Developing a Usable Security Approach for User Awareness Against Ransomware

A thesis submitted for the degree of Doctor of Philosophy

By

Usman Javed Butt

Department of Electronic and Electrical Engineering

January 2023

Abstract

The main purpose of the research presented in this thesis is to design and develop a game prototype for improving user awareness against ransomware, which has been reported as the most significant cyber security threat to the United Kingdom by the National Cyber Security Centre. Digital transformation is helping individuals, organisations, governments and Industrial control systems to modernise and improve their effectiveness. At the same time, cyber crimes are evolving and targeting essential services. A successful cyber attack can compromise users' privacy, bring bad publicity and financial damage to organisations and target national security.

A literature review was conducted to understand threats to the cyber social system. Literature in this thesis reports attackers exploit humans as the weakest link to execute successful security breaches. Therefore to address this challenge, a significant gap has been identified as an opportunity to contribute to user awareness of the ransomware cyber security threat.

The current thesis proposes Ransom*A*ware a novel game prototype to improve user awareness. The game is based on Technology Threat Avoidance Theory (TTAT) model. In this thesis two studies are carried out, study 1 empirically validates the elements of TTAT to be embedded in the Ransom*A*ware prototype and reports a significant change in users' motivation to avoid ransomware cyber security threat 55% and avoidance behaviour 29%, whereas study 2 evaluates game usability and report significant results of SUS average score of 87.58 and statistical results of $p < 0.01$ indicate user's satisfaction of the Ransom*A*ware. Finally, the research provides guidelines on how the proposed Ransom*A*ware game can be adopted by practitioners and individuals to improve their awareness against the ransomware cyber security threat.

Dedication

I am thankful to God Almighty, who has allowed me to fulfil my parent's dream. I dedicate this research thesis to my parents and express my sincere gratitude to them for their prayers and continuous support.

A heartfelt thank you to my wife for your patience, support, and encouragement. You stood by my side throughout this journey, and your continuous motivation helped me to thrive in my research.

My children AbdulHadi, AbdulRehman and Zainab deserve special compliments. I am indebted for your cooperation when I needed to focus on research. Your smiles always nourished me. I love you all.

I would also like to thank my siblings for their support and prayers.

Acknowledgements

I would like to express my deepest gratitude to my supervisor Professor Maysam Abbod for accepting my proposal. I am indebted to him for his academic and emotional guidance at every stage of the PhD. It is a privilege to have had his invaluable support, which was pivotal in completing my thesis.

I sincerely thank Prof. Hamed Al-Raweshidy as well as other faculty members for their invaluable assistance. I am also grateful to my friends and colleagues for their support and for bearing with me on this journey.

Thank you to all.

Publications

Published

- **Butt, U. J.**, Abbod, M., Lors, A., Jahankhani, H., Jamal, A., & Kumar, A. (2019). Ransomware Threat and its Impact on SCADA. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 205212). IEEE. doi: 10.1109/ICGS3.2019.8688327.

- **Butt, U. J.**, & Kumar, A. (2019). Ransomware. London: Cyber Security Practitioner Guide, World Scientific. ISBN 978-981-120-445-6

- **Butt, U. J.**, Abbod, M. F., & Kumar, A. (2020). Cyber Threat Ransomware and Marketing to Networked Consumers. In S. Dadwal (Ed.), Handbook of Research on Innovations in Technology and Marketing for the Connected Consumer (pp. 155185). IGI Global. https://doi.org/10.4018/978179980131-3.ch008

- Alraja, M. N., **Butt, U. J.**, & Abbod, M. F. (2023). Information security policies compliance in a global setting: An employee's perspective. Computers & Security, 103208.

Contents

1 Introduction **15**

1.1 Research Background and Motivation 15

1.2 The Role of Government in Cyber Education and Awareness 18

1.3 Change of Regulations and Its Impact on Businesses and Users 19

1.4 Research Aim and Objectives 21

1.5 Research Methodology 21

1.6 Thesis Structure 22

2 Literature Review **24**

2.1 Overview 24

2.2 Cyber Social System & Human-in-the-loop 24

2.2.1 An Overview of Cyber-Physical Systems 26

2.3 Cyber Security in Digital Life 31

2.3.1 Vulnerabilities Exploited by Attackers 32

2.3.2 Common Cyber-Threats 33

2.3.3 Ransomware Threat and Notable Attacks 38

2.3.4 Humans as the Weakest Link 40

2.4 Game-Based Learning and User Awareness 43

2.4.1 Educational Games for Ransomware 44

2.4.2 Research Gap for Cyber Security Training 46

2.4.3 Mobile Game-Based Learning 52

2.5 Summary 53

3 Research Methodology **54**

3.1 Overview 54

3.2 Research Design Process 54
3.3 Chosen Research Philosophies for The Current Thesis 55
3.4 Justification of The Chosen Approach 57
3.5 Choosing a Methodology for This Thesis 59
3.5.1 Quantiative Methodology 59
3.5.2 Qualitative Methodology 60
3.5.3 Multiple Methods of Research 61
3.6 Research Strategy & Data Collection Techniques 62
3.7 Game Development Methodology Challenge 64
3.8 Data Collection and Analysis 66
3.9 Research Ethics in The Current Thesis 67
3.10 Summary 67

4 Data Collection and Analysis 69
4.1 Overview 69
4.2 Theoretical Foundation 69
4.3 Research Model and Hypotheses Development 71
4.4 Methodology - Study 1 76
4.4.1 Data Collection 76
4.4.2 Measurement Development 77
4.5 Data Analysis and Results - Study 1 80
4.5.1 Measurement Validation 81
4.5.2 Model Testing 88
4.6 Discussion 91
4.7 Research Implications 92
4.8 Implications for Practice 94
4.9 Summary 96

5 Ransom*A*ware Game Design & Development 98
5.1 Overview 98
5.2 Usability – User Experience for User-Centred Design 99
5.3 Story Behind Ransom*A*ware 101
5.4 Game Design High-Level Requirements 103

5.5 Functional and Non-Functional Requirements . . . 104
5.6 Task Modelling to Achieve Usability . . . 107
5.6.1 Task Model 1 - Read Game Instructions . . . 107
5.6.2 Task Model 2 - Delete or Interact with The Alien Message . . 107
5.6.3 Task Model 3 - Exit a Game . . . 108
5.7 User Journeys to Implement Usability . . . 109
5.7.1 User Journey 1 - Time, Score and Feedback Review . . . 109
5.7.2 User Journey 2 - Pay Ransom . . . 110
5.7.3 User Journey 3 - Delete Good Message . . . 111
5.8 Game Ransom*A*ware Architecture . . . 112
5.9 Wireframes Walkthrough of Ransom*A*ware . . . 114
5.10 Game Development Phase . . . 115
5.11 Developers Testing Ransom*A*ware . . . 125
5.12 Summary . . . 126

