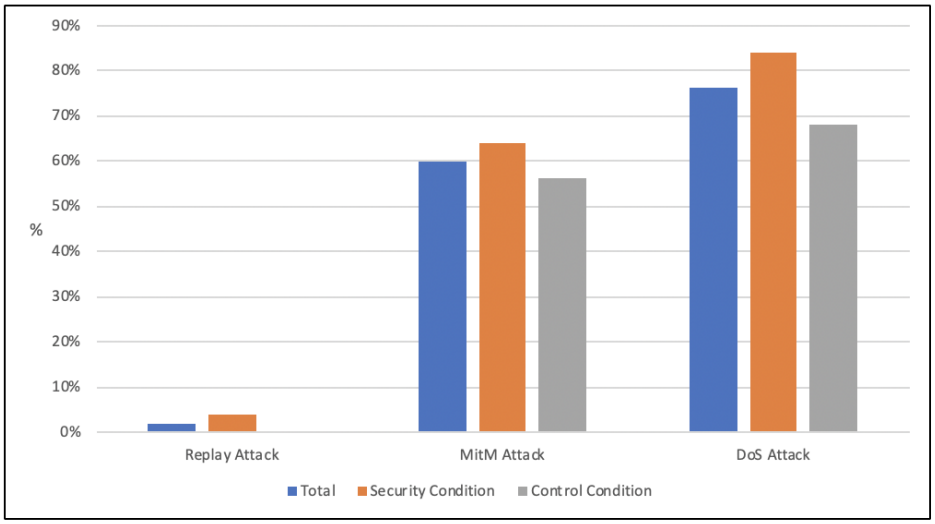


Figure 8.6: Percentage of Individuals Observing the Different Cyber Security Incidents

8.4.2 Are Some Attacks Easier to Observe Than Others?

In order to explore whether some attacks were significantly more likely to be observed than others a Cochrans Q test was run. This test explores whether there are differences in a dichotomous dependent variable (whether or not the attack was observed) between three or more related groups (the different attack conditions).

The results of this test revealed that the number of participants detecting attacks was statistically significant across the different attack scenarios, $X^2(2)= 54.143$, p <.001 (see Figure 8.7).

Test Statistics

N	50
Cochran's Q	54.143[a]
df	2
Asymp. Sig.	.000

a. 0 is treated as a success.

Figure 8.7: Output of the Cochran Q Test

Because the Cochrans Q test results showed significance, Dunn's post hoc analysis consisting of pairwise comparisons were run to allow us to see which conditions had significant differences between them. Adjusted *p* values using Bonferroni's correction were then used to account for the multiple comparisons.

The results showed that the number of participants observing the DoS attack (76%) was statistically significant compared to the number who observed the replay attack (2% observed) p

<.0005. Additionally the man in the middle attack was observed in 60% of the case which was also statistically significant compared to the replay attack p <.0005. There was, however, no statistical difference between the number of people observing the DoS and the man in the middle attacks p=.392 (see Figure 8.8).

Pairwise Comparisons

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
Replay-MitM	-.580	.106	-5.480	.000	.000
Replay-DoS	-.740	.106	-6.992	.000	.000
MitM-DoS	-.160	.106	-1.512	.131	.392

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.
Asymptotic significances (2-sided tests) are displayed. The significance level is .05.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

Figure 8.8: Results of the Cochran Q Post-hoc Tests

8.4.3 The impact of priming on observing different types of attacks

Because only one participant identified the replay attack, the sample size was deemed too small to explore this statistically. To explore whether priming has an impact on whether individuals observe the man in the middle and the DoS attack two chi-square tests for homogeneity were conducted. For full details see Appendix K, Section K.2.1.

Man in the Middle attack: 64% of individuals in the security condition observed the man in the middle attack, compared to 56% of individuals in the control condition, however this difference was not significant, p >.05.

DoS attack: 84% of participants in the security condition reported that they observed the DoS attack compared to 68% of participants in the control condition. Whilst observing Figure 8.6 shows that there is a bigger difference between the two conditions for this attack, the chi-square test showed that the difference was not significant, p >.05.

These analyses highlight that, within this simplified waterplant study, priming individuals to consider security and the possibility of cyber attacks during the study, did not statistically increase the chances that participants would observe the effects of a simulated man in the middle attack or a DoS attack.

8.4.4 Can We Predict Who Will Observe Different Attacks?

Following on from the earlier chapters this study also explored whether certain individual differences could be used to predict who may be able to observe or identify different types of attacks. Once again, the fact that only one participant reported observing the replay attack meant

that this attack was not analysed as it was deemed insufficient to be able to draw any conclusions from one individual. The full analyses can be found in Appendix K, Sections K.3.1 and K.3.2.

Predicting who can observe a man in the middle attack: A binomial logistic regression was performed to explore the effects of IT knowledge, gender and neuroticism on the likelihood that participants will observe the simulated man in the middle attack. The logistic regression model however was not statistically significant, $X^2(3)= 1.316$, p=.725 and the model only explained 3.5% (Nagelkerke R^2) of the variance.

Predicting who can observe a DoS attack: A binomial logistic regression was performed to explore the effects of IT knowledge, gender and neuroticism on the likelihood that participants will observe the simulated man in the middle attack. The logistic regression model however was not statistically significant, $X^2(3)= .210$, p=.976 and the model only explained 0.6% (Nagelkerke R^2) of the variance.

The results of these analyses suggest that IT knowledge, gender and neuroticism cannot be used to predict who can observe attacks against an ICS SCADA system.

8.4.5 Can People Correctly Identify a Cyber Attack?

Another question that this work sought to explore, was whether people are able to correctly identify when an incident is due to a potential cyber attack and what is the impact of security priming on this ability to identify an attack. The results showed that, perhaps unsurprisingly, only the security primed individuals believed that any of the incidents were due to cyber attacks.

Figure 8.9 shows the percentage of individuals within the security primed group who observed each attack in comparison to whether they attributed it to cyber attacks. It demonstrates that the DoS attack was the most likely to be observed, and that primed individuals always believed this was a result of a cyber attack. In the case of the man in the middle attack however (where the participants received conflicting information from the system and emails from technicians), participants were much less likely to attribute it to malicious interference, with some participants commenting that they believed it could be due to delays in the system. This suggests that participants were much more uncertain about events that involved conflicting information, however, it may have been due to unfamiliarity with the study and participants prioritising the SCADA task over the emails.

Interestingly, within the security primed group, 4 participants (16% of the security sample) reported that they believed some large changes in water pressure were the result of a cyber attack, suggesting that the priming caused them to see additional incidents that they then automatically assumed were malicious. This therefore suggests that priming individuals to consider security does also lead to false positive alerts.

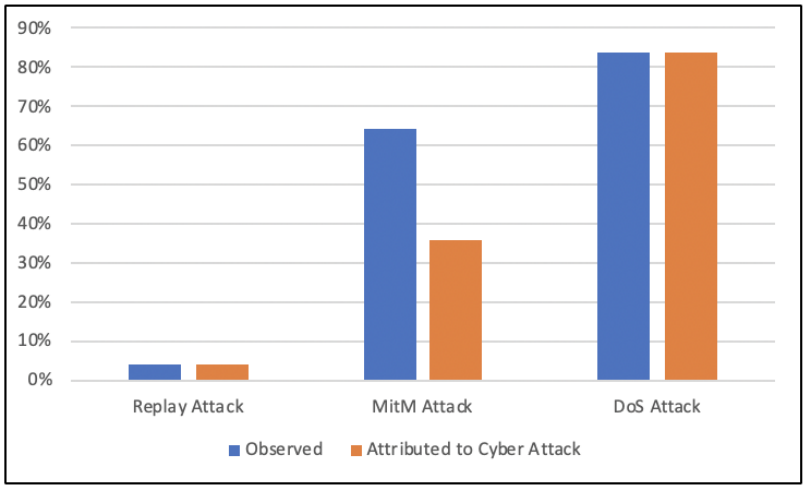


Figure 8.9: Percentage of Security Primed Individuals Observing the Different Cyber Security Incidents and Attributing Them to Cyber Attacks

8.4.6 Did Priming Individuals to Consider Security Impact Participant's Workload

A second question that this study sought to explore was whether or not priming individuals to consider cyber security had any impacts on the participant's mental workload. A Mann-Whitney U test was run to determine if there were differences in workload scores between the security condition and the control condition. Distributions of the workload scores for the two conditions were similar, as assessed by visual inspection, meaning the test was used to examine the median scores between the two groups. However median engagement score were not statistically significantly different between security primed and unprimed participants, U = 347, z = .670, p = .503.

8.5 Discussion

This chapter had five purposes: i) to explore whether participants could observe different attacks in a simulated waterplant SCADA system, ii) to investigate whether people can correctly identify incidents that could be due to a cyber attack, iii) to explore whether we can predict who is more likely to observe an attack, iv) to identify whether priming individuals to consider security increases their ability to observe different cyber attacks and v) to look at whether priming individuals to consider security causes any changes in their workload.

Observing different attacks: This thesis is especially interested in whether individuals can identify different forms of attack against physical systems. The results of this study suggested that some forms of attack are observable by participants supporting work conducted within

the transport industry which showed that pilots and train drivers could observe some attacks [212, 213]. Those two studies also found that the ability to observe an attack varied based on the type attack and this finding was also supported by this study with the replay attack found to be particularly hard to observe. This also supports the findings in Chapter 7 suggesting that a replay attack is hard to observe both in the context of a SCADA system and when observing the physical components and HMI directly. Future work should consider looking at replay attacks in more detail in order to explore whether greater training on a system (e.g. highlighting that repeating values would be unexpected). Additionally work should explore whether having the attack repeated over a longer period of time, and allowing more opportunities for the values to be observed and recognised, would create situations where this attack is more likely to me recognised.

Attributing incidents to a cyber attack: Earlier work in this thesis highlighted that many people will attribute a cyber security incident to a technical failure. When unprimed, this study also found that people automatically assume technical issues, with the few participants who felt comfortable trying to attribute this to either technical or communication failures. One person then believed that they had pressed the wrong button with no individuals suggesting cyber security incidents could be the cause without having been specifically instructed to consider this possibility. When asked to consider that any observed incidents may be related to a cyber attack, the DoS attack was always attributed to a security incident. In the case of the man in the middle attack whilst many more individuals did attribute the issue to a cyber security incident, 44% of the individuals who observed the attack did not deem it to be suspicious suggesting that some attacks are hard to distinguish from other types of incidents.

Can we predict who will detect an attack? Analyses were run to explore whether gender, IT knowledge or neuroticism could be used to predict individuals who may be better at detecting either the DoS or man in the middle attack. In both of these statistical tests however no significant findings were observed. This suggests that findings that males are better able to detect traditional attacks e.g. phishing emails and malicious webpages [144, 152, 153] cannot be applied in this context, although does support research showing no gender differences [132, 155]. Surprisingly this study also contradicts the finding that IT knowledge is linked to a better ability to recognise attacks [142–147]. Overall this study supports Chapter 7 that we cannot reliably use individual differences to predict who will observe an attack.

Does priming individuals to consider security make them better at observing attacks? Whilst there is very little previous research to explore whether priming individuals to consider security improves detection rates this study found that doing so did lead to a slight increase in the number of individuals observing an attack. There were however no statistical differences in observation of attacks suggesting that priming did not have an impact.

Does priming individuals impact their workload? The average workload for the security condition (3.1) was higher than for the control condition (2.7), potentially contradicting

the work by [194] that warnings don't increase workload. Again however this finding was not significant. The only impact of priming individuals therefore was to change how individuals attributed the causes for different incidents.

8.6 Interim Conclusions

Several conclusions can be drawn from this work:

Firstly, this work provides further evidence that individuals do observe the impacts of some cyber attacks, supporting findings in earlier chapters. However, this chapter has also expanded on the earlier work by highlighting that attacks such as man in the middle attacks and DoS attacks, can be observed, not only directly from industrial systems but also from the data outputs of these systems.

Secondly, this Chapter supports the finding from Chapter 7 that replay attacks appear to be particularly challenging for human system users to identify within simulated scenarios of industrial control systems. Again, this work expands on these findings demonstrating that this attack is hard to identify even when presented with the data outputs from industrial systems.

Thirdly, whilst many individuals can observe attacks, gender, IT Knowledge and neuroticism were not able to predict which of the participants would be able to observe these attacks. This provides support for findings throughout this thesis that these individual differences can not be used to reliably identify which types of individuals will be able to detect different forms of cyber attacks.

Fourthly, this chapter looked to expand on current research by exploring the effects of priming by having both security primed and unprimed participants. It was found that priming individuals to consider security does not statistically increase the number of participants who observe the effects of attack. However, security priming does increase the number of people who will attribute the incident to a cyber attack. Despite this however individuals are still better at attributing attacks such as a DoS attack that affect functionality, over attacks where they are receiving conflicting information. In this scenario participants were also likely to consider that the incident may be due to a technical failure.

Finally, priming individuals to think about cyber security did not result in any significant changes in average mental workload across the scenario.

Part IV

Thesis Discussions

CHAPTER 9

THE ROLE OF HUMAN AGENCY IN OBSERVING ATTACKS AGAINST CYBER-PHYSICAL SYSTEMS

This thesis sought to explore what is known about whether people can observe different cyber attacks. In particular it sought to expand current knowledge by exploring whether findings related to the use of security measures in traditional computers can be generalised to the use of security measures across different types of devices and attacks. It also explored whether these findings can be used to identify individuals who are more likely to observe or recognise different attacks. To the author's knowledge, this thesis is the first study to explore this in depth across multiple attacks and contexts. This chapter presents the key findings, before reiterating the key objectives of this work and highlighting how the findings tie back to the thesis recommendations.

9.1 Thesis Objectives Reiterated

This section presents the original research goals and objectives (as mentioned in section 1.2) and an overview of how each goal was accomplished.

The Research Goals of This Thesis:

1. *Can human users identify attacks against cyber-physical systems?* This goal was explored through studies exposing participants to a range of different attacks across both home and industrial contexts. The results of these studies demonstrated that whilst individuals can observe several different forms of attacks, some appear to be more observable than others. In particular in an industrial context, observable attacks are those that completely halt a system e.g. a DoS attack and attacks that involve receiving conflicting information. In the home environment, attacks against a webcam were poorly recognised, however

warnings involving on-screen information or symbols were more likely to be viewed as malicious. Additionally, whether an individual can correctly identify a cyber attack is largely due to whether an individual has been primed to consider cyber security, with unprimed individuals rarely, if ever recognising issues as the result of malicious interference. This is an important finding, suggesting that security warnings may be a useful way of encouraging human system users to report potential security incidents. However work would need to be done to explore the impact of alarm fatigue or the rate of false positives. Finally, even when primed to consider security, forms of attacks involving false but believable information, or warnings occurring 'off-screen' are still unlikely to be detected.

2. *Can we identify individuals who are better able to detect attacks against cyber-physical system?* Based on previous research that certain individual differences are linked to an individual's susceptible to falling victim to a cyber attack, this project explored participants' demographic factors in relation to their ability to detect cyber attacks. This thesis found that gender, IT knowledge and confidence in detecting attacks are statistically related to greater awareness of different attacks and using more security measures. These factors were also sometimes found to be related to the ability to detect attacks, however not all factors are related to detecting all attacks and the level of variance predicted by these factors is small.

3. *Are findings about who can detect attacks generalisable across different systems and attacks?* In order to explore the generalisability of findings, studies were conducted across a range of different attacks and in both home and industrial contexts. The findings suggest that results are largely not generalisable, with none of the explored factors consistently able to predict whether an individual could detect different types of attacks against different types of systems.

9.2 Summary of the Findings

9.2.1 Summary of Findings for Cyber Security in the Home

Chapters 4-6 explored the types of different computer devices that home owners currently own, their level of awareness regarding different attacks, whether they took measures to try and increase the security of different devices. They also explored whether individuals can detect a range of different attacks.

The findings of these studies showed that people use a range of devices and that within a student sample smartphone ownership has overtaken that of laptops, with over half also using electronic notepad devices. Whilst the use of these devices has increased, the findings of this thesis suggest that knowledge about the devices and how they may be vulnerable has not kept pace. In particular many of the participants revealed that they were unaware that many devices

incorporate NFC and motion and orientation sensors, despite the fact that these could be used to maliciously target these devices. People also display a lack of knowledge around attacks that target some of these newer sensors e.g. using movement sensors to generate a users PIN or using NFC to steal financial information, as well as attacks such as using malware against devices to turn them into botnets or ransomware to get money from individuals. This lack of awareness about the devices people are using appears to translate into taking fewer precautions to protect these devices. Firstly, many people appear to fail to apply security techniques that they use on desktops and laptops, i.e. more traditional computers, to newer types of devices. This can be seen in the findings that whilst individuals use antivirus software on desktops and laptops (at 92% and 86% respectively) the use of this software on tablet and smartphone devices (37% and 31%) is much lower despite often holding sensitive data such as messages, personal accounts and bank details. Reduced uptake of security approaches on smartphones and tablets can also be seen with reading of permissions and in using encryption. Additionally, it was found that across all devices many of the participants failed to seek to protect themselves from attacks against physical components, with people reporting that they typically do not take precautions such as covering cameras.

This thesis also explored different factors that have been found to be related to either the use of security factors or the detection of different attacks and investigated whether they also apply to different cyber-physical systems. This thesis supports previous, finding that IT knowledge, awareness of different attacks, gender as well as levels of concern about attacks and the perceived likelihood of being attacked were all statistically correlated with using more security measures on laptops and smartphones. Age and confidence in detecting attacks however, were not related to greater use of security behaviours. Detailed investigations into why people use different security measures across different devices also supports that IT knowledge is a key determinant of whether an individual will use different security mechanisms, with a lack of knowledge presenting a key barrier. Additional motivations for the use of security mechanisms included to protect information that they perceive to be more valuable, the usability of different approaches and concerns about potential attacks. Additional barriers to the use of security included poor usability and poor feedback, prioritising device functionality over security or a belief that the costs of using security approaches is too high.

The use of different security approaches for different devices then relates to a lot of these factors, with a lack of knowledge about security risks or how to mitigate them limiting the use of security mechanisms on non traditional computer devices. Other individuals also reported using less security measures on these devices if they believed they held less sensitive information, however others also perceived that non-traditional computer devices were less vulnerable to being attacked.

Having built up a picture of individual's knowledge and use of security measures this thesis then explored whether individuals could detect a range of different attacks and whether factors

such as knowledge also translate into better detection. This work found that different forms of attacks are more likely to be detected than others, with both phishing emails and attacks involving a malicious .exe pop-up more likely to be detected than control conditions. These two attacks were also statistically more likely to be detected than a simulated RAT attack that involved a LED light switching on next to a camera lens. In fact this attack was not observed with any greater frequency than the control conditions, despite the finding that other visual prompts where observed by most of the participants, suggesting that even when individuals are prompted to consider cyber attacks they focus very specifically on events that are occurring on screen. When exploring what factors can be used to explain some of the variance in individual differences it was found that gender, IT knowledge and confidence in detecting attacks were all each statistically related to the detection of one of the attacks. However, the attack that each variable could predict varied suggesting that that findings are not generalisable across different attacks and that they therefore have limited predictive value.

9.2.2 Summary of Findings for Cyber Security in Industrial Control Systems

Chapters 7 and 8 focused on whether individuals can observe attacks against larger scale systems used within critical national infrastructure. This work was focused on the observation of attacks by non-security individuals and looked at the detection of attacks in a simulated water plant. Specifically the studies observed detection of attacks when observing the system directly (e.g. a technician) and when observing a SCADA system (e.g. a control room operator).

This work concluded that there are several different attacks that can be conducted against a simulated waterplant and be observable to people who may be working with the system. Whilst different attacks were observable some types of attacks were more readily observed that others, with attacks such as a DoS attack that have a large impact more readily observable than attacks such as a potential man in the middle attack where participants may have received conflicting information. Attacks that simulated realistic data, such as a replay attack were very unlikely to be observed even when the data was repeated.

Whilst some forms of attack against physical systems were observable to the participants from both the systems directly and from the SCADA outputs, attribution of blame to a malicious cyber incident was non-existent without participants being primed to consider that they may experience a cyber attack. Without priming attribution was usually then placed on technical failures. When individuals were primed, attribution to cyber attacks was 100% for observed DoS attacks, however where there was conflicting information attribution was more mixed. Priming was also found to have no impact on the participants average workload.

Work exploring whether different factors could help to predict who could observe attacks against the waterplant, simulations identified that factors such as IT knowledge, gender and personality traits were not significantly related to the identification of any of these attacks.

9.2.3 Similarities and Differences Between CPS for Home and Industry

One of the key aims of this project was to explore the extent to which cyber security findings can be generalised across different attacks and different types of CPS.

Exploring the results from across home devices and industry systems highlights several similarities. Firstly, in both home and industrial work contexts some attacks are more easily observed by humans, with attacks that occur on a computer screen appearing to be more easily observed. Attacks that then involve warning indicators off-screen e.g., lights off-screen, or secondary information that conflicts with on-screen information were less likely to be either noticed or labelled as potentially malicious. This could be due to the experimental set-ups but one possible explanation could be that individuals have a preconception of what constitutes a 'cyber-attack' with events that do not fit this mental model harder to observe.

A second finding was that when it comes to actually observing and detecting attacks, factors such as IT knowledge, gender and personality cannot be used to predict who will be better in either a home or industrial setting. Whilst significant findings were occasionally found for some forms of cyber attacks these were not generalisable, suggesting limited utility for their predictive abilities.

Thirdly, this work found that overall detection rates for attacks are relatively low, and that individuals who have not been primed to consider security are unlikely to view this as the cause of any unexpected incidents. Whilst security priming does increase the likelihood of people correctly identifying cyber attacks it was also found that, for both home and industry settings, it did occasionally result in false positives with people considering normal system behaviours to be malicious.

Overall these findings highlight that individuals are unlikely to detect cyber attacks without some form of input to raise their suspicions or awareness that they could become a victim. They also show that factors related to the use of more security measures do not consistently translate to better detection of attacks with factors predicting ability to detect attack being ungeneralisable from one type of attack to another.

9.3 Synthetic Conclusion

Each chapter has presented interim conclusions and discussions throughout this thesis, with these described in more detail in the section above. The key novel findings that this thesis offers to the current literature are listed below:

– Many individuals have limited knowledge of the physical components that many of their devices contain and how these could be compromised or targeted by a cyber attack. However factors such as IT knowledge, awareness of attacks, gender, level of concern and perceived likelihood of attack are related to using more measures to try and protect their devices.

- People take different approaches to protecting different devices. One key reason for this is a lack of knowledge, especially in relation to how to secure non-traditional devices with many individuals unaware of either the different methods for securing different devices or unaware of how to implement these approaches. Other reasons however also included wanting to use more protective methods for devices with more sensitive information or prioritising different types of functionality over security on different types of devices.

- Human users of different physical systems are able to observe various different cyber attacks, and could therefore provide valuable information about attacks or be able to recognise when they have been targeted. However, without priming individuals to consider cyber security, people's abilities to identify a cyber attack as a possible cause of any incidents is poor. Where there is a perceived threat, individuals should therefore be told, with Chapter 8 suggesting that this does not increase workload.

- This work also identified two specific types of attacks that people are especially poor at observing. The first is an attack switching on a camera e.g., a RAT attack, suggesting that people are poor at observing security alerts that appear off-screen. The second type of attack that people are poor at observing is an attack involving replaying spoofed values, e.g., a replay attack. This was true regardless of whether they were observing the physical system or the data directly suggesting that technological measures would be important to try and detect this form of attack. Exploring this further where participants are fully trained on systems or not being directed to other tasks should be considered.

- Factors previously found to be related to an individual's ability to detect phishing attacks or which predict the use of security measures, specifically gender, IT knowledge, confidence in detecting attacks, and personality cannot be used to predict whether an individual will observe an attack. This suggests that findings are not generalisable across different systems or forms of attack and that should researchers wish to predict who is more vulnerable to different cyber attacks then different attacks would need to be studied individually.

These conclusions answer the original research questions and expand on the current knowledge base by highlighting the need to explore observation of different attacks on different systems individually rather than attempting to generalise findings from traditional computer systems.

9.4 Taking These Findings Forward

Two prevalent themes that emerge throughout this thesis are that 1) the human users of systems can observe some attacks against cyber-physical systems. However, the attacks that are observed vary, as do the types of system indicators that participants observe and 2) the findings that emerge from the literature around detection of attacks on traditional PCs do not generalise across

different systems and devices. Both of these themes highlight a large gap in the literature that should be taken forward in order to increase our understanding of whether human users can be used to help identify potentially malicious cyber incidents.

9.4.1 Increasing Our Understanding of Which Attacks People Can Observe

This work has suggested that individuals can observe some attacks but not others, whilst this work has begun to increase our understanding in this area given the variance in whether attacks are witnessed.

Future work should therefore seek to explore a wider range of attacks and attacks across different systems and devices. Studies should also be conducted using a wider range of participants including non-students and participants who own a wider range of personal and IoT devices

In relation to studying which types of attacks people can detect against ICS systems, research should seek to run attacks against a wider range of systems. Ideally these should use larger testbeds that more accurately represent the systems in question, and recruit individuals with real life experience of working with these systems, allowing us to better mimic the complexity of these systems in the real world. In addition research should also be conducted outside of university settings as even when instructed to consider security, participants may be very aware of the fact that this is a simulation and potentially be overly trusting of the system or more willing to attribute any issues as due to a simulation error.

Research should also seek to explore in more detail what it is about these attacks that individuals notice, and what types of system behaviours that they find suspicious e.g. observing on-screen changes vs. light or auditory indicators. Answering these questions could therefore hope to produce either more generalisable findings that can be used to try and predict what attacks could be observed or to produce indicators that are more likely to be observable.

9.4.2 Increasing Our Understanding of Who Can Detect Attacks Against Cyber-Physical Systems

This thesis highlights that previous knowledge, regarding factors that make someone either more susceptible to or more likely to detect attacks, is not generalisable across different attacks. This is true in both a home context and in the context of industrial control systems.

Future work should therefore explore a wider range of variables in the detection of attacks. Examples of variables that could be studied include the personality aspects that were not studied within this thesis such as conscientiousness or by using a standardised test for IT knowledge rather than allowing participants to self-rate their knowledge. However, should these findings also prove ungeneralisable then research should seek to either build up a library to understand what may make people susceptible to different types of attacks or focus on training to improve detection rather than seeking to predict detection rates.

Finally, whilst this thesis has begun to address the research gap into human security for national infrastructure, this work only included a water plant ICS. Future work should therefore seek to explore people's abilities to detect attacks against different types of industrial systems, for example in power grids, manufacturing or transportation networks. This would allow a better understanding on the impacts of different interfaces, systems and processes as well as an exploration of whether any findings from this thesis can be generalised across industrial systems.

9.5 Concluding Remarks

This thesis provides early support that humans are able to observe a range of different cyber attacks and could therefore be used to support security in the event of an attack being successful. This thesis also provides some of the first work exploring the detection of attacks by humans in the context of critical national infrastructure. This is a challenging area to research, due to limitations in accessing equipment and trained personnel, as well as the need for organisations to keep many of their security processes confidential. However, given the extent to which societies rely on these systems and their increasing connectivity it is an important area to consider. Whilst this work provides the first stepping stone in exploring which types of attacks humans can, and can't, detect it is important to note that a much greater understanding is required. This is particularly true for exploring how best to capture perceived information security risks from humans in a manner that is helpful to organisations and to ensure that the rates of false positives versus true detections are better understood. This thesis offers the building blocks to further research such issues and extend our scientific knowledge, in general, on human detection of attacks against cyber-physical systems.

Part V

Appendices

APPENDIX A

ONLINE SURVEY- ETHICS PROPOSAL

This Appendix presents the approved ethics proposal for the online survey study detailed in Chapter 4. Note for clarity of reading, the full survey used in this study has been removed from this document and placed in Appendix B.

Lancaster University

Faculty of Science and Technology Research Ethics Committee (FSTREC)
Lancaster University

Application for Ethical Approval for Research

This form should be used for all projects by staff and research students, whether funded or not, which have not been reviewed by any external research ethics committee. If your project is or has been reviewed by another committee (e.g. from another University), please contact the FST research ethics officer for further guidance.

In addition to the completed form, you need to submit **research materials** such as:

i. Participant information sheets
ii. Consent forms
iii. Debriefing sheets
iv. Advertising materials (posters, e-mails)
v. Letters/emails of invitation to participate
vi. Questionnaires, surveys, demographic sheets that are non-standard
vii. Interview schedules, interview question guides, focus group scripts

Please note that **you DO NOT need to submit pre-existing questionnaires or standardized tests** that support your work, but which cannot be amended following ethical review. These should simply be referred to in your application form.

Please submit this form and any relevant materials **by email as** a **SINGLE attachment** to <email>.

Section One

Applicant and Project Information

Name of Researcher: Emma Hewlett

Project Title: Human Factors in Cyber Security of Cyber Physical Systems

Level: *PhD*

Supervisor (if applicable): Awais Rashid, Paul Taylor, Utz Roedig

Researcher's Email address: <email>
Telephone: <phone>
Address: B59, Infolab

Names and appointments/position of all further members of the research team: N/a

Is this research externally funded? If yes, No

ACP ID number:
Funding source:
Grant code:

Does your research project involve any of the following?

☑ Human participants (including all types of interviews, questionnaires, focus groups, records relating to humans, use of internet or other secondary data, observation etc.)

□ Animals - the term animals shall be taken to include any non-human vertebrates or cephalopods.

□ Risk to members of the research team e.g. lone working, travel to areas where researchers may be at risk, risk of emotional distress

□ Human cells or tissues other than those established in laboratory cultures

□ Risk to the environment

□ Conflict of interest

□ Research or a funding source that could be considered controversial

□ Social media and/or data from internet sources that could be considered private

□ any other ethical considerations

Yes – complete the rest of this form

No – go to Section Five

Section Two

Type of study

☒ Includes *direct* involvement by human subjects. ***Complete all sections apart from Section 3.***

☐ Involves *existing documents/data only*, or the evaluation of an existing project with no direct contact with human participants. ***Complete all sections apart from Section 4.***

Project Details

1. Anticipated project dates (month and year)
Start date: Nov 2017 **End date:** Feb 2020

2. Please briefly describe the background to the research (no more than 150 words, in lay-person's language):
Cyber Physical Systems, (systems incorporating computers and devices which can impact the physical world) such as many manufacturing systems, smart heating devices (e.g. Hive) and web controlled security cameras are becoming increasingly common. With growing interest in automated vehicles and personal medical devices this trend is likely to continue with personal cyber physical systems also becoming increasingly common. Whilst these devices offer individuals many benefits they also introduce potential new risks from cyber-attacks. Examples of these include taking control of a camera to record users, or preventing a user from using a smart device such as heating or lighting control app, unless they pay a fee. However very few pieces of research have investigated if individuals are aware of these risks and whether they have the knowledge and/or ability to protect their systems against a cyber-attack.

3. Please state the aims and objectives of the project (no more than 150 words, in lay-person's language):
This work seeks to investigate the extent to which individuals own and make use of various cyber physical systems and the methods that they use (if any) to protect these devices. The work will also investigate how concerned individuals are that their devices could be maliciously targeted and how likely they think it is that it could happen to them. The main research questions for this work are:

- What devices are the most commonly used and what cyber physical systems do these devices incorporate?
- Do individuals believe that it is likely that their devices could be targeted for malicious means?
- Are individuals concerned that their devices may be targeted for malicious means?
- How confident are individuals that they could detect if their system had been compromised?
- What methods are used by individuals to try and protect these devices?

4. Methodology and Analysis:

<u>Methodology</u>
This work will utilise an online questionnaire design using Qualtrics software, that should take no longer than 20 minutes to complete. In total this survey will aim to achieve a minimum of 116 responses. Responses will be stored by Qualtrics before being downloaded and stored on the university network once the survey period is finished.

<u>Analysis</u>
Analysis of the results will involve a mix of approaches. Descriptive statistics will be used to analysis the types of devices that are owned and the most common methods that are used to protect them with any interesting patterns highlighted and explored.

Statistical analysis will then be used to investigate the following three questions:

- Do individuals believe that it is likely that their devices could be targeted for malicious means?
- Are individuals concerned that their devices may be targeted for malicious means?

- How confident are individuals that they could detect if their system had been compromised?

This will involve running five ordinal logistic regression analyses (one for each question), investigating whether gender, age, ethnicity, self-rated IT knowledge and number of devices owned influences the participant's responses.

Number of responses required

To calculate the sample size for a multiple regression the following formulae have been suggested, for testing an overall relationship:

For testing a relationship and the individual pathways:

$N \geq 104 + m$ (where m is the number of IV variables)

In this instance there are five IVs and so a minimum of 109 participants would be required[1].

An online power calculator then suggested a minimum sample size of 116, when using the following parameters[2]:

Anticipated effect size: 0.15 (medium effect size)
Desired statistical power level: 0.90 (conventionally this value is typically above 0.8 with the higher the level the higher the chance of not committing a type II error.
Number of predictors: 5
Probability level= 0.05

A minimum sample of 116 participants will therefore be recruited

Section Three (NOT APPLICABLE)

Secondary Data Analysis

Complete this section if your project involves *existing documents/data only*, or the evaluation of an existing project with no direct contact with human participants

1. Please describe briefly the data or records to be studied, or the evaluation to be undertaken.

2. How will any data or records be obtained?

3. Confidentiality and Anonymity: If your study involves re-analysis and potential publication of existing data but which was gathered as part of a previous project involving direct contact with human beings, how will you ensure that your re-analysis of this data maintains confidentiality and anonymity as guaranteed in the original study?

4. What plan is in place for the storage of data (electronic, digital, paper, etc)? Please ensure that your plans comply with the Data Protection Act 1998.

[1] Tabachnick, Barbara G., Linda S. Fidell, and Steven J. Osterlind. "Using multivariate statistics." (2001).

[2] http://www.danielsoper.com/statcalc/calculator.aspx?id=1

5. What are the plans for dissemination of findings from the research?

6a. Is the secondary data you will be using in the public domain? YES/NO
6b. If NO, please indicate the original purpose for which the data was collected, and comment on whether consent was gathered for additional later use of the data.

7.What other ethical considerations (if any), not previously noted on this application, do you think there are in the proposed study? How will these issues be addressed?

8a. Will you be gathering data from discussion forums, on-line 'chat-rooms' and similar online spaces where privacy and anonymity are contentious? YES/NO

If yes, your project requires full ethics review. Please complete all sections.

Section Four

Participant Information

Complete this section if your project includes *direct* involvement by human subjects.

1. Please describe briefly the **intended human participants** (including number, age, gender, and any other relevant characteristics):
This study will seek to recruit a minimum of 116 adult participants including a mix of males and females and individuals from different age groups and cultures;

Exclusion criteria for this study is individuals under 18 years old and individuals who are not fluent in English.

2. How will participants be **recruited** and from where?
Participants will be recruited from around the university and online. Methods for advertising will include:
- Using the Lancaster Psychology Research Participation System- SONA
- Flyers placed around campus
- Adverts posted online via social networks

Adverts will include an overview of the study as well as the researcher contact details should individuals wish to ask for more information.

3. Briefly describe your **data collection methods**, drawing particular attention to any potential ethical issues.

Data will be collected via an online survey (see appendices), with data kept anonymous as participants will not be asked to provide any identifiable information.

One ethical consideration is the issue of giving consent and the possibility that individuals under 18 may take part. To minimise the chances of this occurring all adverts will state the exclusion criteria and participants will have to actively declare that they have read the consent information before clicking next. Finally, in the event that any participants respond that they are younger than 18 years of age then their data will be immediately destroyed.

4. Consent

4a. Will you take all necessary steps to **obtain the voluntary and informed consent** of the prospective participant(s) or, in the case of individual(s) not capable of giving informed consent, the permission of a legally authorised representative in accordance with applicable law? **YES**
If yes, please go to question 4b. If no, please go to question 4c.

4b. Please explain the procedure you will use for **obtaining consent**? If applicable, please explain the procedures you intend to use to gain permission on behalf of participants who are unable to give informed consent.

Before taking the online survey, participants will be presented with a consent page (see appendices) which will provide information regarding the conditions that individuals are agreeing to by completing the survey. As the researcher will not be with potential participants, they will be under no pressure to take part and can stop or withdraw at any time.

4c. If it will be necessary for participants to take part in the study **without their knowledge and consent at the time**, please explain why (for example covert observations may be necessary in some settings; some experiments require use of deception or partial deception – not telling participants everything about the experiment).

N/a- participants will be giving consent.

5. Could participation cause **discomfort** (physical and psychological eg distressing, sensitive or embarrassing topics), **inconvenience or danger beyond the risks encountered in normal life**? Please indicate plans to address these potential risks. State the timescales within which participants may withdraw from the study, noting your reasons.

The topics covered in this study are not sensitive or likely to cause any discomfort, however there is a small possibility that this study could cause a participant some concern regarding their vulnerability to a cyber-attack. At the end of the study participants will therefore be given information pointing them towards information sources regarding how best to protect their devices (https://www.cyberaware.gov.uk/).

Participants will be informed that participation is voluntary and that they may withdraw at any point during the study, up to the point of data submission by closing the survey window. They will also be told that partially completed surveys will be deleted (copy of survey settings shown in Appendices).

6. How will you protect participants' **confidentiality and/or anonymity** in data collection (e.g. interviews), data storage, data analysis, presentation of findings and publications?

No identifiable data is gathered or reported, except for emails if participants wish to provide it in order to gain potential benefits (psychology credit or chance to win a voucher), this information will not be pooled with the rest of the responses.

7. Do you anticipate any ethical constraints relating to **power imbalances or dependent relationships**, either with participants or with or within the research team? If yes, please explain how you intend to address these?

No power imbalances are identified.

8. What potential **risks may exist for the researcher** and/or research team? Please indicate plans to address such risks (for example, noting the support available to you/the researcher; counselling considerations arising from the sensitive or distressing nature of the research/topic; details of the lone worker plan you or any researchers will follow, in particular when working abroad.

No potential risks are identified, there will be no direct contact between the researcher or participant.

9. Whilst there may not be any significant direct **benefits to participants** as a result of this research, please state here any that may result from participation in the study.

- Psychology students will be offered 0.5 credits for taking part (gathering credits is a requirement for their undergraduate courses).
- All participants (including psychology students) will be offered the opportunity to be entered into a prize draw for a £20 amazon voucher.

10. Please explain the **rationale for any incentives/payments** (including out-of-pocket expenses) made to participants:
The incentives will be used to encourage participation from individuals.

11. What are your plans for the **storage of data** (electronic, digital, paper, etc.)? Please ensure that your plans comply with the Data Protection Act 1998.
Completed data will be downloaded from Qualtrics and stored for up to 10 years on the university server, in the researcher's university folder until graduation and will be made available via Pure where it will be available for a minimum of 10 years. Stored data will be available to the researcher and supervisors.

12. Please answer the following question *only* if you have not completed a Data Management Plan for an external funder.

12.a How will you make your data available under open access requirements?
Data will be made available through Pure. Data will also be offered to the UK Data Archive as per the standard ESRC procedures (the consent page will declare that by submitting data participants give consent for the data to be shared.)

12b. Are there any restrictions on sharing your data for open access purposes?

No (email addresses will be removed from final data set)

13. Will **audio or video recording** take place? ☑ no □ audio ☐ video

13a. Please confirm that portable devices (laptop, USB drive etc) will be **encrypted** where they are used for identifiable data. If it is not possible to encrypt your portable devices, please comment on the steps you will take to protect the data.
N/a- Neither recording or portable devices will be used.

13b. What arrangements have been made for **audio/video data storage**? At what point in the research will tapes/digital recordings/files be destroyed?
N/a

13c. If your study includes video recordings, what are the implications for participants' anonymity? Can anonymity be guaranteed and if so, how? If participants are identifiable on the recordings, how will you explain to them what you will do with the recordings? How will you seek consent from them?
N/a

14. What are the plans for dissemination of findings from the research? If you are a student, mention here your thesis. Please also include any impact activities and potential ethical issues these may raise.
The results of the research may be submitted for publication in academic/professional journals, for presentation at conferences/ seminars and will also be included in my PhD thesis.

15. What particular ethical considerations, not previously noted on this application, do you think there are in the proposed study? Are there any matters about which you wish to seek guidance from the FSTREC?

One ethical consideration for this study is that the questionnaire allows individuals the option to provide a contact email if they wish to be considered to take part in a follow-up study of interview, individuals may therefore feel pressured to provide information. It is possible they may also be concerned that an email provided for the chance to win the voucher will be used in this manner. To reduce these concerns the questions are presented separately and it is clearly stated that the information will not be used for any other purpose

Additionally, study **FST16126- 'Human Factors in Cyber Security of ICS- Study 2 and 3'** is being run consecutively and involves participants being unaware of the cyber security element of the research. Therefore, FST16126 will need to have participation in this study added as an exclusion criteria. There are no issues in anyone doing FST16126 before doing this survey study.

Section Five

Additional information required by the university insurers

If the research involves either the nuclear industry or an aircraft or the aircraft industry (other than for transport), please provide details below:

Section Six

Declaration and Signatures

I understand that as Principal Investigator/researcher/PhD candidate I have overall responsibility for the ethical management of the project and confirm the following:

- I have read the Code of Practice, Research Ethics at Lancaster: a code of practice and I am willing to abide by it in relation to the current proposal.
- I will manage the project in an ethically appropriate manner according to: (a) the subject matter involved and (b) the Code of Practice and Procedures of the University.
- On behalf of the University I accept responsibility for the project in relation to promoting good research practice and the prevention of misconduct (including plagiarism and fabrication or misrepresentation of results).
- On behalf of the University I accept responsibility for the project in relation to the observance of the rules for the exploitation of intellectual property.
- If applicable, I will give all staff and students involved in the project guidance on the good practice and ethical standards expected in the project in accordance with the University Code of Practice. (Online Research Integrity training is available for staff and students here.)
- If applicable, I will take steps to ensure that no students or staff involved in the project will be exposed to inappropriate situations.

☑ Confirmed

Please note: If you are not able to confirm the statement above please contact the FST Research Ethics Committee and provide an explanation.

Student applicants:

Please tick to confirm that you have discussed this application with your supervisor, and that they agree to the application being submitted for ethical review ☒

Students must submit this application from your Lancaster University email address, and copy your supervisor in to the email in which you submit this application

All Staff and Research Students must complete this declaration:

I confirm that I have sent a copy of this application to my Head of Department (or their delegated representative) . **Tick here to confirm** ☒

Name of Head of Department *(or their delegated representative)* Adrian Friday via Claire Anne Oulton.

Applicant electronic signature: E. Hewlett Date 22.08.2017

Attached Information:

- Advertisement materials
- Copy of survey
- Debrief
- Survey Settings

Advertisement Materials

Online SONA Advert

Study Name	Use of personal 'smart' devices
Study Type	Online survey
Pay	0.5 credits- Chance to win a £20 amazon voucher
Duration	20 minutes
Description	This work involves an online survey investigating the different electronic devices that individuals use and different methods that individuals use to protect these devices.
Eligibility	You must be over 18 years of age and an English speaker
Researcher	Emma Hewlett
Deadlines	Sign up deadline: 0 hours before study Cancellation deadline: 0 hours before study

Lancaster University

Advert/ Flyer (For distribution on Campus)

School of Computing & Communications | Lancaster University

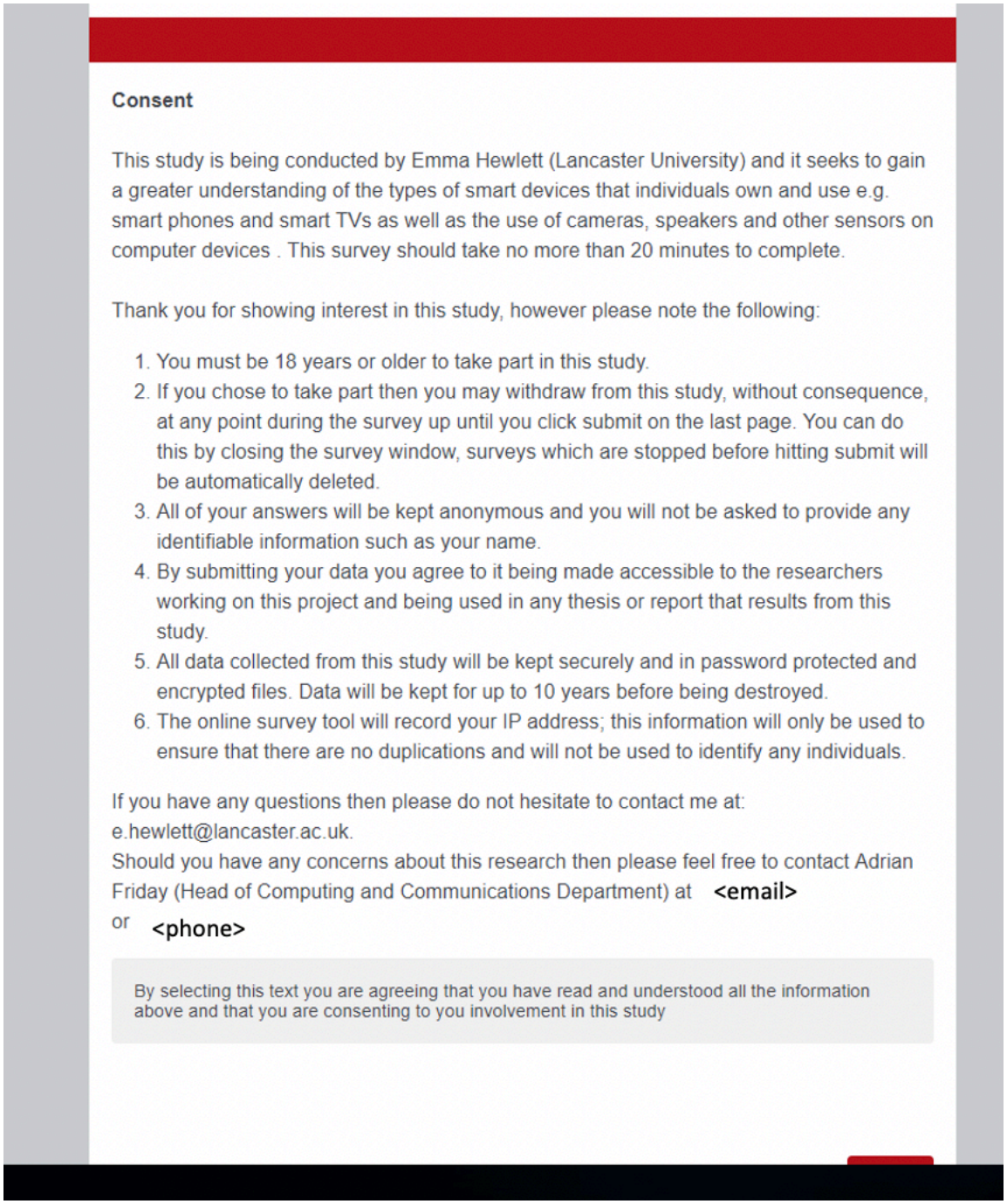
Win a £20 Amazon Voucher!!

Take a short survey on the types of technology you use and have a chance to win a £20 Amazon voucher.

[Link to survey here]
You must be 18+ years old to take part

For more information contact Emma Hewlett: <email>

Consent Page



Consent

This study is being conducted by Emma Hewlett (Lancaster University) and it seeks to gain a greater understanding of the types of smart devices that individuals own and use e.g. smart phones and smart TVs as well as the use of cameras, speakers and other sensors on computer devices . This survey should take no more than 20 minutes to complete.

Thank you for showing interest in this study, however please note the following:

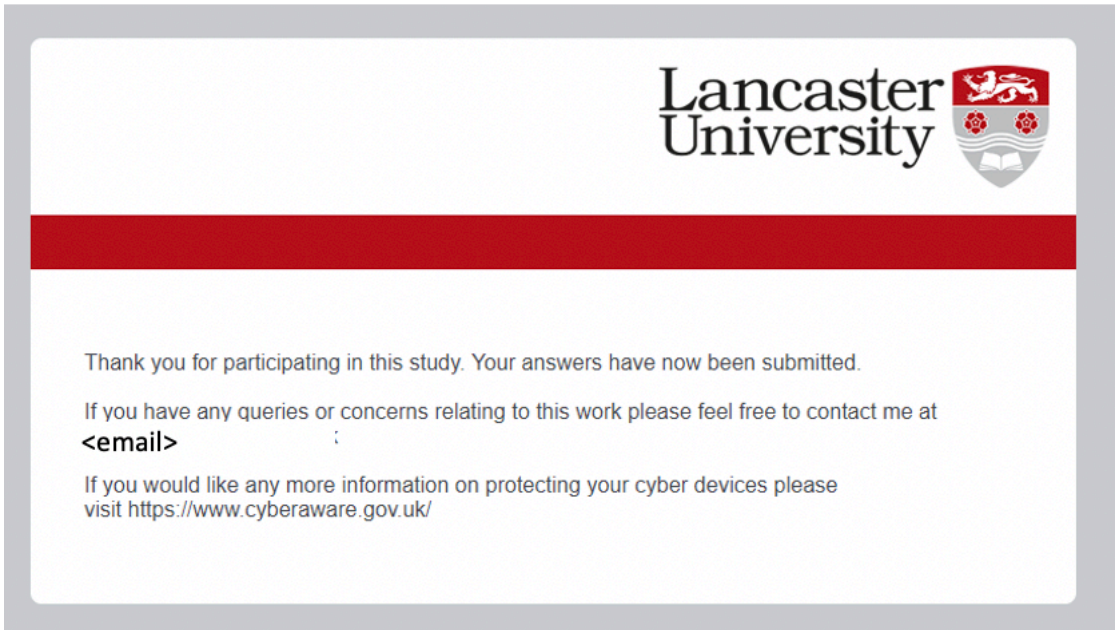
1. You must be 18 years or older to take part in this study.
2. If you chose to take part then you may withdraw from this study, without consequence, at any point during the survey up until you click submit on the last page. You can do this by closing the survey window, surveys which are stopped before hitting submit will be automatically deleted.
3. All of your answers will be kept anonymous and you will not be asked to provide any identifiable information such as your name.
4. By submitting your data you agree to it being made accessible to the researchers working on this project and being used in any thesis or report that results from this study.
5. All data collected from this study will be kept securely and in password protected and encrypted files. Data will be kept for up to 10 years before being destroyed.
6. The online survey tool will record your IP address; this information will only be used to ensure that there are no duplications and will not be used to identify any individuals.

If you have any questions then please do not hesitate to contact me at: e.hewlett@lancaster.ac.uk.
Should you have any concerns about this research then please feel free to contact Adrian Friday (Head of Computing and Communications Department) at <email>
or <phone>

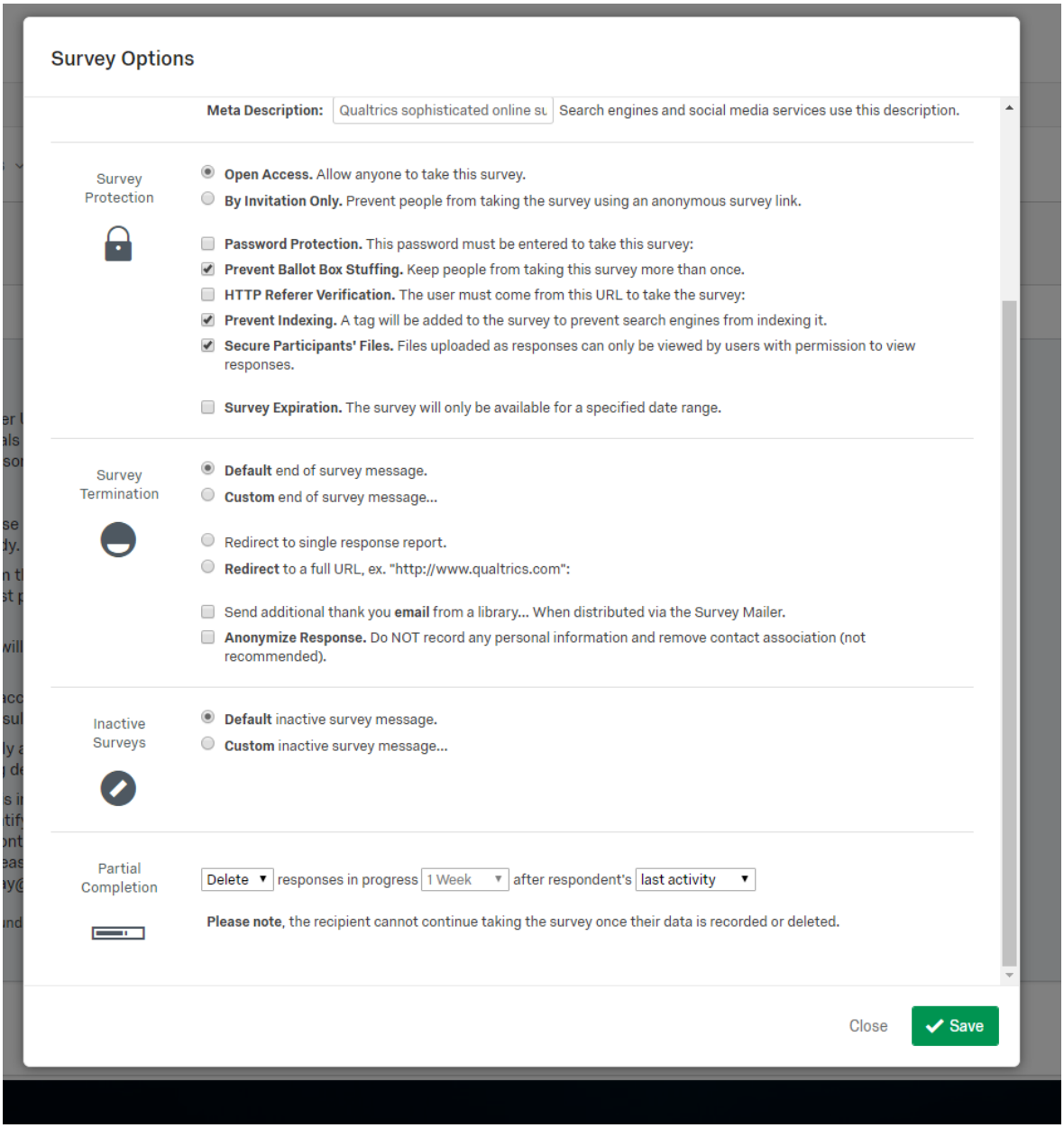
By selecting this text you are agreeing that you have read and understood all the information above and that you are consenting to you involvement in this study

Participants are required to confirm that they have read the information before continuing with the survey.

Debrief Page



Survey settings



APPENDIX B

ONLINE SURVEY- QUESTIONNAIRE

This Appendix presents the online survey that was administered via Qualtrics as part of the study detailed in Chapter 4.

B.1 Demographics

Q1. What is your gender?
Male; Female; prefer not to say

Q2. What is your age?

Q3. Please state your ethnicity:
Caucasian; Latino/Hispanic; Middle Eastern; African; Caribbean; South Asian; East Asian; Mixed; Other

Q4. Please state your occupation:

Q5. How would you rate your IT knowledge?
Very high- e.g. having academic or industrial IT qualifications; High- e.g. able to configure home networks and personal firewalls; Moderate- e.g. able to set up all your personal IT devices and connect them to the internet; Low- e.g. You use IT, but have no knowledge of how to set up devices; Very low- e.g. No experience of using of setting up IT systems

B.2 Use of Smart Devices

Q6. Portable Devices- Which of the following devices do you own? (Select all that apply)
Desktop Computer; Laptop; Notebook e.g. ipad; Smartphone; Smart TV; Games Console; Smart watch; Fitness tracker e.g. Fitbit

Q7. Please specify to the best of you ability what type of device you own. E.g. iPhone7
Participants shown the list of devices they had selected in Q6.

Q8. What sensors do you believe your devices to have?
Participants were shown the list of devices they had selected in Q6. and for each device presented with the following options: Camera; Audio recorders; GPS; Heart rate monitor; NFC; Bluetooth; Motion and orientation sensors; fingerprint scanner; proximity sensor; Light sensor; Barometer.

Q9. Home Devices- Do you use any of the following smart devices within your home? (Select all that apply)
Smart meters (e.g. for gas and/or electricity); Smart thermostats (e.g. Hive); Smart lights (or switched to control lights); Smart locks (or switches to control locks); Security cameras (or smartphone cameras etc. used for security); Smart fridge; Smart kettle; Any other automated or smart devices; None

B.3 Use of Protective Measures

Q10. How do you protect the devices you own?
Participants were shown the list of devices they had selected in Q6. and for each device presented with the following options: Passwords; Antivirus/malware software; Reading application permissions; Installing updates; Encryption; Firewall; Covering up (or disconnecting cameras); Covering up (or disconnecting sound recorders); Disabling GPS; Disabling Bluetooth; Disabling NFC

Q11. The list above gives examples of some conventional security measures, please list any additional security features that you use?

Q12. How do you protect your smart home?
Participants were shown the list of devices they had selected in Q9. and for each device presented with the following options: Reviewing security features before buying; Password protect home wireless network; Change default usernames and passwords on devices; Update devices; Use a router that offers firewall protection; Keeping smart devices on a seperate wi-fi network; Blocking

unencrypted traffic to smart devices; I don't know what security features I use.

Q13. The list above gives examples of some conventional security measures, please list any additional security features that you use?

B.4 Security Concerns

Q14. Have you ever experienced a cyber security issue. If yes please explain the situation and how you dealt with it?

Q15. Are you aware of the following cyber risks?
For each option participants were asked to select 'yes' or 'no' Invasion of privacy through cameras of stationary devices- e.g., PCs, smart TVs; Invasion of privacy through portable devices- e.g., Phones, laptops; Eavesdropping through stationary devices- e.g., PCs, smart TVs; Eavesdropping through portable devices- e.g., Phones, laptops; Malware hijacking devices for botnets; Ransomware denying access to data on devices; Ransomware denying access to smart physical devices e.g. thermostats; Devices sending personal details to third parties; Individuals or organisations stealing personal data; GPS tracking; External individuals hacking into network; Network mapping; Movement sensors being used to deduce passwords; Device usage being tracked to infer daily routines; Malware using NFC to send financial information to attackers.

Q16. For each of the threats please rate how LIKELY you think it that it could occur to you?
Participants shown the list of threats from Q15 and presented with the following options: Extremely unlikely; Moderately unlikely; slightly unlikely; Neither likely or unlikely; Slightly likely; Moderately likely; Extremely likely.

Q17. Overall how LIKELY do you think that it is that your 'smart devices' could be manipulated for malicious means?
Extremely unlikely; Moderately unlikely; slightly unlikely; Neither likely or unlikely; Slightly likely; Moderately likely; Extremely likely.

Q18. Overall how CONCERNED or WORRIED are you that your 'smart devices' could be manipulated for malicious means?
Extremely unlikely; Moderately unlikely; slightly unlikely; Neither likely or unlikely; Slightly likely; Moderately likely; Extremely likely.

Q19. Do you have any additional security or privacy concerns about smart devices or cyber-physical systems?

Q20. Overall how CONFIDENT are you that you could identify if your 'smart devices' had been manipulated for malicious means?
Extremely unlikely; Moderately unlikely; slightly unlikely; Neither likely or unlikely; Slightly likely; Moderately likely; Extremely likely.

Q21. Would privacy concerns ever prevent you from getting a smart device? Please explain
Yes; No; maybe

Q22. Would security concerns ever prevent you from getting a smart device? Please explain
Yes; No; maybe

APPENDIX C

ONLINE SURVEY STATISTICAL TEST DETAILS AND RESULTS

This Appendix presents the statistical outputs that were created for the online survey study detailed in Chapter 4.

C.1 Statistical Tests Conducted into Awareness of Different Attacks

C.1.1 Statistics for Spearman's Rank Correlations into Levels of Awareness of Different Cyber Attacks

These outputs relate to Section 4.5.4 where a Spearman's Rank correlation was run between the following variables to explore the factors influencing awareness of different cyber attacks: i) Age, ii) Level of self reported IT knowledge, iii) Level of concern about attacks, iv) Perceived likelihood of falling victim to an attack, v) Confidence in their ability to detect an attack, vi) No. of measures they used to protect their laptop, vii) No. of measures they used to protect their smartphone, and viii) The number of attacks that they are aware of.

In order to conduct a Spearman's rank correlation test there are three key assumptions that need to be met:

1. Each of the two variables in each correlation should be measured at either the continuous or the ordinal scale.

2. Each of the two variables should represent a paired observations, i.e. they come from the same person.

3. There needs to be a monotonic relationship between the two variables (so if one variable increases the other either increases or decreases).

Assumptions 1 and 2 were met for all of the variables and assumption 3 was tested using scatterplot graphs which can be seen in the Figure C.1.

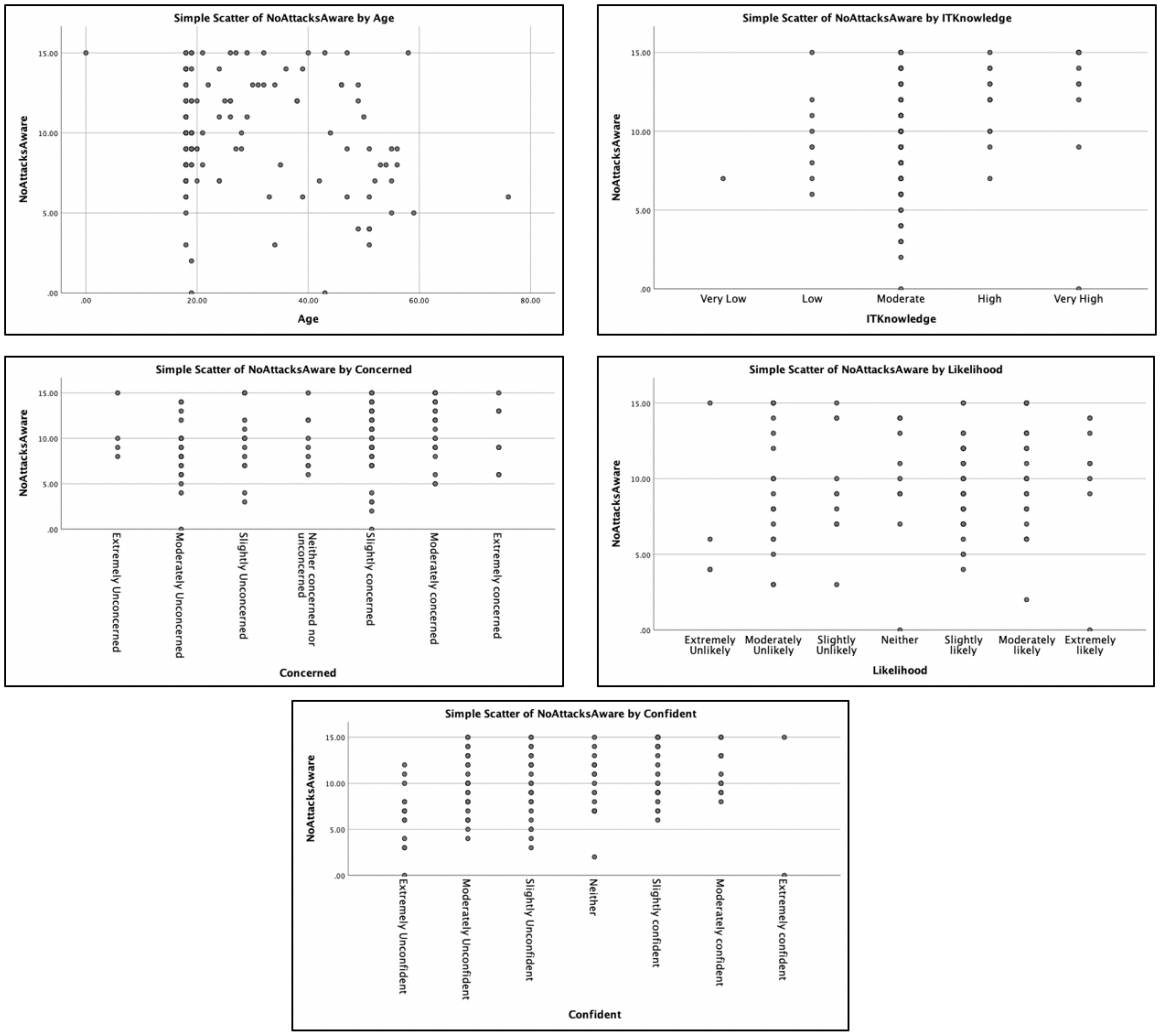


Figure C.1: Scatterplot Diagrams to Test for Monotonic Relationships in Relation to the Number of Attacks that Participants are Aware Of

Looking at these scatterplots shows that the majority of the graphs show weak but positive linear relationships. The one for age was probably the one variable where you could argue against this test, however this was deemed to be distorted by the number of young participants in this sample and so we continued with the Spearman's Rank test.

The output of the Spearman's Rank test that was run can then be seen in Figure C.2 and reveals several statistically significant findings that are discussed in Chapter 4.

Correlations

			Age	IT_Knowledge	Likely	Concern	Confident	AttacksAware	NoMeasuresLaptop	NoMeasuresSmartphone
Spearman's rho	Age	Correlation Coefficient	1.000	-.008	.005	.257**	-.043	-.089	-.055	.038
		Sig. (2-tailed)	.	.930	.955	.005	.643	.336	.560	.684
		N	120	120	120	120	120	120	114	117
	IT_Knowledge	Correlation Coefficient	-.008	1.000	.064	-.025	.289**	.333**	.361**	.272**
		Sig. (2-tailed)	.930	.	.485	.790	.001	.000	.000	.003
		N	120	121	121	121	121	121	115	118
	Likely	Correlation Coefficient	.005	.064	1.000	.487**	.087	.180*	.254**	.253**
		Sig. (2-tailed)	.955	.485	.	.000	.344	.048	.006	.006
		N	120	121	121	121	121	121	115	118
	Concern	Correlation Coefficient	.257**	-.025	.487**	1.000	.118	.213*	.248**	.280**
		Sig. (2-tailed)	.005	.790	.000	.	.196	.019	.008	.002
		N	120	121	121	121	121	121	115	118
	Confident	Correlation Coefficient	-.043	.289**	.087	.118	1.000	.306**	.194*	.173
		Sig. (2-tailed)	.643	.001	.344	.196	.	.001	.038	.061
		N	120	121	121	121	121	121	115	118
	AttacksAware	Correlation Coefficient	-.089	.333**	.180*	.213*	.306**	1.000	.458**	.294**
		Sig. (2-tailed)	.336	.000	.048	.019	.001	.	.000	.001
		N	120	121	121	121	121	121	115	118
	NoMeasuresLaptop	Correlation Coefficient	-.055	.361**	.254**	.248**	.194*	.458**	1.000	.741**
		Sig. (2-tailed)	.560	.000	.006	.008	.038	.000	.	.000
		N	114	115	115	115	115	115	115	112
	NoMeasuresSmartphone	Correlation Coefficient	.038	.272**	.253**	.280**	.173	.294**	.741**	1.000
		Sig. (2-tailed)	.684	.003	.006	.002	.061	.001	.000	.
		N	117	118	118	118	118	118	112	118

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

Figure C.2: Spearman's Rank Correlations Between Awareness of attacks and Age, IT Knowledge, Number of Laptop and Smartphone Security Measures Used, Perceived Likelihood of Attack, Concern about Attacks and Confidence in Detecting Cyber Attacks

C.1.2 Statistics for Mann Whitney U to Test If Gender Affects Awareness of Different Cyber Attacks

The second statistical test that was conducted as part of the survey study (Chapter 4 Section 4.5.4) was a Mann Whitney U test to investigate the impact of gender on attack awareness. This test is a rank based non-parametric test that is used to determine whether there are differences between two groups on a dependent variable that can be continuous or ordinal. In this case the dependent variable is the number of attacks the participants were aware of and so it is continuous. This test was selected as the data was not expected to be normally distributed.

This particular statistical test has four assumptions that need to be met:

1. You have one dependent variable that is either continuous or ordinal. In this case this is the number of cyber attacks each participant was aware of.

2. You have one independent variable that is made up of two categorical, independent groups, in this case this is gender.

3. There needs to be no relationship between the observations in each group of the independent variable or between the groups themselves i.e. each participant only belongs to one of the groups. This assumption was met when assigning participants to groups based on gender.

4. You must determine whether the distribution of scores for both groups of your independent variable (e.g., the distribution of scores for 'males' vs 'females') have the same shape or a different shape. This determines how you interpret the results of the Mann-Whitney U test.

The data set for this test meets assumptions 1-3. The histogram outputs of the Mann-Whitney U test (See Figure C.3) then reveal that the distribution scores are not similar and so in this instance the test is used to compare mean ranks (rather than the medians).

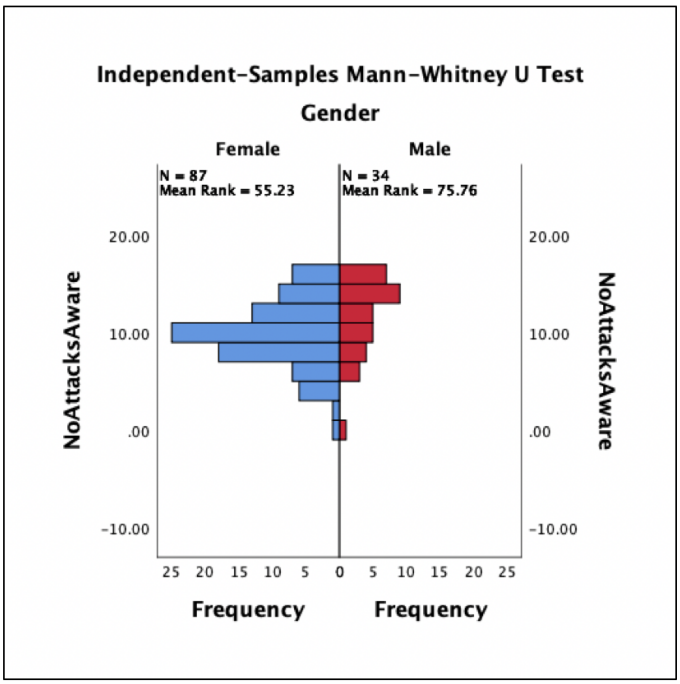


Figure C.3: Histogram Outputs to Examine the Distribution of Attack Awareness Scores for Both Genders

The full outputs from this test can then be seen in Figure C.4. This shows that there was a significant finding between the mean rank scores for males and females, which is discussed in Chapter 4.

C.2 Tests Into Factors Affecting the Use of Security Measures on Laptops

C.2.1 Statistics for Spearman's Rank Correlations for the Use of Security Methods on Laptops

The Spearman's rank correlations described above (Section C.1.1) also include correlation tests for the number of security measures that people use on laptops. However in order to test assumption

NoAttacksAware across Gender

Independent-Samples Mann-Whitney U Test Summary

Total N	121
Mann-Whitney U	1981.000
Wilcoxon W	2576.000
Test Statistic	1981.000
Standard Error	172.643
Standardized Test Statistic	2.908
Asymptotic Sig.(2-sided test)	.004

Figure C.4: Mann-Whitney U Outputs of Attack Awareness Scores for Both Genders

3 that there are monotonic relationships between the independent variables and the dependent variable (number of security measures used on laptops), scattergraph plots the use of security measures on a laptop were also produced. These are shown in Figure C.5.

From visual inspection it was decided there were sufficient positive relationships between the variables for the Spearman's rank correlation tests to be used. The full correlations are then shown in Figure C.2 and discussed in Chapter 4.

C.2.2 Statistics for the Mann Whitney U Test to Test if Gender Affects the Use of Security Measures for Laptops

The Mann Whitney U test has four assumptions that need to be met:

1. You have one dependent variable that is either continuous or ordinal. In this case this is the number of measures each participant uses to protect their laptops.

2. You have one independent variable that is made up of two categorical, independent groups, in this case this is gender.

3. There needs to be no relationship between the observations in each group of the independent variable or between the groups themselves i.e. each participant only belongs to one of the groups. This assumption was met when assigning participants to groups based on gender.

4. You must determine whether the distribution of scores for both groups of your independent variable (e.g., the distribution of scores for 'males' vs 'females') have the same shape or a different shape. This determines how you interpret the results of the Mann-Whitney U test.

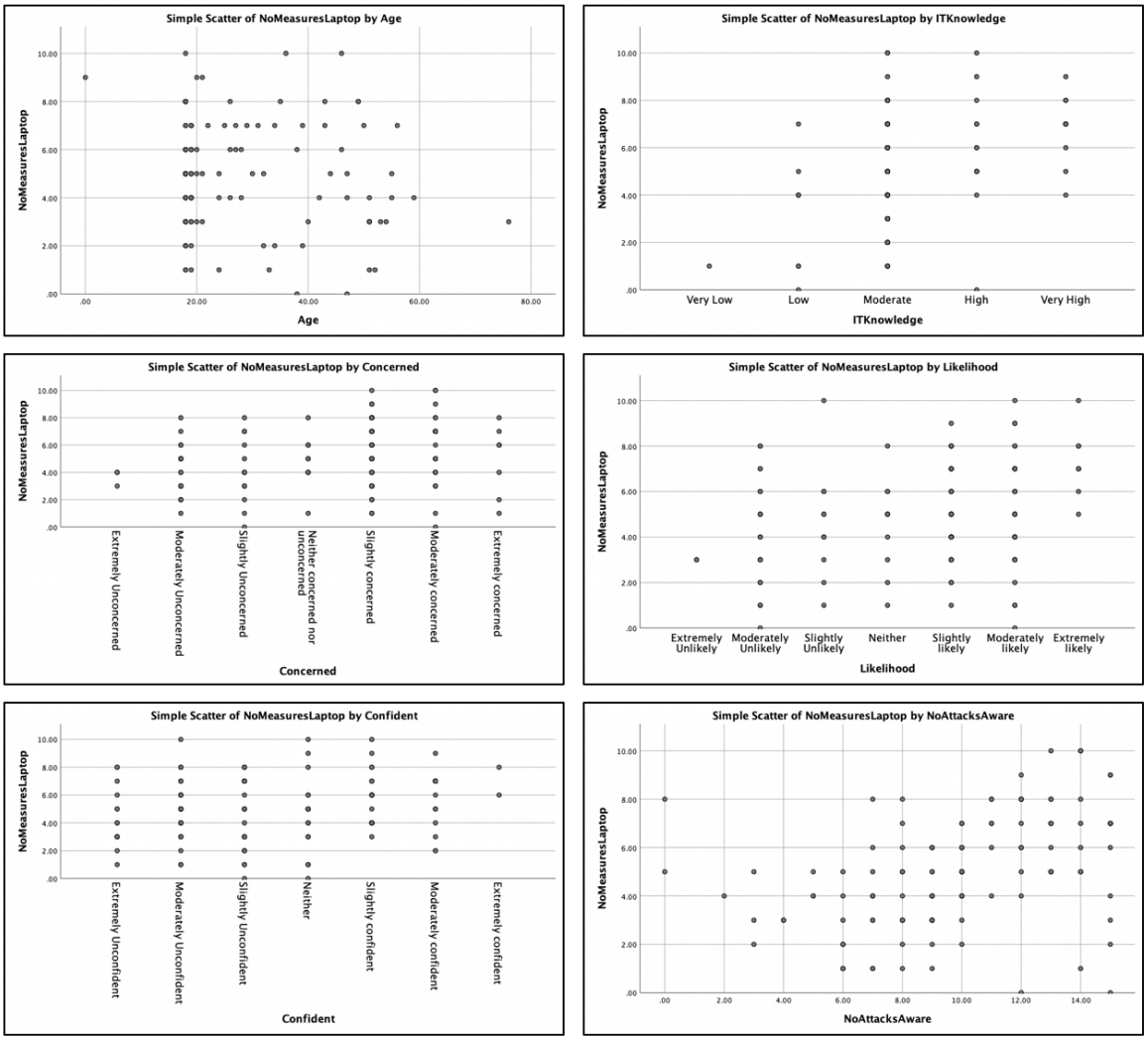


Figure C.5: Scatterplot Diagrams to Test Monotonic Relationships in Relation to the Number of Security Approaches that People Use to Protect Their Laptops

The data set for this test meets assumptions 1-3, the histogram outputs (See Figure C.6) for this test then reveal that the distribution of scores are not similar across genders and so in this instance the test is used to compare mean ranks (rather than the medians).

The full outputs from this test can then be seen in Figure C.7. This figure shows a significant finding, which is discussed in Chapter 4.

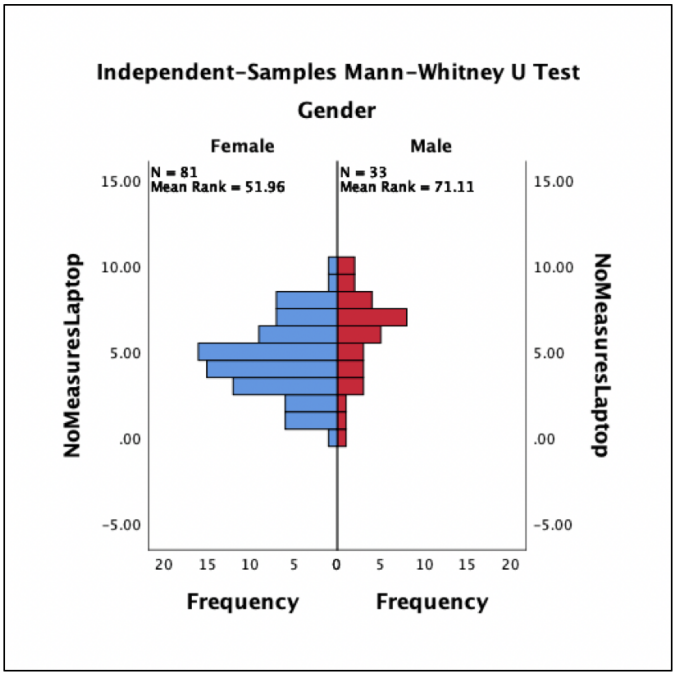


Figure C.6: Histogram Outputs to Examine the Use of Laptop Security Measures for Both Genders

NoMeasuresLaptop across Gender

Independent-Samples Mann-Whitney U Test Summary

Total N	114
Mann-Whitney U	1785.500
Wilcoxon W	2346.500
Test Statistic	1785.500
Standard Error	158.741
Standardized Test Statistic	2.829
Asymptotic Sig.(2-sided test)	.005

Figure C.7: Mann-Whitney U outputs for the Number of Security Measures Used on Laptops by Each Gender

C.3 Tests Into Factors Affecting the Use of Security Measures on Smartphones

C.3.1 Statistics for Spearman's Rank Correlations for the Use of Security Methods on Smartphones

The Spearman Rank correlations described above (Section C.1.1) also include correlation tests for the number of security measures that people use on their smartphones. However in order to test assumption 3 that there are monotonic relationships between the independent variables and the number of security measures used on smartphones, scattergraph plots for these were produced. These are shown in Figure C.8.

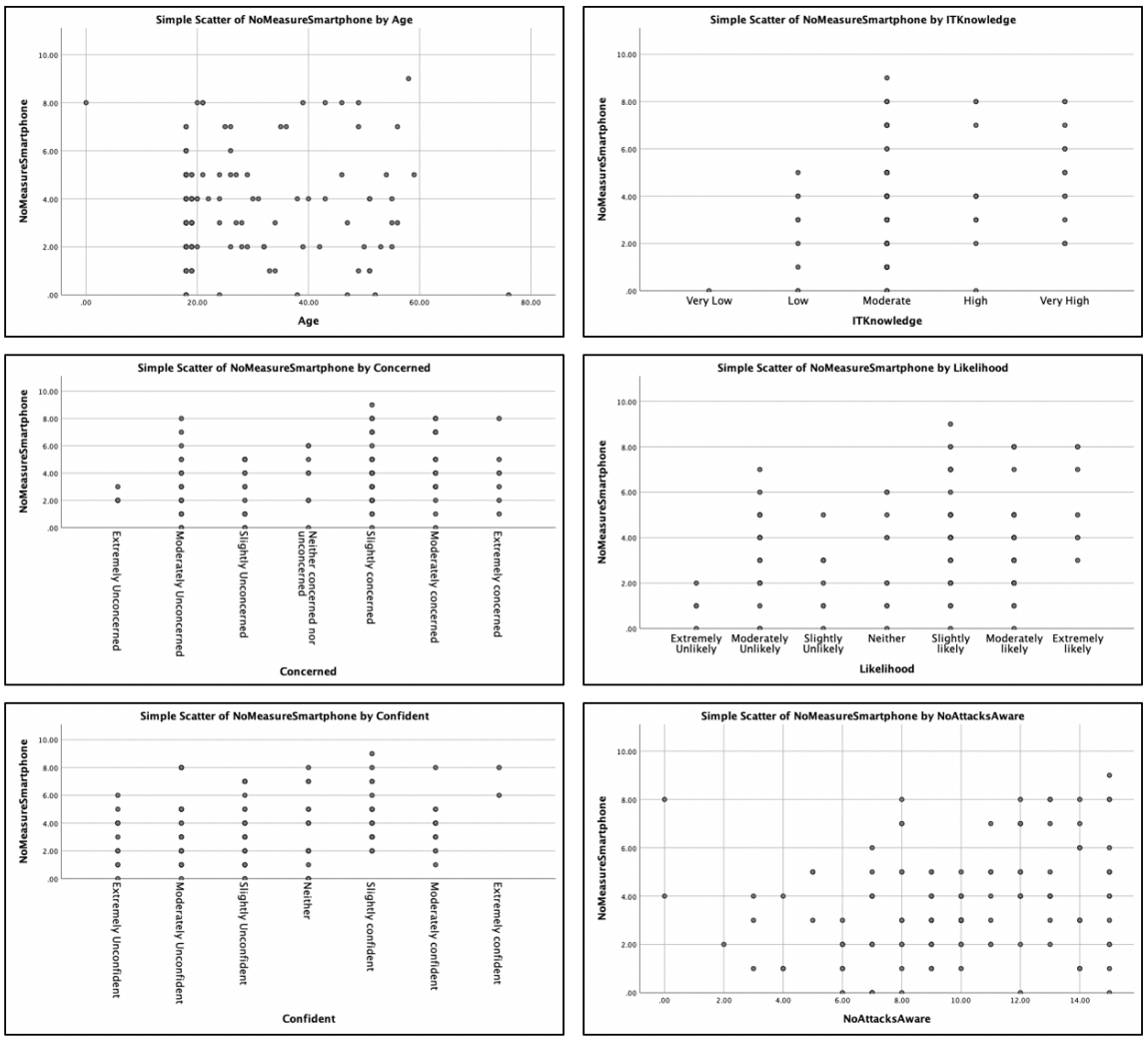


Figure C.8: Scatterplot Diagrams to Test Monotonic Relationships in Relation to the Number of Security Approaches that People Use to Protect Their Smartphones

From visual inspection it was decided there were sufficient positive relationships between the variables for the Spearman's Rank correlation tests to be used. The full correlations are then shown in Figure C.2 and discussed in Chapter 4.

C.3.2 Statistics for Mann Whitney U to Test if Gender Affects the Use of Security Measures for Smartphones

Another Mann Whitney U test was conducted to explore the affects of gender on the use of security measures for smartphones. Again, this test has four assumptions that need to be met:

1. You have one dependent variable that is either continuous or ordinal. In this case this is the number of security measures each participant used on their smartphones.