6 Ransom*A*ware Testing and Evaluation 127
6.1 Overview . . . 127
6.2 Feasibility Study 2 of The Current Research . . . 128
6.3 Study 2 - System Usability Scale Test . . . 129
6.4 Data Collection Procedure . . . 131
6.5 Data Collection Instrument . . . 132
6.6 Experimental Protocol Design . . . 135
6.7 System Usability Scale Test Results . . . 136
6.8 Pre & Post Tests Results Analysis . . . 138
6.9 Pre & Post Test Results Validation . . . 139
6.10 Thematic Analysis to Confirm Elements of TTAT . . . 140
6.11 Discussion on TTAT Themes . . . 149
6.12 Summary . . . 159

7 Discussion of the Findings 160
7.1 Overview . . . 160
7.2 Discussion on Findings of Study 1 & 2 . . . 160
7.3 Reliability and Validity of Study 1 & 2 Results . . . 164

7.4 Implications of The Current Research 170
7.5 Methodology Contribution in The Current Research 172
7.6 Practical Contribution in The Current Research 175
7.7 Summary 179

8 Conclusion and Future Recommendations 180
8.1 Conclusion 180
8.2 Contributions of the Thesis 184
8.3 Research Limitations 184
8.4 Future Research 186
References 188

Appendix A 221

Appendix B 225

List of Figures

2.1 Cyber Social System [60] . . . 25
2.2 Cyber Security [89] . . . 31
2.3 Vulnerabilities exploited by attackers [99] . . . 33
2.4 Ransomware Methodology [120] . . . 38

3.1 Research Design Process . . . 55

4.1 Research Model [141] . . . 72
4.2 Structural Model Path Coefficients . . . 89

5.1 Unified User Experience Development Methodology . . . 100
5.2 User Personas [297] . . . 101
5.3 MoSCoW Analysis . . . 106
5.4 Read Game Instructions . . . 107
5.5 Delete or Interact . . . 108
5.6 Exit a game . . . 108
5.7 User Journey 1 . . . 109
5.8 User Journey 2 . . . 110
5.9 User Journey 3 . . . 111
5.10 Ransom*A*ware Architecture . . . 113
5.11 Homepage . . . 114
5.12 Spaceship Alien Message . . . 114
5.13 Feedback Message . . . 115
5.14 Spaceship EndGame Message . . . 115
5.15 Ransom*A*ware Home Screen . . . 116
5.16 Ransom*A*ware Dashboard . . . 116

5.17 Utilising global variables for key status indicators 117
5.18 Approaching planet animation 118
5.19 Control planet animations 118
5.20 Display alien message 119
5.21 Display alien message and increase message counter 119
5.22 Game timer procedure 120
5.23 Notification Displayed After Accepting a Genuine Alien's Message . . 120
5.24 The land button code block executed when the user accepts an alien message 121
5.25 Animation of Alien ship scanning the player 122
5.26 Procedures controlling the display of the good or bad alien animation sequence 122
5.27 Player defeating the Alien 123
5.28 Alien ship attacking the player depicting successful Ransomware Attack 123
5.29 Procedures determining and displaying the endgame message 124
5.30 Endgame feedback message for a final score of 10 124
5.31 Endgame feedback message for a final score of 40 125
5.32 Endgame feedback message for a final score of 80 125

6.1 Instructions for Participants 135
6.2 Themes and codes 142
6.3 Word Cloud 158

List of Tables

2.1 Related work & Research Gap 48

3.1 Research Paradigms 56

4.1 Participant's Demographics 77
4.2 Harman's single-factor 82
4.3 Normality, reliability, and discriminant validity. 84
4.4 Cross-loading 86
4.5 Fornell-Larcker criterion 87
4.6 Heterotrait-monotrait ratio (HTMT) 87
4.7 Multicollinearity Test 88
4.8 Hypotheses Results 90

5.1 RansomAware Training Rewards 103

6.1 Participants' demographics 131
6.2 System Usability Scale (SUS) questionnaire, Adapted from [224] . . . 134
6.3 Individual participant's SUS Score 137
6.4 SUS Mean and SD 138
6.5 Hypothesis Test Summary 140
6.6 Thematic Analysis 143

A.1 Study 1 Questionnaire 221

B.1 Themes and Codes 226

List of Abbreviations

A_Beh	Avoidance Behaviour
A_Mot	Avoidance Motivation
ACSC	Australian Cyber Security Centre
AI	Artificial Intelligence
AVE	Average Variance Extracted
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CMB	Common Method Bias
CMV	Common Method Variance
CompTIA	Computing Technology Industry Association
CPS	Cyber Physical System
CR	Composite Reliability
CSS	Cyber Social System
CSUQ	Computer System Usability Questionnaire
CyRiM	Cyber Risk Management
DCMS	Department for Digital, Culture, Media & Sport
DDoS	Distributed Denial of Service
DPA	Data Protection Act
EU	European Union
GDPR	General Data Protection Regulation
HiTLCPS	Human-in- the-loop Cyber-Physical Systems
HTMT	Heterotrait-Monotrait Ratio
IC3	Internet Crime Complaint Center
ICO	Information Commissioner's Office
ICT	Information and Communication Technologies

IoT	Internet of Things
IS	Information Systems
(ISC)²	International Information System Security Certification Consortium
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
IVR	Interactive voice response
MIT App	Massachusetts Institute of Technology Application
MoSCoW	MUST-have, SHOULD-have, COULD-have, and WILL NOT-have
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OT	Operational Technology
P_Sev	Perceived Severity
P_Sus	Perceived Susceptibility
P_Thr	Perceived Threat
PII	Personally Identifiable Information
PLS-SEM	Partial least squares structural equation modelling
QUIS	Questionnaire for User Interface Satisfaction
RaaS	Ransomware as a Service
S_Cost	Safeguard Cost
S_eff	Safeguard effectiveness
SCADA	Supervisory Control and Data Acquisition System
S-Eff	Self-Efficacy
SUMI	Software Usability Measurement Inventory
SUS	System Usability Scale
TTAT	Technology Threat Avoidance Theory
UCD	User-centred design
UX	User Experience
UXD	Unified User Experience Development Methodology
VIF	Variance Inflation Factor
WAMMI	Website Analysis and MeasureMent Inventory

Chapter 1

Introduction

1.1 Research Background and Motivation

In the current fast-moving digital era, Cyber Security is defined as implementing processes or controls to protect computers and electronic systems [1]. These systems hold critical data of individuals, companies and organisations and can be at risk of malicious attacks [2], including the digital infrastructure which connects them [3]. Due to the pervasiveness of computing, threats to these digital systems are gradually becoming more frequent and sophisticated [4]. Hackers and Crackers drive these threats to carry out Cybercrime either for their financial gains or information gathering and reconnaissance on opponents through political [1] motivation or to conduct Cyberwar to work on a specific ideology or to cause widespread disruption through controlling and shutting down electronic systems classified as Cyberterrorism [5]. The attacker typically penetrates these electronic systems through either known exploits or by discovering new vulnerabilities [6]. National Cyber Security Centre (NCSC, 2016)[1] define these incidents as a severe violation of the Computer Misuse Act (2010) as it breaches the confidentiality, integrity and availability of the data, system, and software through unauthorised access. The attackers use various techniques to deceive end users, such as malware, phishing [7], Distributed Denial of Service [8] and Man-in-the-middle into carrying out cyber-attacks [9].