2. You have one independent variable that is made up of two categorical, independent groups, in this case this is gender.

3. There needs to be no relationship between the observations in each group of the independent variable or between the groups themselves i.e. each participant only belongs to one of the groups. This assumption was met when assigning participants to groups based on gender.

4. You must determine whether the distribution of scores for both groups of your independent variable (e.g., the distribution of scores for 'males' vs 'females') have the same shape or a different shape. This determines how you interpret the results of the Mann-Whitney U test.

The data set for this test meets assumptions 1-3, the histogram outputs (See Figure C.9) then reveals that the distribution scores are not similar across genders and so in this instance the test is used to compare mean ranks (rather than the medians).

The full outputs from this test can then be seen in Figure C.10, the test shows a statistical difference between the mean rank scores for the used of security measures by males and, this is discussed in more detail in Chapter 4.

C.4 Predicting Who Will Use Security Measures

C.4.1 Predicting the Use of Security Measures on Laptops

In order to explore whether demographic factors could be used to predict the likelihood of individuals using more security on their laptop a Multiple Regression analysis. The assumptions for this test are:

1. You have one dependent variable that is measured at the continuous level. In this case the number of measures used to protect a laptop.

2. You have two or more independent variables that are either continuous or nominal.

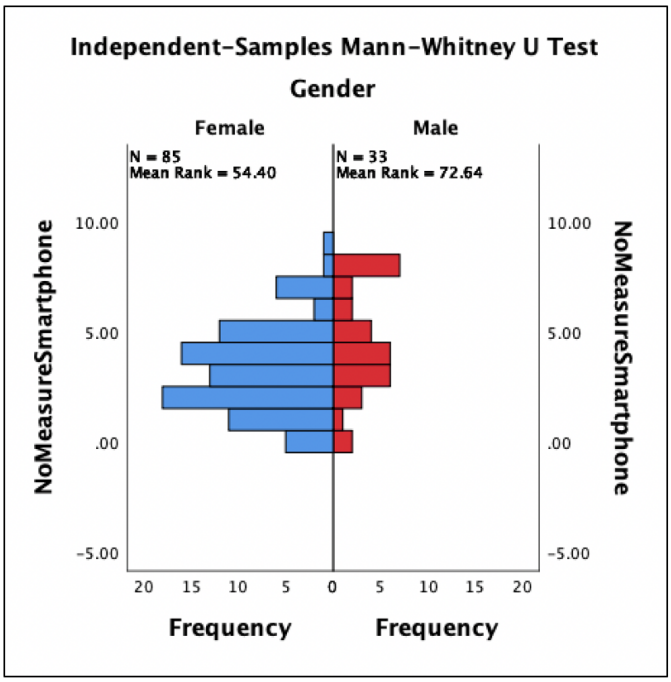


Figure C.9: Histogram Outputs to Examine the Use of Smartphone Security Measures for Both Genders.

NoMeasureSmartphone across Gender

Independent-Samples Mann-Whitney U Test Summary

Total N	118
Mann-Whitney U	1836.000
Wilcoxon W	2397.000
Test Statistic	1836.000
Standard Error	165.052
Standardized Test Statistic	2.626
Asymptotic Sig.(2-sided test)	.009

Figure C.10: Mann-Whitney U Outputs for the Number of Security Measures Used on Smartphones by Each Gender

3. There is independence of observations.

4. There should be a linear relationship between the predictor variables and the dependent variable.

5. There should be homoscedasticity of residuals.

6. There should be no multicollinearity.

7. There should be no significant outliers, high leverage points or highly influential points.

8. The errors (residuals) should be approximately normally distributed.

Assumption 1 is true, and assumption 2 was also satisfied using the variables that were found to have a significant correlation with the number of measures used on laptops. However, in order to preserve the ranking effect the ordinal variables (concern, confidence and perceived likelihood of being attacked) were considered as continuous within this test.

Assumption 3 was tested using the Durbin-Watson statistic. In this test results close to 2 represent that there is no correlation between residuals (which is what we are looking for). The results of this test can be seen in he last column of Figure C.11, and show that there was independence of residuals, with a Durbin-Watson statistic of 2.016.

In this test there was independence of residuals, as assessed by a Durbin-Watson statistic of 2.016. The results of this can be seen in the last column of Figure C.11

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin–Watson
1	.538[a]	.289	.249	1.99451	2.016

a. Predictors: (Constant), Concerned, ITKnowledge, Confident, Gender, NoAttacksAware, Likelihood

b. Dependent Variable: NoMeasuresLaptop

Figure C.11: Output of the Multiple Regression Analysis for Predicting the Use of Security Measures on Laptops

Assumption 4, the assumption of linearity, needs to be tested in two parts. First, you need to establish whether there is a linear relationship between the dependent variables and the independent variable. In this case this was established by only including those for which their is a statistical correlation. However, scatter graph plots were also created and can be see in Figure C.12. Secondly we need to establishing if a linear relationship exists between the dependent and independent variables 'collectively'. This can be seen in the 6th image in Figure C.12 and the desired outcome is a graph with a horizontal band. In this case the data was deemed to meet this assumption.

Assumption 5 to test for homoscedasticity is to test that the variance is equal for all values of the predicted dependent variable. To check this we can use the plot of studentized residuals against the unstandardized predicted values. This is shown in Figure C.12 but is also shown again

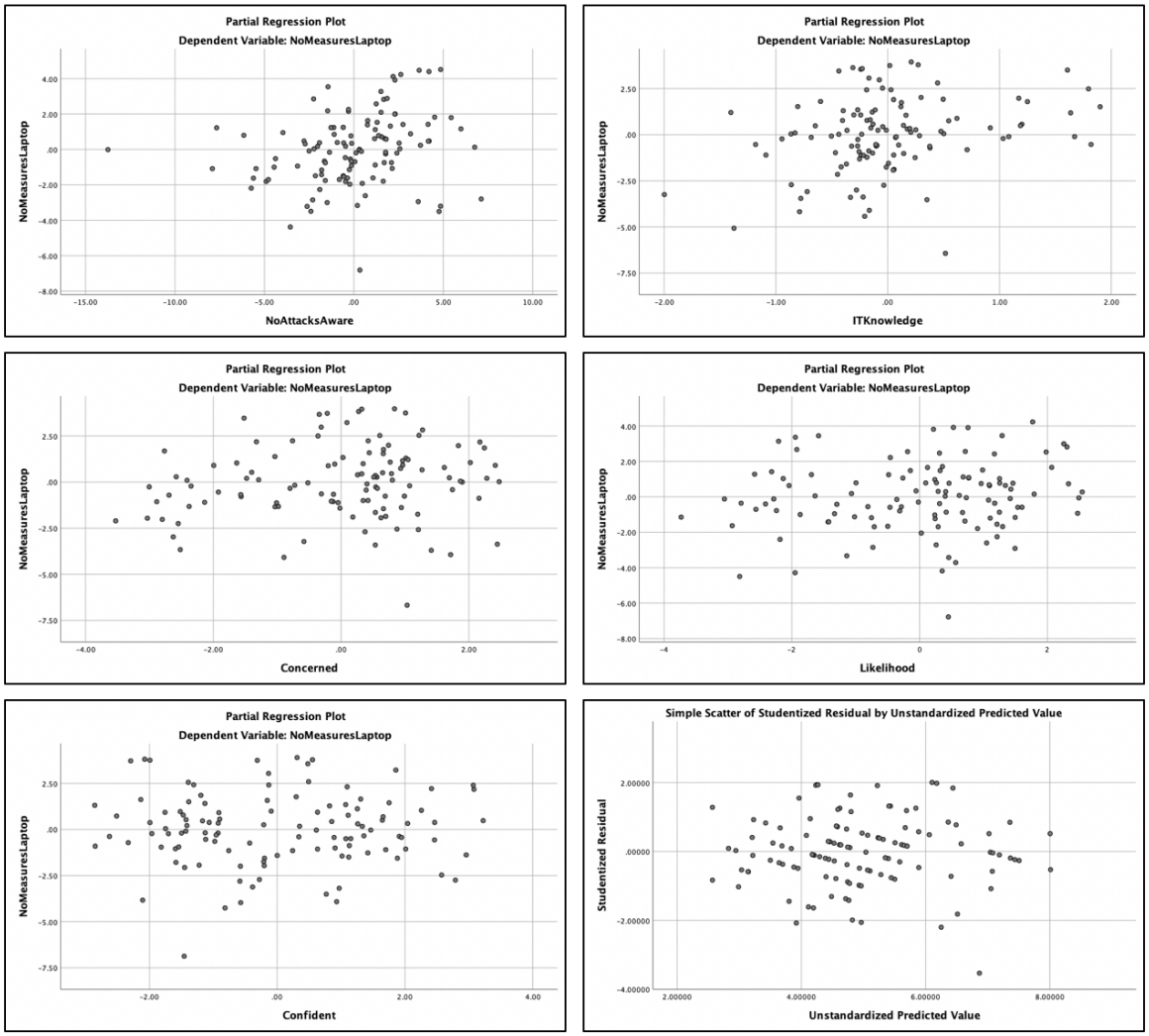


Figure C.12: Testing the Assumption of Linearity, Through Scatter Graph Plots for Use of Security Measures on Laptops

in Figure C.13. Here we are looking to check that the spread of the residuals does not particularly increase or decrease as you move across the predicted values and again this assumption was deemed to be met.

Assumption 6 requires no Multicollinearity which occurs you have two or more independent variables that are highly correlated with each other, and can lead to problems understanding which variable contributes to the variance explained. There are two approaches to identifying multicollinearity: inspection of correlation coefficients or Tolerance/VIF values. Firstly we inspect the correlations to ensure that none of the independent variable have correlations greater than 0.7. This assumption was met as can be seen in Figure C.14

Multicollinearity can also be tested by observing the 'Tolerance' and 'VIF' values in the

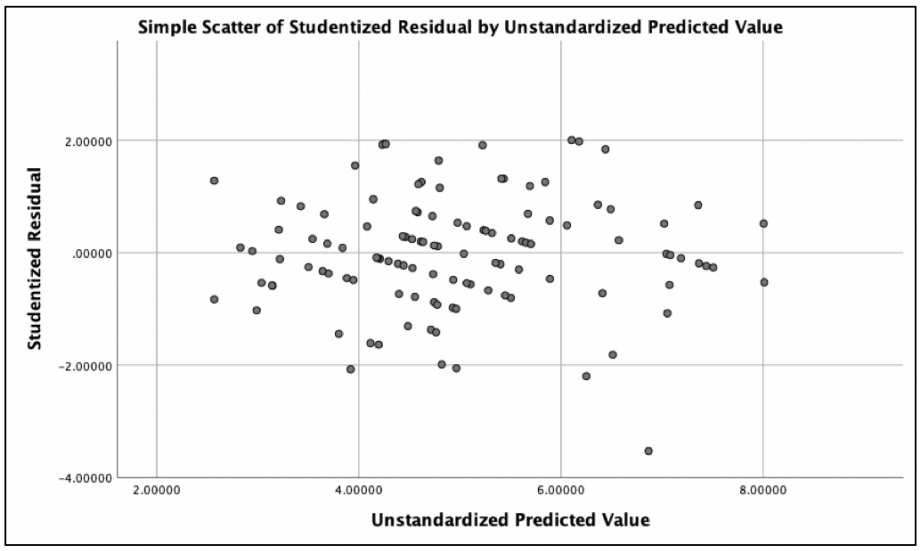


Figure C.13: Testing the Assumption of Homoscedasticity for Use of Security Measures on Laptops

Correlations

		NoMeasuresLaptop	NoAttacksAware	Likelihood	Gender	Confident	ITKnowledge	Concerned
Pearson Correlation	NoMeasuresLaptop	1.000	.389	.266	.260	.200	.384	.253
	NoAttacksAware	.389	1.000	.165	.232	.272	.291	.210
	Likelihood	.266	.165	1.000	.147	.102	.091	.428
	Gender	.260	.232	.147	1.000	.242	.314	.100
	Confident	.200	.272	.102	.242	1.000	.299	.116
	ITKnowledge	.384	.291	.091	.314	.299	1.000	.019
	Concerned	.253	.210	.428	.100	.116	.019	1.000
Sig. (1-tailed)	NoMeasuresLaptop	.	.000	.002	.003	.016	.000	.003
	NoAttacksAware	.000	.	.040	.007	.002	.001	.012
	Likelihood	.002	.040	.	.060	.140	.169	.000
	Gender	.003	.007	.060	.	.005	.000	.144
	Confident	.016	.002	.140	.005	.	.001	.109
	ITKnowledge	.000	.001	.169	.000	.001	.	.421
	Concerned	.003	.012	.000	.144	.109	.421	.
N	NoMeasuresLaptop	114	114	114	114	114	114	114
	NoAttacksAware	114	114	114	114	114	114	114
	Likelihood	114	114	114	114	114	114	114
	Gender	114	114	114	114	114	114	114
	Confident	114	114	114	114	114	114	114
	ITKnowledge	114	114	114	114	114	114	114
	Concerned	114	114	114	114	114	114	114

Figure C.14: Testing the Assumption of Multicollinearity with Correlation Coefficients for the Use of Security Measures on Laptops

Coefficients table (See Figure C.15). In this context if the tolerance value is less than 0.1 (which equates to a VIF of greater than 10) then there may be a collinearity problem. As can be seen however in this case the assumption of no multicollinearity has been met.

Assumption 7 states that there should be no significant outliers, high leverage points or highly influential points that may influence the results. These were assessed by Casewise Diagnostics in SPSS which highlights any standardised residual that is greater than + or - 3 and so could

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B		Correlations			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	-1.083	1.051		-1.031	.305	-3.166	1.000					
	NoAttacksAware	.158	.059	.239	2.675	.009	.041	.274	.389	.250	.218	.832	1.202
	Likelihood	.190	.130	.133	1.459	.147	-.068	.447	.266	.140	.119	.801	1.249
	Gender	.435	.446	.086	.976	.331	-.448	1.318	.260	.094	.080	.855	1.170
	Confident	.006	.123	.004	.050	.960	-.237	.249	.200	.005	.004	.853	1.172
	ITKnowledge	.839	.279	.272	3.005	.003	.285	1.392	.384	.279	.245	.811	1.233
	Concerned	.185	.130	.131	1.430	.156	-.072	.442	.253	.137	.117	.789	1.267

a. Dependent Variable: NoMeasuresLaptop

Figure C.15: Testing the Assumption of Multicollinearity with Tolerance/VIF Values for the Use of Security Measures on Laptops

be considered an outlier. In this case one data entry was highlighted (See Figure C.16) as one participant had used no protective measures. Whilst an outlier this was still deemed an important individual and so the data point was kept in the data sample.

Casewise Diagnostics[a]

Case Number	Std. Residual	NoMeasuresLaptop	Predicted Value	Residual
109	-3.442	.00	6.8657	-6.86571

a. Dependent Variable: NoMeasuresLaptop

Figure C.16: Testing the Assumption of No Outliers in the Data on Security Measures on Laptops

SPSS Leverage values were then used to assess for any values that had any undue influence. Fortunately none of the values were greater than 0.5 (which can be deemed risk) and so this assumption was met.

Finally, influential points were assessed using Cook's Distance values. Fortunately no Cook's Distance values above 1 and so this assumption continued to be met.

Assumption 8 then requires that for inferential statistics to be run, then the residual values need to be normally distributed. This was assessed via a histogram plot which can be seen in Figure C.17 which from visual observation suggests that this assumption was met.

The final outputs can then also be seen in Figure C.11 and are discussed in Chapter 4.

C.4.2 Predicting the Use of Security Measures on Smartphones

In order to explore whether the demographic factors that had had a significant impact could be used to predict the likelihood of individuals using more security on their smartphones a Multiple Regression analysis.

The assumptions for this test are:

1. You have one dependent variable that is measured at the continuous level. In this case the number of measures used to protect a laptop.

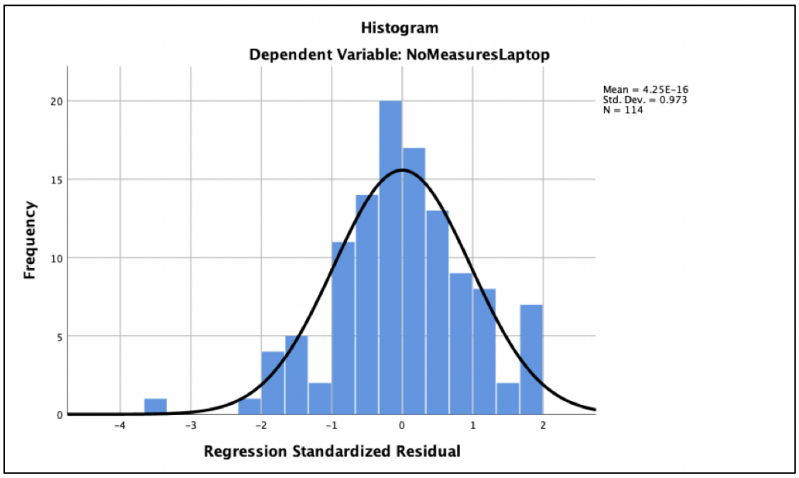


Figure C.17: Testing the Assumption of Normality in the Data on Security Measures on Laptops

2. You have two or more independent variables that are either continuous or nominal.
3. There is independence of observations.
4. There should be a linear relationship between the predictor variables and the dependent variable.
5. There should be homoscedasticity of residuals.
6. There should be no multicollinearity.
7. There should be no significant outliers, high leverage points or highly influential points.
8. The errors (residuals) should be approximately normally distributed.

Assumption 1 is true, assumption 2 was also satisfied, although in order to preserve the ranking effect the ordinal variables were considered as continuous within this test.

Assumption 3 was tested using the Durbin-Watson statistic. In this test, results close to 2 represent that there is no correlation between residuals (which is what we are looking for). In this test there was independence of residuals, as assessed by a Durbin-Watson statistic of 1.967. The results of this can be seen in the last column of Figure C.18.

Assumption 4, the assumption of linearity, in a multiple regression needs to be tested in two parts. First you need to establish whether there is a linear relationship between the dependent variables and the independent variable. This was established by only including those for which their was a statistical correlation, however scatter graph plots were also created and can be see in Figure C.12. Secondly, we need to establishing if a linear relationship exists between the dependent (number of smartphone security measures used) and the independent variables

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin–Watson
1	.471[a]	.222	.187	1.98336	1.967

a. Predictors: (Constant), Concerned, ITKnowledge, Gender, NoAttacksAware, Likelihood

b. Dependent Variable: NoMeasureSmartphone

Figure C.18: Output of the Multiple Regression Analysis for Predicting the Use of Security Measures on Smartphones

'collectively' using a scatterplot- in this case we wish for a graph with a horizontal band. This can be seen in the 5th image in Figure C.19.

Assumption 5 to test for homoscedasticity is to test that the variance is equal for all values of the predicted dependent variable. To check this we can use the plot of studentized residuals against the unstandardized predicted values. This is shown in Figure C.19 but is also shown again in Figure C.20. Here we are looking to check that the spread of the residuals does not particularly increase or decrease as you move across the predicted values. In this case, this was true and so the condition was met.

Assumption 6 requires no Multicollinearity which occurs you have two or more independent variables that are highly correlated with each other, and can lead to problems understanding which variable contributes to the variance explained. There are two approaches to identifying multicollinearity: inspection of correlation coefficients and Tolerance/VIF values. Firstly we inspect the correlations to ensure that none of the independent variable have correlations greater than 0.7. This assumption was met as can be seen in Figure C.21

Multicollinearity can also be tested by observing the 'Tolerance' and 'VIF' values in the Coefficients table (See Figure C.22). In this context if the tolerance value is less than 0.1 (which equates to a VIF of greater than 10) then there may be a collinearity problem. As can be seen however in this case the assumption of no multicollinearity has been met.

Assumption 7 states that there should be no significant outliers, high leverage points or highly influential points that may influence the results. These were assessed by Casewise Diagnostics in SPSS which highlights any standardised residual that is greater than + or - 3 and so could be considered an outlier. In this case there were no outliers and so this assumption was met.

SPSS Leverage values were then used to assess for any values that had any undue influence. Fortunately none of the values were greater than 0.5 (which can be deemed risk) and so this assumption was met.

Finally, influential points were assessed using Cook's Distance values. Fortunately no Cook's Distance values above 1 and so this assumption continued to be met.

Assumption 8 then requires that for inferential statistics to be run then the residual values

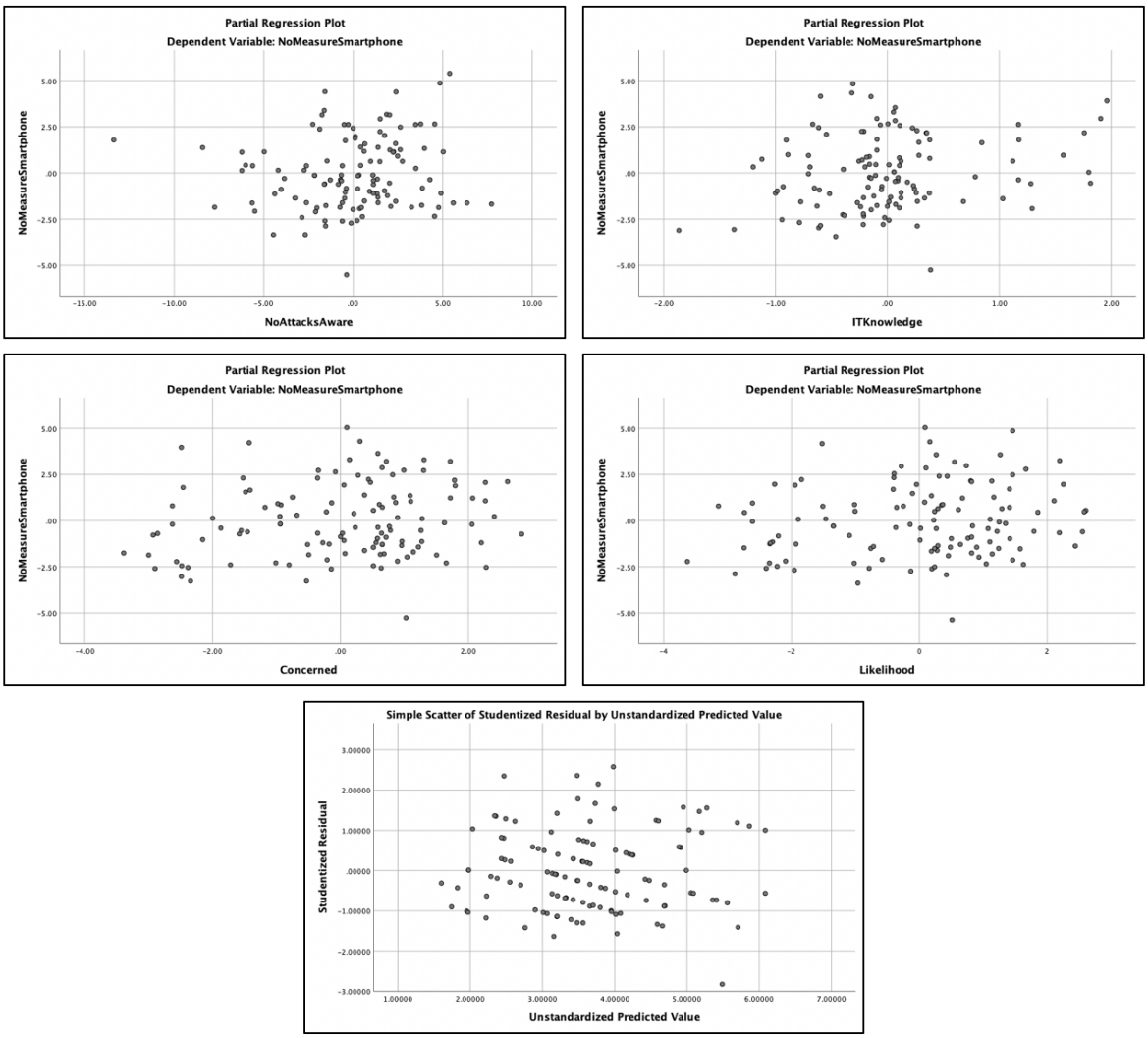


Figure C.19: Testing the Assumption of Linearity for Use of Security Measures on Smartphones

need to be normally distributed. This was assessed via a histogram plot which can be seen in Figure C.23 which from visual observation suggests that this assumption was met.

The final outputs can then also be seen in Figure C.18 and are discussed in Chapter 4.

C.5 The Relationship Between Gender and IT Knowledge

An additional Mann Whitney U test was performed to explore whether any gender differences may instead be due to differing levels of IT knowledge. This test was therefore to investigate the impact of gender on self reported IT knowledge. Again this particular statistical test has four assumptions that need to be met:

1. You have one dependent variable that is either continuous or ordinal. In this case this is

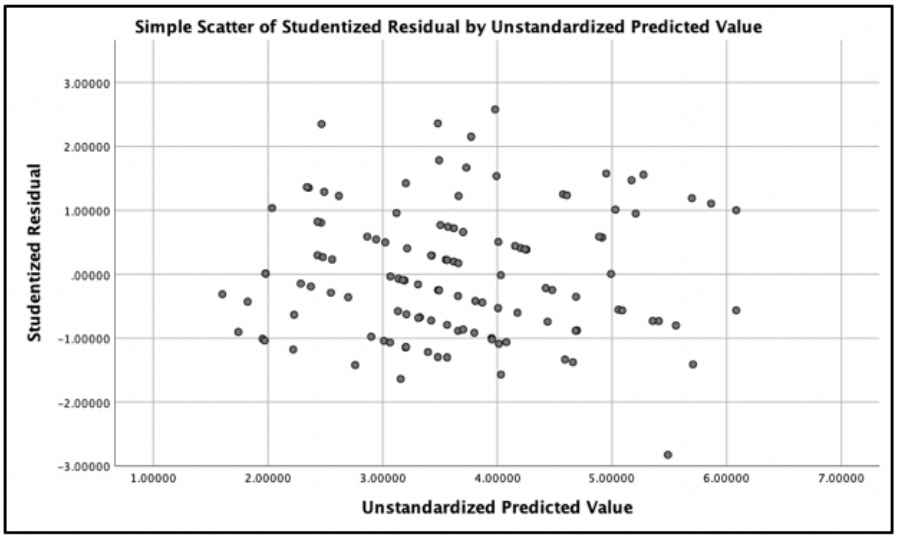


Figure C.20: Testing the Assumption of Homoscedasticity for Use of Security Measures on Smartphones

Correlations

		NoMeasureSmartphone	NoAttacksAware	Likelihood	Gender	ITKnowledge	Concerned
Pearson Correlation	NoMeasureSmartphone	1.000	.269	.292	.260	.293	.269
	NoAttacksAware	.269	1.000	.159	.240	.307	.191
	Likelihood	.292	.159	1.000	.089	.044	.462
	Gender	.260	.240	.089	1.000	.358	.057
	ITKnowledge	.293	.307	.044	.358	1.000	-.036
	Concerned	.269	.191	.462	.057	-.036	1.000
Sig. (1-tailed)	NoMeasureSmartphone	.	.002	.001	.002	.001	.002
	NoAttacksAware	.002	.	.042	.004	.000	.019
	Likelihood	.001	.042	.	.170	.318	.000
	Gender	.002	.004	.170	.	.000	.271
	ITKnowledge	.001	.000	.318	.000	.	.348
	Concerned	.002	.019	.000	.271	.348	.
N	NoMeasureSmartphone	118	118	118	118	118	118
	NoAttacksAware	118	118	118	118	118	118
	Likelihood	118	118	118	118	118	118
	Gender	118	118	118	118	118	118
	ITKnowledge	118	118	118	118	118	118
	Concerned	118	118	118	118	118	118

Figure C.21: Testing the Assumption of Multicollinearity with Correlation Coefficients for Use of Security Measures on Smartphones

self-reported IT knowledge.

2. You have one independent variable that is made up of two categorical, independent groups, in this case this is gender.

3. There needs to be no relationship between the observations in each group of the independent variable or between the groups themselves i.e. each participant only belongs to one of the

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			95.0% Confidence Interval for B		Correlations			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Lower Bound	Upper Bound	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	-1.177	1.026		-1.146	.254	-3.210	.857					
	NoAttacksAware	.070	.056	.113	1.244	.216	-.041	.181	.269	.117	.104	.846	1.181
	Likelihood	.237	.127	.176	1.868	.064	-.014	.489	.292	.174	.156	.778	1.285
	Gender	.651	.441	.133	1.474	.143	-.224	1.525	.260	.138	.123	.850	1.176
	ITKnowledge	.607	.269	.209	2.257	.026	.074	1.140	.293	.209	.188	.810	1.235
	Concerned	.221	.127	.166	1.735	.085	-.031	.473	.269	.162	.145	.762	1.312

a. Dependent Variable: NoMeasureSmartphone

Figure C.22: Testing the Assumption of Multicollinearity with Tolerance/VIF Values for Use of Security Measures on Smartphones

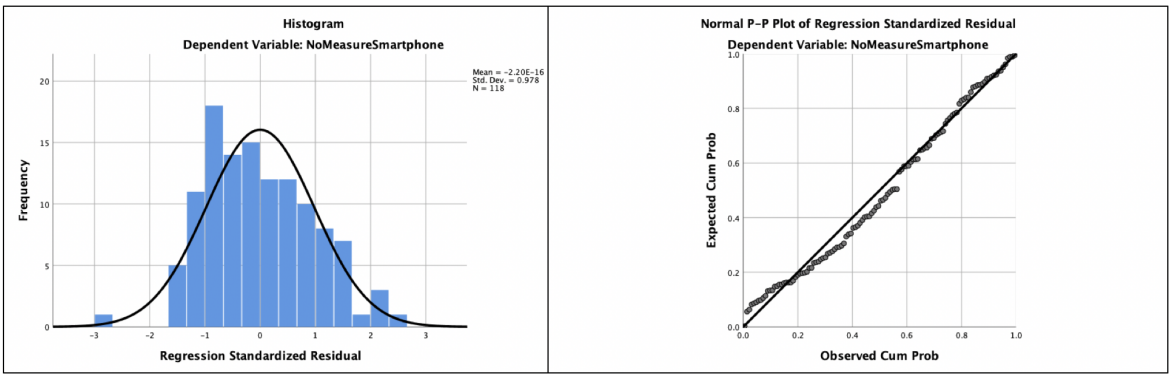


Figure C.23: Testing the Assumption of Normality in the Data on Use of Security Measures on Smartphones

groups. This assumption was met when assigning participants to groups based on gender.

4. You must determine whether the distribution of scores for both groups of your independent variable (e.g., the distribution of scores for 'males' vs 'females') have the same shape or a different shape. This determines how you interpret the results of the Mann-Whitney U test.

The data set for this test meets assumptions 1-3, the outputs (See Figure C.24) then reveals that the distribution scores are not similar across genders and so in this instance the test is used to compare mean ranks (rather than the medians).

The full outputs from this test can then be seen in Figure C.25. This test shows a statistical significance which is discussed more in Chapter 4.

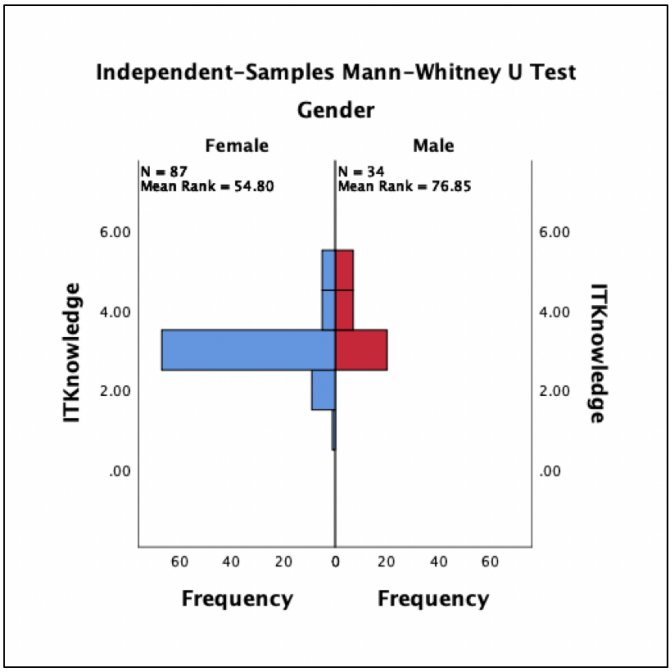


Figure C.24: Histogram Outputs to Examine IT Knowledge Across Genders

ITKnowledge across Gender

Independent-Samples Mann-Whitney U Test Summary

Total N	121
Mann-Whitney U	2018.000
Wilcoxon W	2613.000
Test Statistic	2018.000
Standard Error	137.204
Standardized Test Statistic	3.928
Asymptotic Sig.(2-sided test)	.000

Figure C.25: Mann-Whitney U Outputs for IT Knowledge by Each Gender

APPENDIX D

INTERVIEW STUDY- ETHICS PROPOSAL

This Appendix presents the approved ethics proposal for the interview study conducted in Chapter 5. The full interview protocol can also be found in Appendix E.

Lancaster University

Faculty of Science and Technology Research Ethics Committee (FSTREC)
Lancaster University

Application for Ethical Approval for Research

This form should be used for all projects by staff and research students, whether funded or not, which have not been reviewed by any external research ethics committee. If your project is or has been reviewed by another committee (e.g. from another University), please contact the FST research ethics officer for further guidance.

In addition to the completed form, you need to submit **research materials** such as:

i. Participant information sheets
ii. Consent forms
iii. Debriefing sheets
iv. Advertising materials (posters, e-mails)
v. Letters/emails of invitation to participate
vi. Questionnaires, surveys, demographic sheets that are non-standard
vii. Interview schedules, interview question guides, focus group scripts

Please note that **you DO NOT need to submit pre-existing questionnaires or standardized tests** that support your work, but which cannot be amended following ethical review. These should simply be referred to in your application form.

Please submit this form and any relevant materials **by email as** a **SINGLE attachment** to <email>

Section One

Applicant and Project Information

Name of Researcher: Emma Hewlett

Project Title: Human Factors in Cyber Security of Cyber Physical Systems- Interviews on use of personal electronic devices and use of cyber security.

Level: *PhD*

Supervisor (if applicable): Paul Taylor (psychology), Utz Roedig (computer science) and Awais Rashid (external)

Researcher's Email address: <email?>
Telephone: <phone>

Names and appointments/position of all further members of the research team:

Is this research externally funded? If yes,

ACP ID number:
Funding source:
Grant code:

Does your research project involve any of the following?

☑ Human participants (including all types of interviews, questionnaires, focus groups, records relating to humans, use of internet or other secondary data, observation etc.)

□ Animals - the term animals shall be taken to include any non-human vertebrates or cephalopods.

□ Risk to members of the research team e.g. lone working, travel to areas where researchers may be at risk, risk of emotional distress

□ Human cells or tissues other than those established in laboratory cultures

□ Risk to the environment

□ Conflict of interest

□ Research or a funding source that could be considered controversial

□ Social media and/or data from internet sources that could be considered private

□ any other ethical considerations

Yes – complete the rest of this form

No – your project does not require ethical review or submission of this form

Section Two

Type of study

☒ Includes *direct* involvement by human subjects. ***Complete all sections apart from Section 3.***

☐ Involves *existing documents/data only*, or the evaluation of an existing project with no direct contact with human participants. ***Complete all sections apart from Section 4.***

If your research involves data from chat rooms and similar online spaces where privacy and anonymity are contentious, please complete all sections

Project Details

1. Anticipated project dates (month and year)
Start date: March 2018 **End date:** February 2020

2. Please briefly describe the background to the research (no more than 150 words, in lay-person's language):
Personal electronic devices are virtually ubiquitous, however their quick advancement and the increasing use of new sensors and physical components introduces new potential cyber-security risks.

An earlier study investigated the types of technology that individuals are using and whether they take any measure to protect these devices from cyber-attacks and the findings from this work suggested that security approaches such as reading application permissions, using encryption and covering up recording devices when not in use are not widely used by many individuals. This research seeks to take this further by exploring the factors that influences an individual's decision making when they seek to secure device. It also explores the decision making behind why individuals choose to use or not use various the security measures they are aware of.

3. Please state the aims and objectives of the project (no more than 150 words, in lay-person's language):
The aim of this research is to explore the findings from a previous online survey (FST17027) in order to investigate why people make take the actions they use. The research questions are:

- Which factors weigh in on people's decisions to secure electronic devices?
- How do people decide whether to use different security measures?
- Do people perceive any barriers to using security?

4. Methodology and Analysis:
Methodology:
This study will involve interviews using both a critical decision-making approach and semi-structured questions. Interviews should typically last no more than 45 minutes and will be conducted face-to-face with participants also to draw out a timeline of decisions with the researcher.

Analysis:
This work will use qualitative approaches:

Thematic analysis: identify key themes regarding the decisions that are being made
Differences across devices: Explore themes across different types of devices to identify any similarities or differences.
Develop timeline: Identify the key times when an individual is most likely to consider security issues.

Section Three (NOT APPLICABLE)

Secondary Data Analysis

Complete this section if your project involves *existing documents/data only*, or the evaluation of an existing project with no direct contact with human participants

1. Please describe briefly the data or records to be studied, or the evaluation to be undertaken.

2. How will any data or records be obtained?

3. Confidentiality and Anonymity: If your study involves re-analysis and potential publication of existing data but which was gathered as part of a previous project involving direct contact with human beings, how will you ensure that your re-analysis of this data maintains confidentiality and anonymity as guaranteed in the original study?

4. What plan is in place for the storage of data (electronic, digital, paper, etc)? Please ensure that your plans comply with the Data Protection Act 1998.

5. What are the plans for dissemination of findings from the research?

6a. Is the secondary data you will be using in the public domain? YES/NO
6b. If NO, please indicate the original purpose for which the data was collected, and comment on whether consent was gathered for additional later use of the data.

7.What other ethical considerations (if any), not previously noted on this application, do you think there are in the proposed study? How will these issues be addressed?

8a. Will you be gathering data from discussion forums, on-line 'chat-rooms' and similar online spaces where privacy and anonymity are contentious? YES/NO

If yes, your project requires full ethics review. Please complete all sections.

Section Four

Participant Information

Complete this section if your project includes *direct* involvement by human subjects.

1. Please describe briefly the **intended human participants** (including number, age, gender, and any other relevant characteristics):
This study will aim to initially recruit 20 individuals to take part in the interviews, however should new topics still be emerging then this number will be increased until it is believed that data saturation has been achieved (no new topics or points of view are emerging). To maximise getting a range of views male and female participants will be recruited from a range of ages. All participants must own a computer or laptop and a smartphone.

2. How will participants be **recruited** and from where?
Initially participants will be recruited via:

- The Lancaster Psychology Research Participation System- SONA
- Flyers placed around campus
- Adverts posted online via social networks

Individuals will then need to declare their interest in the study at which point if recruitment is still ongoing they will be offered timeslots to take part.

Additionally, some participants will be recruited from individuals who took part in an earlier online survey and who stated that they would be interested in taking part in future research. This was a total of twenty-five individuals and this pool of individuals will be used to try and make the demographic splits more even. These participants will be approached via the email address they left for this purpose, which will inform them of the study and invite them to reply if they wish to take part.

Once data saturation has been achieved then any new potential participants will be turned away.

3. Briefly describe your **data collection methods**, drawing particular attention to any potential ethical issues.
Data will be collected via semi-structured interviews, which will be audio-recorded.

Consent for the voice recording will be gained at the start of the interview and recordings will be transcribed within six weeks. Audio recordings will not be stored with any identifiable information.

4. Consent
4a. Will you take all necessary steps to **obtain the voluntary and informed consent** of the prospective participant(s) or, in the case of individual(s) not capable of giving informed consent, the permission of a legally authorised representative in accordance with applicable law? **YES**
If yes, please go to question 4b. If no, please go to question 4c.

4b. Please explain the procedure you will use for **obtaining consent**?. If applicable, please explain the procedures you intend to use to gain permission on behalf of participants who are unable to give informed consent.
Individuals who volunteer to take part in the research will be given a copy of the Participant Information Sheet (see Appendices) to read and be given the opportunity to ask any questions that they may have. If they are still happy to take part then they will be given two consent forms to sign (one for themselves and one for the experimenter).

4c. If it will be necessary for participants to take part in the study **without their knowledge and consent at the time**, please explain why (for example covert observations may be necessary in some settings; some experiments require use of deception or partial deception – not telling participants everything about the experiment).
Not applicable- participants will be fully informed before giving consent.

5. Could participation cause **discomfort** (physical and psychological e.g. distressing, sensitive or embarrassing topics), **inconvenience or danger beyond the risks encountered in normal life**? Please indicate plans to address these potential risks. State the timescales within which participants may withdraw from the study, noting your reasons.
The topics covered in this study are not sensitive or likely to cause any discomfort, however there is a small possibility that this study could cause a participant some concern regarding their vulnerability

to a cyber-attack. At the end of the study participants will therefore be given a debrief sheet which will point them towards information sources regarding how best to protect their devices (https://www.cyberaware.gov.uk/).

Participants will be told that they may withdraw at any point during the interview and for two weeks after the interview, by contacting the researcher (contact details will be provided on the debrief sheet). After two weeks recordings will start to be transcribed and withdrawal will no longer be possible.

6. How will you protect participants' **confidentiality and/or anonymity** in data collection (e.g. interviews), data storage, data analysis, presentation of findings and publications?
Participants will be kept anonymous, with transcripts and any quotes in reports using pseudonyms. Additionally, no personal information (such as demographics) will be contained with any of the transcripts so that individuals cannot be identified.

There is a very small chance that in the discussion about cyber-attacks an individual may raise examples of them engaging in malicious or bullying behaviours which could require a breach of confidentiality. The participant information sheet raises this possibility and asks that participants do not discuss these topics.

7. Do you anticipate any ethical constraints relating to **power imbalances or dependent relationships**, either with participants or with or within the research team? If yes, please explain how you intend to address these?
No power imbalances are identified, individuals being targeted for recruitment are not the subordinate of the researcher in any way.

8. What potential **risks may exist for the researcher** and/or research team? Please indicate plans to address such risks (for example, noting the support available to you/the researcher; counselling considerations arising from the sensitive or distressing nature of the research/topic; details of the lone worker plan you or any researchers will follow, in particular when working abroad.
The researcher will be meeting with participants alone so there is a small risk, however this will be mitigated by holding all the interviews in university office-buildings during the working day.

9. Whilst there may not be any significant direct **benefits to participants** as a result of this research, please state here any that may result from participation in the study.
There are no direct benefits to taking part in this research, however participants will be offered £5 for taking part.

10. Please explain the **rationale for any incentives/payments** (including out-of-pocket expenses) made to participants:
Participants will be offered £5 to remunerate them for their time, and to encourage participation.

11. What are your plans for the **storage of data** (electronic, digital, paper, etc.)? Please ensure that your plans comply with the Data Protection Act 1998.
Voice recordings will be stored digitally on the University server, in the researcher's university folder until graduation and would only be shared in the event of publication reviewers needing to audit data. Following graduation- the recordings will be destroyed.

Demographic data and transcripts will be recorded digitally and stored on the University server, in the researcher's university folder until graduation. Following graduation, the data will be made available

via Pure where it will be available for a minimum of 10 years. Stored data will be available to the researcher and supervisors.

12. Please answer the following question *only* if you have not completed a Data Management Plan for an external funder.

12.a How will you make your data available under open access requirements?
At graduation or at publication, data will be made available through Pure. Data will also be offered to the UK Data Archive as per the standard ESRC procedures (the consent page will declare that by submitting data participants give consent for the data to be shared.)

12b. Are there any restrictions on sharing your data for open access purposes?
Original voice recordings will not be shared except in the event of an audit- any identifiable data such as names will be omitted.

13. Will **audio or video recording** take place? ☐ no ☑ audio ☐ video

13a. Please confirm that portable devices (laptop, USB drive etc) will be **encrypted** where they are used for identifiable data. If it is not possible to encrypt your portable devices, please comment on the steps you will take to protect the data.
Recordings will be made on a portable voice recorder- before being transferred either directly onto the University server, or if necessary onto a password protected laptop (with the recordings encrypted using 7-zip software) until they can be placed on the University server. Upon transfer the recording will be removed from the portable device.

13b. What arrangements have been made for **audio/video data storage**? At what point in the research will tapes/digital recordings/files be destroyed?
Audio data will be stored on the University server until publication of the thesis at which point they will be destroyed. Transcripts will be retained in line with question 11 and destroyed at graduation.

13c. If your study includes video recordings, what are the implications for participants' anonymity? Can anonymity be guaranteed and if so, how? If participants are identifiable on the recordings, how will you explain to them what you will do with the recordings? How will you seek consent from them?
Not applicable

14. What are the plans for dissemination of findings from the research? If you are a student, mention here your thesis. Please also include any impact activities and potential ethical issues these may raise.
Results from the research may be submitted for publication in an academic/professional journals, for presentation at conferences/ seminars and will also be included in my PhD thesis.

15. What particular ethical considerations, not previously noted on this application, do you think there are in the proposed study? Are there any matters about which you wish to seek guidance from the FSTREC?
All issues have been discussed.

Section Five

Additional information required by the university insurers

If the research involves either the nuclear industry or an aircraft or the aircraft industry (other than for transport), please provide details below:
Not applicable

Section Six

Declaration and Signatures

I understand that as Principal Investigator/researcher/PhD candidate I have overall responsibility for the ethical management of the project and confirm the following:

- I have read the Code of Practice, Research Ethics at Lancaster: a code of practice and I am willing to abide by it in relation to the current proposal.
- I will manage the project in an ethically appropriate manner according to: (a) the subject matter involved and (b) the Code of Practice and Procedures of the University.
- On behalf of the University I accept responsibility for the project in relation to promoting good research practice and the prevention of misconduct (including plagiarism and fabrication or misrepresentation of results).
- On behalf of the University I accept responsibility for the project in relation to the observance of the rules for the exploitation of intellectual property.
- If applicable, I will give all staff and students involved in the project guidance on the good practice and ethical standards expected in the project in accordance with the University Code of Practice. (Online Research Integrity training is available for staff and students here.)
- If applicable, I will take steps to ensure that no students or staff involved in the project will be exposed to inappropriate situations.
- I confirm that I have completed all risk assessments and other Health and Safety requirements as advised by my departmental Safety Officer.

☑ Confirmed

Please note: If you are not able to confirm the statement above please contact the FST Research Ethics Committee and provide an explanation.

Student applicants:
Please tick to confirm that you have discussed this application with your supervisor, and that they agree to the application being submitted for ethical review ☒
Students must submit this application from your Lancaster University email address, and copy your supervisor in to the email in which you submit this application

All Staff and Research Students must complete this declaration:
I confirm that I have sent a copy of this application to my Head of Department (or their delegated representative) . **Tick here to confirm** ☒

Name of Head of Department *(or their delegated representative)* Adrian Friday (HoD) via Claire Ann Oulton (Postgraduate Coordinator)

Applicant electronic signature: Emma Hewlett Date 21/03/2018

Advertisement Materials

Online SONA Advert (Psychology research participant system)

Study Name	Interview study- cyber security knowledge and levels of concern
Study Type	Standard (lab) study
Pay	£5
Duration	45 mins
Description	This study is a interview investigating knowledge and concerns about different types of cyber-attacks. You will be asked about what security precautions you take online and be presented with several scenarios to discuss.
Eligibility	Native English speaker or highly fluent in English; 18+ years Must own a computer/laptop AND a smartphone
Researcher	Emma Hewlett
Deadlines	Sign-Up: 12 hours before the appointment Cancellation: 12 hours before the appointment

To help with recruiting an even sample- the advert may change to males only (or vice versa) if recruitment is skewed towards one gender.

Advert/ Flyer (For distribution on Campus)

Own a computer/laptop and a smartphone?
Take part in an interview study- Earn £5

Come and discuss you use of technology and cyber security and earn £5 for 45 minutes of your time. If you're interested then contact Emma Hewlett on <email>.

School of Computing and Communications

Participant information sheet

I am a PhD student at Lancaster University and I would like to invite you to take part in an interview investigating knowledge of cyber-attacks and cyber security methods

Please take time to read the following information carefully before you decide whether or not you wish to take part.

What is the study about?
This study aims to explore the degree to which people perceive different devices to be vulnerable to cyber-attacks and the reason that people have for using (or not using) different security measures.

Why have I been invited?
You have been approached, either because you have responded to an advert or you gave your permission to be invited to future studies when you completed an earlier survey.

What will I be asked to do if I take part?
If you decide to take part, the interview will involve a series of questions, and your responses will be explored in detail, some of these questions will involve reading from lists and discussing these topics.

What are the possible benefits from taking part?
There are no specific benefits to you taking part in this study, however you will be given £5 as a thank you for your time.

Do I have to take part?
No. It's completely up to you to decide whether or not you take part. Your participation is voluntary, and you are free to withdraw at any time during the study, without giving any reason and without any adverse consequence.

If you decide not to take part in this study, this will not affect your studies and the way you are assessed on your course.

What if I change my mind?
You may withdraw at any time during the interview, you may also withdraw your data at anytime for up to two weeks after the experiment, at which point data may transcribed and analysed. If you wish to withdraw you will need to contact the researcher, using the details below, and provide your participant reference number so please keep a record of this.

What are the possible disadvantages and risks of taking part?
There should be no major disadvantages to taking part, however please note that in the unlikely event that you declare that you have been involved in malicious online behaviours e.g. cyber bullying that these may need to be reported and confidentiality may be breached. Please therefore avoid mention of any illegal behaviours, or behaviours against the university code of conduct.

In addition this study may take around 45 minutes of your time.

Will my data be identifiable?
After the interview only myself, the researcher conducting this study, and my supervisors will have access to the data you share with me.

I will keep all personal information about you (e.g., your name and other information about you that can identify you) confidential, that is I will not share it with others. I will anonymise any audio recordings and hard copies of any data. This means that I remove any personal information.

Note: In the unlikely event that you reference engaging in bullying or illegal behaviour it may require anonymity and confidentiality to be broken.

How will my data be stored?
Your data will be stored securely on the university system or in encrypted files (that is no-one other than me, the researcher will be able to access them) on password-protected computers.

In accordance with University guidelines, I will keep the data securely for a minimum of ten years.

How will we use the information you have shared with us and what will happen to the results of the research study?
The data that you share will only be used for academic purposes, this may include:

- My PhD thesis
- Academic journal papers
- Conference proceedings

When writing up the findings from this study, I would like to reproduce some of the views and ideas you shared with me. When doing so, I will only use anonymised quotes (e.g. from our interview with you), so that although I will use your exact words, you cannot be identified in our publications.

Who has reviewed the project?
This study has been reviewed and approved by the Faculty of Science and Technology Research Ethics Committee.

What if I have a question or concern?

If you have any queries or if you are unhappy with anything that happens concerning your participation in the study, please contact myself (Emma Hewlett) at: <email>**;**
Please be aware that after two weeks data will be pooled and it may no longer possible to identify and remove.

Alternatively, you may contact my supervisor Prof. Utz Roedig at:<email>;

If you have any concerns or complaints that you wish to discuss with a person who is not directly involved in the research, you can also contact Prof. Adrian Friday: <email>; or <phone>.
Infolab21, Lancaster University

Thank you for considering your participation in this project.

CONSENT FORM

Project Title: Human Factors in Cyber Physical Systems

Name of Researchers: Emma Hewlett
Email: <email>

Please tick each box

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily ☐
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason or experiencing any adverse consequence. If I withdraw within 2 weeks of commencement of the study my data will be removed. ☐
3. I understand that any information given by me may be used in future reports, academic articles, publications or presentations by the researcher/s, but my personal information will not be included and I will not be identifiable. ☐
4. I understand that confidentiality and anonymity may be breached if you discuss engaging in any malicious behaviours online. ☐
5. I understand that my name and my organisation's name will not appear in any reports, articles or presentation without my consent. ☐
6. I understand that audio recording will occur throughout the interview and that this will be transcribed with data protected on encrypted devices and kept secure. ☐
7. 'I consent that my data (including anonymised interview transcript) can be made open access (NB: You are free to leave this box unchecked and to still participate in the study). ☐
8. I understand that data will be kept according to University guidelines for a minimum of 10 years after the end of the study. ☐
9. I agree to take part in the above study. ☐

_____	_____	_____
Name of Participant	Date	Signature

I confirm that the participant was given an opportunity to ask questions about the study, and all the questions asked by the participant have been answered correctly and to the best of my ability. I confirm that the individual has not been coerced into giving consent, and the consent has been given freely and voluntarily.

Signature of Researcher /person taking the consent_____ **Date**

_____ Day/month/year

One copy of this form will be given to the participant and the original kept in the files of the researcher at Lancaster University

Interview Schedule

Interview Approach:

Critical Decision Making to explore: Walking through security decisions and exploring in depth key decision points, goals and final actions and how these fit into an overall timeline.

Semi-structured Interviews: To explore approaches people are aware of but don't use and why.

Interview Schedule (CDM):

1. In this interview I will be exploring your use of cyber security on different devices, can you confirm that you own both a computer or a laptop and a smartphone?
2. Do you own any additional 'smart' or internet enabled devices?
    a. If yes, discuss one to use within the interview
3. Please confirm your gender and age:

(Repeat questions for: computer/laptop; smart phone; and one additional IoT/ smart device if applicable)

4. Can you walk me through how you protected/ currently protect your device, including when you implemented them and if you still take any additional actions?
    a. Did you look into security before buying the device?
    b. Do any of your security approaches require you to continue taking any regular action?

[A timeline will then be drawn from the responses e.g. research before buying, during set-up, ongoing security actions or following any security incidents, with detail for each section, seeking input from the participant]. For each of the decisions to use a security approach the following questions will then be asked:

5. What was your motivation for using this approach?
6. Did you consider using any other security methods instead of this one? Why did you reject these approaches?
7. Where did you get information regarding this approach from?
8. What types of attacks do you hope that this approach will protect you from?
9. Did you experience any problems or barriers in seeking to use this approach?

[Once timelines have been established, the following questions will be asked where appropriate]

10. You've used approach X for device Y, but not device Z can you explain the reasoning behind this?
11. Are you happy with the level of security you have achieved for your device? Why?

Interview schedule (part2):

12. Are you aware of any additional security approaches that we have not discussed?
    a. Do you use any of these approaches in addition to the ones we discussed? (Link to Q4-8)

   b. What were your reasons for not using these approaches?
13. For each device discussed can you rank the approaches that you use, based on how important they are? Please explain why you think each approach is more important than those below it.
14. Where would you go to find out further security information?
15. Are there any barriers that prevent you from using security approaches?

Lancaster University

Debrief

School of Computing and Communications

Debrief sheet- Human Factors in Cyber Security of Cyber Physical Systems

Thank you for participating in this interview, we hope that you found it interesting and have not been upset or worried by the topics discussed.

What if I have a question or would like to withdraw?
If you have any queries or if you are unhappy with anything that happens concerning your participation in the study, please contact myself (Emma Hewlett) at: <email>
Please be aware that after two weeks data will be pooled and it may no longer possible to identify and remove.

Alternatively, you may contact my supervisor Prof. Utz Roedig at: <email>.

If you have any concerns or complaints that you wish to discuss with a person who is not directly involved in the research, you can also contact Prof. Adrian Friday:
<email>;
<phone>;
Infolab21, Lancaster University

Additional information:
If you would like more information on the cyber threats that are faced by Cyber Physical Systems then this can be found at the following government website:
https://www.cyberaware.gov.uk/

Finally if you would like to be provided with a brief summary of the findings once the study is complete, then please contact me at: <email>

Thank you for your participation in this project.

APPENDIX E

INTERVIEW STUDY SCRIPT

This Appendix presents the interview schedule used in the study detailed in Chapter 5. Interviews were semi-structured and used a critical decision making approach was taken.

E.1 Interview Schedule

Q1. In this interview I will be exploring your use of cyber security on different devices, can you confirm that you own both a computer or a laptop and a smartphone?

Q2a. Do you own any additional 'smart' or internet enabled devices?

Q2b. If yes, discuss one to use within the interview

(Repeat questions for: computer/laptop; smart phone; and one additional IoT/ smart device if applicable)

Q3. Please confirm your gender and age

Q4a. Can you walk me through how you protected/ currently protect your device, including when you implemented them and if you still take any additional actions?

Q4b. Did you look into security before buying the device?

Q4c. Do any of your security approaches require you to continue taking any regular action?

[A timeline was then drawn from the responses e.g. research before buying, during set-up, ongoing security actions or following any security incidents. participants were asked to review these timelines and make any corrections or additions as necessary]. For each of the decisions to use a security approach the following questions were then asked:

Q5. What was your motivation for using this approach?

Q6. Did you consider using any other security methods instead of this one? Why did you reject these approaches?

Q7. Where did you get information regarding this approach from?

Q8. What types of attacks do you hope that this approach will protect you from?

Q9. Did you experience any problems or barriers in seeking to use this approach?

Once questions 5 to 9 had been asked for each device, the following questions were asked to explore differences in security approaches across each of the devices.

Q10. You have used approach X for device Y, but not device Z can you explain the reasoning behind this?

Q11. Are you happy with the level of security you have achieved for your devices? Why?

Q12a. Are you aware of any additional security approaches that we have not discussed?

Q12b. Do you use any of these approaches in addition to the ones we discussed? (If yes, link bank to Q5-9)

Q12c. What were your reasons for not using these approaches?

Q13. For each device discussed can you rank the approaches that you use, based on how important they are? Please explain why you think each approach is more important than those below it.

Q14. Where would you go to find out further security information?

Q15. Are there any barriers that prevent you from using security approaches?

APPENDIX F

DETECTING ATTACKS AGAINST HOME DEVICES- ETHICS PROPOSAL

This Appendix presents the approved ethics proposal for the experimental study on attacks against home devices conducted in Chapter 6.

Lancaster University

Faculty of Science and Technology Research Ethics Committee (FSTREC)
Lancaster University

Application for Ethical Approval for Research

This form should be used for all projects by staff and research students, whether funded or not, which have not been reviewed by any external research ethics committee. If your project is or has been reviewed by another committee (e.g. from another University), please contact the FST research ethics officer for further guidance.

In addition to the completed form, you need to submit **research materials** such as:

i. Participant information sheets
ii. Consent forms
iii. Debriefing sheets
iv. Advertising materials (posters, e-mails)
v. Letters/emails of invitation to participate
vi. Questionnaires, surveys, demographic sheets that are non-standard
vii. Interview schedules, interview question guides, focus group scripts

Please note that **you DO NOT need to submit pre-existing questionnaires or standardized tests** that support your work, but which cannot be amended following ethical review. These should simply be referred to in your application form.

Please submit this form and any relevant materials **by email as** a **SINGLE attachment** to <email>.

Section One

Applicant and Project Information

Name of Researcher: Emma Hewlett

Project Title: Human Factors in Cyber Security of Cyber Physical Systems- Detection of attacks against computer systems and IoT devices (Website Study)

Level: *PhD*

Supervisor (if applicable): Paul Taylor (psychology), Utz Roedig (computer science) and Awais Rashid (external)

Researcher's Email address: <email>
Telephone: <phone>

Address: B59, Infolab

Names and appointments/position of all further members of the research team:

Is this research externally funded? If yes, *No*

ACP ID number:
Funding source:
Grant code:

Does your research project involve any of the following?

☑ Human participants (including all types of interviews, questionnaires, focus groups, records relating to humans, use of internet or other secondary data, observation etc.)

□ Animals - the term animals shall be taken to include any non-human vertebrates or cephalopods.

□ Risk to members of the research team e.g. lone working, travel to areas where researchers may be at risk, risk of emotional distress

□ Human cells or tissues other than those established in laboratory cultures

□ Risk to the environment

□ Conflict of interest

□ Research or a funding source that could be considered controversial

□ Social media and/or data from internet sources that could be considered private

□ any other ethical considerations

Yes – complete the rest of this form

No – your project does not require ethical review or submission of this form

Section Two

Type of study

☒ Includes *direct* involvement by human subjects. ***Complete all sections apart from Section 3.***

☐ Involves *existing documents/data only*, or the evaluation of an existing project with no direct contact with human participants. ***Complete all sections apart from Section 4.***

If your research involves data from chat rooms and similar online spaces where privacy and anonymity are contentious, please complete all sections

Project Details

1. Anticipated project dates (month and year)
Start date: Oct 2018 **End date:** Feb 2020

2. Please briefly describe the background to the research (no more than 150 words, in lay-person's language):
Early work has established that many people don't protect various cyber physical devices and that they often lack security knowledge regarding how these devices are vulnerable and how they could be attacked. This study therefore looks to explore whether the lack of security knowledge regarding these devices translates into people being less likely to detect a range of cyber-attack against these devices.

3. Please state the aims and objectives of the project (no more than 150 words, in lay-person's language):
The aim of this study is to explore whether people can identify attacks against physical devices that may be present in a home or office environment such as a smart camera or artificial assistant. The study also presents several traditional attack scenarios in order to explore whether these attacks are more likely to be identified.

4. Methodology and Analysis:

Methodology:
This work will involve a lab study, conducted at the university.

1. Participants will all have volunteered and arranged a time to attend and should therefore be aware of the study topic. On arrival they will be given be the full participant information sheet and given the chance to ask any questions, before being asked to sign two consent forms (one copy for the researcher and one copy for themselves) if they still wish to take part.

2. Participants will then be seated at a computer and given instructions asking them to work through a series of webpages containing personality questions or instructions to explore the site contained at a link. They will be informed that they may encounter one or more cyber attacks.

3. They will be given a basic demographic question page, they will then be shown the following pages in a randomised order with each page followed by some questions on whether they believed a cyber attack occurred on that page:

    - Page 1: Link to an email account with a phishing email
    - Page 2: Link to an email account without a phishing email (Email control)
    - Page 3: Questionnaire and pop-up asking to run an exe. file
    - Page 4: Questionnaire and modal pop-up asking if they would like to provide feedback on the website (pop-up control)
    - Page 5: Questionnaire and symbol that if examined will state that keyboard logging is occurring

- Page 6: Questionnaire and IoT camera LED switched on
- Page 7: Questionnaire and audio (Cortana/ Siri start up sound)
- Page 8 and 9: Questionnaire, no events (controls)

4. Once participants have completed the study participants will be fully debriefed about the study. After being given the opportunity to ask any questions that they may have they will be given a debrief sheet to take away. The total amount of time taken for this experiment should be approximately 20 minutes.

Analysis

Analysis of this data will be exploratory and largely descriptive, recording which issues people notice, and how likely people are that it is a malicious event. It will also explore whether when primed to consider security people falsely identify attacks when there aren't any.

To test for any significant differences across detection of different types of attacks a Cochrans Q analysis will be done. this test examines whether there is a difference on a dichotomous dependent variable across three or more related groups. This will allow all the conditions involving a different attack to be examined against each other and identify if the percentage of people detecting an attack differs for different attack conditions.

If any significant findings are found then further post-hoc tests will be conducted to identify which finding(s) are significant. These tests will be Dunn's post hoc tests or multiple McNemars tests, dependent on whether the results meet certain assumptions. The data will also be explored descriptively looking at the number of detections for each attack.

Section Three- Not Applicable

Secondary Data Analysis

Complete this section if your project involves *existing documents/data only*, or the evaluation of an existing project with no direct contact with human participants

1. Please describe briefly the data or records to be studied, or the evaluation to be undertaken.

2. How will any data or records be obtained?

3. Confidentiality and Anonymity: If your study involves re-analysis and potential publication of existing data but which was gathered as part of a previous project involving direct contact with human beings, how will you ensure that your re-analysis of this data maintains confidentiality and anonymity as guaranteed in the original study?

4. What plan is in place for the storage of data (electronic, digital, paper, etc)? Please ensure that your plans comply with the Data Protection Act 1998.

5. What are the plans for dissemination of findings from the research?

6a. Is the secondary data you will be using in the public domain? YES/NO
6b. If NO, please indicate the original purpose for which the data was collected, and comment on whether consent was gathered for additional later use of the data.

7.What other ethical considerations (if any), not previously noted on this application, do you think there are in the proposed study? How will these issues be addressed?

8a. Will you be gathering data from discussion forums, on-line 'chat-rooms' and similar online spaces where privacy and anonymity are contentious? YES/NO

If yes, your project requires full ethics review. Please complete all sections.

Section Four

Participant Information

Complete this section if your project includes *direct* involvement by human subjects.

1. Please describe briefly the **intended human participants** (including number, age, gender, and any other relevant characteristics):
The minimum sample size for using the Cochrans Q test is:
$nk \geq 24$ and $n \geq 4$ where n is the participant number and k is the number of related groups (or trials)[1].

Only a small number of individuals are required therefore, and this would be in line with similar research by Alsharnouby et al. (2015) whose phishing role-play study used 21 participants[2], however many researchers in this area have used larger sample sizes for their detections studies. Work into phishing detection by Canfield (2016)[3] used 152 participants and work by Parsons (2017)[4] used 117.

Based on current research trends within the topic area this work will aim to recruit beyond the minimum sample requirement and aim to recruit closer to 50 participants.

[1] Tate, M. W. & Brown, S. M. (1970). Note on the Cochran Q test. *Journal of the American Statistical Association*, *65*, 155-160
[2] Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69-82.
[3] Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human factors*, *58*(8), 1158-1172.
[4] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, *52*, 194-206.

2. How will participants be **recruited** and from where?
Participants will be recruited mainly from the university population using SONA (the psychology research recruitment portal), posters across the university campus and social media.

3. Briefly describe your **data collection methods**, drawing particular attention to any potential ethical issues.
Data will be collected from participants via the webpages that they will be using as part of the study. They will also be asked to complete some demographic questions including, age, gender and whether they are a student.

4. Consent
4a. Will you take all necessary steps to **obtain the voluntary and informed consent** of the prospective participant(s) or, in the case of individual(s) not capable of giving informed consent, the permission of a legally authorised representative in accordance with applicable law? **YES**
If yes, please go to question 4b. If no, please go to question 4c.

4b. Please explain the procedure you will use for **obtaining consent**?. If applicable, please explain the procedures you intend to use to gain permission on behalf of participants who are unable to give informed consent.
Participants will be provided with a participant information sheet that will provide details on the study intentions and that they may be presented with some cyber attacks. Having read the information sheet and been given the opportunity to ask questions participants will be asked to sign two consent forms (one copy for the researcher and one for their own records), they will be informed that they can withdraw at any point prior to and during the study.

4c. If it will be necessary for participants to take part in the study **without their knowledge and consent at the time**, please explain why (for example covert observations may be necessary in some settings; some experiments require use of deception or partial deception – not telling participants everything about the experiment).

5. Could participation cause **discomfort** (physical and psychological eg distressing, sensitive or embarrassing topics), **inconvenience or danger beyond the risks encountered in normal life**? Please indicate plans to address these potential risks. State the timescales within which participants may withdraw from the study, noting your reasons.
This study will not introduce any danger or risk beyond that typically encountered during an office environment. There is however a small chance that participants will become concerned about cyber security issues and so at the end of the study they will be offered a debrief form that includes information on cyber attacks if they have any ongoing concerns.

Participants will be informed that they are free to withdraw at any point during the study with no consequences. They will also be told that they can withdraw their data for up to two weeks following the study but that after this point data may be pooled together so that this is no longer possible. They will be reminded of this right on the debriefing form.

6. How will you protect participants' **confidentiality and/or anonymity** in data collection (e.g. interviews), data storage, data analysis, presentation of findings and publications?
All data from this study will be anonymised, names will only be included on the consent forms and these will be stored separately to the results.

7. Do you anticipate any ethical constraints relating to **power imbalances or dependent relationships**, either with participants or with or within the research team? If yes, please explain how you intend to address these?
No power imbalances are identified, individuals being targeted for recruitment are not the subordinate of the researcher in any way.

8. What potential **risks may exist for the researcher** and/or research team? Please indicate plans to address such risks (for example, noting the support available to you/the researcher; counselling considerations arising from the sensitive or distressing nature of the research/topic; details of the lone worker plan you or any researchers will follow, in particular when working abroad.
The researcher will be meeting with participants alone so there is a small risk, however this will be mitigated by conducting all the studies in university office-buildings during the working day.

9. Whilst there may not be any significant direct **benefits to participants** as a result of this research, please state here any that may result from participation in the study.
There are no direct benefits to taking part in this research, however participants will be offered £3.50 for taking part.

10. Please explain the **rationale for any incentives/payments** (including out-of-pocket expenses) made to participants:
Participants will be offered £3.50 to remunerate them for their time, and to encourage participation.

11. What are your plans for the **storage of data** (electronic, digital, paper, etc.)? Please ensure that your plans comply with the Data Protection Act 1998.
Questionnaire data (from the personality questions on the webpages, questions on whether attacks were detected and the demographic questionnaire) will be stored on the university servers in the researcher's university folder until graduation. Following graduation, the data will be made available via Pure where it will be available for a minimum of 10 years. Stored data will be available to the researcher and supervisors.

12. Please answer the following question *only* if you have not completed a Data Management Plan for an external funder.

12.a How will you make your data available under open access requirements?
At graduation or at publication, data will be made available through Pure.

12b. Are there any restrictions on sharing your data for open access purposes?
None are foreseen.

13. Will **audio or video recording** take place? ☑ no □ audio ☐ video

13a. Please confirm that portable devices (laptop, USB drive etc) will be **encrypted** where they are used for identifiable data. If it is not possible to encrypt your portable devices, please comment on the steps you will take to protect the data.
No recordings are taken place

13b. What arrangements have been made for **audio/video data storage**? At what point in the research will tapes/digital recordings/files be destroyed?
No arrangements have been made, as no recordings will be made or stored.

13c. If your study includes video recordings, what are the implications for participants' anonymity? Can anonymity be guaranteed and if so, how? If participants are identifiable on the recordings,

how will you explain to them what you will do with the recordings? How will you seek consent from them?
N/a as no recordings will be made during the study

14. What are the plans for dissemination of findings from the research? If you are a student, mention here your thesis. Please also include any impact activities and potential ethical issues these may raise.
Results from the research may be submitted for publication in an academic/professional journals, for presentation at conferences/ seminars and will also be included in my PhD thesis.

15. What particular ethical considerations, not previously noted on this application, do you think there are in the proposed study? Are there any matters about which you wish to seek guidance from the FSTREC?
No additional ethical risks are identified

Section Five

Additional information required by the university insurers

If the research involves either the nuclear industry or an aircraft or the aircraft industry (other than for transport), please provide details below:

Section Six

Declaration and Signatures

I understand that as Principal Investigator/researcher/PhD candidate I have overall responsibility for the ethical management of the project and confirm the following:

- I have read the Code of Practice, Research Ethics at Lancaster: a code of practice and I am willing to abide by it in relation to the current proposal.
- I will manage the project in an ethically appropriate manner according to: (a) the subject matter involved and (b) the Code of Practice and Procedures of the University.
- On behalf of the University I accept responsibility for the project in relation to promoting good research practice and the prevention of misconduct (including plagiarism and fabrication or misrepresentation of results).
- On behalf of the University I accept responsibility for the project in relation to the observance of the rules for the exploitation of intellectual property.
- If applicable, I will give all staff and students involved in the project guidance on the good practice and ethical standards expected in the project in accordance with the University Code of Practice. (Online Research Integrity training is available for staff and students here.)
- If applicable, I will take steps to ensure that no students or staff involved in the project will be exposed to inappropriate situations.

- I confirm that I have completed all risk assessments and other Health and Safety requirements as advised by my departmental Safety Officer.

☑ Confirmed

Please note: If you are not able to confirm the statement above please contact the FST Research Ethics Committee and provide an explanation.

Student applicants:

Please tick to confirm that you have discussed this application with your supervisor, and that they agree to the application being submitted for ethical review ☒

Students must submit this application from your Lancaster University email address, and copy your supervisor in to the email in which you submit this application

All Staff and Research Students must complete this declaration:

I confirm that I have sent a copy of this application to my Head of Department (or their delegated representative) . **Tick here to confirm** ☒

Name of Head of Department *(or their delegated representative)*

Adrian Friday (HoD) via Jonathon Hughes (Postgraduate Coordinator)

Applicant electronic signature: Emma Hewlett Date: 21/09/2018

Appendices and Additional Information

Advertisement Materials
Participant Information Sheet
Consent Forms
Copies of the Study Webpages
Debrief Form

Advertisement Materials

Online SONA Advert (Psychology research participant system)

Study Name	Can you detect a cyber-attack?
Study Type	Standard (lab) study
Pay	£3.50
Duration	25 mins
Description	This study is looking at whether people can detect different cyber-attacks. You will be asked to work your way through a series of web-pages and asked to identify if you notice any unusual events and whether you believe these are due to a cyber attack. (You will be using a university computer and fake accounts- so there is no danger to you or your information.)
Eligibility	Native English speaker or highly fluent in English; 18+ years
Restrictions	Must not have participated in ICS study
Researcher	Emma Hewlett
Deadlines	Sign-Up: 12 hours before the appointment Cancellation: 12 hours before the appointment

Poster/ Social Media Advert

Can You Detect A Cyber Attack?

Earn money by participating in a computer lab study and see if you can detect a malicious event.

No security experience required. Reward = £3.50

To take part you must be at least 18 years old and speak fluent English. If you are interested, please contact <email>.

School of Computing and Communications

Participant information sheet

I am a PhD student at Lancaster University and I would like to invite you to take part in a lab experiment investigating your ability to detect cyber attacks.

Please take time to read the following information carefully before you decide whether or not you wish to take part.

What is the study about?
This study is looking at people's ability to identify different types of cyber attacks and you will therefore be asked to work through several web pages and identify whether you see anything suspicious.

Why have I been invited?
You have been approached, because you have responded to an advert or poster advertising for participants.

In order to take part you must be at least 18 years old, have normal or corrected normal vision and speak fluent English

What will I be asked to do if I take part?
You will be asked to work your way through a series of webpages, these will consist of either a list of personality questions to answer or a link to an external email account or social media account. After visiting each page you will be presented with a short questionnaire asking whether you believe any security threats were present, whether you believe this could be a result of a cyber attack and how confident you are with your decision.

What are the possible benefits from taking part?
There are no specific benefits to you taking part in this study, however you will be given £3.50 as a thank you for your time.

Do I have to take part?
No. It's completely up to you to decide whether or not you take part. Your participation is voluntary, and you are free to withdraw at any time during the study, without giving any reason.

If you decide not to take part in this study, this will not affect your studies and the way you are assessed on your course.

What if I change my mind?
You may withdraw at any time during the study, you may also withdraw your data at anytime for up to two weeks after the experiment, at which point data may pooled together and analysed. If you wish to withdraw you will need to contact the

researcher, using the details below, and provide your participant reference number so please keep a record of this.

What are the possible disadvantages and risks of taking part?
There should be no major disadvantages to taking part, however this study may take around 25 minutes of your time.

Will my data be identifiable?
After the study only myself, the researcher conducting this study, my supervisors and any researchers involved in analysing the data will have access to the results of the study.

I will keep all personal information about you (e.g. your name and other information about you that can identify you) confidential, that is I will not share it with others. I will anonymise hard copies of any data. This means that I remove any personal information.

How will my data be stored?
Your data will be stored securely on the university system or in encrypted files (that is no-one other than me, the researcher will be able to access them) on password-protected computers.

I will store hard copies of any data securely in locked cabinets in my office.

In accordance with University guidelines, I will keep the data securely for a minimum of ten years.

For further information about how Lancaster University processes personal data for research purposes and your data rights please visit our webpage: www.lancaster.ac.uk/research/data-protection

How will we use the information you have shared with us and what will happen to the results of the research study?
The data that you share will only be used for academic purposes, this may include:

- My PhD thesis
- Academic journal papers
- Conference proceedings

Who has reviewed the project?

This study has been reviewed and approved by the Faculty of Science and Technology Research Ethics Committee.

What if I have a question or concern?
If you have any queries or if you are unhappy with anything that happens concerning your participation in the study, please contact myself (Emma Hewlett) at: <email>**;**
Please be aware that after two weeks data will be pooled and it may no longer possible to identify and remove.

Alternatively, you may contact my supervisor Prof. Utz Roedig at: <email>;

If you have any concerns or complaints that you wish to discuss with a person who is not directly involved in the research, you can also contact Prof. Adrian Friday:
<email>;
<phone>;
Infolab21, Lancaster University

Thank you for considering your participation in this project.

CONSENT FORM

Project Title: Detection of Cyber Attacks

Name of Researchers: Emma Hewlett
Email: e.hewlett@lancaster.ac.uk

Please tick each box

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily ☐
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving any reason. If I withdraw within 2 weeks of commencement of the study my data will be removed. ☐
3. I understand that any information given by me may be used in future reports, academic articles, publications or presentations by the researcher/s, but my personal information will not be included, and I will not be identifiable. ☐
4. I understand that my name/my organisation's name will not appear in any reports, articles or presentation without my consent. ☐
5. I understand that any interviews or focus groups will be audio-recorded and transcribed and that data will be protected on encrypted devices and kept secure. ☐
6. I understand that data will be kept according to University guidelines for a minimum of 10 years after the end of the study. ☐
7. I agree to take part in the above study. ☐

_____ _____ _____
Name of Participant Date Signature

I confirm that the participant was given an opportunity to ask questions about the study, and all the questions asked by the participant have been answered correctly and to the best of my ability. I confirm that the individual has not been coerced into giving consent, and the consent has been given freely and voluntarily.

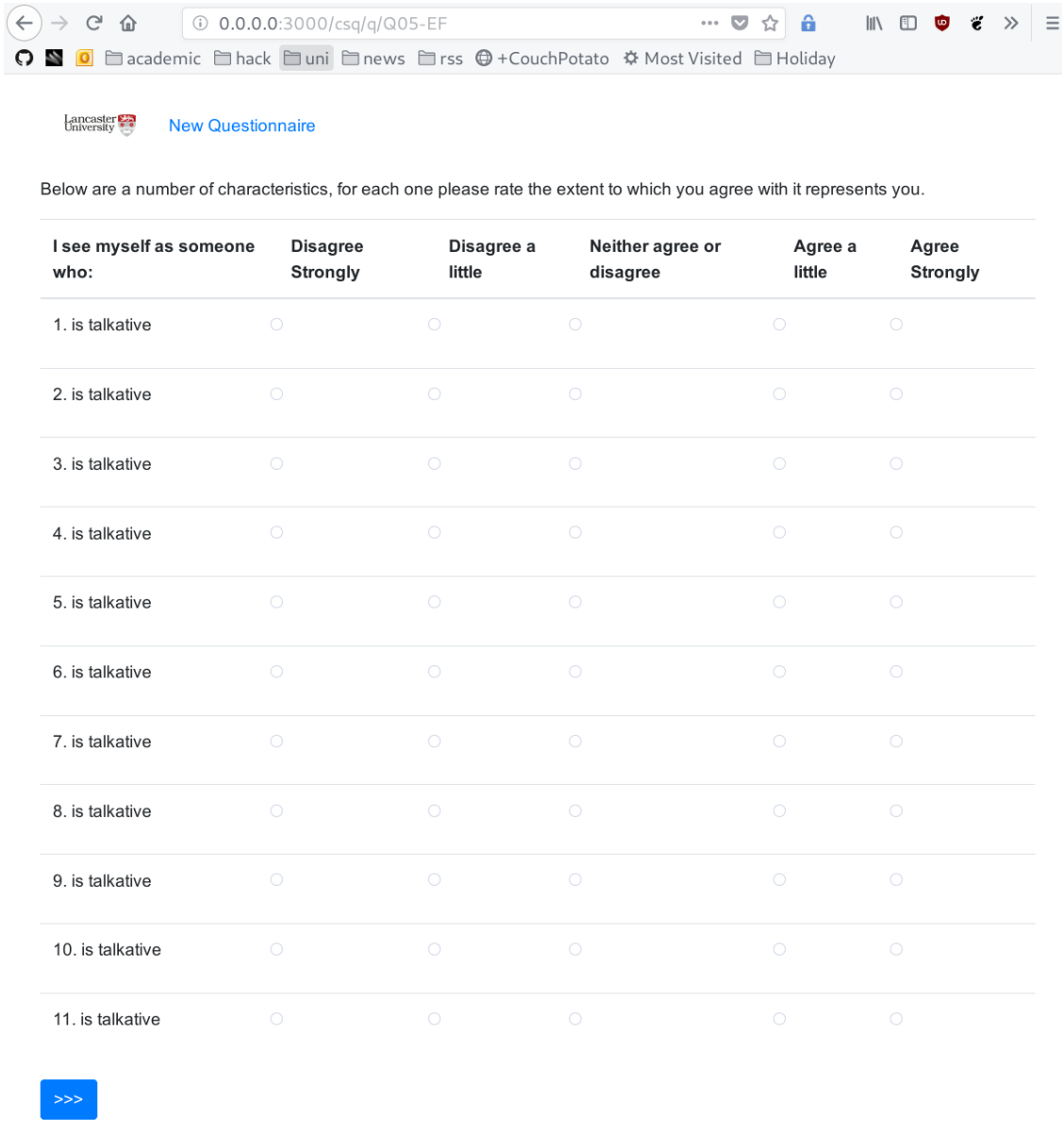
Signature of Researcher /person taking the consent_____ **Date** _____ Day/month/year

One copy of this form will be given to the participant and the original kept in the files of the researcher at Lancaster University

Web page Stimuli.

Examples of the website design can be seen in the images below (the site is still under construction and the final list of questions will be based on two well established psychological questionnaires, the Big Five Personality questionnaire[5] and the Barratt Impulsiveness Scale[6]):

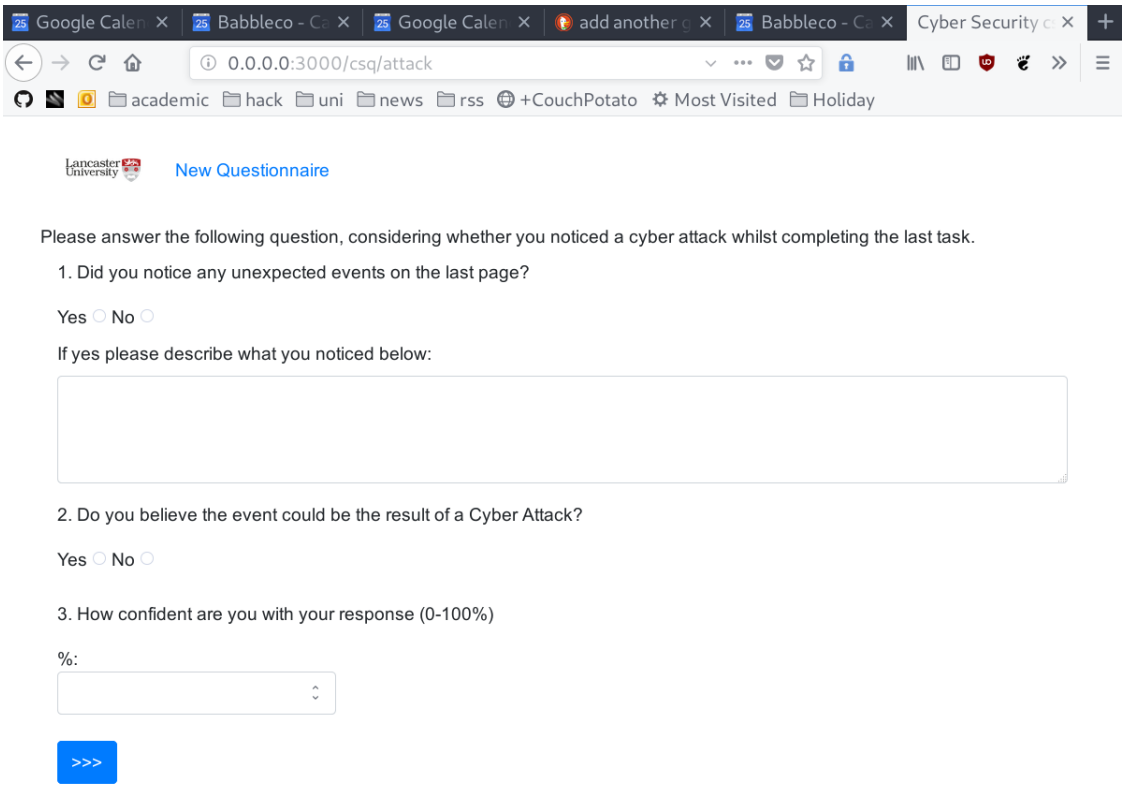
Trial page:



[5] (John, O. P., & Srivastava, S. (1999). The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), Handbook of personality: Theory and research (Vol. 2, pp. 102–138). New York: Guilford Press. http://moityca.com.br/pdfs/bigfive_John.pdf)

[6] Barratt Impulsiveness Scale http://www.impulsivity.org/measurement/bis11

Detection Page



Lancaster University

School of Computing and Communications

Debrief sheet- Human Factors in Cyber Security of Cyber Physical Systems

Thank you for participating in this experiment, we hope that you found it interesting and have not been upset or worried by the topic being explored.