Cyberspace's complex growth due to the evolution of the Internet of Things (IoT) and the inclusion of smart mobile devices has made end users more vulnerable [10].

[1] `https://www.ncsc.gov.uk/articles/what-cyber-incident`

Some notable incidents, such as US 2016 Elections hacked by Russians through email theft to influence elections in a foreign country, have been dominant in the media[11]. Distributed Denial of Service (DDoS) against Dyn, which owns most of the Domain Name System infrastructure, is considered a powerful reflection-based volumetric DDoS attack [12]. It left a significant number of web services inaccessible to Internet users. Cybercriminals executed this attack through a network of several thousand-compromised Internet-connected machines called botnets to overwhelm the target machine with spoofed source IP addresses [13]. The major cyber-attack against a Panama-based law firm was due to the exploitation of vulnerabilities exposed from un-patched open-source web server software, resulting in a breach of massive 11.5 million records from the company's database. Although the actual attacker is unknown, initial investigation links this breach to the user's access privileges [14].

In recent years, ransomware has emerged as malicious software used by attackers [15]. It employs robust encryption techniques to hostage the target user and prevent him from accessing his computer or data. Ransomware locks the machine to make it inaccessible or encrypts the user's data. This attack usually propagates via email attachments [16]. WannaCry is one of the ransomware cyber-attacks which caused worldwide disruption in 2017 and brought UK National Health Services offline for several hours. It is also reported to be propagated via email attachments accepted by the end user [17].

Facebook privacy row has been a new headline in all the media. The firm Cambridge Analytica (CA) obtained the personal data of Facebook users through the Facebook-linked app without users' consent, and it is estimated that 87 million users' data were inappropriately shared [18]. Although users' data mined by CA was a breach of trust between Facebook, its users and the CA, this scandal also escalated a need for the user to develop technology adoption awareness. In another incident, a cyber-attack against Ukrainian power suppliers left hundreds of thousands of customers without electricity [19]. The hackers exploited vulnerabilities in the communication architecture of the grid system to gain unauthorised access to the companies' Supervisory Control and Data Acquisition System (SCADA) [19]. The attackers used spear-phishing emails attached to Microsoft word files to penetrate malware in the system. It infected the master boot records of the operating

system used by the workers [20]. The attackers' methodology exploited workers as the weakest link through emails, compromising companies' corporate networks and causing havoc and severe disruption of the electricity supply.

Yahoo!, the Internet company, revealed in 2016 that a massive data breach hit them in 2013-2014. Hackers have stolen 4 billion user accounts [21], which include critical information like passwords, bank account details and other personal information. According to the company, attackers used users' browser cookies to steal their email passwords and get access to their personal information also highlights the need for user awareness of cookies [22].

According to the MIT press book 'The Internet of Things you Don't own' [23] also highlights the hacking concern associated with high-tech toys. Children's data is vulnerable to privacy invasion, creating realisation among parents about technology adoption. Wi-Fi-enabled Barbie doll manufactured by a company called ToyTalk is seen as a potential risk of children's privacy invasion, as this intelligent toy can be turned into a surveillance device [24]. This smart device uses Interactive voice response (IVR) technology to engage with children. The recorded conversation is not only stored on the cloud-based platform for data analytics to improve the response but also shared this data with third-party vendors for research development. So technically, the company owns all the conversations between the toy and children [25]. In the wake of the recent data theft of Hong Kong based smart toys manufacturer VTech, the companies' poor security practices led to the compromise of 11.6 million user's data, including children, which includes their personal information such as date of birth and audio files [26]. This data breach poses serious security risks concerning the Barbie doll, how data is communicated between the toy and the company's servers, and the measures taken to protect stored data and user privacy.

Cyber-attacks also threaten critical infrastructure because of modern cyberwarfare or espionage [27]. In the case of the Stuxnet worm, a foreign state-funded programme penetrated Iran's nuclear plant by exploiting vulnerabilities in the operating system and infected around 30,000 machines. Stuxnet, a social engineering cyber-attack. It propagated into critical nuclear infrastructure by compromising all the Windows operating system machines. One of the employees unintentionally executed this by plugging an infected USB into one of the industrial machines. This

worm was not only capable of searching the target machines and was able to connect to the Internet for updates to its source code. Worm resided on infected machines to gather operations of target logic controllers before deceiving target machines with wrong data input that caused them to malfunction [28].

To the best of the author's knowledge, from these cyber incidents, it can be seen that nobody is safe, from home computer users to the corporate sector and government organisations. Humans are exploited as the weakest link in cyber security. This led to the motivation of current research to work in this area. Further studies report [29], [30] skills shortage in the domain of Cyber Security. Reports consider everyone responsible in any organisation to combat these challenges through an entanglement of *learning and training culture among employees* [31] and the technological controls interdependencies instead of relying only on a technical mitigation plan. Therefore the current research aims to improve user awareness in the field of cyber security.

1.2 The Role of Government in Cyber Education and Awareness

In a socio-technical era, the complex interaction between people and Information and Communication Technologies (ICT) has made Cyber security a public concern rather than an individual [32]. This requires computer users to be more educated against cyber threats and reflect their high level of awareness through best practices [33]. The UK government has published National Cyber Security Strategy 2016-2021. The policy's objective is to work closely with National Cyber Security Programme. To safeguard UK cyberspace and ***improve user's cyber awareness through building knowledge*** and skills and implement a defend, deter and develop a plan (Government, 2017)[2] and intend to spend £1.9bn by 2021 on better security controls and skills gap [34]. As a part of the national Cyber strategy, the government has taken several initiatives and run different campaigns for user awareness. Cyber Essentials is one of them [35]. It aims to mitigate cyber security risks to any organisation by helping them understand the fundamental technical controls

[2] `https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021`

required to implement best security practices and security risks to the government supply chain process by making its adoption compulsory in government procurement policy since 2014 [36]. One of the articles published on Cyber Crime and Security in Parliament's briefing paper [37] highlights the importance of the government's 'Be Cyber streetwise' campaign to raise awareness among users to prevent [38].