As discussed in the Participant Information Sheet this work was exploring whether people can identify a range of different cyber attacks, however we would like to assure you that all of the attacks were only simulations. One of these involved an LED light coming on beside a camera lens however the camera was disconnected and no recordings were made. If you would like any more detail on this or any of the other simulated attacks please feel free to ask.

What if I have a question or would like to withdraw?
If you have any queries or if you are unhappy with anything that happens concerning your participation in the study, please contact myself (Emma Hewlett) at:<email>**;**
Please be aware that after two weeks data will be pooled and it may no longer possible to identify and withdraw your data.

Alternatively, you may contact my supervisor Prof. Utz Roedig at:<email>

If you have any concerns or complaints that you wish to discuss with a person who is not directly involved in the research, you can also contact Prof. Adrian Friday:<email>;
<phone>;
Infolab21, Lancaster University

Additional information:
If you would like more information on the cyber threats that are faced by different computer systems then this can be found at the following government website: https://www.cyberaware.gov.uk/

Finally if you would like to be provided with a brief summary of the findings once the study is complete, then please contact me at: <email>

Thank you for your participation in this project.

APPENDIX G

STATISTICAL OUTPUTS FROM THE CPS AT HOME STUDY

This Appendix presents the statistical outputs that were created for the experimental study on the detection of attacks at home in Chapter 6.

G.1 Statistical Analyses to Investigate Whether Some Attacks Are Easier to Detect Than Others

G.1.1 Outputs From the Cochrans Q Test to Explore Which Attacks Are Easier to Detect

A Cochrans Q test can be used to determine whether or not there are any differences in a dichotomous dependent variable between three or more related groups. In this context it was used to explore whether participants could identify various cyber attacks against home devices.

This test has three conditions that must be met:

1. It must have one dichotomous dependent variable, in this case whether a scenario is rated as an attack or non-attack.

2. It must have one independent variable that consists of three or more categorical, related groups, in this case the various attack and control conditions.

3. The participants were recruited from a random sample.

All three of these assumptions were met, there is also however some guidance on the number of participants required in order to be able to run the standard Cochrans Q test and to be able to interpret the asymptotic p-value. To meet the sample size conditions n (where n= total no. of

participants minus the number of participants who scored the same across each condition e.g. thought they were all attacks or all not attacks) must be equal to or greater than 4. Additionally, nk (where k is number of conditions) must be equal to or greater than 24.

In this study N= 69 and 5 individuals thought that none of the events were an attack and 0 thought all of the conditions were attacks. Therefore n=64 and nk=640, this study therefore meets the sample size requirements.

Running this test then produces the following outputs (Figure G.1, showing that it is significant.

Test Statistics

N	69
Cochran's Q	157.846[a]
df	9
Asymp. Sig.	.000

a. 0 is treated as a success.

Figure G.1: Output of the Cochran Q Test

Since this test was statistically significant, post hoc tests were conducted using Dunn's test with Bonferroni corrections (to account for multiple comparisons) to identify which of the conditions were significantly different from each other. The results of these tests can be seen in Figures G.2 and G.3.

G.2 What Level of Variance in the Detection of Attacks Can be Explained by Looking at a Participant's Demographic Factors

G.2.1 Predicting the Probability That an Individual Will Detect a Phishing Attack

A binomial logistic regression analysis attempts to predict the probability that an observation falls into one of two categories in a dichotomous dependent variable (in this case whether an incident, is or isn't, identified as a phishing email) based on one or more categorical or continuous independent variables. In this test the independent variables were IT Knowledge, gender, confidence in detecting the attacks, and neuroticism.

This test has six assumptions that must be met:

Pairwise Comparisons

Sample 1–Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
ExePopup–MouseTracking	–.203	.069	–2.949	.003	.143
ExePopup–PhishingEmail	.290	.069	4.213	.000	.001
ExePopup–ProgramAudio	–.435	.069	–6.320	.000	.000
ExePopup–ModalPopup	–.449	.069	–6.531	.000	.000
ExePopup–EmailControl1	.493	.069	7.163	.000	.000
ExePopup–EmailControl2	.580	.069	8.427	.000	.000
ExePopup–Control2	–.594	.069	–8.637	.000	.000
ExePopup–WebcamAttack	–.609	.069	–8.848	.000	.000
ExePopup–Control1	–.609	.069	–8.848	.000	.000
MouseTracking–PhishingEmail	.087	.069	1.264	.206	1.000
MouseTracking–ProgramAudio	–.232	.069	–3.371	.001	.034
MouseTracking–ModalPopup	.246	.069	3.581	.000	.015
MouseTracking–EmailControl1	.290	.069	4.213	.000	.001
MouseTracking–EmailControl2	.377	.069	5.477	.000	.000
MouseTracking–Control2	–.391	.069	–5.688	.000	.000
MouseTracking–WebcamAttack	.406	.069	5.899	.000	.000
MouseTracking–Control1	–.406	.069	–5.899	.000	.000
PhishingEmail–ProgramAudio	–.145	.069	–2.107	.035	1.000
PhishingEmail–ModalPopup	–.159	.069	–2.317	.020	.922

Pairwise Comparisons

Sample 1–Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
PhishingEmail–EmailControl1	–.203	.069	–2.949	.003	.143
PhishingEmail–EmailControl2	–.290	.069	–4.213	.000	.001
PhishingEmail–Control2	–.304	.069	–4.424	.000	.000
PhishingEmail–WebcamAttack	–.319	.069	–4.635	.000	.000
PhishingEmail–Control1	–.319	.069	–4.635	.000	.000
ProgramAudio–ModalPopup	.014	.069	.211	.833	1.000
ProgramAudio–EmailControl1	.058	.069	.843	.399	1.000
ProgramAudio–EmailControl2	.145	.069	2.107	.035	1.000
ProgramAudio–Control2	–.159	.069	–2.317	.020	.922
ProgramAudio–Control1	–.174	.069	–2.528	.011	.516
ProgramAudio–WebcamAttack	.174	.069	2.528	.011	.516
ModalPopup–EmailControl1	.043	.069	.632	.527	1.000
ModalPopup–EmailControl2	.130	.069	1.896	.058	1.000
ModalPopup–Control2	–.145	.069	–2.107	.035	1.000
ModalPopup–WebcamAttack	–.159	.069	–2.317	.020	.922
ModalPopup–Control1	–.159	.069	–2.317	.020	.922
EmailControl1–EmailControl2	–.087	.069	–1.264	.206	1.000
EmailControl1–Control2	–.101	.069	–1.475	.140	1.000
EmailControl1–WebcamAttack	–.116	.069	–1.685	.092	1.000
EmailControl1–Control1	–.116	.069	–1.685	.092	1.000
EmailControl2–Control2	–.014	.069	–.211	.833	1.000
EmailControl2–Control1	–.029	.069	–.421	.674	1.000

Figure G.2: Results of the Cochran Q Post-Hoc Tests

Pairwise Comparisons

Sample 1–Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
EmailControl2–Control1	–.029	.069	–.421	.674	1.000
EmailControl2–WebcamAttack	–.029	.069	–.421	.674	1.000
Control2–WebcamAttack	.014	.069	.211	.833	1.000
Control2–Control1	.014	.069	.211	.833	1.000
WebcamAttack–Control1	.000	.069	.000	1.000	1.000

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.
Asymptotic significances (2–sided tests) are displayed. The significance level is .05.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

Figure G.3: Results of the Cochran Q Post-Hoc Tests Continued

1. You have one dichotomous dependent variable, in this case this is whether a participant detects the phishing attack.
2. You have one or more independent variables that are either continuous or nominal.
3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.
4. You should have a minimum of 15 participants for each independent variable.
5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.
6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, assumption 4 was the reason why this test was limited to the four independent variables believed to most likely have an effect. Assumptions 5-7 required further tests to confirm.

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure G.4 and to understand if the assumption is met we need look at the three lines highlighted. In this test if the result is significant- 'sig.' is lower than 0.5 then the continuous independent variable is not linearly related to the logit of the dependent variable and it has failed the assumption of linearity, fortunately however as can be seen in this case the assumption is met.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	2.755	.977	7.946	1	.005	15.725
	Neuroticism	1.772	1.433	1.528	1	.216	5.882
	ITKnowledge	-2.595	5.483	.224	1	.636	.075
	AverageConfidence	1.965	1.575	1.555	1	.212	7.132
	Neuroticism by ln_Neuro	-.416	.339	1.507	1	.220	.660
	ITKnowledge by ln_ITKnowledge	1.349	2.454	.302	1	.583	3.853
	AverageConfidence by ln_Confidence	-.370	.295	1.565	1	.211	.691
	Constant	-36.008	25.576	1.982	1	.159	.000

a. Variable(s) entered on step 1: Gender, Neuroticism, ITKnowledge, AverageConfidence, Neuroticism * ln_Neuro , ITKnowledge * ln_ITKnowledge , AverageConfidence * ln_Confidence .

Figure G.4: Testing Assumption 5 that There is a Linear Relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variables

Assumption 6 states that their should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2 standard deviations. As can be seen in Figure G.5, none were identified and so this assumption was met.

Casewise List[a]

a. The casewise plot is not produced because no outliers were found.

Figure G.5: Testing Assumption 7 that There are No Outliers in the Data Sample

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure G.6. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the model, as can be seen from the model row, the model fit was significant with p=.021. The second table then shows Hosmer and Lemeshow goodness of fit test which analyses how poor the model is at predicting the categorical outcomes, in this case we want the model to be insignificant, as it is.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	11.592	4	.021
	Block	11.592	4	.021
	Model	11.592	4	.021

Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	7.959	8	.437

Figure G.6: Outputs of the Binomial Regression Analysis

Since the model is significant we can look at the table in Figure G.7 so that we can see how much variance in the detection of phishing emails is explained by tested independent variables. This Nagelkerke R2 value in this table shows that the model explains 21.7% of the variance.

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	75.428[a]	.157	.217

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Figure G.7: Model Fit to Look at the Level of Variance Explained in Whether Individuals Detect Phishing Attacks.

We can assess the observed and predicted classifications in Figure G.8, and these results are discussed in Chapter 6.

Finally, we can produce a ROC curve which can be used to calculate an overall measure of discrimination. You can see in Figure G.9 that the area under the ROC curve is .707. The area can range from 0.5 to 1.0 with higher values representing better discrimination. According to [233] a value of .707 puts the discrimination of this model at the lower border of acceptable discrimination.

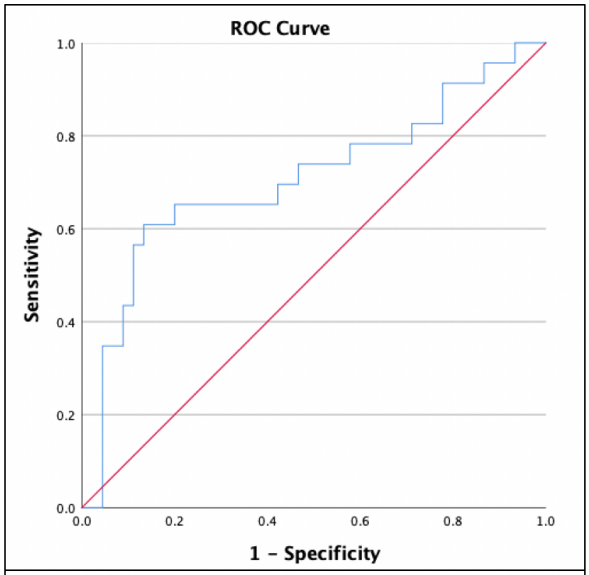
Having established that the model is significant we can explore in detail which of the tested

Classification Table[a]

			Predicted		
			PhishingDetection		Percentage Correct
	Observed		Non-attack	Attack	
Step 1	PhishingDetection	Non-attack	40	5	88.9
		Attack	12	11	47.8
	Overall Percentage				75.0

a. The cut value is .500

Figure G.8: The Observed and Predicted Classifications for Phishing Email Detection.



Area Under the Curve

Test Result Variable(s): Predicted probability

Area	Std. Error[a]	Asymptotic Sig.[b]	Asymptotic 95% Confidence Interval	
			Lower Bound	Upper Bound
.707	.073	.005	.565	.850

a. Under the nonparametric assumption

b. Null hypothesis: true area = 0.5

Figure G.9: ROC Curve Figure and Results for Phishing Email Detection

independent variables had a significant effect on the model using the variables in the equation table (Figure G.10).

G.2.2 Predicting the Probability that an Individual Will Detect an Attack Involving an .Exe Pop-Up Attack

A binomial logistic regression analysis was then run to explore whether we could predict who would detect an .exe pop-up attack based on IT Knowledge, gender, confidence in detecting the

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	2.088	.771	7.334	1	.007	8.070
	Neuroticism	.017	.054	.105	1	.746	1.018
	ITKnowledge	.282	.398	.500	1	.479	1.325
	AverageConfidence	-.002	.023	.011	1	.917	.998
	Constant	-2.382	2.598	.840	1	.359	.092

a. Variable(s) entered on step 1: Gender, Neuroticism, ITKnowledge, AverageConfidence.

Figure G.10: Impact of Each of the Variables in the Phishing Email Detection Model

attacks and neuroticism.

Again this test has six assumptions that needed be met:

1. You have one dichotomous dependent variable, in this case this is whether a participant detects the .exe pop-up attacks.

2. You have one or more independent variables that are either continuous or nominal.

3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.

4. You should have a minimum of 15 participants for each independent variable.

5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.

6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, again assumption 4 was the reason why this test was limited to the four independent variables believed to most likely have an effect. Assumptions 5-7 required further tests to confirm.

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure G.11 and to understand if the assumption is met we need look at the three lines highlighted. In this test if the result is significant 'sig.' is lower than 0.5 then the continuous independent variable is not linearly related to the logit of the dependent variable and it has failed the assumption of linearity. Fortunately however as can be seen in this case the assumption is met.

Assumption 6 states that their should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2 standard deviations. As can be seen in Figure G.12, five cases were flagged. The general assumption is that data points with + or - 2.5 standard deviation should be inspected to determine why they are outliers, and this applied to one of the five cases. However after inspection it was decided to keep the result as it was not missclassified.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	.163	1.117	.021	1	.884	1.177
	Neuroticism	-1.724	1.627	1.122	1	.289	.178
	ITKnowledge	6.430	14.395	.200	1	.655	620.347
	AverageConfidence	-.490	2.131	.053	1	.818	.612
	Neuroticism by ln_Neuro	.426	.383	1.234	1	.267	1.531
	ITKnowledge by ln_ITKnowledge	-2.201	6.168	.127	1	.721	.111
	AverageConfidence by ln_Confidence	.104	.398	.068	1	.795	1.109
	Constant	-3.477	34.319	.010	1	.919	.031

a. Variable(s) entered on step 1: Gender, Neuroticism, ITKnowledge, AverageConfidence, Neuroticism * ln_Neuro , ITKnowledge * ln_ITKnowledge , AverageConfidence * ln_Confidence .

Figure G.11: Testing Assumption 5 that There is a Linear Relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variable (.Exe Attack Detection)

Casewise List[b]

Case	Selected Status[a]	Observed ExeDetection	Predicted	Predicted Group	Temporary Variable Resid	ZResid	SResid
1	S	A**	.151	N	.849	2.373	2.015
13	S	A**	.200	N	.800	2.002	2.008
21	S	A**	.030	N	.970	5.718	2.690
28	S	A**	.146	N	.854	2.418	2.059
31	S	A**	.174	N	.826	2.181	2.134

a. S = Selected, U = Unselected cases, and ** = Misclassified cases.

b. Cases with studentized residuals greater than 2.000 are listed.

Figure G.12: Testing Assumption 6 that There Are No Outliers in the Data Sample for .Exe Attack Detection

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure G.13. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the mode, as can be seen from the model row the model fit was significant with p=.044. The second table then shows Hosmer and Lemeshow goodness of fit test which analyses how poor the model is at predicting the categorical outcomes, in this case we want the model to be insignificant, as it is.

Since the model is significant we can look at the table in Figure G.14 so that we can see how much variance in the detection of a malicious .exe pop-up is explained by tested independent variables. The Nagelkerke R2 value in this table shows that the model explains 24.8% of the variance.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	9.808	4	.044
	Block	9.808	4	.044
	Model	9.808	4	.044

Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	3.359	8	.910

Figure G.13: Outputs of the Binomial Regression Analysis into Detection of .Exe Pop-Up Attacks

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	43.346[a]	.134	.248

a. Estimation terminated at iteration number 6 because parameter estimates changed by less than .001.

Figure G.14: Model Fit to Look at the Level of Variance Explained in Whether Individuals can Detect .Exe Pop-Up Attacks

We can assess the observed and predicted classifications in Figure G.15.

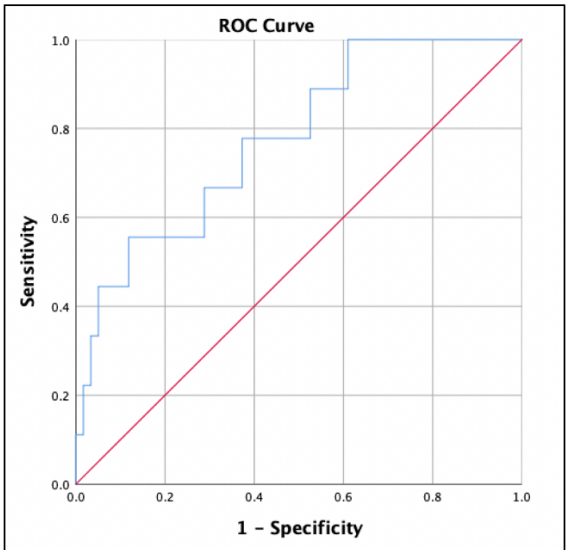
Classification Table[a]

			Predicted		
			ExeDetection		Percentage Correct
	Observed		Non-attack	Attack	
Step 1	ExeDetection	Non-attack	58	1	98.3
		Attack	7	2	22.2
	Overall Percentage				88.2

a. The cut value is .500

Figure G.15: The Observed and Predicted Classifications for .Exe Pop-Up Detection

Finally, we can produce a ROC curve which can be used to calculate an overall measure of discrimination. It can be seen in Figure G.16 that the area under the ROC curve is .776. The area can range from 0.5 to 1.0 with higher values representing better discrimination. According to [233] a value of .776 puts the discrimination of this model at the upper border of acceptable discrimination.



Area Under the Curve

Test Result Variable(s): Predicted probability

Area	Std. Error[a]	Asymptotic Sig.[b]	Asymptotic 95% Confidence Interval	
			Lower Bound	Upper Bound
.776	.080	.008	.619	.933

a. Under the nonparametric assumption

b. Null hypothesis: true area = 0.5

Figure G.16: ROC Curve Figure and Results for .Exe Pop-Up Detection.

Having established that the model is significant we can explore in detail which of the tested independent variables had a significant effect on the model using the variables in the equation table (Figure G.17). The implications of these findings are discussed in Chapter 6.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	.460	1.096	.176	1	.675	1.584
	Neuroticism	.086	.074	1.345	1	.246	1.090
	ITKnowledge	1.335	.559	5.712	1	.017	3.800
	AverageConfidence	.051	.037	1.926	1	.165	1.053
	Constant	−12.959	4.780	7.349	1	.007	.000

a. Variable(s) entered on step 1: Gender, Neuroticism, ITKnowledge, AverageConfidence.

Figure G.17: Impact of Each of the Variables in the .Exe Detection Model

G.2.3 Predicting the Probability That an Individual Will Detect an Attack involving a Webcam

A third binomial logistic regression analysis was conducted to explore whether IT Knowledge, gender, confidence in detecting the attacks and neuroticism could be used to predict who would detect an attack against a webcam. Again, this test has six assumptions that must be met:

1. You have one dichotomous dependent variable, in this case this is whether a participant detects the webcam attack.
2. You have one or more independent variables that are either continuous or nominal.
3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.
4. You should have a minimum of 15 participants for each independent variable.
5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.
6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, assumption 4 was the reason why this test was limited to the four independent variables believed to most likely have an effect. Assumptions 5-7 required further tests to confirm.

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure G.18 and to understand if the assumption is met we need look at the three lines highlighted. In this test if the result is significant- 'sig.' is lower than 0.5 then the continuous independent variable is not linearly related to the logit of the dependent variable and it has failed the assumption of linearity. Fortunately however as can be seen in this case the assumption is met.

Assumption 6 states that their should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2 standard deviations. As can be seen in Figure G.19, three data points were flagged. The general assumption is that data points with + or - 2.5 standard deviations should be inspected to determine why they are outliers, fortunately none of the three flagged data points violated this assumption.

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure G.20. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the mode, as can be seen from the model row the model fit was significant with p=.031. The second table then shows Hosmer and Lemeshow goodness of fit test which analyses how poor the model is at predicting the categorical outcomes, in this case we want the model to be insignificant, as it is.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	-21.226	7066.511	.000	1	.998	.000
	Neuroticism	-5.647	5.588	1.021	1	.312	.004
	ITKnowledge	-23.463	26.254	.799	1	.371	.000
	AverageConfidence	15.535	20.889	.553	1	.457	5580801.07
	Neuroticism by ln_Neuro	1.368	1.316	1.080	1	.299	3.928
	ITKnowledge by ln_ITKnowledge	11.014	12.860	.734	1	.392	60715.071
	AverageConfidence by ln_Confidence	-3.023	4.025	.564	1	.453	.049
	Constant	-126.537	255.021	.246	1	.620	.000

a. Variable(s) entered on step 1: Gender, Neuroticism, ITKnowledge, AverageConfidence, Neuroticism * ln_Neuro , ITKnowledge * ln_ITKnowledge , AverageConfidence * ln_Confidence .

Figure G.18: Testing Assumption 5 that There is a Linear relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variable (Detection of a Webcam Attack)

Casewise List[b]

Case	Selected Status[a]	Observed WebcamDetection	Predicted	Predicted Group	Temporary Variable Resid	ZResid	SResid
20	S	A**	.127	N	.873	2.618	2.319
21	S	A**	.123	N	.877	2.668	2.096
34	S	A**	.230	N	.770	1.830	2.407

a. S = Selected, U = Unselected cases, and ** = Misclassified cases.

b. Cases with studentized residuals greater than 2.000 are listed.

Figure G.19: Testing Assumption 6 That There Are No Outliers in the Data Sample for Detecting a Webcam Attack

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	10.613	4	.031
	Block	10.613	4	.031
	Model	10.613	4	.031

Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	2.123	8	.977

Figure G.20: Outputs of the Binomial Regression Analysis on Detecting Webcam Attacks

Since the model is significant we can look at the table in Figure G.21 so that we can see how much variance in the detection of phishing emails is explained by tested independent variables.

The Nagelkerke R2 value in this table shows that the model explains 40.1% of the variance.

Model Summary

Step	−2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	19.813[a]	.145	.401

a. Estimation terminated at iteration number 20 because maximum iterations has been reached. Final solution cannot be found.

Figure G.21: Model Fit to Look at the Level of Variance Explained in Whether Individuals Can Detect Webcam Attacks

We can assess the observed and predicted classifications in Figure G.22.

Classification Table[a]

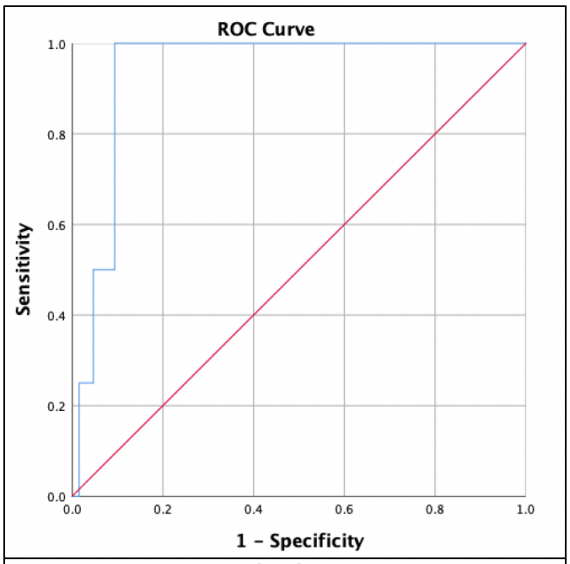
			Predicted		
			WebcamDetection		Percentage Correct
	Observed		Non-attack	Attack	
Step 1	WebcamDetection	Non-attack	63	1	98.4
		Attack	3	1	25.0
	Overall Percentage				94.1

a. The cut value is .500

Figure G.22: The Observed and Predicted Classifications for Predicting Webcam Attack Detection

Finally, we can produce a ROC curve which can be used to calculate an overall measure of discrimination. You can see in Figure G.23 that the area under the ROC curve is .938. The area can range from 0.5 to 1.0 with higher values representing better discrimination. According to [233] a value of .938 puts the discrimination of this model at outstanding level of discrimination.

Having established that the model is significant we can explore in detail which of the tested independent variables had a significant effect on the model using the variables in the equation table (Figure G.24). The implications of these findings are discussed in Chapter 6.



Area Under the Curve

Test Result Variable(s): Predicted probability

Area	Std. Error[a]	Asymptotic Sig.[b]	Asymptotic 95% Confidence Interval	
			Lower Bound	Upper Bound
.938	.031	.004	.876	.999

a. Under the nonparametric assumption

b. Null hypothesis: true area = 0.5

Figure G.23: ROC Curve Figure and Results for Webcam Attack Detection

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	-19.228	8203.513	.000	1	.998	.000
	Neuroticism	.096	.094	1.039	1	.308	1.101
	ITKnowledge	.247	1.029	.058	1	.810	1.281
	AverageConfidence	-.148	.064	5.309	1	.021	.862
	Constant	4.981	5.363	.863	1	.353	145.659

a. Variable(s) entered on step 1: Gender, Neuroticism, ITKnowledge, AverageConfidence.

Figure G.24: Impact of Each of the Variables on the Detecting Webcam Attacks Model

APPENDIX H

DETECTION OF CYBER ATTACKS IN AN ICS TESTBED- ETHICS PROPOSAL

This Appendix presents the approved ethics proposal for the experimental study into the detection of cyber attacks in an ICS conducted in Chapter 7.

Lancaster University

Faculty of Science and Technology Research Ethics Committee (FSTREC)
Lancaster University

Application for Ethical Approval for Research

This form should be used for all projects by staff and research students, whether funded or not, which have not been reviewed by any external research ethics committee. If your project is or has been reviewed by another committee (e.g. from another University), please contact the FST research ethics officer for further guidance.

In addition to the completed form, you need to submit **research materials** such as:

i. Participant information sheets
ii. Consent forms
iii. Debriefing sheets
iv. Advertising materials (posters, e-mails)
v. Letters/emails of invitation to participate
vi. Questionnaires, surveys, demographic sheets that are non-standard
vii. Interview schedules, interview question guides, focus group scripts

Please note that **you DO NOT need to submit pre-existing questionnaires or standardized tests** that support your work, but which cannot be amended following ethical review. These should simply be referred to in your application form.

Please submit this form and any relevant materials **by email as** a **SINGLE attachment** to <email>

Section One

Applicant and Project Information

Name of Researcher: Emma Hewlett

Project Title: Human Factors in Cyber Security of ICS- Study 2 and 3

Level: PhD

Supervisor (if applicable): Awais Rashid, Utz Roedig, Paul Taylor

Researcher's Email address: <email>
Telephone: <phone>
Address: B59, Infolab

Names and appointments/position of all further members of the research team: An MSc Computer science student who is funded by the department to work on the testbed may be available to assist with set up and to offer technical support.

Is this research externally funded? No
ACP ID number:
Funding source:
Grant code:

Does your research project involve any of the following?

☑ Human participants (including all types of interviews, questionnaires, focus groups, records relating to humans, use of internet or other secondary data, observation etc.)

□ Animals - the term animals shall be taken to include any non-human vertebrates or cephalopods.

☑ Risk to members of the research team e.g. lone working, travel to areas where researchers may be at risk, risk of emotional distress

☐ Human cells or tissues other than those established in laboratory cultures

☐ Risk to the environment

☐ Conflict of interest

☐ Research or a funding source that could be considered controversial

☐ Social media and/or data from internet sources that could be considered private

☑ any other ethical considerations

- Deception

Yes – complete the rest of this form

No – go to Section Five

Section Two

Type of study

☒ Includes *direct* involvement by human subjects. ***Complete all sections apart from Section 3.***

☐ Involves *existing documents/data only*, or the evaluation of an existing project with no direct contact with human participants. ***Complete all sections apart from Section 4.***

Project Details

1. Anticipated project dates (month and year)

Start date: Apr 2017 **End date:** Oct 2017 (thesis submission: Feb 2020)

2. Please briefly describe the background to the research (no more than 150 words, in lay-person's language):

Work under this PhD seeks to consider the human element in cyber security by asking if, within Cyber Physical Systems, the human operators and end users can actively contribute to the cyber security of the system.

It will use a test bed of a water-plant which controls water levels in two containers which will be targeted with various cyber-attacks to seek to provide experimental evidence of how computer users respond in the event of a cyber-attack with emphasis on whether users detect these attacks and the influences of system knowledge, security knowledge and personality.

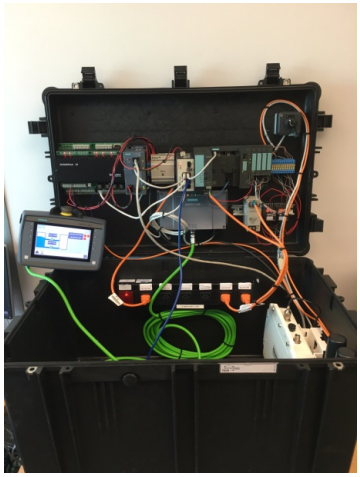


Fig 1. The test-bed (two water containers are inside box).

The second study will investigate the decision-making processes and information required for an individual to determine if an event is a malicious attack or a technical fault or failure.

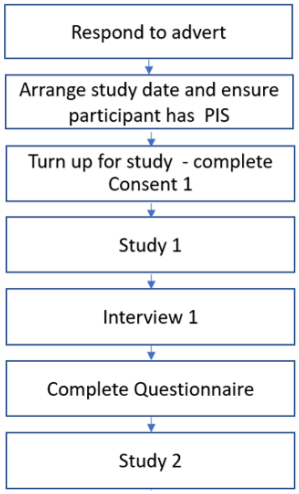
3. Please state the aims and objectives of the project (no more than 150 words, in lay-person's language):

The aim of the project is to provide exploratory data to begin answering the following research questions:

- Study one:
  - Do operators/ computer users detect when their systems are being maliciously manipulated?
  - Is the detection of a cyber-attack influenced by system knowledge/ security knowledge or personality?
  - Where do users attribute blame for suspicious system behaviour (e.g. do they blame the technology or identify that it is the result of malicious intent.)
  - Does a cyber-attack impact a computer user's primary task performance?
- Study two:
  - When primed to consider cyber-attacks as a possible cause of any errors, what actions do individuals take to determine the cause?
  - What information do operators wish to have to make a decision regarding the cause of any errors.

4. Methodology and Analysis:

The methodology for this study can be seen in the flow chart and this is elaborated below.



Methodology

Participant information: This will involve discussing the participant information sheet with the participants, giving them the chance to ask any questions and inviting them to sign consent forms.

Experiment 1

A lab experiment consisting of observations and video recordings of individuals asked to take on the role of a water plant controller, who then will be targeted with several different cyber-attacks (video recording will be monitoring the water levels on the test-bed not focussed on the participants).

Participants will have the test bed demonstrated to them and they will be given a Human Machine Interface (HMI) and a laptop, although the water tanks will be in close proximity and easily observable, and a laptop. Participants will then be asked to complete a primary task of recording water levels at 1 minute intervals and to answer any queries presented via email (these can be responded to via email or by voice to simulate radio/ phone calls). During this time, they will be subjected to various requests and cyber-attacks which will be counter-balanced (see table below).

Time	**4mins**	**8mins**	**12mins**	**14mins**	**18mins**	**20mins**
Participant 1	Email request	Replay attack (1)	Man-in-the middle-attack (2)	Man-in-the middle-attack (4)	Fuzzing attack/ system crash (3)	Webcam attack
Participant 2	Email request	Man-in-the middle-attack (2)	Fuzzing attack/ system crash (3)	Replay attack (1)	Man-in-the middle-attack (4)	Webcam attack
Participant 3	Email request	Fuzzing attack/ system crash (3)	Man-in-the middle-attack (4)	Man-in-the middle-attack (2)	Replay attack (1)	Webcam attack
Participant 4	Email request	Man-in-the middle-attack (4)	Replay attack (1)	Fuzzing attack/ system crash (3)	Man-in-the middle-attack (2)	Webcam attack

Scenario incidents

Email request: Will be a message from a technician conducting measurements asking for confirmation of the water levels at start+5mins.
Replay Attack (1): This will involve data being played back after a delay e.g. 30 seconds so that the water readings whilst following the correct pattern will be out of sync with the water tanks.
Man-in-the-middle Attack (2): This will involve the water readings showing the complete opposite (water tanks switched) but realistic levels
Fuzzing Attack (3): This will involve crashing the system so that the HMI is unable to display the readings
Man-in-the-middle Attack (4): This will involve the levels remaining steady.
Webcam attack: This will involve the webcam (and corresponding LED) on, although no recordings will be taken.

[Attacks may be varied slightly based on testbed configuration]

Notes will be taken to capture any relevant information in regards to the study, e.g. that they have noticed any discrepancies or ask if I am causing any of the issues and during what attack this occurs. Observations of how participants respond during and following an incident will also be recorded, on an observer form e.g. they express frustration or use the water tanks if HMI is not working.
This task should take 25 minutes

Interview 1
Following the experiment, participants will be asked to explain their behaviours in a short semi-structured interview, that will be audio recorded (with permission) and if they noticed anything suspicious they will be asked what they believe is to blame for the suspicious activities. Finally, participants who did not notice suspicious behaviours will be prompted as to whether they noticed any suspicious behaviours and what they were.

Debrief and Re-consent:
Following experiment one it will be explained to participants that the real aim of the study was to investigate the impacts of cyber-attacks and participants will be offered the opportunity to raise any questions or issues that they may have regarding the true nature of the study.

Questionnaire
Once individuals have confirmed that they are happy to continue they will be asked to complete a short questionnaire to capture their knowledge and experience levels and personality. This questionnaire included
- Demographic assessment
- Questionnaires: Personality (44 Item- Big Five Inventory)[1] expertise, IT expertise

Experiment 2

[1] (John, O. P., & Srivastava, S. (1999). The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), Handbook of personality: Theory and research (Vol. 2, pp. 102–138). New York: Guilford Press. http://moityca.com.br/pdfs/bigfive_John.pdf); Industrial Control System

This will be a second experiment that will involve a detailed interview/ discussion. Participants will be provided with a series of scenarios (see below) that could represent a cyber-attack and be asked to explain what they would do in this situation e.g. run anti-virus , whether they would consider such an event as likely to result from a cyber-attack and what information they would need or seek to determine if this was the case.

For system operators:

Scenario 1: The control room human user interface crashes and no longer provides any information.

Scenario 2: The information you are receiving in the control room is not accurate e.g. in a water plant the water levels are consistently a little lower than being reported.

For non-system operators:

Scenario 1: you notice that your webcam light is turned on even when you are not using the webcam and believe it to be turned off. What actions would you take?

Scenario 2: The load up time on your 6 month old laptop has noticeably increased, now taking several minutes. What actions would you take?

Debrief: following the experiments all participants will be fully debriefed on the work, reminded as to how data will be stored and used. They will also begiven a debrief sheet with a reminder of procedure for withdrawing their data and researcher contact information should they have any questions in the future.

Analysis
Experiment one

Do operators/ computer users detect when their systems are being maliciously manipulated?
This question will be answered using descriptive statistics of whether attacks were detected using data from the observations (e.g. do they verbalise that they believe they are being 'messed with') and the interviews (do they report being suspicious following the experiment), considering if certain attacks are more likely to be detected or if the number of attacks experienced is more important (e.g. after three attacks people become suspicious).

Is the detection of a cyber-attack influenced by system knowledge/ security knowledge or personality?
The Dependent variable for this question is therefore detection with outcomes being either yes or no and If enough individuals are able to identify a malicious attack then any significant differences between these two groups will be analysed using a logistic regression analysis will be conducted.

Number of participants: the generally accepted rule for the number of variables for this type of analysis is that the minimum number of participants (in either condition so identified attack or didn't identify attack) should be 10 times the number of independent variables. This work seeks to test two types of knowledge and several personality constructs, giving ideally 5-6 independent variables and so the smallest group should ideally have at least 50 individuals. Because this topic has been poorly studied in the past it is impossible to estimate how many individuals will detect the attacks, the only

similar previous study only looked at webcam attacks finding detection ranged from 0-46.4%[2] depending on the task they were given. Since this task will involve actively looking at the systems to be effected I will assume detection closer to the higher level and assume a 50:50 split between conditions this will require 100-120 participants, the aim will be to recruit 120 split between individuals including ICS control room operators, security students and students from other courses however these will be adjusted based on recruitment restraints (it may be necessary to recruit more students than operators). http://logisticregressionanalysis.com/1532-how-big-a-sample-how-many-x-variables/
Should only a small percentage of individuals detect an attack (or a large number detect attacks) then the number of variables tested will be reduced (giving priority to those identified as influencing susceptibility in previous research) and greater emphasis will be placed on descriptive statistics.

Where do users attribute blame for suspicious system behaviour? (e.g. do they blame the technology or identify that it is the result of malicious intent.)
This will be analysed via content analysis from the outputs of the interviews (interview schedule in Appendix D).

Does a cyber-attack impact a computer user's primary task performance?
The dependent variable for this will be the score for recorded water levels during time periods of attack, versus the safe period at the start. This will involve a within-participants related t-test

Experiment two
This work will be exploratory and so the analysis will be descriptive, investigating any patterns in behaviour between individuals rather than using formal statistics, do they follow similar strategies or do they form and test hypothesises.

When primed to consider cyber-attacks as a possible cause of any errors, what actions do individuals take to determine the cause?
This will be analysed thematically based on audio recordings discussing the scenarios.

What information do operators wish to have to make a decision regarding the cause of any errors?
Same as the previous research question this will be analysed thematically based on audio recordings discussing the scenarios.

Section Three (NOT APPLICABLE)

Secondary Data Analysis

Complete this section if your project involves *existing documents/data only*, or the evaluation of an existing project with no direct contact with human participants

1. Please describe briefly the data or records to be studied, or the evaluation to be undertaken.

2. How will any data or records be obtained?

[2] Portnoff, R. S., Lee, L. N., Egelman, S., Mishra, P., Leung, D., & Wagner, D. (2015). *Somebody's watching me?: Assessing the effectiveness of Webcam indicator lights.* Paper presented at the Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems

3. Confidentiality and Anonymity: If your study involves re-analysis and potential publication of existing data but which was gathered as part of a previous project involving direct contact with human beings, how will you ensure that your re-analysis of this data maintains confidentiality and anonymity as guaranteed in the original study?

4. What plan is in place for the storage of data (electronic, digital, paper, etc)? Please ensure that your plans comply with the Data Protection Act 1998.

5. What are the plans for dissemination of findings from the research?

6a. Is the secondary data you will be using in the public domain? YES/NO
6b. If NO, please indicate the original purpose for which the data was collected, and comment on whether consent was gathered for additional later use of the data.

7.What other ethical considerations (if any), not previously noted on this application, do you think there are in the proposed study? How will these issues be addressed?

8a. Will you be gathering data from discussion forums, on-line 'chat-rooms' and similar online spaces where privacy and anonymity are contentious? NO YES/NO

If yes, your project requires full ethics review. Please complete all sections.

Section Four

Participant Information

Complete this section if your project includes *direct* involvement by human subjects.

1. Please describe briefly the **intended human participants** (including number, age, gender, and any other relevant characteristics):
- This study will seek to recruit up to 120 participants from a mixture of Industrial Control System operators, computer science students and additional students and staff from around the university. The aim will be to be recruit at least 30 participants from each group however if too few operators are willing to take part then more students will be recruited. Using fewer operators will still be in line with previous work as they are a known hard to recruit group

2. How will participants be **recruited** and from where?
- Recruitment emails (See supporting docs.) will be sent out to industry and power plants through contacts within the department to recruit system operators, or individuals who work in close proximity to Industrial Control Systems (ICS).
- Security students will be targeted by targeted either by announcements in lectures or emails.