To address the growing number of Cyber threat challenges to our digital lives and prepare technology-led generations to protect from online threats. The government has launched a £20 million pilot programme called the Cyber School Hub programme 'CyberFirst' [39], aiming to strengthen the computer science and cyber capabilities of both school students and teachers supported by the National Cyber Security Centre [40]. Debbie Tunstall, head of education at Cyber Security challenges UK suggests that this programme will help to fill the critical skills gap in Cyber Security field and prepare youth for lucrative careers through education and awareness [41]. National Cyber Security Strategy 2022, published by the UK Government, also reiterate the importance of cyber education at every level (Office, 2022)[3], [42]. To the best of author's understanding there is no game-based learning on ransomware awareness. The current thesis identifies this opportunity as a research gap and introduce a novel concept of game-based learning to raise user awareness and develop resilience against ransomware.

1.3 Change of Regulations and Its Impact on Businesses and Users

With the rise of sophisticated cyber threats and compromise to user's data, 'Privacy' breach incidents have impacted and changed information governance. After years of consultation in the Parliament, the new EU privacy law 'General Data Protection Regulation (GDPR), came into effect on 25th May 2018 [43], replacing the existing UK Data Protection Act 1998 [44]. The United Kingdom withdrew from the EU on 31st January 2020, UK adopted DPA 2018 [45] to replace the GDPR [46]. This allows individuals to control how their personal or sensitive information (online profiling,

[3] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

IP addresses, Biometric data, Cookies and other personal information) is collected, processed, and shared by organisations and their accountability and governance to protect collected data. According to the information commission office (ICO, 2018)[4], DPA is a must compliance for all organisations holding users' personal information and their due diligence of best practices and policies to improve data governance and information security. It strengthens individual rights by enforcing organisations to implement transparent data collection processes, seeking valid user consent, and providing an understanding of how their data will be processed [47].

Users will be in more control of their right to restrict data processing and portability and request to erase and correct their data [48]. This requires organisations to be more responsible and demonstrate rigorous compliance. This can be achieved by ensuring data accountability through maintaining logs of data processing activities, implementing security controls to protect data security, notification of data breaches and ensuring adequate controls are in place before data is travelled outside the EU territory. Failing will result in heavy fines and bad publicity for the organisation and damage customer trust. This new rule will reshape the organisations currently use user online data for data analytics and marketing purposes without user consent [49]. The legal impact of DPA has also raised awareness of cyber security attacks among corporate managers ever than before. The organisations understand the risks of data breaches to their critical assets and their responsibilities towards improving cyber security. The information security frameworks adopted by the organisation guide implementation of physical control and employees' education and awareness of cyber threats. Security risk mitigations can help organisations to avoid heavy fines of up to 4% of their global revenue in the case of GDPR and DPA [50]. Considering cyber compliance is vital for individuals and organisations, the current thesis aims to develop a user-friendly approach to awareness against the ransomware cyber security threat.

It is impossible to achieve 100% security. However, implementing better controls, education and awareness can mitigate these risks.

[4] `https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/`

1.4 Research Aim and Objectives

Aim

To Improve User Awareness Against Ransomware Cyber Security Threat Using Game-Based Learning.

Objectives

- Critically appraise the cyber-social model to explore the challenging relationship between cyber-technology and end users.
- Critically identify factors contributing to the lack of user awareness of the Ransomware threat.
- Design a usable game-based prototype to improve user awareness of ransomware
- Empirically evaluate the effectiveness of a game-based prototype to assess awareness of ransomware.

1.5 Research Methodology

There are several research approaches. However, the current research thesis adopts a positivist philosophy. This will help to answer the research question, i.e., 'Developing a usable security approach to user's awareness against ransomware'. The motivation to select these choices during the research design is influenced by the ontology belief that objectivity and subjectivity are critically important to gain trustworthy factual knowledge [51].

The need for usable security training for the user is a key mitigation strategy, which can be adopted to provide an effective defence against cyber-attacks [52]. Therefore, research first aims to understand user understanding of the threat before designing a mobile prototype.

Two studies are reported in this thesis. In the first study, the author adopted a quantitative research methodology, which is also associated with positivist philosophy. This will help to understand the empiricist view and the position of social

entities represented by objectivism [53]. This study focuses on the deductive approach, examines the relationship between different variables, and analyses them statistically to identify critical elements to be addressed in the proposed game design framework and enhance user awareness against ransomware threat.

In the second study, the research aims to evaluate usability, which is defined as the user's interaction with the product efficiently and effectively to complete the desired task. To achieve this, the author adopted a mix-method approach. Firstly, a pre-test questionnaire will be designed; the purpose is to evaluate the subjective understanding of the design usability, followed by a usability test and post-test questionnaire and used deductive approach associated with social constructionism to emphasise quantitative data [54]. Semi-structured interviews were conducted to remove any bias, and results were interpreted using an inductive approach [55].

1.6 Thesis Structure

This thesis has been structured into the following chapters.

Chapter 1: This chapter introduces research, the problem statement in the context of cyber security, the Scope of research and the motivation behind selecting the research topic. It outlines the research question, objectives, and a thesis structure to outline the journey to meet the research goal and objectives.

Chapter Two: It provides a literature review related to the concept of the cyber social system in today's world and user interaction, the impact of cyber threats in general with a particular focus on ransomware and the effectiveness of a game-based learning approach for users in the context of current research.

Chapter Three: This chapter focuses on research design and methodology. It discusses the research paradigm and justification of the research design process. It specifies the research philosophy, approach, methodologies and strategies adopted for data collection, analysis, and interpretation during the study. This chapter also includes ethical issues implied by the current study.

Chapter Four: This chapter reports on findings and analysis. The Technology Threat Avoidance Theory (TTAT) process is examined to understand the factors influencing individual users related to IT threat avoidance behaviour. It is used

as a baseline to design a questionnaire for users' understanding of the perceived threats. This empirical study is used to identify critical components required to include in the Game design, which is proposed in this thesis for users' awareness against ransomware.

Chapter Five: focuses on designing and developing a usable Game Design prototype to improve user education awareness against ransomware threats. The study will use the open-source Android mobile application development tool MIT App Inventor to design and develop a usable solution based on the findings reported in chapter four. The study will also report consideration of usability factors critically crucial for a practical design.

Chapter Six: This chapter evaluates and tests the proposed Game design prototype and presents empirical findings. The evaluation process involves a pre-experiment questionnaire, SUS test and post-experiment questionnaire to evaluate the usability of the game design. Then followed by semi-structured interviews to evaluate the effectiveness of the TTAT elements embedded in the proposed game prototype for user education and awareness.

Chapter Seven: This chapter discusses the findings of studies 1 & 2 and how the results were validated using quantitative and qualitative data analysis approaches. The findings were interpreted to evaluate their significance in the context of current research. Then concludes with a detailed discussion of the current research's theoretical, methodological and practical implications.

Chapter Eight: This chapter highlights research contributions. Provide a conclusion derived from the research thesis and make future recommendations on how the proposed prototype can implement a Cyber Security Management Framework for effective user education against ransomware. Finally, this chapter also identifies research limitations and future work opportunities to extend the findings of this research.

Chapter 2

Literature Review

2.1 Overview

The current research in this thesis aims to improve user awareness of the ransomware cyber security threat. In pursuit of the research goal, chapter 2 proceeds with exploring the concept of the cyber social system and cyber-physical systems and identifies humans as an integral part of this system. The chapter provides a discussion on how technological advancement enables humans to collaborate via smart devices and then focuses on how this relationship is challenged by the rise in more organised cyber-attacks. This chapter provides an understanding of cyber security threats in general and then focuses on the impact of Ransomware threat. It also identifies humans are vulnerable and provides a discussion on the common attack vector adopted by the attacker to exploit them. Finally, this chapter highlights the research gap and identifies game-based learning as an opportunity to enhance user learning of the ransomware cyber security threat.

2.2 Cyber Social System & Human-in-the-loop

The social system is where humans interact with each other on mutually accepted norms and values [56]. Each Individual play a significant role in the system to perform its goal. Hence the interdependency and cooperation between the system entities require a trustworthy and reliable relationship to make the system functional effectively [57]. However, the concept of a *Cyber Social System* (CSS) has emerged

due to the growing interaction of Cyber technologies with the existing human social system and the way these two are closely knitted together to form digital lives [58]. The National Institute of Standards and Technologies (NIST) define *Cyber Physical System* (CPS) as *"A co-engineered smart system of physical networks and computational segments, which communicates together to form a critical infrastructure for digital lives and improve humans' quality of life"* [59]. From the definition, it is evident that the main elements of CPS are 'communication', 'computation' and 'humans'. Therefore, it is comprehensible for the CPS to function efficiently and accurately to achieve its goal as shown in **Figure** 2.1

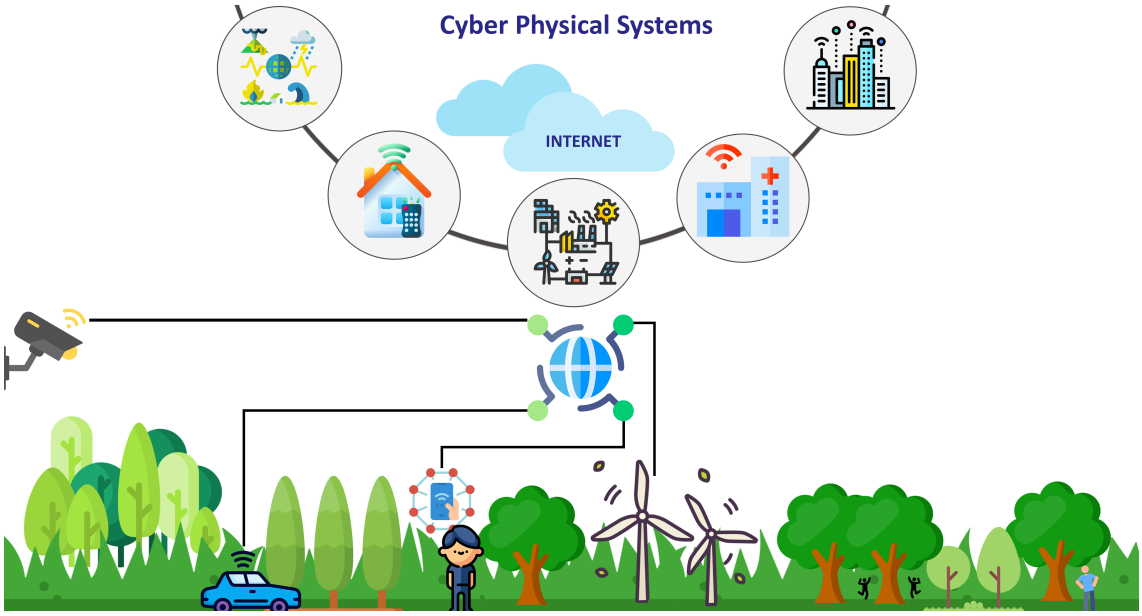

Figure 2.1: Cyber Social System [60]

In CPS, the interconnected systems of physical processes, networking and computation are considered real-time and intelligent and act as an adoptive feedback system for humans to make informed decisions [61], [62]. However, the authors do not consider any implications which could result from humans as a source of failure in the heterogeneous CPS. Whereas Nunes *et al.* [63] draw attention to the concept of Human-in-the-loop Cyber-Physical Systems (HiTLCPS) and argue that pervasive computing requires trustworthy relations between human beings and cyber technologies, which is only possible through user awareness of the technology adoption and security best practices. The current thesis takes these findings as an opportunity to address cyber security awareness against ransomware threat.

Due to *humans* in the loop, these systems' financial and societal capabilities are immense and provide an opportunity for technology businesses to develop smart solutions for transforming human lives [64]. However, the design and development of CPS require addressing cyber security concerns related to confidentiality, integrity and authorisation [65]. The systems should be resilient to confirm their availability to its stakeholders and should be able to provide privacy to avoid any intrusion or malicious act [66]. Sometimes CPS are interchangeably used for terms like the Internet of things, smart (homes, cities, grids, disaster management, healthcare, etc.) and has become an integral part of our digital lives. Its applications are everywhere in modern societies [67].

2.2.1 An Overview of Cyber-Physical Systems

This section provides an overview of some of the cyber-physical system's applications and their interaction with humans.

- *Smart homes* are popular application of CPS. It works on an automation system and provides remote control and monitoring of home devices to its inhabitants either through a single click using a smartphone, tablet, laptop or voice command [68]. A previous study review on security in a smart home by [69] concluded that Internet-connected smart home devices communicate with each other in CPS. Therefore the user is not in control of data and is subject to surveillance or privacy invasion. Most studies on smart home focus only on cyber-attacks on the physical devices of CPS. However, research by [70] suggests significant efforts are required to create awareness among end users for setting up strong passwords for devices in CPS to avoid any security compromise. In their research paper, the authors open further future opportunities to explore user awareness education against cyber threats, which will be addressed by designing and developing a usable prototype in the current thesis.

- *Smart Cities as CPS:* Today, 55% of the world population lives in urban areas, and it is predicted to increase up to 68% by 2050, says the United Nations department of economic and social affairs [71]. Smart Cities are seen as a

widely used mitigating cyber-physical system solution by the governments to overcome the increasing demands of the urban population in the transport, climate, environment and energy sectors and are expected to improve their well-being [72]. In comprehensive studies of smart cities' challenges and opportunities by [73], the authors argue that sustainable development and improved urban population well-being are impossible without addressing rising cyber security challenges to smart cities. Authors further argued that emerging smart city applications such as; e-government, smart transport, traffic controls, smart parking, smart meters, and smart landfills are meant to make people's lives easy. However, these applications are vulnerable to security breaches and implementing technical controls such as; encryption, firewall, and intrusion detection systems are not an adequate solution to overcome these challenges.