- General students and staff will be advertised via the Lancaster Psychology Research participation System- SONA (https://lancs.sona-systems.com/default.aspx?logout=Y) and flyers and word of mouth around campus.
- Individuals will only be turned away if they are under 18 years old or when enough participants have been recruited.

  Targeted emails will include a participant information sheet and this will also be provided to anyone who expresses an interest before arranging to take part in the studies.

3. Briefly describe your **data collection methods**, drawing particular attention to any potential ethical issues.
   Data collection methods will include:
- Demographic questionnaire (See supporting docs): however no identifiable information will be collected and no information will be gathered on any of the participant's organisational affiliations.
- Personality questionnaires: however, participants will be informed that personal profiles will not be given to them and that this data will not be shared outside of the research team.
- Observations of how individuals respond, e.g. physically going and checking the water levels and task performance. These will be used to help confirm whether individuals detect attacks and then destroyed.
- Task performance will be a score of 0-22, with points being scored for correctly recording water levels on each minute and correctly responding to email requests.
- Videos (with permission): these will be collected only to verify observations and for audio, participants will be informed of this in advance. Following verification of observations and transcription of audio these videos will be destroyed.
- Audio recordings of interviews- these will be transcribed using pseudonyms for any personal information including names with recordings destroyed following transcription.

4. Consent

4a. Will you take all necessary steps to **obtain the voluntary and informed consent** of the prospective participant(s) or, in the case of individual(s) not capable of giving informed consent, the permission of a legally authorised representative in accordance with applicable law?
No initial consent will be based on withholding certain aspects of the study
If yes, please go to question 4b. If no, please go to question 4c.

4b. Please explain the procedure you will use for **obtaining consent**? If applicable, please explain the procedures you intend to use to gain permission on behalf of participants who are unable to give informed consent.

4c. If it will be necessary for participants to take part in the study **without their knowledge and consent at the time**, please explain why (for example covert observations may be necessary in some settings; some experiments require use of deception or partial deception – not telling participants everything about the experiment).

Participants will be fully briefed on all the activities that they will be performing; however, they will initially not be told that the study is looking at cyber security to ensure that they are not primed to expect cyber-attacks. Instead individuals will be informed that I am investigating how personality affects decision making, operators will be assured that we are NOT assessing job performance both in the Participation Information Sheet and by the researcher. They will then be asked to read and sign a consent Form.

Following the completion of study one participants will be informed of the deception and be asked if they wish to continue. Participants will also be reminded of their right to withdraw at this point. At the end of both studies individuals will be reminded of their right to withdraw over the next two weeks and be given a debriefing sheet.

5. Could participation cause **discomfort** (physical and psychological eg distressing, sensitive or embarrassing topics), **inconvenience or danger beyond the risks encountered in normal life**? Please indicate plans to address these potential risks. State the timescales within which participants may withdraw from the study, noting your reasons.

Operators may feel discomfort that they are being 'evaluated' as an individual or believe that any outputs will be given directly to their employers, they will therefore be assured that the raw data will not be shared and that no data will be linked directly to them or their organisation.

There is also a small possibility that this study could cause a participant some concern regarding their vulnerability to a cyber-attack, they will therefore be given a debrief sheet containing links to information regarding computer security.

Participants will be informed that participation is voluntary and that they may withdraw at any point during the study and for up to two weeks following participation, after which point data may be analysed and it may no longer be possible to identify the data which belongs to them.

6. How will you protect participants' **confidentiality and/or anonymity** in data collection (e.g. interviews), data storage, data analysis, presentation of findings and publications?
All quantitative data will be pooled based on participant knowledge and, any qualitative data reported will use a pseudonym ensuring all individuals are kept anonymous be used. Any data that needs to be transported before being placed on the University systems will be encrypted and stored on a password protected laptop.

7. Do you anticipate any ethical constraints relating to **power imbalances or dependent relationships**, either with participants or with or within the research team? If yes, please explain how you intend to address these?
No

8. What potential **risks may exist for the researcher** and/or research team? Please indicate plans to address such risks (for example, noting the support available to you/the researcher; counselling considerations arising from the sensitive or distressing nature of the research/topic; details of the lone worker plan you or any researchers will follow, in particular when working abroad.

Lone working: To maximise recruitment of operators, the option to participate at their own work site will be given, as the necessary lab equipment (testbed, laptop and audio recorders) are portable. In this case to minimise the risks from lone working, all experimental sessions will be arranged at the work site and during standard office hours. All arranged sessions will be shared with supervisors and the researcher will be contactable at all times.

9. Whilst there may not be any significant direct **benefits to participants** as a result of this research, please state here any that may result from participation in the study.
No direct benefits to participants.

10. Please explain the **rationale for any incentives/payments** (including out-of-pocket expenses) made to participants:
This study should take up too 1 hour, including familiarisation, participants will be offered £6 to thank them for taking the time to take part in the study

11. What are your plans for the **storage of data** (electronic, digital, paper, etc.)? Please ensure that your plans comply with the Data Protection Act 1998.

- Video Recordings: to be downloaded onto researcher's password protected laptop and encrypted using 7-zip software (http://lancasteranswers.lancs.ac.uk/portal/app/portlets/results/viewsolution.jsp;jsessionid=3A0B1AA7201D9749D08C353C28AF36E9?solutionid=130903180102327&SToken=CFC1082F2FF8FC56E0FC45D257A354FE) and protected. Video recordings will be destroyed once they have been used to assess accuracy of individuals on water levels task.
- Audio recordings will be destroyed once transcripted and transcripts will be encrypted and stored for up to 10 years.
- Questionnaires: To be completed using Qualtrics online, completed data will be downloaded and stored for up to 10 years.
- Consent forms to be scanned and then encrypted and stored for up to 10 years.
- Stored data will be accessible to the researcher and supervisors.
- Data to be stored for up 10 years will be kept on the University server in researcher's folder until graduation and within the School of Computing and Communications filestore post-graduation.

12. Please answer the following question *only* if you have not completed a Data Management Plan for an external funder.

12.a How will you make your data available under open access requirements?
Quantitative data and interview transcripts will be made available through Pure, although any identifiable data (such as mention of company name or systems used) will be removed and replaced with pseudonyms. Data will also be offered to the UK Data Archive as per the standard ESRC procedures. Permission to make data open access will be requested in the consent form (individuals who do not wish for this to occur will still be allowed to take part and their data will not be released.

12b. Are there any restrictions on sharing your data for open access purposes?
No- only potentially identifiable data will be removed

13. Will **audio or video recording** take place? ☐ no ☑ audio ☑ video

13a. Please confirm that portable devices (laptop, USB drive etc) will be **encrypted** where they are used for identifiable data. If it is not possible to encrypt your portable devices, please comment on the steps you will take to protect the data.
Recordings will be stored on a password laptop with the recordings encrypted using 7-zip software until they can be placed on the University server (where possible data will be placed straight on they University server).

13b. What arrangements have been made for **audio/video data storage**? At what point in the research will tapes/digital recordings/files be destroyed?
Video recordings will be destroyed once they have been viewed to verify water levels, this will occur within a month from recording. Audio data will be transcribed and then destroyed.

13c. If your study includes video recordings, what are the implications for participants' anonymity? Can anonymity be guaranteed and if so, how? If participants are identifiable on the recordings, how will you explain to them what you will do with the recordings? How will you seek consent from them?
Participants will be informed of the recordings from the outset and information on their use will be included on the consent forms. Additionally, cameras will be focused on the water tank levels and not focused on the participants.

14. What are the plans for dissemination of findings from the research? If you are a student, mention here your thesis. Please also include any impact activities and potential ethical issues these may raise.
Results of the research may be submitted for publication in an academic/professional journals, for presentation at conferences/ seminars and will also be included in my PhD thesis.

15. What particular ethical considerations, not previously noted on this application, do you think there are in the proposed study? All issues believed to have been discussed.

Are there any matters about which you wish to seek guidance from the FSTREC? No

Section Five

Additional information required by the university insurers

If the research involves either the nuclear industry or an aircraft
or the aircraft industry (other than for transport), please provide details below: N/a

Section Six

Declaration and Signatures

I understand that as Principal Investigator/researcher/PhD candidate I have overall responsibility for the ethical management of the project and confirm the following:

- I have read the Code of Practice, Research Ethics at Lancaster: a code of practice and I am willing to abide by it in relation to the current proposal.
- I will manage the project in an ethically appropriate manner according to: (a) the subject matter involved and (b) the Code of Practice and Procedures of the University.
- On behalf of the University I accept responsibility for the project in relation to promoting good research practice and the prevention of misconduct (including plagiarism and fabrication or misrepresentation of results).
- On behalf of the University I accept responsibility for the project in relation to the observance of the rules for the exploitation of intellectual property.
- If applicable, I will give all staff and students involved in the project guidance on the good practice and ethical standards expected in the project in accordance with the

University Code of Practice. (Online Research Integrity training is available for staff and students here.)

- If applicable, I will take steps to ensure that no students or staff involved in the project will be exposed to inappropriate situations.

☑ Confirmed

Please note: If you are not able to confirm the statement above please contact the FST Research Ethics Committee and provide an explanation.

Student applicants:

Please tick to confirm that you have discussed this application with your supervisor, and that they agree to the application being submitted for ethical review ☑

Students must submit this application from your Lancaster University email address, and copy your supervisor in to the email in which you submit this application

All Staff and Research Students must complete this declaration:

I confirm that I have sent a copy of this application to my Head of Department (or their delegated representative) . **Tick here to confirm** ☑

Name of Head of Department *(or their delegated representative)* Adrian Friday

Applicant electronic signature: Emma M. Hewlett Date 31.03.2017

Attached Information:

- Advertisement materials
- Participant Information Sheet
- Consent 1
- Study 1 details and interview schedule
- Questionnaires
- Debrief
- Consent 2
- Study 2 interview guide
- Final debrief

Advertisement Materials

Online SONA Advert (aimed at psychology students)

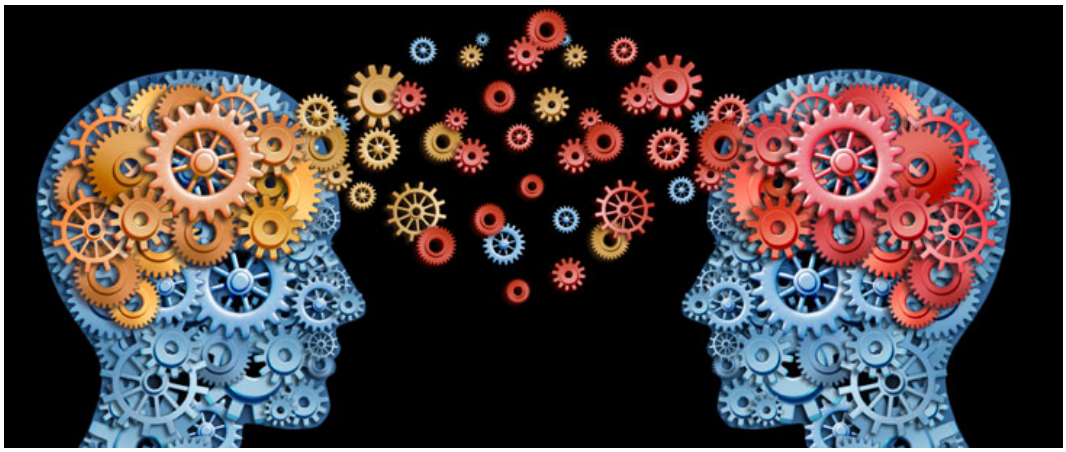
Study Name	Human factors in Cyber Physical Systems
Study Type	Standard (lab) study
Pay	£6
Duration	60 mins
Description	This work looks at personality, system knowledge and decision-making within a cyber physical system context. If you are happy to take part, then you will be given an online personality test to complete and asked to take part in two studies one lab experiment and two interviews (these occur during the same session).
Preparation	Following sign-up, you will be asked to fill in a demographic and personality questionnaire, please have completed this before you arrive.
Eligibility	Native English speaker or highly fluent in English
Researcher	Emma Hewlett
Deadlines	Sign-Up: 9 hours before the appointment Cancellation: 12 hours before the appointment

Flyer

Lancaster University

Participants Wanted!

Take part in a simple simulation study & earn money



We are looking for individuals to take part in simulation of an industry plant to investigate personality and decision-making:

Who can take part? Anyone who speaks English ☺

Where? Infolab on campus

How Much? £6 for up to 1 hour

Interested?

Contact: <email>
<phone>

Targeted invitation email

Subject: Research study- earn extra money!

Dear *[Insert name]*,

I would like to invite your organisation to take part in a study looking at decision making in relation to Cyber Physical System. This work is targeted at individuals who work closely with industrial control systems on a daily basis such as system operators and/ or engineers and will involve taking part in a simulation study. I would be grateful if you could disseminate this study and the attached information sheet to any relevant individuals, anybody who would like to take part will be given £6 as a thank-you for their time (up to 1 hour).

If you anyone else would like to take part in this work then please read the attached information and get in touch with me.

Kind regards,

Emma Hewlett

[Participant Information Sheet to be attached]

School of Computing and Communications

Participant information sheet- Human Factors in Cyber Physical Systems

I am a PhD student at Lancaster University and I would like to invite you to take part in a research study about personality and decision making in cyber physical systems.

Please take time to read the following information carefully before you decide whether or not you wish to take part.

What is the study about?
This work looks at personality, system knowledge and decision-making within a cyber physical system context. If you are happy to take part, then you will be given an online personality test to complete and asked to take part in two studies.

Why have I been invited?
I have approached you because you because as well as personality I would like to investigate how different types of system knowledge impact decision-making and so I am seeking to recruit both experts and novices in different systems.

What will I be asked to do if I take part?
If you decided to take part, this would involve the following activities (It should take no longer than 1 hour):

Study one:
This study uses a simplified water plant test-bed and involves observations of you reporting water levels and responding to any simulated email requests for information relating to the system. During this study, I will be watching behaviour, and a video recording of the test-bed will be taken (this is for assessing the test-bed and to verify water levels at different time points, whilst you may enter the frame it will not be aimed at you). The video will be destroyed once it has been used to record water values.

Questions:
Following this study, you will be interviewed before being asked to complete a short questionnaire and personality test. The interview will be audio recorded.

Study two:
This study interview will be presented with various scenarios regarding different issues and presented with various options to determine the cause while being asked to explain your thinking aloud. This study will be audio recorded.

What are the possible benefits from taking part?

There are no specific benefits to you taking part in this study, however your participation may increase our understanding of this topic area. You will also be given £6 as a thank you for your time

Do I have to take part?
No. It's completely up to you to decide whether or not you take part. Your participation is voluntary and you are free to withdraw at any time before or during the study, you may also withdraw your data for up to two weeks after the study.

If you decide not to take part in this study, this will not affect your studies and the way you are assessed on your course/ If you decide not to take part in this study, this will not affect your position in the company and your relations with your employer. *[To be deleted as appropriate]*

What if I change my mind?
You may withdraw your data anytime up to two weeks after the experiment, at which point data may be pooled together. If you wish to withdraw you will need to contact the researcher, using the details below, and provide your participant reference number so please keep a record of this.

What are the possible disadvantages and risks of taking part?
There should be no major disadvantages to taking part, however this study may take around one hour of your time.

Will my data be identifiable?
After the observations and interview only I, the researcher conducting this study, and my supervisors will have access to the data you share with me

I will keep all personal information about you (e.g. your name and other information about you that can identify you) confidential, that is I will not share it with others. Audio recordings will be transcribed and anonymised

How will my data be stored?
Your data will be stored in encrypted files (that is no-one other than me, the researcher will be able to access them) and on password-protected computers.

I will keep hard copies of any data (such as consent forms) securely in a locked cabinet in my office.

In accordance with University guidelines, the data will be kept securely for a minimum of ten years.

How will we use the information you have shared with us and what will happen to the results of the research study?
The data that you share will only be used for academic purposes, this may include:

- My PhD thesis
- Academic journal papers
- Conference proceedings

When writing up the findings from this study, I would like to reproduce some of the views and ideas you shared with me. When doing so, I will only use anonymised quotes (e.g. from our interview with you), so that although I will use your exact words, you cannot be identified in our publications.

Who has reviewed the project?
This study has been reviewed and approved by the Faculty of Science and Technology Research Ethics Committee.

What if I have a question or concern?
If you have any queries or if you are unhappy with anything that happens concerning your participation in the study, please contact myself (Emma Hewlett) at: <email>;
B64, B - Floor, Infolab21, Lancaster University

Alternatively, you may contact my supervisor Prof. Awais Rashid at: <email>
<phone>
B52, B - Floor, Infolab21, Lancaster University

Alternatively, if you have any concerns or complaints that you wish to discuss with a person who is not directly involved in the research, you can also contact Prof. Adrian Friday: <email>
<phone>;
Infolab21, Lancaster University

Thank you for considering your participation in this project.

CONSENT FORM 1

Project Title: Human Factors in Cyber Physical Systems

Name of Researchers: Emma Hewlett
Email: <email>

Please tick each box

1. I confirm that I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily ☐
2. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason. If I withdraw within 2 weeks of commencement of the study my data will be removed. ☐
3. 'I consent that my data (including anonymised interview transcript) can be made open access (NB: You are free to leave this box unchecked and to still participate in the study). ☐
4. I understand that any information given by me may be used in future reports, academic articles, publications or presentations by the researcher/s, but my personal information will not be included and I will not be identifiable. ☐
5. I understand that my name and my organisation's name will not appear in any reports, articles or presentation without my consent. ☐
6. I understand that audio recording will occur throughout the study and that this will be transcribed with data protected on encrypted devices and kept secure. ☐
7. I understand that a video recorder will be used to record the test-bed and this may capture images of me, I understand that this video will be destroyed once the data has been viewed. ☐
8. I understand that data will be kept according to University guidelines for a minimum of 10 years after the end of the study. ☐
9. I understand that some of the reasons for conducting this study may have been withheld and will be explained to be fully following completion of the study. ☐
10. I agree to take part in the above study. ☐

Name of Participant	Date	Signature

I confirm that the participant was given an opportunity to ask questions about the study, and all the questions asked by the participant have been answered correctly and to the best of my ability. I

confirm that the individual has not been coerced into giving consent, and the consent has been given freely and voluntarily.

Signature of Researcher /person taking the consent_____ Date

_____ Day/month/year

One copy of this form will be given to the participant and the original kept in the files of the researcher at Lancaster University

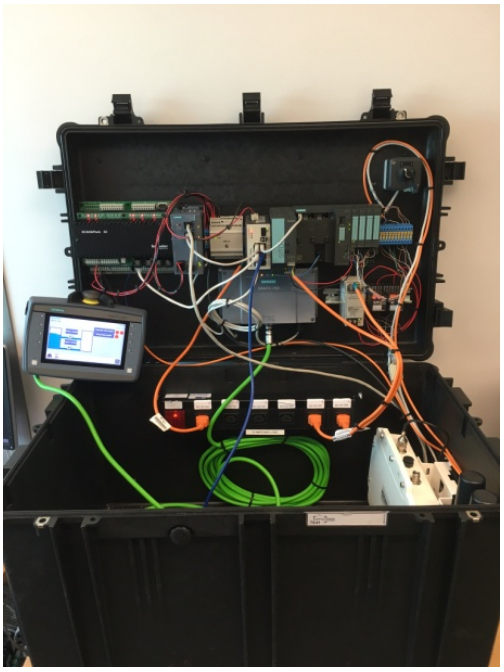
Study 1

Participant instructions:

This system is a very simplified representation of a water treatment plant containing two connected water containers that pump water between them. The water levels in these containers are then displayed on a Human Machine Interface (HMI). Within this task you are playing the role of a control room operator and will be in charge of monitoring the water levels, since this is a simplified task you are also asked to record these water levels every minute and to respond to any organisational 'requests', you can choose to verbally respond to these requests as if you were phoning back or via email.

If you have any questions about the test-bed or your task please let me know.

Image of portable portion of the testbed



Scenario: Participants within each group (student, IT student, system operators) will complete their activity while the following conditions are implemented (order counterbalanced via using Latin squares).

Time	4mins	8mins	12mins	14mins	18mins	20mins
Participant 1	Email request	Replay attack (1)	Man-in-the middle-attack (2)	Man-in-the middle-attack (4)	Fuzzing attack/ system crash (3)	Webcam attack
Participant 2	Email request	Man-in-the middle-attack (2)	Fuzzing attack/ system crash (3)	Replay attack (1)	Man-in-the middle-attack (4)	Webcam attack

Participant 3	Email request	Fuzzing attack/ system crash (3)	Man-in-the middle-attack (4)	Man-in-the middle-attack (2)	Replay attack (1)	Webcam attack
Participant 4	Email request	Man-in-the middle-attack (4)	Replay attack (1)	Fuzzing attack/ system crash (3)	Man-in-the middle-attack (2)	Webcam attack

Scenario incidents

Email request: Will be a message from a technician conducting measurements asking for confirmation of the water levels at start+5mins.

Replay Attack (1): This will involve data being played back after a delay e.g. 30 seconds so that the water readings whilst following the correct pattern will be out of sync with the water tanks.

Man-in-the-middle Attack (2): This will involve the water readings showing the complete opposite (water tanks switched) but realistic levels

Fuzzing Attack (3): This will involve crashing the system so that the HMI is unable to display the readings

Man-in-the-middle Attack (4): This will involve the levels remaining steady.

Webcam attack: This will involve the webcam (and corresponding LED) on, although no recordings will be taken.

Whilst these attacks are not representative of the how these attacks may be used (e.g. a man-in-the-middle attack may be used to show correct looking information while water is drained they will show a discrepancy between water levels and HMI readings as well as potentially sudden changes in readings that will allow consideration of how an individual may respond. *[Attacks may be varied slightly based on testbed configuration]*

Observation Sheet Example (For Participants)

Time	Water Level	Notes

Lancaster University

Observation Sheet Example (For Experimenter)

Time	Water level Correct (Y/N)	Behaviours	Comments

Interview schedule:

Thank for participation and explain audio recording

Did not identify attack (ask as appropriate, if nothing strange detected can end questions):

1. Did you have any issues during the simulation?
2. Were there any strange behaviours during the simulation?
    a. Can you describe them
3. If these types of issues occurred during a work day what would you consider to be the possible causes?
    a. What would you consider to be the most likely cause?
    b. How would you investigate the cause?

Did identify the attack:

1. You mentioned strange behaviours, can you describe these behaviours?
2. What did you think was the cause?
3. If these types of issues occurred during a work day what would you consider to be the possible causes?
    a. What would you consider to be the most likely cause?
    b. How would you investigate the cause?

Lancaster University

Questionnaire- Human Factors in Cyber Physical Systems

Participant reference number:

Demographics
Gender: Male/Female/Prefer not to say
Age: 18-21yrs/ 22-25yrs/26-30/31-35/36-40/41-45/46-50/ 51+years
Are you a student? If yes: What department are you based in?
If no: What is your job title?

Security Expertise

1. Have you ever taken or taught a course on computer security?
2. Have you attended a computer security conference in the past year?
3. Has computer security ever been one of your primary job responsibilities in the last five years?
4. Have you ever used SSH?
5. Have you ever configured a firewall?
6. Do you have an up-to-date virus scanner on your computer?

Cyber Physical System Expertise

1. Does your role involve you working with Cyber Physical Systems/ Industrial Control Systems on a regular basis?
    a. Daily/ Weekly/ Monthly
2. How long have you worked with these systems? <1year/ 1-2years/ 3-5 years/ 6-10years/ 10years+
3. Are you involved in the system operation/ maintenance/ or repair?
4. Have you received any security training in relating to this system?

Personality
Using Big Five Inventory (44-item inventory)[3]
Study 2

Please would you talk me through the actions you would take when presented with the following scenarios, in which order and why (please feel free to define alternative actions). Please also describe whether you would consider such an event as likely to result from a cyber-attack and what information you would need or seek to determine if this was the case.

For system operators:

Scenario 1: The control room human user interface crashes and no longer provides any information.

[3] (John, O. P., & Srivastava, S. (1999). The Big-Five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), Handbook of personality: Theory and research (Vol. 2, pp. 102–138). New York: Guilford Press. http://moityca.com.br/pdfs/bigfive_John.pdf); Industrial Control System

Scenario 2: The information you are receiving in the control room is not accurate e.g. in a water plant the water levels are consistently a little lower than being reported.

For non-system operators:

Scenario 1: you notice that your webcam light is turned on even when you are not using the webcam and believe it to be turned off. What actions would you take?

Scenario 2: The load up time on your 6 month old laptop has noticeably increased, now taking several minutes. What actions would you take?

Lancaster University

School of Computing and Communications

Debrief sheet- Human Factors in Cyber Security of Cyber Physical Systems

What this study was really about?
Whilst this work is interested in knowledge, personality and decision making its focus is on cyber security and whether individuals can identify when their systems are being maliciously manipulated. Therefore, throughout the simulation, the system was subjected to several potential cyber-attacks such as a Man-in the-middle attacks: where the HMI displayed false information relating to the water levels. Additionally, the laptop webcam was switched on towards the end of the simulation to observe if suspicious activity could be recognised on a computer system.

Why was I not informed of this?
This study wanted to examine if individuals consider malicious intervention to be a reason for suspicious behaviour, you were therefore not informed to make sure that you were not prime to consider security aspects.
previous work has suggested that having different types of knowledge, experience and personality types can aid individuals in identifying cyber-attacks, this work therefore examined whether this remains the case within a cyber physical system.

What if I have a question or would like to withdraw?
If you have any queries or if you are unhappy with anything that happens concerning your participation in the study, please contact myself (Emma Hewlett) at: <email>**;**
Please be aware that after two weeks data will be pooled and it may no longer possible to identify and remove.

Alternatively, you may contact my supervisor Prof. Awais Rashid at: <email>;

If you have any concerns or complaints that you wish to discuss with a person who is not directly involved in the research, you can also contact Prof. Adrian Friday:
<email>;
<phone>;
Infolab21, Lancaster University

Additional information:
If you would like more information on the cyber threats that are faced by organisations and Cyber Physical Systems then this can be found on the website of the Centre for Protection of National Infrastructure (CPNI):
https://www.cpni.gov.uk/.

Thank you for your participation in this project.

APPENDIX I

STATISTICAL OUTPUTS FROM THE CYBER ATTACKS IN AN INDUSTRIAL CONTROL SYSTEM

This Appendix presents the statistical outputs that were created for the experimental study into the detection of cyber attacks against an Industrial Control System detailed in Chapter 7.

I.1 Statistical Analyses to Investigate Whether Some Attacks are Easier to Observe Than Others in a Waterplant Testbed

I.1.1 Outputs From the Cochrans Q Test to Explore Which Attacks Are Easier to Observe

A Cochrans Q test can be used to determine whether or not there are any differences in a dichotomous dependent variable between three or more related groups. In this context it was used to explore the number of people who observed different attack scenarios.

This test has three conditions:

1. It must have one dichotomous dependent variable, in this case whether an attack scenario is observed or not.
2. It must have one independent variable that consists of three or more categorical, related groups, in this case the various cyber attack conditions.
3. The participants were recruited from a random sample.

All three of these assumptions were met, there is also however some guidance on the number of participants required in order to be able to run the standard Cochrans Q test and to be able

to interpret the asymptotic p-value. To meet the sample size conditions n (where n= total no. of participants, minus the number of who scored the same across each condition e.g. observed all attacks or none of the attacks) must be equal or greater than 4. Additionally, nk (where k is number of conditions) must be equal to or greater than 24.

In this study N= 41 (participants who were unable to clearly articulate which attacks they observed were removed from this analysis), 13 individuals failed to identify any of the attacks, and no individuals identified all of the attacks. Therefore n (41-13)= 28. nk is then 28 x 5= 140. This study therefore meets the minimum sample size requirements.

Running this test then produces the output seen in Figure I.1. This figure shows a significant finding.

Test Statistics

N	41
Cochran's Q	34.247[a]
df	4
Asymp. Sig.	.000

a. 1 is treated as a success.

Figure I.1: Output of the Cochran Q Test for Detecting Attacks in an ICS

Since this test was statistically significant, post hoc tests were conducted using Dunn's test with Bonferroni corrections, to identify which of the conditions were significantly different from each other. The results of these tests can be seen in Figure I.2. This figure shows five significant results that are discussed in Chapter 7.

I.2 What Level of Variance in the Observation of Different Cyber Attacks Can Be Explained By Looking at Participant's Demographic Factors

I.2.1 Predicting the Probability That an Individual Will Observe a Logic Upload Attack

A binomial logistic regression analysis attempts to predict the probability that an observations falls into one of two categories in a dichotomous dependent variable (in this case whether a logic upload attack was observed) based on one or more categorical or continuous independent variables. In this test the independent variables were gender, extraversion and neuroticism.

This test has six assumptions that must be met:

Pairwise Comparisons

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
Webcam-Replay	-.024	.093	-.262	.794	1.000
Webcam-Logic_Upload	-.195	.093	-2.094	.036	.363
Webcam-Value_Tampering	-.293	.093	-3.141	.002	.017
Webcam-DoS	-.463	.093	-4.973	.000	.000
Replay-Logic_Upload	-.171	.093	-1.832	.067	.670
Replay-Value_Tampering	-.268	.093	-2.879	.004	.040
Replay-DoS	-.439	.093	-4.711	.000	.000
Logic_Upload-Value_Tampering	-.098	.093	-1.047	.295	1.000
Logic_Upload-DoS	.268	.093	2.879	.004	.040
Value_Tampering-DoS	.171	.093	1.832	.067	.670

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.
Asymptotic significances (2-sided tests) are displayed. The significance level is .05.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

Figure I.2: Results of the Cochran Q Post-Hoc Tests for Observing Attacks in an ICS

1. You have one dichotomous dependent variable, in this case this is whether a participant observes the logic upload attack.
2. You have one or more independent variables that are either continuous or nominal.
3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.
4. You should have a minimum of 15 participants for each independent variable.
5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.
6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, assumption 4 would suggest that only two independent variables should be explored, however whilst it would reduce the reliability of any estimates, because this research was exploratory it was determined that it would still be beneficial to explore a third variable.

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure I.3. To understand if the assumption is met we need look at the three highlighted lines.

In this test if the result is significant the 'sig.' column is lower than 0.5 then the continuous independent variable is not linearly related to the logit of the dependent variable, and it has failed the assumption of linearity. Fortunately however as can be seen in this case the assumption is met as none of the results are significant.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	1.288	.825	2.438	1	.118	3.627
	Extraversion	1.467	2.484	.349	1	.555	4.338
	Neuroticism	-3.970	2.266	3.070	1	.080	.019
	Extraversion by ln_extraversion	-.335	.583	.329	1	.566	.716
	Neuroticism by ln_neuroticism	.940	.531	3.132	1	.077	2.561
	Constant	11.719	20.584	.324	1	.569	122885.535

a. Variable(s) entered on step 1: Gender, Extraversion, Neuroticism, Extraversion * ln_extraversion , Neuroticism * ln_neuroticism .

Figure I.3: Testing Assumption 5 that There is a Linear Relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variable (Whether the Logic Upload Attack Was Observed)

Assumption 6 states that their should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2.5 standard deviations. As can be seen in Figure I.4 and the 'ZResid' column, one was identified as beyond + or -2 however it was still within the acceptable limits.

Casewise List[b]

Case	Selected Status[a]	Observed Logic_Upload	Predicted	Predicted Group	Temporary Variable Resid	ZResid	SResid
28	S	Y**	.114	N	.886	2.787	2.200

a. S = Selected, U = Unselected cases, and ** = Misclassified cases.

b. Cases with studentized residuals greater than 2.000 are listed.

Figure I.4: Testing Assumption 6 that There Are No Outliers in the Data Sample for the Logic Upload Attack

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure I.5. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the mode, as can be seen from the model row the model fit was insignificant with p=.366.

This is likely due to the model predicting a very small amount of the variance in detection of logic upload attacks. This Nagelkerke R2 value in this table shows that the model explains only 10.8% of the variance.

Given that this model was insignificant the rest of the outputs are not detailed here.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	3.171	3	.366
	Block	3.171	3	.366
	Model	3.171	3	.366

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	44.517[a]	.074	.108

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Figure I.5: Outputs of the Binomial Regression Analysis for Observing Logic Upload Attacks

I.2.2 Predicting the Probability That an Individual Will Detect a Value Tampering Attack

A second binomial logistic regression analysis was conducted to explore if we could predict who would observe a Values tampering Attack. Again, this test has six assumptions that must be met:

1. You have one dichotomous dependent variable, in this case this is whether a participant observes the value tampering attack.
2. You have one or more independent variables that are either continuous or nominal.
3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.
4. You should have a minimum of 15 participants for each independent variable.
5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.
6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, assumption 4 would suggest that only two independent variables should be explored, however whilst it would reduce the reliability of any estimates because this research is exploratory it was determined that it would still be beneficial to explore a third variable.

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure I.6 and to understand if the assumption is met we need look at the three highlighted lines. In this test if the result is significant the 'sig.' column is lower than 0.5 then the continuous independent variable is not linearly related to the logit of the dependent variable and it has failed the assumption of linearity. Fortunately however as can be seen in this case the assumption is met.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	-.121	.741	.027	1	.870	.886
	Extraversion	1.835	2.024	.822	1	.365	6.263
	Neuroticism	-2.522	2.016	1.565	1	.211	.080
	Extraversion by ln_extraversion	-.420	.475	.784	1	.376	.657
	Neuroticism by ln_neuroticism	.601	.473	1.613	1	.204	1.824
	Constant	1.903	17.027	.012	1	.911	6.705

a. Variable(s) entered on step 1: Gender, Extraversion, Neuroticism, Extraversion * ln_extraversion , Neuroticism * ln_neuroticism .

Figure I.6: Testing Assumption 5 that There is a Linear Relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variable (Observing a Value Tampering Attack)

Assumption 6 states that their should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2 standard deviations. As can be seen in Figure I.7, there were no outliers in this dataset in relation to values tampering attack and so this assumption was me.

Casewise List[a]

a. The casewise plot is not produced because no outliers were found.

Figure I.7: Testing Assumption 6 that There Are No Outliers in the Value Tampering Attack Data Sample

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure I.8. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the model, as can be seen from the model row the model fit was insignificant with p=.880.

This is likely due to the model predicting a very small amount of the variance in observation of logic upload attacks. The Nagelkerke R2 value in this table shows that the model explains only 2.2% of the variance.

Given that this model was insignificant the rest of the outputs are not detailed here.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	.670	3	.880
	Block	.670	3	.880
	Model	.670	3	.880

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	53.180[a]	.016	.022

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Figure I.8: Outputs of the Binomial Logistic Regression Analysis into Observing Value Tampering Attacks

I.2.3 Predicting the Probability That an Individual Will Observe a Replay Attack

A third binomial logistic regression analysis was conducted to explore whether gender, extraversion and neuroticism could be used to predict who would observe a replay attack. This test has six assumptions that must be met:

1. You have one dichotomous dependent variable, in this case this is whether a participant observes the replay attack.
2. You have one or more independent variables that are either continuous or nominal.
3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.
4. You should have a minimum of 15 participants for each independent variable.
5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.
6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, assumption 4 would suggest that only two independent variables should be explored, however whilst it would reduce the reliability of any estimates because this research is exploratory it was determined that it would still be beneficial to explore a third variable.

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure I.9 and to understand if the assumption is met we need look at the three highlighted lines. In this test if the result is significant so the 'sig.' column is lower than 0.5 then the continuous independent variable is not linearly related to the logit of the dependent variable and it has failed the assumption of linearity. Fortunately however as can be seen in this case the assumption is met.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	.539	1.233	.191	1	.662	1.715
	Extraversion	9.445	12.653	.557	1	.455	12639.843
	Neuroticism	.824	5.986	.019	1	.890	2.280
	Extraversion by ln_extraversion	-2.073	2.839	.533	1	.465	.126
	Neuroticism by ln_neuroticism	-.257	1.477	.030	1	.862	.773
	Constant	-74.185	95.589	.602	1	.438	.000

a. Variable(s) entered on step 1: Gender, Extraversion, Neuroticism, Extraversion * ln_extraversion , Neuroticism * ln_neuroticism .

Figure I.9: Testing Assumption 5 That There is a Linear Relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variable (Observing a Replay Attack)

Assumption 6 states that their should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2 standard deviations. As can be seen in Figure I.10, there were no outliers in this dataset in relation to observing the replay attack and so this assumption was met.

Casewise List[b]

Case	Selected Status[a]	Observed Replay	Predicted	Predicted Group	Temporary Variable Resid	ZResid	SResid
3	S	Y**	.099	N	.901	3.020	2.240
41	S	Y**	.154	N	.846	2.341	2.027

a. S = Selected, U = Unselected cases, and ** = Misclassified cases.

b. Cases with studentized residuals greater than 2.000 are listed.

Figure I.10: Testing Assumption 6 That There Are No Outliers in the Replay Attack Data Sample

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure I.11. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the mode, as can be seen from the model row, the model fit was significant with p=.045. The second table then shows Hosmer and Lemeshow goodness of fit test which analyses how poor the model is at predicting the categorical outcomes, in this case we want the model to be insignificant, as it is.

Since the model is significant we can look at the table in Figure I.12 so that we can see how much variance in the observation of a replay attack is explained by tested independent variables. The Nagelkerke R2 value in this table shows that the model explains 37.7% of the variance.

We can then assess the observed and predicted classifications in Figure I.13.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	8.035	3	.045
	Block	8.035	3	.045
	Model	8.035	3	.045

Hosmer and Lemeshow Test

Step	Chi-square	df	Sig.
1	7.374	8	.497

Figure I.11: Outputs of the Binomial Logistic Regression Analysis for Observing a Replay Attack

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	18.179[a]	.178	.377

a. Estimation terminated at iteration number 7 because parameter estimates changed by less than .001.

Figure I.12: Model Fit to Look at the Level of Variance Explained in Whether Individuals Observe Replay Attacks

Classification Table[a]

			Predicted		
			Replay		
	Observed		No	Yes	Percentage Correct
Step 1	Replay	No	37	0	100.0
		Yes	3	1	25.0
	Overall Percentage				92.7

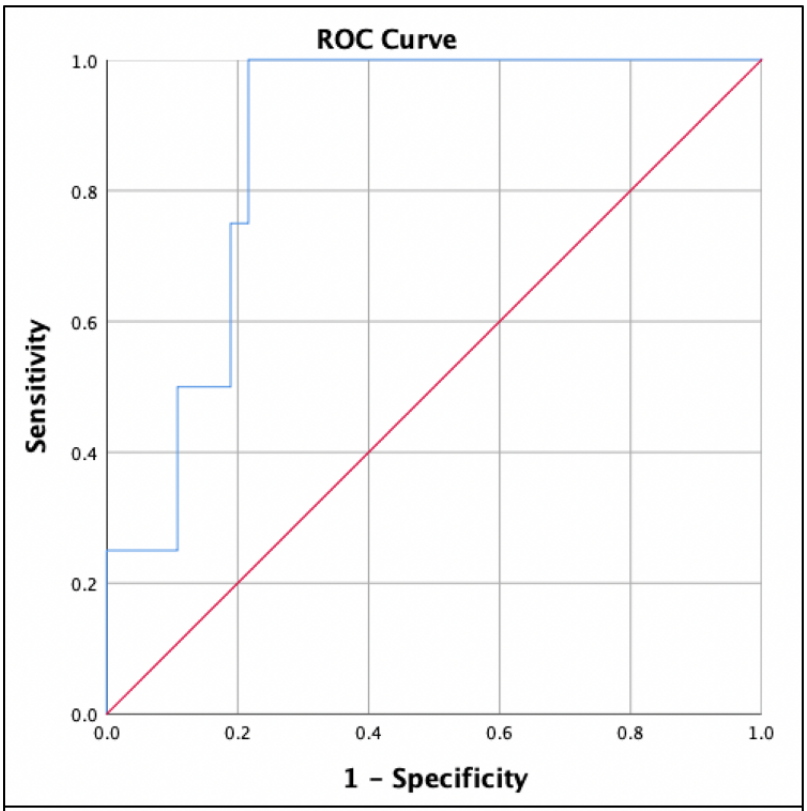
a. The cut value is .500

Figure I.13: The Observed and Predicted Classifications for Observing a Replay Attack

Finally, we can produce a ROC curve which can be used to calculate an overall measure of discrimination for the model.

You can see in Figure I.14 that the area under the ROC curve is .872. The area can range from 0.5 to 1.0 with higher values representing better discrimination. According to [233] a value of .872 puts the discrimination of this model at the upper border of acceptable discrimination.

Having established that the model is significant we can explore in detail which of the tested independent variables had a significant effect on the model using the variables in the equation



Area Under the Curve

Test Result Variable(s): Predicted probability

Area	Std. Error[a]	Asymptotic Sig.[b]	Asymptotic 95% Confidence Interval	
			Lower Bound	Upper Bound
.872	.062	.016	.750	.993

a. Under the nonparametric assumption

b. Null hypothesis: true area = 0.5

Figure I.14: ROC Curve Figure and Results for Observing a Replay Attack

table (Figure I.15). The implications of these findings are discussed on Chapter 7.

I.2.4 Predicting the Probability That an Individual Will Observe a DoS Attack

A fourth binomial logistic regression analysis was conducted to explore whether gender, extraversion and neuroticism could be used to predict who would successfully observe a DoS attack. This test has six assumptions that must be met:

1. You have one dichotomous dependent variable, in this case this is whether a participant observes the DoS attack.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)	95% C.I.for EXP(B) Lower	Upper
Step 1[a]	Gender(1)	.575	1.225	.220	1	.639	1.777	.161	19.611
	Extraversion	.262	.163	2.574	1	.109	1.299	.944	1.789
	Neuroticism	-.277	.191	2.103	1	.147	.758	.522	1.102
	Constant	-3.995	5.646	.501	1	.479	.018		

a. Variable(s) entered on step 1: Gender, Extraversion, Neuroticism.