Another previous research by [74] focuses more on cyber threats to smart cities at the individual and community levels. The research explains that due to the heterogeneous nature of smart cities, cyber-physical systems and emergent technologies, the data sharing between infrastructure (ICT & IoT) and the applications running on it are subject to data privacy invasion. The study would have been more helpful if it had also included other characteristics such as connectivity, scalability, mobility and resource constraint of smart cities to implement more efficient countermeasures against the cyber threats for stable and secure smart cities. However, other studies of smart cities' challenges and opportunities by [73] conclude that smart cities' cyber-physical systems are not just about cutting-edge technologies and devices. Infect human Involvement is considered an essential characteristic of the smart cities CPS and offers a research opportunity to explore how human learning and education can play a role in protecting smart cities CPS.

- *Smart Grid:* International Energy Agency, world energy outlook report 2014 indicates a 37% increase in global energy demand by 2040 (IEA, 2014)[1]. It is estimated that renewable energy initiatives can meet the global energy demand [75]. In contrast to traditional legacy grid systems, smart grid cyber-

[1] `https://www.instituteforenergyresearch.org/fossil-fuels/coal/ieas-world-energy-outlook-2014/`

physical systems are emerging solutions due to rising efficient and cleaner energy demands and the limited availability of non-renewable natural resources. It allows a two-way dialogue of electricity/information exchanged between its utility and customers [76]. A smart grid or SCADA is a cyber-physical system, a network of communications, sensing, computation, controls and other technologies. These components work together to produce cost-effective and efficient services to its users. However, due to the interdependency between these components, authors [77] indicate that smart grid system operations are at risk of cyber-attacks such as denial of service attacks and false data injection attacks. Such attacks could potentially compromise the security and efficiency of the smart grid physical system and suggest an auto-corrective control mechanism to mitigate cyber-attack risks. However, much of this study only focused on technical controls as a solution and has failed to address human factors, which is an essential part of the smart grid cyber-physical systems. Another study [78] argues that future interaction between the smart grid-cyber social system and the users would only be successful if cyber security implementation and awareness were considered. The authors suggest protecting users' and systems' confidentiality, integrity and authorisation against unauthorised access.

- *Disaster management as CPS:* is also playing a critical role in disaster management and recovery system for predicting earthquakes, tsunamis, volcanoes and tornadoes [62]. Studies on Cyber Systems using intelligent sensors [79] explain that when cyber-physical systems are applied to the disaster management system. Due to its data-sharing ability in the network, it can detect unusual air pressure noise, temperatures and humidity from a remote location. This can be used as preventive measures to raise an advanced auto alarm to unusual behaviour or can also be used to prepare and respond to any remote catastrophic incident more effectively and promptly. However, the study fails to consider the factors required to make the CPS secure, efficient, and reliable. In a comprehensive study by [80], the authors explore the importance of smart disaster management system's functionalities, such as; communication services and situation awareness detection for accurate reporting of conditions

from the affected area for appropriate prevention mechanisms and also point out the technical and security challenges of the smart disaster management system. This study also indicates that smart disaster management CPS involves many communication equipment. The integration of these devices is critical for the system to work efficiently. At the same time, interoperability of these devices can pose serious cyber security threats to its integrity and require the stakeholders to ensure system security to establish a trustworthy relationship and maintain the availability, authentication and accuracy of the system at all times [80].

- *Smart Healthcare* also uses Cyber-Physical systems, which are plausible for improving patients' well-being. Life-saving devices such as the implantation of a heart pacemaker and an insulin pump significantly improve patients' health (NHS, 2022)[2]. In recent years, smart healthcare cyber-physical systems have attracted more attention due to the rise of ubiquitous computing and the Internet of Things. The cost of healthcare will increase due to the rise in chronic conditions, and predict that health organisations around the world will adopt smart healthcare as an innovative solution to tackle the rise in the ageing population and transform social care [81]. Although this report highlights the benefits of smart health services in terms of reduced cost, patient independence and improved outcomes, it fails to draw any attention to cyber threats to these devices for their effective functioning. Research by [82], the authors provide a comprehensive evaluation of the cutting-edge technologies used in the Internet of Things for Smart Healthcare, its challenges and opportunities.

  This study also indicates that security considerations are paramount for the reliability of smart healthcare CPS. It provides remote health monitoring. Data transmission between a patient and the database must be protected against any malicious cyber-attack. It can reveal patient-sensitive data and need constant availability to provide the availability to its stakeholders or authorised parties such as doctors, nurses and emergency services. Smart healthcare CPS is also widely used in the health sector to improve elderly care. One of its applications is the use of smart sensory wearable devices, which im-

[2] `https://www.nhs.uk/conditions/pacemaker-implantation/`

proves patient healthcare, particularly emergency response [62]. Their studies of Ubiquitous healthcare [83] highlight the importance of secure authentication mechanism requirements for IoT-enabled healthcare systems to protect them against cyber-attacks. In contrast, studies by [84] on U-Healthcare propose an authentication system for transmitting secure critical medical data in CPS. However, authors would require a more systematic approach to identify other factors, such as usability and user awareness in CPS, to combat evolving cyber-threats, as many threats are caused by a lack of awareness or human errors [85].

The ability of cyber-physical systems to act as intelligent and real-time feedback systems have become an integral part of digital lives to improve humans' quality of life. However, their heterogeneous integration and constant online connectivity mean an increase in attack surface, which can be exploited by cybercriminals, either for financial gain or to bring a bad reputation [65]. The literature informs smart grids have been subject to Denial-of-Service attacks [77] and the rise of ransomware attacks [72]. Smart Homes have been compromised due to users' poor cyber hygiene [70], and Smart Healthcare and Disaster management systems have been compromised by cyber-attacks too [80]. Cyber threats target confidentiality, integrity and availability of these systems and compromise the relationship between humans and cyber-physical systems [83]. Previous studies suggest that the reliability of this relationship hinges on improving user awareness against cyber security threats [70], [73], [78] and [85].

The rise of ubiquitous or pervasive computing has led to the emergence of the *Cyber-Physical Social System* (CPSS). This transition from a social system to a cyber world has revolutionised the interaction of computers, humans and the environment. It requires a dire need to address the challenges of creating cyber security awareness among system users [86]. Massachusetts Institute of Technology media research group publications also provides insight into technology adoption and diffusion in human dynamics [87] and explore how social networks influence digital lives such as transport, medical, governance and businesses. The research draws special attention to human digital footprinting. It considers human digital crumbs a crucial element in examining human behaviour and establishing a trustworthy,

efficient and secure relationship between humans and the cyber world. If security is not addressed, this can affect the reliability of this relationship [88].