Figure I.15: Impact of Each of the Independent Variables on the Model for Observing a Replay Attack

2. You have one or more independent variables that are either continuous or nominal.

3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.

4. You should have a minimum of 15 participants for each independent variable.

5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.

6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, assumption 4 would suggest that only two independent variables should be explored, however whilst it would reduce the reliability of any estimates because this research is exploratory it was determined that it would still be beneficial to explore a third variable.

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure I.16 and to understand if the assumption is met we need look at the three highlighted lines. In this test if the result is significant- 'sig.' is lower than 0.5 then the continuous independent variable is not linearly related to the logit of the dependent variable and it has failed the assumption of linearity. Fortunately however as can be seen in this case, the assumption is met.

Assumption 6 states that there should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2 standard deviations. As can be seen in Figure I.17, there were no outliers in this dataset in relation to a DoS attack.

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure I.18. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the mode, as can be seen from the model row the model fit was insignificant with p=.706. The Nagelkerke R2 value in this table shows that the model only explained 4.5% of the variance.

Given that this model was insignificant the rest of the outputs are not detailed here.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	.639	.715	.800	1	.371	1.895
	Extraversion	1.535	1.733	.785	1	.376	4.642
	Neuroticism	.793	1.924	.170	1	.680	2.210
	Extraversion by ln_extraversion	-.356	.408	.762	1	.383	.701
	Neuroticism by ln_neuroticism	-.178	.451	.156	1	.693	.837
	Constant	-15.001	15.483	.939	1	.333	.000

a. Variable(s) entered on step 1: Gender, Extraversion, Neuroticism, Extraversion * ln_extraversion , Neuroticism * ln_neuroticism .

Figure I.16: Testing Assumption 5 That There is a Linear Relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variable (Observing a DoS Attack)

Casewise List[a]

a. The casewise plot is not produced because no outliers were found.

Figure I.17: Testing Assumption 6 That There Are No Outliers in the Data Sample for Observing a DoS Attack

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	1.399	3	.706
	Block	1.399	3	.706
	Model	1.399	3	.706

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	55.220[a]	.034	.045

a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.

Figure I.18: Output of the Binomial Logistic Regression Analysis into Observing a DoS Attack.

I.2.5 Predicting the Probability That An Individual Will Observe a Webcam Attack

A fifth binomial logistic regression analysis was conducted to explore whether gender, extraversion and neuroticism could be used to predict who can observe a webcam attack. This test has six assumptions that must be met:

1. You have one dichotomous dependent variable, in this case this is whether a participant observes the webcam attack.
2. You have one or more independent variables that are either continuous or nominal.
3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.
4. You should have a minimum of 15 participants for each independent variable.
5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.
6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, assumption 4 would suggest that only two independent variables should be explored, however whilst it would reduce the reliability of any estimates because this research is exploratory it was determined that it would still be beneficial to explore a third variable.

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure I.19 and to understand if the assumption is met we need look at the highlighted three lines. In this test if the result is significant i.e. the 'sig.' column is lower than 0.5 then the continuous independent variable is not linearly related to the logit of the dependent variable and it has failed the assumption of linearity. Fortunately however as can be seen in this case the assumption is met.

Assumption 6 states that their should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2 standard deviations. As can be seen in Figure I.20, there were three data points that were highlighted, fortunately however none of these were greater than + or - 2.5 standard deviations out and so this assumption was met.

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure I.21. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the mode, as can be seen from the model row the model fit was insignificant with p=.641.

This is likely due to the model predicting a very small amount of the variance in detection of logic upload attacks. This Nagelkerke R2 value in this table shows that the model explains only 9.9% of the variance.

Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Gender(1)	1.271	1.885	.455	1	.500	3.563
	Extraversion	33.918	33.061	1.053	1	.305	5.373E+14
	Neuroticism	13.630	13.193	1.067	1	.302	830581.787
	Extraversion by ln_extraversion	-7.713	7.525	1.050	1	.305	.000
	Neuroticism by ln_neuroticism	-3.191	3.107	1.055	1	.304	.041
	Constant	-314.737	249.875	1.587	1	.208	.000

a. Variable(s) entered on step 1: Gender, Extraversion, Neuroticism, Extraversion * ln_extraversion , Neuroticism * ln_neuroticism.

Figure I.19: Testing Assumption 5 That There is a Linear Relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variable (Observing a Webcam Attack)

Casewise List[b]

Case	Selected Status[a]	Observed Webcam	Predicted	Predicted Group	Temporary Variable Resid	ZResid	SResid
8	S	Y**	.098	N	.902	3.034	2.281
12	S	Y**	.069	N	.931	3.663	2.361
31	S	Y**	.132	N	.868	2.562	2.112

a. S = Selected, U = Unselected cases, and ** = Misclassified cases.

b. Cases with studentized residuals greater than 2.000 are listed.

Figure I.20: Testing Assumption 6 That There Are No Outliers in the Webcam Attack Data Sample

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	1.682	3	.641
	Block	1.682	3	.641
	Model	1.682	3	.641

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	19.782[a]	.040	.099

a. Estimation terminated at iteration number 6 because parameter estimates changed by less than .001.

Figure I.21: Outputs of the Binomial Logistic Regression Analysis into Who Can Observe a Webcam Attack

Given that this model was insignificant the rest of the outputs are not detailed here.

I.2.6 Statistics for the Mann Whitney U to Test If Gender Affects Observations of Attacks in an ICS

The final statistical test that was conducted as part of the ICS observation study was a Mann Whitney U test to investigate the impact of gender on attack observation. This test is a rank based non-parametric test that is used to determine whether there are differences between two groups on a dependent variable that can be continuous or ordinal- in this case the dependent variable is the number of attacks observed so continuous. This test was selected as the data was not expected to be normally distributed.

This particular statistical test has four assumptions that need to be met:

1. You have one dependent variable that is either continuous or ordinal.

2. You have one independent variable that is made up of two categorical, independent groups, in this case this is gender.

3. There needs to be no relationship between the observations in each group of the independent variable or between the groups themselves i.e. each participant only belongs to one of the groups. This assumption was met when assigning participants to groups based on gender.

4. You must determine whether the distribution of scores for both groups of your independent variable (e.g., the distribution of scores for 'males' vs 'females') have the same shape or a different shape. This determines how you interpret the results of the Mann-Whitney U test.

The data set for this test meets assumptions 1-3. The outputs of the Mann-Whitney U test (See Figure I.22) then reveals that the distribution scores are not similar and so in this instance the test is used to compare mean ranks (rather than the medians).

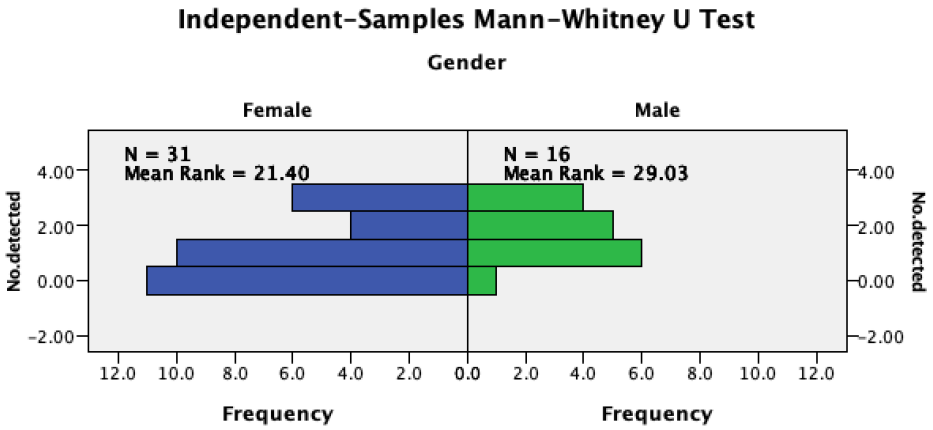


Figure I.22: Histogram Outputs to Examine the Distribution of Attack Observation Scores for Both Genders

The full outputs from this test can then be seen in Figure I.23. The figure shows that this finding was not significant and this is discussed in more detail in Chapter 7.

Total N	47
Mann-Whitney U	167.500
Wilcoxon W	663.500
Test Statistic	167.500
Standard Error	42.901
Standardized Test Statistic	-1.876
Asymptotic Sig. (2-sided test)	.061

Figure I.23: Mann-Whitney U Outputs of Attack Observation Scores for Both Genders

APPENDIX J

DETECTING ATTACKS USING SCADA DATA OUTPUTS- ETHICS PROPOSAL

This Appendix presents the approved ethics proposal for the experimental study into whether people can detect attacks from a SCADA system, detailed in Chapter 8.

Faculty of Engineering Research Ethics Committee
APPLICATION FOR RESEARCH ETHICS APPROVAL

Reference Number (for office use):

1. Title of the research:
Human Factors in Cyber Security of Cyber Physical Systems- Detection of attacks against a water control plant (OpenScada)

2. Name of Applicant, with their job title:
Emma Hewlett- PhD Student
Contact No: <phone>

3. Name of Supervisor (if applicant is a postgraduate or undergraduate student), with their job title:
Bristol supervisor: Awais Rashid (Professor of Cyber Security)
External Supervisors: Paul Taylor (Professor of Psychology, Aston University), Utz Roedig (Professor of Computer Science at University College Cork)

4. Other investigator(s) involved, with their job title:
N/a

5. Source of funding and grant code:
Bristol Cyber Security Group

6. Does this source of funding place any restrictions on public dissemination (publication, etc.) of the results of the research? If yes, please say what these are.
No

7. Background and aims of the research:
Earlier work identified that a fair proportion of people were able to detect attacks against an industrial Control System (ICS) using the security Lancaster waterplant testbed, however all of the participants were poor at detecting one particular attack, a replay attack.

This research explores whether cyber attacks, including a replay attack, are observable by human users from the data outputs of an ICS. In addition, it explores the effects of priming on where individuals attribute the blame of any suspicious behaviour and whether an attack has an impact on the participants workload.

8. Who will be recruited to participate in the research?
This work will seek to recruit approximately 75 participants. Participants will need to be at least 18 years of age, speak fluent English and have normal or corrected normal vision.

9. How many participants will be recruited?
This study will aim to recruit 50-100 participants

10. How will the participants be recruited?
Participants will be recruited through the following methods:
1. Via School of Psychological Science's experiment webpage.
2. In posters placed around the Merchants Venturers Building and wider campus
3. On social media

11. Are there any potential participants who will be excluded. If so, what are the exclusion criteria?

Individuals will only be excluded if they have poor English skills (i.e. are likely to not understand descriptions of technical systems), or if they are visually impaired, this is due to the requirement to use a visual interface for the experiment.

12. Where will the research take place?

The research will take place in the Merchants Venturers Building during office hours and possibly within meeting rooms at Lancaster University Library under either the Society of College, National and University Libraries (SCONUL) scheme or with the support of an external supervisor.

13. How will informed consent be obtained from all participants or their parents/guardians prior to individuals entering the research study?

Participants will be given a participant information sheet to read prior to being tested, after which they will be asked to sign a consent form. Copies of these documents are attached.

14. Will the study involve actively deceiving the participants?

Yes- Half of the participants will not be informed that there may be incidents representing cyber attacks throughout the study, this is so that the effects of priming for cyber security can be explored. However, participants will not be deceived about the activities that they will be doing, and the full details of the study will be given to them in the debrief sheet, where they will also be reminded of their right to withdraw if they are unhappy about their data being used.

15. Will participants be made aware they can drop out of the research study at any time without having to give a reason for doing so?

Yes- participants will be told in the information sheet and consent form that they can withdraw at any point and without giving a reason. Participants will be warned however that they should withdraw within two weeks, at which time their data may be pooled and no longer identifiable. This will also be stated on the debrief sheets.

16. Outline the design of the research study and list the procedures to which the participants will be subjected, the anticipated testing time and any treatments administered.

1. Participants will be assigned to either the primed or un-primed group and given the appropriate participant information sheet.
2. Participants will be asked to fill in a questionnaire about age, gender, level of IT and security knowledge and personality.
3. Participants will be given a short demonstration of the study set up with an explanation of the information and study controls (Figure 1). They will also be shown the Bedford workload scale so that they can provide a workload score every time they open the water pumps.

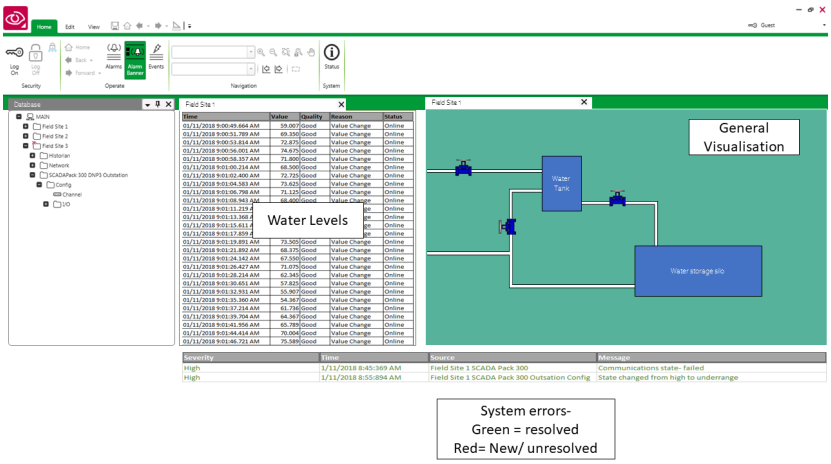


Figure 1: Demonstration slide

4. Participants will be asked to begin the simulation which should last approximately 15 minutes. During the task they will be asked to monitor the water levels on screen and respond whenever they see the water rise above 80. Additional tasks will involve monitoring emails about the system and providing a workload score after each time they open the water pumps.
5. During the simulation the following attacks will be run:

   Replay attack: Thirty seconds worth of values will be repeated three times. Time stamps will continue to change but the water levels will be repeated.

   A Man-in -the-middle attack: Water levels will reach above eighty more frequently. Participants will also receive emails stating that water pressure within the local infrastructure is decreasing and can they confirm that water levels within the system are lower than average.

   DDoS attack against the PLC controlling the pump: They will receive two emails early in the simulation stating that the PLC controlling the pump has been reset following failure (the PLC failures will also be recorded as system errors in the simulation). During this attack they will then find that the key inputs fail to work and they will need to wait until another email states that the PLC has been reset.

   A phishing email: claiming to be from the organisation's security team and requesting that they change their password by following the instructions in a pdf document.
6. Participants will be fully debriefed and paid.

17. Describe potential risks to participants (physical, psychological, legal, social) arising from these procedures.

The research will not involve risks beyond those normally encountered by the participants in their life outside research or within a standard office environment.

All studies will take place on University premises (Bristol or Lancaster), during standard office hours, so there is no foreseen risk to the researchers.

18. How will participants be debriefed?

Participants will be debriefed with a debrief sheet that summarises the aims of the study, reminds them of their right to withdraw and will provide the researcher's email address should they have any questions or wish to be emailed a summary of the results of the study

19. Is any reimbursement of expenses or other payment to be made to participants?
Participants will be offered £3.50 to remunerate them for their time, and to encourage participation.

20. Will personal data, beyond those recorded on the consent form, be used in the research?
No

21. Will the participants be audio-recorded or video-recorded?
No

22. When will this research be completed? (Give a date)
This study should be completed by September 2019

23. How will the data be made available at the end of the project? (You must declare your level of access)

Data will be **open** and made available via the Bristol Research Data Repository

24. Any other relevant information
No

Signature of Applicant: E. Hewlett **Date:** 05/06/2019
Signature of Supervisor: A. Rashid **Date:** 06/06/2019

Appendices and Additional Information
Advertisement Materials
Participant Information Sheet
Consent Forms
Study instructions and forms
Debrief Form

Appendix A – Advertisement Materials

Participants Wanted!!!
Take part in a simple simulation study & earn money

We are looking for individuals to take part in a computer simulation of an industry water plant.

Who can take part? Anyone who speaks English, is over 18 years old and has normal or corrected normal vision.

Where? Merchant Venturers Building/ Lancaster University Library

How Much? £3.50 for a 20 minute study

Interested?

Contact: <email>

Appendix B1- Participant Information Sheet 1 (Primed Individuals)

Human Factors in Security of Cyber Physical Systems

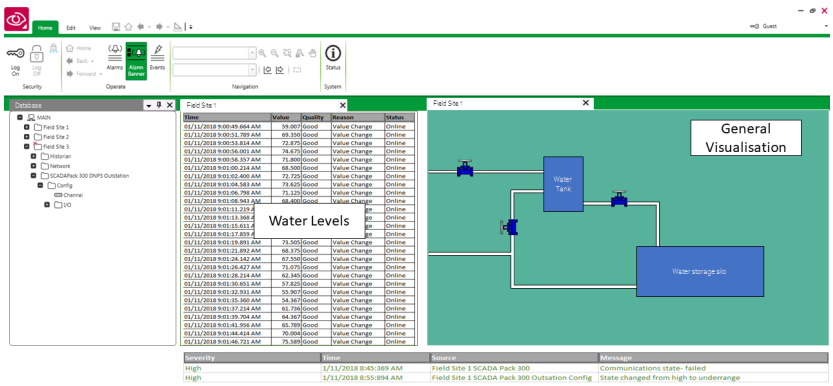
I am a PhD student at Bristol University, and I would like to invite you to take part in a research study about cyber security in cyber physical systems.

Please take time to read the following information carefully before you decide whether or not you wish to take part.

What is the study about?
This study uses a simulation of the data outputs from a water plant to explore whether people can identify:

1. When the system behaves in an unusual manner
2. When unusual behaviours may be the result of a cyber attack

What will I be asked to do if I take part?
If you decide to take part, then this study will take approximately 25 minutes and will involve sitting at a desk with a computer. You will be monitoring a system, similar to the one shown in the image and you will be asked to monitor the water levels and hit a button to open a pump in the system whenever the water levels go above 80. In addition you will have a second screen showing an email account, which will provide you with extra information to refer to and will be asked to provide a workload score on multiple occasions.



What are the possible benefits from taking part?
There are no specific benefits to you taking part in this study, however your participation may increase our understanding of this topic area. You will also be given £3.50 as a thank you for your time

Do I have to take part?
No. It's completely up to you to decide whether or not you take part. Your participation is voluntary and you are free to withdraw at any time before or during the study, you may also withdraw your data for up to two weeks after the study.

If you decide not to take part in this study, this will not affect your studies or the way you are assessed on your course.

What if I change my mind?
You may withdraw your data anytime for up to two weeks after the experiment, at which point data may be pooled together. If you wish to withdraw you will need to contact the researcher, using the details below.

What are the possible disadvantages and risks of taking part?
There should be no major disadvantages to taking part, however this study will take around 25 minutes of your time.

Will my data be identifiable?
The only identifiable information will be on your consent forms and these will be kept separately to the study results.

How will my data be stored?
Your data will be stored in encrypted files (that is no-one other than me, the researcher will be able to access them) and on password-protected computers.

In addition, if you consent then your anonymised data will also be added to the Bristol Research Data Repository where it may be shared with other researchers.

How will we use the information you have shared with us and what will happen to the results of the research study?
The data that you share will only be used for academic purposes, this may include:

- My PhD thesis
- Academic journal papers
- Conference proceedings

Who has reviewed the project?

This study has been reviewed and approved by the Faculty of Engineering Research Ethics Committee at Bristol University.

What if I have a question or concern?
If you have any queries or if you are unhappy with anything that happens concerning your participation in the study, please contact myself (Emma Hewlett) at: <email>
<phone>
Merchant Venturers Building

Alternatively, you may contact my supervisor Prof. Awais Rashid at: <email>
Merchant Venturers Building
Alternatively, if you have any concerns or complaints that you wish to discuss with a person who is not directly involved in the research, you can also contact Mr Liam McKervey (Tel: <phone> email: <email>)

Thank you for considering your participation in this project.

Faculty of Engineering Research Ethics Committee
APPLICATION FOR RESEARCH ETHICS APPROVAL
Participant Information Sheet 2 (Unprimed Individuals)

Human Factors in Safety of Cyber Physical Systems

I am a PhD student at Bristol University, and I would like to invite you to take part in a research study about monitoring information in cyber physical systems. Please take time to read the following information carefully before you decide whether or not you wish to take part.

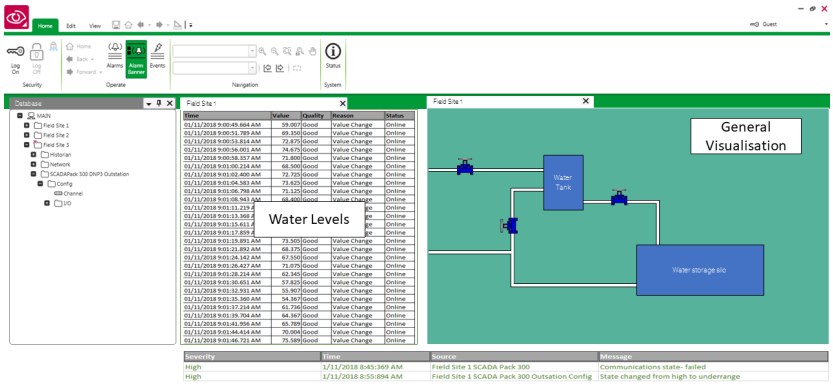
What is the study about?

This study uses a simulation of the data outputs from a water plant to explore whether people can identify:

1. When the system behaves in an unusual manner
2. What individuals believe may be the cause of any issues

What will I be asked to do if I take part?

If you decide to take part, then this study will take approximately 25 minutes and will involve sitting at a desk with a computer. You will be monitoring a system, similar to the one shown in the image and you will be asked to monitor the water levels and hit a button to open a pump in the system whenever the water levels go above 80. In addition you will have a second screen showing an email account, which will provide you with extra information to refer to and will be asked to provide a workload score on multiple occasions.



What are the possible benefits from taking part?

There are no specific benefits to you taking part in this study, however your participation may increase our understanding of this topic area. You will also be given £3.50 as a thank you for your time

Do I have to take part? No. It's completely up to you to decide whether or not you take part. Your participation is voluntary, and you are free to withdraw at any time before or during the study, you may also withdraw your data for up to two weeks after the study.

If you decide not to take part in this study, this will not affect your studies or the way you are assessed on your course.

What if I change my mind?
You may withdraw your data anytime for up to two weeks after the experiment, at which point data may be pooled together. If you wish to withdraw you will need to contact the researcher, using the details below.

What are the possible disadvantages and risks of taking part?
There should be no major disadvantages to taking part, however this study will take around 25 minutes of your time.

Will my data be identifiable?
The only identifiable information will be on your consent forms and these will be kept separately to the study results.

How will my data be stored?
Your data will be stored in encrypted files (that is no-one other than me, the researcher will be able to access them) and on password-protected computers. In addition, if you consent then your anonymised data will also be added to the Bristol Research Data Repository where it may be shared with other researchers.

How will we use the information you have shared with us and what will happen to the results of the research study?
The data that you share will only be used for academic purposes, this may include:

- My PhD thesis
- Academic journal papers
- Conference proceedings

Who has reviewed the project?

This study has been reviewed and approved by the Faculty of Engineering Research Ethics Committee at Bristol University.

What if I have a question or concern?
If you have any queries or if you are unhappy with anything that happens concerning your participation in the study, please contact myself (Emma Hewlett) at: <email> <phone>
Merchant Venturers Building

Alternatively, you may contact my supervisor Prof. Awais Rashid at:
<email>
Merchant Venturers Building
Alternatively, if you have any concerns or complaints that you wish to discuss with a person who is not directly involved in the research, you can also contact Mr Liam McKervey (Tel: <phone> email: <email>).

Thank you for considering your participation in this project.

Faculty of Engineering Research Ethics Committee
APPLICATION FOR RESEARCH ETHICS APPROVAL

Consent Form

Project Title: Human Factors in Safety/Security of Cyber Physical Systems

Name of Researcher: Emma Hewlett
Email: <email>

Please read the following statements and if you agree and are happy to proceed, initial each one.

DO YOU CONFIRM THAT YOU:

1. Are over 18 years of age ☐
2. Have read and understood the information sheet for the above study. ☐
3. Have had the opportunity to consider the information, ask questions and have had these questions answered satisfactorily ☐
4. Understand that your participation is voluntary and that you are free to withdraw at any time, without giving a reason. ☐
5. Understand the data I provide will be anonymous. No link will be made between my name or other identifying information and my study data. ☐
6. Consent that your anonymised data can be made open access and stored on the Bristol University system, and that you understand that for up to two weeks following participation you may contact the researcher to have your data removed. ☐
7. Understand that any information given by me may be used in future reports, academic articles, publications or presentations by the researcher/s. ☐
8. Understand that some of the reasons for conducting this study may have been withheld and will be explained to be fully following completion of the study. ☐

Having read the above information, I hereby fully and freely consent to my participation in this study

Participant's signature: _____ Date: _____

Name in BLOCK Letters: _____

Final consent

Having participated in this study

I agree to the University of Bristol keeping and processing the data I have provided during the course of this study. I understand that these data will be used only for the purpose(s) set out in the information sheet, and my consent is conditional upon the University complying with its duties and obligations under the Data Protection Act.

Participant's signature: _____ Date: _____

Name in BLOCK Letters: _____

If you have any concerns related to your participation in this study please direct them to the Faculty of Engineering Research Ethics Committee, via Liam McKervey, Research Governance and Ethics Officer (Tel: <phone> email: <email>).

Study Instructions

Participant instructions:

This system is a very simplified representation of a Supervisory Control and Data Acquisition (SCADA) system for a water treatment plant. It will be providing you with simulated real-time data, telling you the water levels within the system and how the pump is working.

You will be shown what the various parts of the systems represent and then asked to monitor the water levels and record any issues that you observe alongside any thoughts you have about what may be the cause of the issues.

Whilst observing the water levels, please also observe the email account and respond as appropriate. Additionally, each time you open the water pump please provide a workload score.

Observation Sheet

Time	What was unusual? Why was it unusual	What do you think could be a cause of the issue?

Debrief Sheet

Faculty of Engineering

Debrief sheet- Human Factors in Security of Cyber Physical Systems

What this study was really about?

This study explored several different types of cyber-attacks against the system to explore which types of attacks people can observe, with half of the participants primed to consider cyber security. The work sought to explore:

1. what types of attacks people can observe and what behaviours they consider to be unusual?
2. Do individual differences influence identification of attacks?
3. Where do people attribute the blame for unusual behaviour and what effect does priming for cyber security have on this?

Why was I not informed of this?

This study sought to explore the effect of priming on whether people would consider any issues to be the result of a cyber attack. In order not to bias this, half of participants were not informed that they may be presented with cyber attacks. If you have any questions or issues about this please feel free to ask.

What if I have a question or would like to withdraw?

If you have any queries or if you are unhappy with anything that happens concerning your participation in the study, please contact myself (Emma Hewlett) at:
<email>;
If you wish to withdraw your data, again please contact me on the email above. Please be aware that after two weeks data will be pooled and it may no longer possible to identify and remove.

Alternatively, you may contact my supervisor Prof. Awais Rashid at:
<email>

If you have any concerns or complaints that you wish to discuss with a person who is not directly involved in the research, you can also contact Mr Liam McKervey (<email>)

Additional information:

If you would like more information on the cyber threats that are faced by organisations and Cyber Physical Systems then this can be found on the website of the Centre for Protection of National Infrastructure (CPNI): https://www.cpni.gov.uk/.

Thank you for your participation in this project.

APPENDIX K

STATISTICAL OUTPUTS FROM THE SCADA CYBER ATTACK DETECTION STUDY

This Appendix presents the statistical outputs that were created for Chapter 8.

K.1 Statistical Analyses To Investigate Whether Some Attacks Are Easier To Observe Than Others in a Waterplant SCADA System

K.1.1 Outputs From The Cochrans Q Test to Explore Which Attacks Are Easier to Detect

A Cochrans Q test can be used to determine whether or not there are any differences in a dichotomous dependent variable between three or more related groups. In this context it was used to explore whether the number of people who observed the different cyber attack incidents was statistically different across the different attack conditions.

This test has three conditions that must be met:

1. It must have one dichotomous dependent variable, in this case whether a an attack is observed.

2. It must have one independent variable that consists of three or more categorical, related groups, in this case the various cyber attack conditions.

3. The participants were recruited from a random sample.

All three of these assumptions were met, there is also however some guidance on the number of participants required in order to be able to run the standard Cochrans Q test. To meet the sample size conditions n (where n= total no. of participants, minus the number of participants who scored the same across each condition e.g. detected all or none of the attacks) must be equal or greater than 4. Additionally, nk (where k is number of conditions) must be equal to or greater than 24.

In this study N= 50 and 7 individuals failed to observe any of the attacks, with one participant observing all three. Therefore n (50-7-1)= 42 and nk is 42x3= 126. This study therefore meets the sample size requirements.

Running this test then produces the outputs seen in Figure K.1, which shows a significant result.

Test Statistics

N	50
Cochran's Q	54.143[a]
df	2
Asymp. Sig.	.000

a. 0 is treated as a success.

Figure K.1: Output of the Cochran Q Test for Detecting Attacks Against a SCADA System

Since this test was statistically significant, post hoc tests were conducted using Dunn's test with Bonferroni corrections to identify which of the conditions were significantly different from each other. The results of these tests can be seen in Figure K.2. Two of the comparisons show significant results which are discussed at Chapter 9

Pairwise Comparisons

Sample 1-Sample 2	Test Statistic	Std. Error	Std. Test Statistic	Sig.	Adj. Sig.[a]
Replay-MitM	-.580	.106	-5.480	.000	.000
Replay-DoS	-.740	.106	-6.992	.000	.000
MitM-DoS	-.160	.106	-1.512	.131	.392

Each row tests the null hypothesis that the Sample 1 and Sample 2 distributions are the same.
Asymptotic significances (2-sided tests) are displayed. The significance level is .05.

a. Significance values have been adjusted by the Bonferroni correction for multiple tests.

Figure K.2: Results of the Cochran Q Post-Hoc tests

K.2 Statistical Analyses for Investigating the Effects of Security Priming on Attack Detection

K.2.1 Chi-square Test to Investigate the Impacts of Priming on Detecting the Man in the Middle Attack

The chi-square test was used to explore whether there was a difference between two dichotomous dependent variables.

This test has four assumptions that need to be met:

1. You need to have one independent (primed vs. unprimed participants) and one dependent variable (detection of the man in the middle attack), both of which are dichotomous.
2. You should have independence of observations.
3. Participants are randomly assigned to one of the condition groups
4. You have a sufficiently large sample size

In this test we are exploring whether an individual in either the security primed or control condition does or doesn't observe the attacks and so assumption one was met. Assumption two was met by having a between subjects design and because participants were randomly assigned, assumption three was also met.

Sufficient sample sizes for this test are usually defined by having each expected frequency as a minimum of 5, the expected frequencies for this test can be seen in Table K.3, showing that assumption 4 was met.

Condition * MitM Crosstabulation

			MitM		
			No	Yes	Total
Condition	Control	Count	11	14	25
		Expected Count	10.0	15.0	25.0
		% within Condition	44.0%	56.0%	100.0%
	Security	Count	9	16	25
		Expected Count	10.0	15.0	25.0
		% within Condition	36.0%	64.0%	100.0%
Total		Count	20	30	50
		Expected Count	20.0	30.0	50.0
		% within Condition	40.0%	60.0%	100.0%

Figure K.3: Expected Frequencies for the Man in the Middle Attack

Because all of the conditions were met the Chi-square test was run with the outputs shown in Figure K.4. This test shows that the result was not significant.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.333[a]	1	.564		
Continuity Correction[b]	.083	1	.773		
Likelihood Ratio	.334	1	.563		
Fisher's Exact Test				.773	.387
Linear-by-Linear Association	.327	1	.568		
N of Valid Cases	50				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 10.00.

b. Computed only for a 2x2 table

Figure K.4: Results of the Chi-square test to Investigate Detection of the Man in the Middle Attack Between the Primed and Unprimed Condition

K.2.2 Chi-Square Test to Investigate the Impacts of Priming on Detecting the DoS Attack

In this test we were exploring whether an individual in either the security primed or unprimed condition observes the DoS attack. This test has four assumptions that need to be met:

1. You need to have one independent and one dependent variable, both of which are dichotomous.

2. You should have independence of observations.

3. Participants are randomly assigned to one of the condition groups

4. You have a sufficiently large sample size

Assumption one was met, assumption two was also met by having a between subjects design and because participants were randomly assigned assumption three was also met.

Sufficient sample sizes for this test are usually defined by having each expected frequency as a minimum of 5, the expected frequencies for this test can be seen in Table K.5, showing that assumption 4 was met as the minimum expected sample size was 6.0.

Because all of the conditions were met the Chi-square test was run with the outputs shown in Figure K.6, showing that the result was not significant.

Condition * DoS Crosstabulation

			DoS		
			No	Yes	Total
Condition	Control	Count	8	17	25
		Expected Count	6.0	19.0	25.0
		% within Condition	32.0%	68.0%	100.0%
	Security	Count	4	21	25
		Expected Count	6.0	19.0	25.0
		% within Condition	16.0%	84.0%	100.0%
Total		Count	12	38	50
		Expected Count	12.0	38.0	50.0
		% within Condition	24.0%	76.0%	100.0%

Figure K.5: Expected Frequencies for the DoS Attack

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.754[a]	1	.185		
Continuity Correction[b]	.987	1	.321		
Likelihood Ratio	1.781	1	.182		
Fisher's Exact Test				.321	.160
Linear-by-Linear Association	1.719	1	.190		
N of Valid Cases	50				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 6.00.

b. Computed only for a 2x2 table

Figure K.6: Results of the Chi-Square Test to Investigate Detection of the DoS Attack Between the Primed and Unprimed Conditions

K.3 Statistical Analyses For If We Can Predict Who Will Observe Different Cyber Attacks

K.3.1 Predicting the Probability That an Individual Will Observe a Man in the Middle Attack

A binomial logistic regression analysis attempts to predict the probability that an observations falls into one of two categories in a dichotomous dependent variable (in this case whether a man in the middle attack was observed) based on one or more categorical or continuous independent variables. In this test the independent variables were gender, IT Knowledge and neuroticism.

This test has six assumptions that must be met:

1. You have one dichotomous dependent variable.

2. You have one or more independent variables that are either continuous or nominal.

3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.

4. You should have a minimum of 15 participants for each independent variable.

5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.

6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, assumption 4 meant that only three independent variables could be explored (N=50).

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure K.7 and to understand if the assumption is met we need look at the three highlighted lines.. In this test if the result is significant then the continuous independent variable is not linearly related to the logit of the dependent variable and it has failed the assumption of linearity. Fortunately however as can be seen in this case the assumption is met.

Variables not in the Equation

			Score	df	Sig.
Step 0	Variables	Gender(1)	.057	1	.812
		ITKnowledge	.439	1	.508
		neuroticism	.212	1	.645
		ITKnowledge by ln_ITKnowledge	.216	1	.642
		ln_neuro by neuroticism	.255	1	.613
	Overall Statistics		4.959	5	.421

Figure K.7: Testing Assumption 5 That There is a Linear Relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variable (Observing a Man in th Middle Attack)

Assumption 6 states that their should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2 standard deviations. As can be seen in Figure K.8, there were no outliers in this dataset in relation to values tampering attack.

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure K.9. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the mode, as can be seen from the model row the model fit was insignificant with p=.725.

Casewise List[a]

a. The casewise plot is not produced because no outliers were found.

Figure K.8: Testing Assumption 6 That There Are No Outliers in the Man in the Middle Data Sample

This is likely due to the model predicting a very small amount of the variance in detection of logic upload attacks. This Nagelkerke R2 value in this table shows that the model explains only 3.5% of the variance.

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	1.316	3	.725
	Block	1.316	3	.725
	Model	1.316	3	.725

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	65.985[a]	.026	.035

a. Estimation terminated at iteration number 3 because parameter estimates changed by less than .001.

Figure K.9: Outputs of the Binomial Logistic Regression Analysis for Who Can Observe a Man in the Middle Attack

Given that this model was insignificant the rest of the outputs are not detailed here.

K.3.2 Predicting the Probability That An Individual Will Observe a DoS Attack

A binomial logistic regression analysis attempts to predict the probability that an observations falls into one of two categories in a dichotomous dependent variable (in this case whether a DoS attack was detected) based on one or more categorical or continuous independent variables. In this test the independent variables were gender, IT Knowledge and neuroticism.

This test has six assumptions that must be met:

1. You have one dichotomous dependent variable.

2. You have one or more independent variables that are either continuous or nominal.

3. You should have independence of observations, with categories for the dependent and independent variables being mutually exclusive and exhaustive.
4. You should have a minimum of 15 participants for each independent variable.
5. There needs to be a linear relationship between the continuous independent variables and the logit transformation of the dependent variable.
6. There should be no significant outliers, high leverage points or highly influential points.

Assumptions 1-3 were all met, assumption 4 meant that only three independent variables could be explored (N=50).

Assumption 5 was tested using the Box-Tidwell procedure, the output of this is seen in Figure K.10 and to understand if the assumption is met we need look at the three highlighted lines . In this test if the result is significant then the continuous independent variable is not linearly related to the logit of the dependent variable and it has failed the assumption of linearity. Fortunately however as can be seen in this case the assumption is met.

Variables not in the Equation

			Score	df	Sig.
Step 0	Variables	Gender(1)	.090	1	.764
		ITKnowledge	.023	1	.879
		neuroticism	.045	1	.833
		ITKnowledge by ln_ITKnowledge	.000	1	.992
		ln_neuro by neuroticism	.065	1	.799
	Overall Statistics		2.284	5	.809

Figure K.10: Testing Assumption 5 That There is a Linear Relationship Between the Continuous Independent Variables and the Logit Transformation of the Dependent Variable (Observation of a DoS Attack)

Assumption 6 states that their should be no significant outliers, high leverage points or highly influential point. To test this we looked for cases of standardized residuals with greater than + or - 2 standard deviations. As can be seen in Figure K.11, there were no outliers in this dataset in relation to values tampering attack.

Since all of the assumptions were met we can run the test and the outputs can be seen in Figure K.12. The Omnibus Tests of Model Coefficients provides the overall statistical significance of the mode, as can be seen from the model row the model fit was insignificant with p=.976.

This is likely due to the model predicting a very small amount of the variance in detection of logic upload attacks. This Nagelkerke R2 value in this table shows that the model explains only .06% of the variance.

Given that this model was insignificant the rest of the outputs are not detailed here.

Casewise List[a]

a. The casewise plot is not produced because no outliers were found.

Figure K.11: Testing Assumption 6 That There Are No Outliers in the DoS Data Sample

Block 1: Method = Enter

Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	.210	3	.976
	Block	.210	3	.976
	Model	.210	3	.976

Model Summary

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	54.898[a]	.004	.006

a. Estimation terminated at iteration number 4 because parameter estimates changed by less than .001.

Figure K.12: Outputs of the Binomial Logistic Regression Analysis for Who Can Observe a DoS Attack

K.4 A Mann Whitney U Test to Test if Priming Individuals Impacts On Average Workload

A Mann Whitney U test is used to test if there are differences between two groups on a continuous or ordinal scale, in this context it was used to explore if there were any differences in average workload between the security and control conditions. This test has four assumptions that need to be met:

1. You have one dependent variable that is either continuous or ordinal. In this case this is the participant's average workload.

2. You have one independent variable that is made up of two categorical, independent groups, in this case whether a participant was primed.

3. There needs to be no relationship between the observations in each group of the independent variable or between the groups themselves i.e. each participant only belongs to one of the groups. This assumption was met when assigning participants to groups based on gender.

4. You must determine whether the distribution of scores for both groups of your independent variable have the same shape. This determines how you interpret the results of the Mann-Whitney U test.

The data set for this test meets assumptions 1-3, the outputs (See Figure K.13) then reveals that the distribution scores are similar and so in this instance the test is used to investigate differences in the median scores between the two conditions.

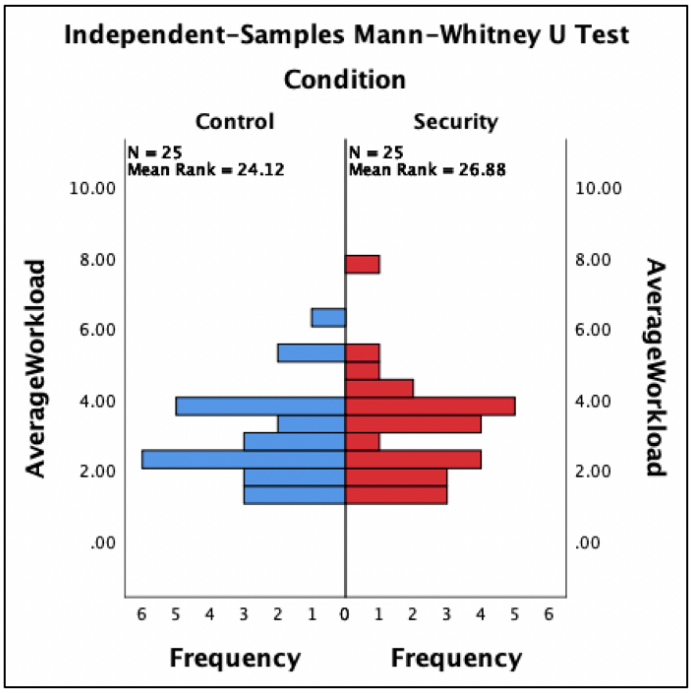


Figure K.13: Histogram Outputs to Examine the Distribution of Workload Scores for Primed and Unprimed Individuals

The full outputs from this test can then be seen in Figure K.14, showing that the test was not significant.