2.3 Cyber Security in Digital Life

The National Cyber Security Centre (NCSC) U.K. define 'cyber security as the core function in protecting all digital devices and services accessible through the internet from theft or damage' (NCSC, 2020)[3] and requires all individuals and organisations to protect themselves from cyber-attacks [89] is presented in **Figure 2.2**. Cyber security is a functional exercise to achieve confidentiality, integrity, and availability of computer systems against these cyber-attacks. Controls implementation, which can minimise the risks of cyber-attacks against any unlawful intent [89]. Hence protecting the financial and reputational damage of the business [90]. However, [89] states that cyber security protects information assets and humans, which can be potential targets of these cyber threats.

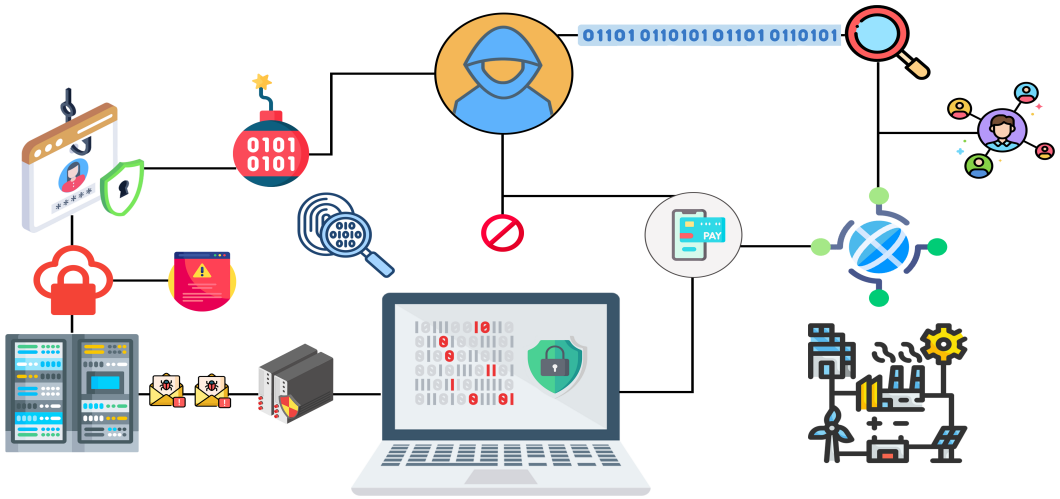

Figure 2.2: Cyber Security [89]

The way ***Internet*** has evolved has transformed the world into a global village and revolutionised the connectivity between people. Similarly, the Internet of Things (IoT) has reshaped the world into a smarter place [91]. There has been a sharp rise in digital security attacks from known and unknown sources (NCSC, 2022)[4].

[3] https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

[4] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/

This highlight a dire need to address cyber security threats against Internet-enabled devices so they can be efficient for their purpose without being compromised by the cyber threat.

2.3.1 Vulnerabilities Exploited by Attackers

Today cyber security is critical for any individual, families, businesses, financial institutions, the military and governments as they use computers and smart devices using the Internet to store and transmit their confidential information, which requires protecting this data from unauthorised access [92]. The Internet is an integral part of our digital lives, which helps users to share and communicate on a common platform and help them to save time, and cost and improve the efficiency of their daily tasks. However, at the same time, cybercriminals are exploiting new ways to steal users' confidential data, which makes cyberspace insecure. Hence, the need to integrate cyber security education is paramount for the users to prepare a future skilled workforce to tackle growing cyber threats and secure the nation [93]. The report from Cisco considers cyber security everyone's responsibility (Cisco, 2010)[5]. It emphasises the need to take care of their data to achieve confidentiality, integrity and availability, authentication, and authorisation of the data. To ensure data is not altered, it is known to its recipient only and available to its intended user all the time. International Information System Security Certification Consortium (ISC²) suggests that organisations need security & risk management policies to deal with governance and user awareness challenges [94].

Moreover, all organisations are responsible for protecting their employees, data and equipment against cyber threats. However, the security policy implementation is not one size fit for all and cannot be the same for all organisations, as their business operations vary [95]. Today organisations have dedicated roles to ensure the design and implementation of an effective security programme to achieve their business goals. They have due care to ensure their legal responsibilities and diligence through security systems risk assessment [96]. This allows to review, update and

cyber-security-breaches-survey-2022

[5] https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/C45-626825-00_Cyber_Security_Responsibility_AAG.pdf

test equipment and creates a culture of training and awareness among its users to adhere to the organisations' security policy [97].

According to NIST [98], for an organisation to mitigate the risks against any information technology system, it will be imperative to determine the scope of any potential vulnerability, threat and risks associated with organisational tangible and intangible assets and employees. **Figure 2.3** shows to achieve security, ***People***, Processes and Technology are identified as the weakest link [99]. However, the scope of current research addresses only human vulnerabilities as they are identified as an integral part of the cyber-physical systems in the previous section.

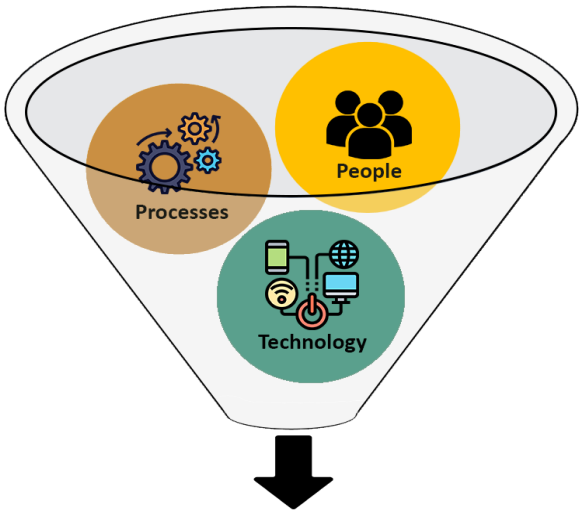

Figure 2.3: Vulnerabilities exploited by attackers [99]

2.3.2 Common Cyber-Threats

McAfee Labs[6] report provides a critical analysis of threat intelligence, how it has impacted every segment of cyber-physical systems and advice on best practices to reduce the likelihood of these threats. Among many other threats, malware, phishing, spear phishing and denial of service are the top cyber threats targeting cyber-physical systems [100]. As part of one of the research objectives, the current thesis will examine different cyber threats and then narrow the investigation to the research aim of investigating ransomware and usable way to educate and create awareness among users.

[6] https://www.trellix.com/en-us/advanced-research-center/threat-reports/feb-2023.html

The Computing Technology Industry Association (CompTIA) has pointed out some common cyber threats, such as; viruses, malware, ransomware, worm, Trojans, rootkit, spyware, adware, backdoor and Bots [101]. These threats are indicators of security compromise and further elaborate how adversaries employ different techniques to hack computer systems. One such popular common technique is ***'hacking the human'***, which is carried out using ***Social Engineering attacks***. The attacker can deceive the humans by making a phone call and impersonating a legitimate person to get access to the user credentials [102]. Social engineering tries to exploit human behaviour and demand a quick response. To make the attack more persuasive. The attackers usually adopt their convincing charismatic abilities, pretending to be superior in rank to the person they are speaking to and even use shoulder surfing, lunchtime attack and tailgating techniques to get physical access to the system [103].