AverageWorkload across Condition

Independent-Samples Mann-Whitney U Test Summary

Total N	50
Mann-Whitney U	347.000
Wilcoxon W	672.000
Test Statistic	347.000
Standard Error	51.483
Standardized Test Statistic	.670
Asymptotic Sig.(2-sided test)	.503

Figure K.14: Results of the Mann Whitney U Test to Explore Workload Across Conditions

BIBLIOGRAPHY

[1] N. Falliere, L. Murchu, and E. Chien, "W32. stuxnet dossier version 1.3, november 2010," *Symantec Security Response.*, 2010, [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[2] K. Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid," 2016, [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[3] B. Kesler, "The vulnerability of nuclear facilities to cyber attack; strategic insights: Spring 2010," *Strategic Insights*, 2011, [Online]. Available: https://core.ac.uk/download/pdf/36718376.pdf.

[4] J. Finkle, "After 'godzilla attack!' U.S. warns about traffic-sign hackers," *Reuters*, 2014, [Online]. Available: https://www.reuters.com/article/us-usa-hacking-traffic/after-godzilla-attack-u-s-warns-about-traffic-sign-hackers-idUSKBN0EH2CM20140606.

[5] ICS-CERT, *ICS-ALERT-14-155-01A*, 2014, [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-155-01A.

[6] M. Abrams and J. Weiss, "Malicious control system cyber security attack case study-Maroochy water services, Australia," *The MITRE Corporation*, 2008, [Online]. Available: https://www.mitre.org/sites/default/files/pdf/08_1145.pdf.

[7] NCCIC/ICS-CERT, "National cybersecurity and communications integration center/industrial control systems cyber emergency response team year in review fiscal year 2015," *Homeland Security*, 2016, [Online]. Available: https://www.hsdl.org/?view&did=792876.

[8] S. Boddy and J. Shattuck, "The hunt for IoT: The growth and evolution of thingbots ensures chaos," *f5 Labs*, 2018, [Online]. Available: https://www.f5.com/content/dam/f5/f5-labs/articles/20180313_iot_vol4/F5_Labs_Hunt_for_IOT_Vol_4_rev30MAR18.pdf.

[9] Symantec Corporation, "2018 internet security threat report executive summary," 2018, [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf.

[10] E. Ross, "Baby monitors 'hacked': Parents warned to be vigilant after voices heard coming from speakers," *The Independent*, 2016, [Online] Available: https://www.independent.co.uk/life-style/gadgets-and-tech/news/baby-monitors-hacked-parents-warned-to-be-vigilant-after-voices-heard-coming-from-speakers-a6843346.html.

[11] J. Tidy, "Pewdiepie printer hackers strike again," December 2018, [Online]. Available: https://www.bbc.co.uk/news/technology-46552339.

[12] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "DDoS-capable IoT malwares: Comparative analysis and mirai investigation," *Security and Communication Networks*, 2018, [Online]. Available: https://doi.org/10.1155/2018/7178164.

[13] BBC, "Smart home devices used as weapons in website attack," October 2016, [Online]. Available http://www.bbc.co.uk/news/technology-37738823.

[14] A. Le, U. Roedig, and A. Rashid, "Lasarus: Lightweight attack surface reduction for legacy industrial control systems," in *International Symposium on Engineering Secure Software and Systems*. Springer, 2017, pp. 36–52.

[15] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *International Conference on Critical Infrastructure Protection*. Springer, 2007, pp. 73–82.

[16] L. Tam, M. Glassman, and M. Vandenwauver, "The psychology of password management: a tradeoff between security and convenience," *Behaviour & Information Technology*, vol. 29, no. 3, pp. 233–244, 2010.

[17] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, "Do users' perceptions of password security match reality?" in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 3748–3760.

[18] E. Von Zezschwitz, A. De Luca, and H. Hussmann, "Survival of the shortest: A retrospective analysis of influencing factors on password composition," in *IFIP Conference on Human-Computer Interaction*. Springer, 2013, pp. 460–467.

[19] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, "'i added '!'at the end to make it secure': Observing password creation in the lab," in *Proceedings of Eleventh Symposium On Usable Privacy and Security*, 2015.

[20] C. Shen, T. Yu, H. Xu, G. Yang, and X. Guan, "User practice in password security: An empirical study of real-life passwords in the wild," *Computers & Security*, vol. 61, pp. 130–141, 2016.

[21] R. Veras, J. Thorpe, and C. Collins, "Visualizing semantics in passwords: The role of dates," in *Proceedings of the Ninth International Symposium on Visualization for Cyber Security*. ACM, 2012, pp. 88–95.

[22] G. Notoatmodjo and C. Thomborson, "Passwords and perceptions," in *Proceedings of the Seventh Australasian Conference on Information Security*, vol. 98, 2009, pp. 71–78.

[23] E. Hayashi and J. Hong, "A diary study of password usage in daily life," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2627–2630.

[24] E. Stobert and R. Biddle, "The password life cycle: user behaviour in managing passwords," in *10th Symposium On Usable Privacy and Security SOUPS 2014)*, 2014, pp. 243–255.

[25] R. Wash, E. Rader, R. Berman, and Z. Wellmer, "Understanding password choices: How frequently entered passwords are re-used across websites," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 2016, pp. 175–188.

[26] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: user attitudes and behaviors," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2010, pp. 1–20.

[27] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: measuring the effect of password-composition policies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2595–2604.

[28] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 383–392.

[29] J. Abbott and V. M. Garcia, "Password differences based on language and testing of memory recall," *International Journals of N&N Global Technology on Information Security*, vol. 2, pp. 1–6, 2015.

[30] J. Campbell, D. Kleeman, and W. Ma, "The good and not so good of enforcing password composition rules," *Information Systems Security*, vol. 16, no. 1, pp. 2–8, 2007.

[31] B. Grawemeyer and H. Johnson, "Using and managing multiple passwords: A week to a view," *Interacting with Computers*, vol. 23, no. 3, pp. 256–267, 2011.

[32] G. B. Duggan, H. Johnson, and B. Grawemeyer, "Rational security: Modelling everyday password use," *International journal of human-computer studies*, vol. 70, no. 6, pp. 415–431, 2012.

[33] L. J. Camp, J. Abbott, and S. Chen, "Cpasswords: leveraging episodic memory and human-centered design for better authentication," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016, pp. 3656–3665.

[34] L. J. Camp, "Aligning authentication with human cognition, aka making passwords work," in *Security and Human Behavior*. Cambridge University, (Cambridge UK) 9-11 June 2014.

[35] M. Grimes, J. Marquardson, and J. Nunamaker, "Broken windows, bad passwords: Influencing secure user behavior via website design," in *Proceedings of 20th Americas Conference on Information Systems, AMCIS 2014*, 2014.

[36] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer *et al.*, "How does your password measure up? the effect of strength meters on password creation," in *Proceedings of the 21st USENIX Security Symposium USENIX Security 12)*, 2012, pp. 65–80.

[37] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, "Does my password go up to eleven?: the impact of password meters on password selection," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2013, pp. 2379–2388.

[38] J. L. Jenkins, M. Grimes, J. G. Proudfoot, and P. B. Lowry, "Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals," *Information Technology for Development*, vol. 20, no. 2, pp. 196–213, 2014.

[39] L. Zhang and W. C. McDowell, "Am I really at risk? determinants of online users' intentions to use strong passwords," *Journal of Internet Commerce*, vol. 8, no. 3-4, pp. 180–197, 2009.

[40] D. Wang, H. Cheng, Q. Gu, and P. Wang, "Understanding passwords of Chinese users: Characteristics, security and implications," *CACR Report, Presented at ChinaCrypt*, 2015.

[41] J. Abbott, D. Calarco, and L. J. Camp, "Factors influencing password reuse: A case study." TPRC, 2018.

[42] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? security awareness in smartphone platforms," *Computers & Security*, vol. 34, pp. 47–66, 2013.

[43] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner, "Are you ready to lock?" in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 750–761.

[44] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 213–230.

[45] W. Melicher, D. Kurilova, S. M. Segreti, P. Kalvani, R. Shay, B. Ur, L. Bauer, N. Christin, L. F. Cranor, and M. L. Mazurek, "Usability and security of text passwords on mobile devices," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 527–539.

[46] Y. Yang, J. Lindqvist, and A. Oulasvirta, "Text entry method affects password security," in *The (LASER) Workshop: Learning from Authoritative Security Experiment Results (LASER 2014)*, 2014.

[47] Z. Li, W. Han, and W. Xu, "A large-scale empirical analysis of chinese web passwords," in *proceedings of the 23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 559–574.

[48] G. Han, Y. Yu, X. Li, K. Chen, and H. Li, "Characterizing the semantics of passwords: The role of Pinyin for Chinese netizens," *Computer Standards and Interfaces*, vol. 54, pp. 20–28, 2017.

[49] H. Petrie and B. Merdenyan, "Cultural and gender differences in password behaviors: Evidence from China, Turkey and the UK," in *Proceedings of the 9th Nordic Conference on Human-Computer Interaction*. ACM, 2016, p. 9.

[50] M. Bidgoli, B. P. Knijnenburg, and J. Grossklags, "When cybercrimes strike undergraduates," in *Electronic Crime Research (eCrime), 2016 APWG Symposium on*. IEEE, 2016, pp. 1–10.

[51] R. Vrana, "Making the internet a safer place: students' perceptions about internet security threats," in *23rd Central European Conference on Information and Intelligent Systems*, 2012, pp. 91–98.

[52] F. Raja, K. Hawkey, P. Jaferian, K. Beznosov, and K. S. Booth, "It's too complicated, so i turned it off!: expectations, perceptions, and misconceptions of personal firewalls," in *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*. ACM, 2010, pp. 53–62.

[53] H. Sharma, E. Meenakshi, and S. K. Bhatia, "A comparative analysis and awareness survey of phishing detection tools," in *Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017 2nd IEEE International Conference on*. IEEE, 2017, pp. 1437–1442.

[54] F. L. Lévesque, S. Chiasson, A. Somayaji, and J. M. Fernandez, "Technological and human factors of malware attacks: A computer security clinical trial approach," in *ACM Transactions on Privacy and Security (TOPS)*, vol. 21, no. 4. ACM, 2018, p. 18.

[55] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the eighth symposium on usable privacy and security*. ACM, 2012, pp. 1–14.

[56] A. Mylonas, D. Gritzalis, B. Tsoumas, and T. Apostolopoulos, "A qualitative metrics vector for the awareness of smartphone security users," in *International Conference on Trust, Privacy and Security in Digital Business*. Springer, 2013, pp. 173–184.

[57] E. Struse, J. Seifert, S. Üllenbeck, E. Rukzio, and C. Wolf, "Permissionwatcher: Creating user awareness of application permissions in mobile systems," in *International Joint Conference on Ambient Intelligence*. Springer, 2012, pp. 65–80.

[58] H. Krasnova, N. Eling, O. Schneider, H. Wenninger, T. Widjaja, P. Buxmann *et al.*, "Does this app ask for too much data? the role of privacy perceptions in user behavior towards facebook applications and permission dialogs," in *ECIS 2013 Completed Research. Paper 179*, 2013.

[59] P. Rajivan and J. Camp, "Influence of privacy attitude and privacy cue framing on android app choices," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, 2016.

[60] M. Fagan, M. M. H. Khan, and R. Buck, "A study of users' experiences and beliefs about software update messages," *Computers in Human Behavior*, vol. 51, pp. 504–519, 2015.

[61] Y. Tian, B. Liu, W. Dai, B. Ur, P. Tague, and L. F. Cranor, "Supporting privacy-conscious app update decisions with user reviews," in *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, 2015, pp. 51–61.

[62] K. E. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: how negative experiences affect future security," in *Proceedings of the 32nd annual ACM conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2671–2674.

[63] J. B. Gross and M. B. Rosson, "Looking for trouble: understanding end-user security management," in *Proceedings of the 2007 Symposium on Computer Human Interaction For the Management of Information Technology*. ACM, 2007, p. 10.

[64] J. M. Blythe, L. Coventry, and L. Little, "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 103–122.

[65] B.-Y. Ng, A. Kankanhalli, and Y. C. Xu, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, no. 4, pp. 815–825, 2009.

[66] M. B. Line, A. Zand, G. Stringhini, and R. Kemmerer, "Targeted attacks against industrial control systems: Is the power industry prepared?" in *Proceedings of the 2nd Workshop on Smart Energy Grid Security*. ACM, 2014, pp. 13–22.

[67] H. Liang and Y. Xue, "Avoidance of information technology threats: a theoretical perspective," *MIS quarterly*, pp. 71–90, 2009.

[68] ——, "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *Journal of the Association for Information Systems*, vol. 11, no. 7, pp. 394–413, 2010.

[69] D. K. Young, D. Carpenter, and A. McLeod, "Malware avoidance motivations and behaviors: A technology threat avoidance replication," *AIS Transactions on Replication Research*, vol. 2, no. 8, pp. 1–17, 2016.

[70] G. R. Milne, L. I. Labrecque, and C. Cromer, "Toward an understanding of the online consumer's risky behavior and protection practices," *Journal of Consumer Affairs*, vol. 43, no. 3, pp. 449–473, 2009.

[71] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp. 304–312, 2014.

[72] J. M. Blythe and L. Coventry, "Costly but effective: Comparing the factors that influence employee anti-malware behaviours," *Computers in Human Behavior*, vol. 87, pp. 87–97, 2018.

[73] H.-L. Chou and J. C.-Y. Sun, "The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers," *Computers & Education*, vol. 112, pp. 83–96, 2017.

[74] G. White, T. Ekin, and L. Visinescu, "Analysis of protective behavior and security incidents for home computers," *Journal of Computer Information Systems*, pp. 1–11, 2016.

[75] P. van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *Computers in Human Behavior*, vol. 75, pp. 547–559, 2017.

[76] N. Davinson and E. Sillence, "It won't happen to me: Promoting secure behaviour among internet users," *Computers in Human Behavior*, vol. 26, no. 6, pp. 1739–1747, 2010.

[77] J. Boehmer, R. LaRose, N. Rifon, S. Alhabash, and S. Cotten, "Determinants of online safety behaviour: towards an intervention strategy for college students," *Behaviour & Information Technology*, vol. 34, no. 10, pp. 1022–1035, 2015.

[78] M. G. Mariani and S. Zappalà, "PC virus attacks in small firms: Effects of risk perceptions and information technology competence on preventive behaviours," *TPM: Testing, Psychometrics, Methodology in Applied Psychology*, vol. 21, no. 1, 2014.

[79] K. D. Nguyen, H. Rosoff, and R. S. John, "Valuing information security from a phishing attack," *Journal of Cybersecurity*, vol. 3, no. 3, pp. 159–171, 2017.

[80] I. Ion, R. Reeder, and S. Consolvo, ""... no one can hack my mind": Comparing expert and non-expert security practices," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 327–346.

[81] B. Hanus and Y. A. Wu, "Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective," *Information Systems Management*, vol. 33, no. 1, pp. 2–16, 2016.

[82] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur, "Measuring password guessability for an entire university," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. ACM, 2013, pp. 173–186.

[83] A. A. Aldossary and A. M. Zeki, "Web user'knowledge and their behavior towards security threats and vulnerabilities," in *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*. IEEE, 2015, pp. 256–260.

[84] M. Harbach, S. Fahl, and M. Smith, "Who's afraid of which bad wolf? a survey of IT security risk awareness," in *2014 IEEE 27th Computer Security Foundations Symposium*. IEEE, 2014, pp. 97–110.

[85] J. C.-Y. Sun, S.-J. Yu, S. S. Lin, and S.-S. Tseng, "The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference," *Computers in Human Behavior*, vol. 59, pp. 249–257, 2016.

[86] T. Dinev, J. Goo, Q. Hu, and K. Nam, "User behaviour towards protective information technologies: the role of national cultural differences," *Information Systems Journal*, vol. 19, no. 4, pp. 391–412, 2009.

[87] J. Uhomoibhi, M. Al-Hamar, R. Dawson, and J. Al-Hamar, "The need for education on phishing: a survey comparison of the UK and Qatar," *Campus-Wide Information Systems*, vol. 28, no. 5, pp. 308–319, 2011.

[88] E. Rader, R. Wash, and B. Brooks, "Stories as informal lessons about security," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, pp. 1–17.

[89] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong, "The effect of social influence on security sensitivity," in *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 143–157.

[90] S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong, "Increasing security sensitivity with social proof: A large-scale experimental confirmation," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 739–749.

[91] R. Wash and E. Rader, "Too much knowledge? security beliefs and protective behaviors among united states internet users," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, 2015, pp. 309–325.

[92] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, ""my data just goes everywhere:" user mental models of the internet and implications for privacy and security," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 39–52.

[93] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, 2009.

[94] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong, "Password sharing: implications for security design based on social practice," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2007, pp. 895–904.

[95] J. Jansen and P. van Schaik, "Persuading end users to act cautiously online: A fear appeals study on phishing," *Information and Computer Security*, 2018.

[96] J. J. Kaye, "Self-reported password sharing strategies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2619–2622.

[97] A. A. Aldossary and A. M. Zeki, "The influence of students' knowledge on security towards their behavior with security risks within the context of Saudi Arabia," in *2013 International Conference on Advanced Computer Science Applications and Technologies*. IEEE, 2013, pp. 1–4.

[98] J. Chen, M. Paik, and K. McCabe, "Exploring internet security perceptions and practices in urban ghana," in *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 2014, pp. 129–142.

[99] S. Egelman and E. Peer, "Predicting privacy and security attitudes," *ACM SIGCAS Computers and Society*, vol. 45, no. 1, pp. 22–28, 2015.

[100] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Computers & Security*, vol. 73, pp. 345–358, 2018.

[101] W. R. Flores, H. Holm, M. Ekstedt, and M. Nohlberg, "Investigating the correlation between intention and action in the context of social engineering in two different national cultures," in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. IEEE, 2015, pp. 3508–3517.

[102] C. Rinn, K. Summers, E. Rhodes, J. Virothaisakun, and D. Chisnell, "Password creation strategies across high-and low-literacy web users," *Proceedings of the Association for Information Science and Technology*, vol. 52, no. 1, pp. 1–9, 2015.

[103] M. Whitty, J. Doodson, S. Creese, and D. Hodges, "Individual differences in cyber security behaviors: an examination of who is sharing passwords," *Cyberpsychology, Behavior, and Social Networking*, vol. 18, no. 1, pp. 3–7, 2015.

[104] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang, "Do or do not, there is no try: user engagement may not improve security outcomes," in *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, 2016, pp. 97–111.

[105] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Computers in Human Behavior*, vol. 69, pp. 151–156, 2017.

[106] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior*, vol. 69, pp. 437–443, 2017.

[107] R. W. Reeder, A. P. Felt, S. Consolvo, N. Malkin, C. Thompson, and S. Egelman, "An experience sampling study of user reactions to browser warnings in the field," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 2018, p. 512.

[108] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying wolf: An empirical study of SSL warning effectiveness," in *USENIX security symposium*, 2009, pp. 399–416.

[109] D. Akhawe and A. P. Felt, "Alice in warningland: A large-scale field study of browser security warning effectiveness." in *Usenix Security*, 2013, pp. 257–272.

[110] B. B. Anderson, C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance, "How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 2883–2892.

[111] B. B. Anderson, J. L. Jenkins, A. Vance, C. B. Kirwan, and D. Eargle, "Your memory is working against you: How eye tracking and memory explain habituation to security warnings," *Decision Support Systems*, vol. 92, pp. 3–13, 2016.

[112] B. B. Anderson, A. Vance, C. B. Kirwan, D. Eargle, and J. L. Jenkins, "How users perceive and respond to security messages: a neuroIS research agenda and empirical study," *European Journal of Information Systems*, vol. 25, no. 4, pp. 364–390, 2016.

[113] J. C. Brustoloni and R. Villamarín-Salomón, "Improving security decisions with polymorphic and audited dialogs," in *Proceedings of the 3rd symposium on Usable Privacy and Security*. ACM, 2007, pp. 76–85.

[114] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, "Your attention please: designing security-decision UIs to make genuine risks harder to ignore," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, pp. 1–12.

[115] Y. Chen, F. M. Zahedi, and A. Abbasi, "Interface design elements for anti-phishing systems," in *International Conference on Design Science Research in Information Systems*. Springer, 2011, pp. 253–265.

[116] S. Egelman, L. F. Cranor, and J. Hong, "You've been warned: an empirical study of the effectiveness of web browser phishing warnings," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2008, pp. 1065–1074.

[117] S. Egelman and S. Schechter, "The importance of being earnest [in security warnings]," in *International Conference on Financial Cryptography and Data Security*. Springer, 2013, pp. 52–59.

[118] M. Harbach, M. Hettig, S. Weber, and M. Smith, "Using personal examples to improve risk communication for security and privacy decisions," in *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2647–2656.

[119] H. Almuhimedi, A. P. Felt, R. W. Reeder, and S. Consolvo, "Your reputation precedes you: History, reputation, and the chrome malware warning," in *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, 2014, pp. 113–128.

[120] K. Krol, M. Moroz, and M. A. Sasse, "Don't work. Can't work? Why it's time to rethink security warnings," in *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*. IEEE, 2012, pp. 1–8.

[121] S. Motiee, K. Hawkey, and K. Beznosov, "Investigating user account control practices," in *CHI'10 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2010, pp. 4129–4134.

[122] K. Baxter, L. W. Malahy, and J. Lubin, "Pirates of the search results page," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2013, pp. 3023–3026.

[123] T. Bakhshi, "Social engineering: revisiting end-user awareness and susceptibility to classic attack vectors," in *2017 13th International Conference on Emerging Technologies (ICET)*. IEEE, 2017, pp. 1–6.

[124] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: user strategies for combating phishing attacks," *International Journal of Human-Computer Studies*, vol. 82, pp. 69–82, 2015.

[125] A. Darwish and E. Bataineh, "Eye tracking analysis of browser security indicators," in *2012 International Conference on Computer Systems and Industrial Informatics*. IEEE, 2012, pp. 1–6.

[126] K. Radke, C. Boyd, J. G. Nieto, and L. Buys, "Who decides? Security and privacy in the wild," in *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration*. ACM, 2013, pp. 27–36.

[127] S. Schecter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2007, pp. 51–65.

[128] T. Kelley and B. I. Bertenthal, "Real-world decision making: Logging into secure vs. insecure websites," in *Proceedings of the USEC'16.*, 2016.

[129] K. Radke, C. Boyd, M. Brereton, and J. G. Nieto, "How HCI design influences web security decisions," in *Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction*. ACM, 2010, pp. 252–255.

[130] M. Blythe, H. Petrie, and J. A. Clark, "F for fake: four studies on how we fall for phish," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 3469–3478.

[131] J. Wang, T. Herath, R. Chen, A. Vishwanath, and H. R. Rao, "Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email," *IEEE Transactions on Professional Communication*, vol. 55, no. 4, pp. 345–362, 2012.

[132] K. Parsons, M. Butavicius, M. Pattinson, D. Calic, A. Mccormac, and C. Jerram, "Do users focus on the correct cues to differentiate between phishing and genuine emails?" *arXiv preprint arXiv:1605.04717*, 2016.

[133] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Systems*, vol. 51, no. 3, pp. 576–586, 2011.

[134] S. Goel, K. Williams, and E. Dincelli, "Got phished? Internet security and human vulnerability," *Journal of the Association for Information Systems*, vol. 18, pp. 22–44, 2017.

[135] H. Holm, W. R. Flores, M. Nohlberg, and M. Ekstedt, "An empirical investigation of the effect of target-related information in phishing attacks," in *Enterprise Distributed Object Computing Conference Workshops and Demonstrations (EDOCW), 2014 IEEE 18th International*. IEEE, 2014, pp. 357–363.

[136] R. T. Wright, M. L. Jensen, J. B. Thatcher, M. Dinger, and K. Marett, "Research note—influence techniques in phishing attacks: An examination of vulnerability and resistance," *Information Systems Research*, vol. 25, no. 2, pp. 385–400, 2014.

[137] E. J. Williams, J. Hinds, and A. N. Joinson, "Exploring susceptibility to phishing in the workplace," *International Journal of Human-Computer Studies*, vol. 120, pp. 1–13, 2018.

[138] D. Oliveira, H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin, and N. Ebner, "Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 6412–6424.

[139] J. Lee, L. Bauer, and M. L. Mazurek, "The effectiveness of security images in internet banking," *IEEE Internet Computing*, vol. 19, no. 1, pp. 54–62, 2015.

[140] C. Marforio, R. Jayaram Masti, C. Soriente, K. Kostiainen, and S. Čapkun, "Evaluation of personalized security indicators as an anti-phishing mechanism for smartphone applications," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 540–551.

[141] E. J. Williams, A. Beardmore, and A. N. Joinson, "Individual differences in susceptibility to online influence: A theoretical review," *Computers in Human Behavior*, vol. 72, pp. 412–421, 2017.

[142] J. Andrić, D. Oreški, and T. Kišasondi, "Analysis of phishing attacks against students," in *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 2016, pp. 1423–1429.

[143] R. T. Wright and K. Marett, "The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived," *Journal of Management Information Systems*, vol. 27, no. 1, pp. 273–303, 2010.

[144] C. Iuga, J. R. Nurse, and A. Erola, "Baiting the hook: Factors impacting susceptibility to phishing attacks," *Human-centric Computing and Information Sciences*, vol. 6, no. 1, pp. 1–20, 2016.

[145] J. Abawajy and T.-h. Kim, "Performance analysis of cyber security awareness delivery methods," in *Security Technology, Disaster Recovery and Business Continuity*. Springer, 2010, pp. 142–148.

[146] I. Alseadoon, T. Chan, E. Foo, and J. Gonzales Nieto, "Who is more susceptible to phishing emails?: A Saudi Arabian study," in *Proceedings of the 23rd Australasian Conference on Information Systems (ACIS 2012)*. ACIS, 2012, pp. 1–11.

[147] B. Harrison, E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails: How attention and elaboration protect against phishing," *Online Information Review*, vol. 40, no. 2, pp. 265–281, 2016.

[148] J. S. Downs, M. Holbrook, and L. F. Cranor, "Behavioral response to phishing risk," in *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*. ACM, 2007, pp. 37–44.

[149] B. M. Bowen, R. Devarajan, and S. Stolfo, "Measuring the human factor of cyber security," in *2011 IEEE International Conference on Technologies for Homeland Security (HST)*. IEEE, 2011, pp. 230–235.

[150] S. Purkait, S. Kumar De, and D. Suar, "An empirical investigation of the factors that influence internet user's ability to correctly identify a phishing website," *Information Management & Computer Security*, vol. 22, no. 3, pp. 194–234, 2014.

[151] R. Heartfield, G. Loukas, and D. Gan, "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks," *IEEE Access*, vol. 4, pp. 6910–6928, 2016.

[152] Z. Alqarni, A. Algarni, and Y. Xu, "Toward predicting susceptibility to phishing victimization on facebook," in *2016 IEEE International Conference on Services Computing (SCC)*. IEEE, 2016, pp. 419–426.

[153] K. W. Hong, C. M. Kelley, R. Tembe, E. Murphy-Hill, and C. B. Mayhorn, "Keeping up with the Joneses: Assessing phishing susceptibility in an email task," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 57, no. 1. SAGE Publications Sage CA: Los Angeles, CA, 2013, pp. 1012–1016.

[154] M. Silic and A. Back, "The dark side of social networking sites: Understanding phishing risks," *Computers in Human Behavior*, vol. 60, pp. 35–43, 2016.

[155] J. G. Mohebzada, A. El Zarka, A. H. BHojani, and A. Darwish, "Phishing in a university community: Two large scale phishing experiments," in *the 2012 International Conference on Innovations in Information Technology (IIT)*. IEEE, 2012, pp. 249–254.

[156] F. Lalonde Levesque, J. Nsiempba, J. M. Fernandez, S. Chiasson, and A. Somayaji, "A clinical study of risk factors related to malware infections," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. ACM, 2013, pp. 97–108.

[157] F. L. Lévesque, J. M. Fernandez, and A. Somayaji, "Risk prediction of malware victimization based on user behavior," in *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*. IEEE, 2014, pp. 128–134.

[158] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "Phishing for the truth: A scenario-based experiment of users' behavioural response to emails," in *IFIP International Information Security Conference*. Springer, 2013, pp. 366–378.

[159] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 373–382.

[160] T. Vidas, E. Owusu, S. Wang, C. Zeng, L. F. Cranor, and N. Christin, "QRishing: The susceptibility of smartphone users to QR code phishing attacks," in *International Conference on Financial Cryptography and Data Security*. Springer, 2013, pp. 52–69.

[161] O. P. John, S. Srivastava *et al.*, "The big five trait taxonomy: History, measurement, and theoretical perspectives," *Handbook of personality: Theory and research*, vol. 2, no. 1999, pp. 102–138, 1999.

[162] N. Clarke, S. Furnell, M. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. Butavicius, "Why do some people manage phishing e-mails better than others?" *Information Management & Computer Security*, vol. 20, no. 1, pp. 18–28, 2012.

[163] R. S. El-Din, P. Cairns, and J. Clark, "Mobile users' strategies for managing phishing attacks," *Journal of Management and Strategy*, vol. 5, no. 2, p. 70, 2014.

[164] T. Halevi, J. Lewis, and N. Memon, "A pilot study of cyber security and privacy related behavior and personality traits," in *Proceedings of the 22nd International Conference on World Wide Web*. ACM, 2013, pp. 737–744.

[165] T. Halevi, N. Memon, and O. Nov, "Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks," *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*, 2015.

[166] J. Herrero, A. Urueña, A. Torres, and A. Hidalgo, "My computer is infected: The role of users' sensation seeking and domain-specific risk perceptions and risk attitudes on computer harm," *Journal of Risk Research*, pp. 1–14, 2016.

[167] C. Mayhorn, A. Welk, O. A. Zielinska, and E. Murphy-Hill, "Assessing individual differences in a phishing detection task," in *Proceedings of the 19th Triennial Congress of the IEA, Melbourne*, 2015.

[168] S. M. Albladi and R. George, "Personality traits and cyber-attack victimisation: Multiple mediation analysis," in *Internet of Things Business Models, Users, and Networks, 2017*. IEEE, 2017, pp. 1–6.

[169] B. Harrison, A. Vishwanath, and R. Rao, "A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016, pp. 5628–5634.

[170] D. Canali, L. Bilge, and D. Balzarotti, "On the effectiveness of risk prediction based on users browsing behavior," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*. ACM, 2014, pp. 171–182.

[171] E. Leukfeldt, "Comparing victims of phishing and malware attacks," *International Journal of Advanced Studies in Computer Since and Engineering*, vol. 5, no. 5, pp. 26–32, 2015.

[172] C. I. Canfield, B. Fischhoff, and A. Davis, "Quantifying phishing susceptibility for detection and behavior decisions," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 58, no. 8, pp. 1158–1172, 2016.

[173] R. Tembe, K. W. Hong, E. Murphy-Hill, C. B. Mayhorn, and C. M. Kelley, "American and Indian conceptualizations of phishing," in *2013 Third Workshop on Socio-Technical Aspects in Security and Trust*. IEEE, 2013, pp. 37–45.

[174] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, 2010, p. 11.

[175] O. A. Zielinska, A. K. Welk, C. B. Mayhorn, and E. Murphy-Hill, "Exploring expert and novice mental models of phishing," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 59, no. 1. SAGE Publications, 2015, pp. 1132–1136.

[176] F. Asgharpour, D. Liu, and L. J. Camp, "Mental models of security risks," in *International Conference on Financial Cryptography and Data Security*. Springer, 2007, pp. 367–377.

[177] C. B. Mayhorn and P. G. Nyeste, "Training users to counteract phishing," *Work*, vol. 41, no. 1, pp. 3549–3552, 2012.

[178] A. Abbasi, F. M. Zahedi, and Y. Chen, "Phishing susceptibility: The good, the bad, and the ugly," in *the 2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. IEEE, 2016, pp. 169–174.

[179] M. Ovelgönne, T. Dumitraş, B. A. Prakash, V. Subrahmanian, and B. Wang, "Understanding the relationship between human behavior and susceptibility to cyber attacks: A data-driven approach," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 8, no. 4, p. 51, 2017.

[180] E. R. Leukfeldt, "Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization," *Cyberpsychology, Behavior, and Social Networking*, vol. 17, no. 8, pp. 551–555, 2014.

[181] J.-H. Cho, H. Cam, and A. Oltramari, "Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis," in *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*. IEEE, 2016, pp. 7–13.

[182] A. Vishwanath, "Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack," *Journal of Computer-Mediated Communication*, vol. 20, no. 5, pp. 570–584, 2015.

[183] A. Neupane, N. Saxena, K. Kuruvilla, M. Georgescu, and R. K. Kana, "Neural signatures of user-centered security: An fMRI study of phishing, and malware warnings," in *NDSS*, 2014.

[184] A. Neupane, N. Saxena, J. O. Maximo, and R. Kana, "Neural markers of cybersecurity: An fMRI study of phishing and malware warnings," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1970–1983, 2016.

[185] W. Rocha Flores, H. Holm, M. Nohlberg, and M. Ekstedt, "Investigating personal determinants of phishing and the effect of national culture," *Information & Computer Security*, vol. 23, no. 2, pp. 178–199, 2015.

[186] H. A. Kruger, S. Flowerday, L. Drevin, and T. Steyn, "An assessment of the role of cultural factors in information security awareness," in *Information Security South Africa (ISSA), 2011*. IEEE, 2011, pp. 1–7.

[187] C. M. Kelley, K. W. Hong, C. B. Mayhorn, and E. Murphy-Hill, "Something smells phishy: Exploring definitions, consequences, and reactions to phishing," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 56, no. 1. SAGE Publications, 2012, pp. 2108–2112.

[188] R. Shay, I. Ion, R. W. Reeder, and S. Consolvo, "My religious aunt asked why I was trying to sell her viagra: Experiences with account hijacking," in *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2657–2666.

[189] J. D. Elhai and B. J. Hall, "Anxiety about internet hacking: Results from a community sample," *Computers in Human Behavior*, vol. 54, pp. 180–185, 2016.

[190] N. Stembert, A. Padmos, M. S. Bargh, S. Choenni, and F. Jansen, "A study of preventing email (spear) phishing by enabling human intelligence," in *the 2015 European Intelligence and Security Informatics Conference (EISIC)*. IEEE, 2015, pp. 113–120.

[191] A. Vance, B. B. Anderson, C. B. Kirwan, and D. Eargle, "Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG)," *Journal of the Association for Information Systems*, vol. 15, no. 10, p. 679, 2014.

[192] N. Ben-Asher, J. Meyer, Y. Parmet, S. Moeller, and R. Englert, "Security and usability research using a microworld environment," in *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, 2009, p. 54.

[193] T. Fechner and C. Kray, "Attacking location privacy: Exploring human strategies," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM, 2012, pp. 95–98.

[194] P. Gontar, H. Homans, M. Rostalski, J. Behrend, F. Dehais, and K. Bengler, "Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior," *Journal of Air Transport Management*, vol. 69, pp. 26–37, 2018.

[195] A. Neupane, N. Saxena, and L. Hirshfield, "Neural underpinnings of website legitimacy and familiarity detection: An fNIRS study," in *Proceedings of the 26th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 2017, pp. 1571–1580.

[196] A. Neupane, M. L. Rahman, N. Saxena, and L. Hirshfield, "A multi-modal neuro-physiological study of phishing detection and malware warnings," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 479–491.

[197] N. Bos, C. L. Paul, J. R. Gersh, A. Greenberg, C. Piatko, S. Sperling, J. Spitaletta, D. L. Arendt, and R. Burtner, "Effects of gain/loss framing in cyber defense decision-making," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 60, no. 1. SAGE Publications, 2016, pp. 168–172.

[198] N. Christin, S. Egelman, T. Vidas, and J. Grossklags, "It's all about the Benjamins: An empirical study on incentivizing users to ignore security advice," in *International Conference on Financial Cryptography and Data Security*. Springer, 2011, pp. 16–30.

[199] L.-C. Chen and D. Farkas, "An investigation of decision-making and the tradeoffs involving computer security risk," *Proceedings of the Americas Conference on Information Systems (AMCIS 2009)*, p. 610, 2009.

[200] A. Algarni, Y. Xu, T. Chan, and Y.-C. Tian, "Social engineering in social networking sites: how good becomes evil," in *Proceedings of the 18th Pacific Asia Conference on Information Systems (PACIS 2014)*. The Association for Information Systems (AIS), 2014.

[201] F. Zhu, S. Carpenter, A. Kulkarni, and S. Kolimi, "Reciprocity attacks," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 2011, pp. 1–14.

[202] A. Vishwanath, B. Harrison, and Y. J. Ng, "Suspicion, cognition, and automaticity model of phishing susceptibility," *Communication Research*, vol. 45, no. 8, pp. 1146–1166, 2018.

[203] B. Harrison, A. Vishwanath, Y. J. Ng, and R. Rao, "Examining the impact of presence on individual phishing victimization," in *2015 48th Hawaii International Conference on System Sciences*. IEEE, 2015, pp. 3483–3489.

[204] S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, and S. A. Naqvi, "The good, the bad and the ugly: a study of security decisions in a cyber-physical systems game," *IEEE Transactions on Software Engineering*, vol. 45, no. 5, pp. 521–536, 2017.

[205] S. McElwee, G. Murphy, and P. Shelton, "Influencing outcomes and behaviors in simulated phishing exercises," in *SoutheastCon 2018*. IEEE, 2018, pp. 1–6.

[206] A. D'Amico and K. Whitley, "The real work of computer network defense analysts," in *VizSEC 2007*. Springer, 2008, pp. 19–37.

[207] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human factors*, vol. 37, no. 1, pp. 32–64, 1995.

[208] R. M. Villamarín-Salomón and J. C. Brustoloni, "Using reinforcement to strengthen users' secure behaviors," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 363–372.

[209] R. S. Portnoff, L. N. Lee, S. Egelman, P. Mishra, D. Leung, and D. Wagner, "Somebody's watching me?: Assessing the effectiveness of webcam indicator lights," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 1649–1658.

[210] M. Smith, M. Strohmeier, J. Harman, V. Lenders, and I. Martinovic, "Safety vs. security: Attacking avionic systems with humans in the loop," *arXiv preprint arXiv:1905.08039*, 2019.

[211] ——, "A view from the cockpit: Exploring pilot reactions to attacks on avionic systems," 02 2020.

[212] European Aviation Safety Agency, *Impact assessment of cybersecurity threats*, Jul. 2018, [Online]. Available: https://www.easa.europa.eu/sites/default/files/dfu/EASA-REP-RESEA-2016-1-v0.2-cln.pdf.

[213] P. Millot, M. Mouchel, and C. Paglia, "The human operator as the ultimate barrier to cyber attacks," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2018, pp. 603–608.

[214] C. Dietrich, K. Krombholz, K. Borgolte, and T. Fiebig, "Investigating system operators' perspective on security misconfigurations," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 1272–1289.

[215] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *The Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975.

[216] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *Journal of Experimental Social Psychology*, vol. 19, no. 5, pp. 469–479, 1983.

[217] K. Witte, "Putting the fear back into fear appeals: The extended parallel process model," *Communications Monographs*, vol. 59, no. 4, pp. 329–349, 1992.

[218] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "Stealing pins via mobile sensors: Actual risk versus user perception," *International Journal of Information Security*, pp. 1–23, 2017.

[219] K. Crager, A. Maiti, M. Jadliwala, and J. He, "Information leakage through mobile motion sensors: User awareness and concerns," in *Proceedings of the European Workshop on Usable Security (EuroUSEC)*, 2017.

[220] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, "Little brothers watching you: Raising awareness of data leaks on smartphones," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 12.

[221] P. Rajivan, P. Moriano, T. Kelley, and L. J. Camp, "Factors in an end user security expertise instrument," *Information & Computer Security*, 2017.

[222] T. McGill and N. Thompson, "Old risks, new challenges: exploring differences in security between home computer and mobile device use," *Behaviour & Information Technology*, vol. 36, no. 11, pp. 1111–1124, 2017.

[223] M. Alsaleh, N. Alomar, and A. Alarifi, "Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods," *PloS one*, vol. 12, no. 3, 2017.

[224] B. Crandall, G. Klein, G. A. Klein, R. R. Hoffman *et al.*, *Working minds: A practitioner's guide to cognitive task analysis*. Mit Press, 2006.

[225] M. Fagan, M. M. H. Khan, and N. Nguyen, "How does this message make you feel? A study of user perspectives on software update/warning message design," *Human-centric Computing and Information Sciences*, vol. 5, no. 1, p. 36, 2015.

[226] J. Nicholson, L. Coventry, and P. Briggs, "" if it's important it will be a headline" cybersecurity information seeking in older adults," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–11.

[227] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," *IEEE Security & Privacy*, vol. 12, no. 1, pp. 28–38, 2014.

[228] M. L. Jensen, M. Dinger, R. T. Wright, and J. B. Thatcher, "Training to mitigate phishing attacks using mindfulness techniques," *Journal of Management Information Systems*, vol. 34, no. 2, pp. 597–626, 2017.

[229] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham, "School of phish: a real-world evaluation of anti-phishing training," in *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, 2009, pp. 1–12.

[230] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Protecting people from phishing: the design and evaluation of an embedded training email system," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2007, pp. 905–914.

[231] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Computers in Human Behavior*, vol. 48, pp. 51–61, 2015.

[232] J. R. Goodall, W. G. Lutters, and A. Komlodi, "I know my network: collaboration and expertise in intrusion detection," in *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*. ACM, 2004, pp. 342–345.

[233] D. W. Hosmer Jr, S. Lemeshow, and R. X. Sturdivant, *Applied logistic regression*. John Wiley & Sons, 2013, vol. 398.