The Cyber Security Breaches Survey 2022, commissioned by Department for Digital, Culture, Media & Sport [104]. It influences U.K. cyber resilience strategy and shows that 39% of U.K. businesses reported cyber-attack in the last 12 months. These attacks were mainly the result of phishing used as an attack vector. ***Phishing*** is a type of social engineering [105] that employs spoofing techniques. It can be carried out using social media platforms, emails and websites. The attacker usually sends an email from a legitimate website, such as a bank, to its target user. The email message appears legitimate but contains a disguised link directing to a spoofed website of the attacker hence resulting in stealing user confidential information. Because phishing requires user action to execute the attack, it can sometimes install malicious software in the user's computer, which can act as a back door to steal crucial information or sabotage the system. NCSC recommends a multi-layer security approach to defeat phishing through user training, which can help them spot and report fraudulent suspicious phishing emails and encourage them to use strong passwords for authentication on the system.

Spear Phishing is a more refined version of phishing [106]. This, which is more target-focused and usually already has some information about the target, makes it more likely to be successfully executed. The attacker emails are more bespoke and reach the target inbox, addressing the recipient's name. As a result, the target user

can find these emails safe to open, which enables cyber criminals to compromise the target user's confidential information or install malicious backdoor software. These cyber-threats have one thing in common, i.e., exploiting humans as the weakest link, traditional hardware controls such as firewalls are ineffective in mitigating these attacks and require a cooperative cyber security strategy to educate computer users. CompTIA Security+ [101] recommends user training as a best practice against social engineering attacks. It recommends educating users to adhere to corporate security policies. Furthermore, engage them in continuous training to make them aware of new attacks in the evolving cyber landscape. Effective training can help them not disclose confidential information to social networking or third-party websites.

Cisco Systems considers adversaries and nation-state actors the real threats as they are believed to have the required resources, sophisticated tools, expert skills and financial motivation to lunch a cyber-attack and cripple any critical infrastructure (CISCO, 2018)[7]. The report shows a sharp rise in cyber criminal activities and provides insight into the attacker's behaviour in the booming land shift of the cyber world. The report also reveals emerging sophisticated encryption techniques used by malware to compromise heterogeneous computer environments, using unpatched installed operating systems, cloud applications and un-monitored deployed IoT devices. This compromises them by creating botnets of hundreds of millions of zombies to carry out distributed denial of service attacks, making them inaccessible for their legitimate users. Cisco recommends the need for a strong defence against these attacks and suggests some good corporate best practices such as network segmentation, regular applications patching process for auto updates, use of endpoint monitoring tools, backing up critical data, firewalls implementation, use of secure protocols, data analytics and scanning of network traffic. However, the report fails to consider any hybrid approach for defence in depth, as humans are also considered the weakest link and need education and awareness against cyber threats [107].

Corporate policy: ' bring your own device', allow usability to the user [108]. However, this also risks organisational network infrastructure security, hence suggesting a need to develop a cyber-security culture, which can focus on employee training and awareness against cyber security threats [109]. The author further

[7] https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

emphasises the need for education and awareness, as any poor practice, such as a weak password by the user, can be vulnerable and result in escalation privileges. In his detailed analysis of security culture, the author concluded that effective security training could not be implemented only with hardware controls. The organisations must develop a continuous education and awareness process rather than one-off exercises. The author also mentioned the need to adopt innovative education and awareness, i.e., game-based learning, as the purpose is to engage and educate users against security threats robustly. The study provides an opportunity to explore this innovative learning technique, which will be addressed in this research paper by designing a usable interactive prototype for users' learning against the ransomware cyber threat. Cyber criminals exploited the vulnerabilities of the remote workforce during the pandemic. A sharp rise in cyber-attacks [110] suggests the need for individual users to practice cyber hygiene and recommends that organisations improve user awareness against cyber security threats.

According to [111] *malware* is a generic term used for malicious software to sabotage the computer's security. There is a comprehensive list of different malware that differ in their execution and behaviour. The malware is categorised into two types those that target to crash a Host or a Network, i.e. (Viruses, worms and logic bombs) and those that intend to take control over computer systems through command-and-control mechanisms, i.e., (Trojans, Rootkits, Spyware and Ransomware) (Microsoft, 2018)[8]. However, the scope of current research is Ransomware only.

Stuxnet is malicious software that targeted SCADA systems by exploiting zero-day vulnerabilities and is believed to be designed to sabotage Iran's nuclear programme in 2010 [112]. It arrived at Natanz nuclear facility through an infected USB. It was plugged in physically by someone into the computer networks of the plant either intentionally or unintentionally before it proliferated and infiltrated into the computer network without being detected. The authors [113] draw special attention to the fact and describe Stuxnet as a different malware compared to its predecessors as it only targeted industrial systems. These unlikely other worms infect any number of computers on the network [113]. The payload of Stuxnet was designed to search

[8] `https://support.microsoft.com/en-us/help/129972/how-to-prevent-and-remove-viruses-and-other-malware`

and sabotage only the computers associated with Programmable logic controllers responsible for controlling the automated process of centrifuges. The *Stuxnet* payload was complicated and written in multiple languages. This is why it was unnoticed for several months before it was executed. It is believed that its creator had immense knowledge of its targets and had enough resources to carry out this sophisticated attack. The author term this attack as a first cyber warfare weapon and highlights that isolating critical infrastructure from the Internet is not enough as the attacker can utilise a combination of insider threat (humans) and advanced technical skills for future cyber-attacks [114]. Although this was a state-sponsored attack, humans were exploited using social engineering. The authors highlight the importance of user awareness of cyber security threats. The current thesis will address the gap in user awareness of the changing landscape of cyber security threats and will focus on improving user awareness to thwart ransomware threat.

Spyware is malware that collects users' data such as browsing behaviour, computer screen shorts, keystrokes, personal information, i.e. (financial information, medical information, username, passwords, etc.) and business trade secrets using keyloggers. It uses the Internet to transfer it to third parties without consent [115], compromising the user's confidentiality and privacy. It reaches to user's computer or mobile device through an email attachment or file-sharing platform. It executes secretly without knowing the user to start its operations as a background process [116]. Spyware often exploit users to action any unusual prompt, such as pop-up ads, requiring users to take extreme caution to avoid accepting any unknown and unwanted attachments or other downloads. According to Federal Trade Commission [117], spyware's regulatory and legislative definition is too broad. Even the use of parental control software and banking monitoring software is also considered spyware. However, due to the preventive nature of this software, the commission recommends using Spyware terminology only for the software capable of deceptive privacy invasion. The report also highlights that spyware compromises computers' performance as it consumes system resources, making computers slow or unreachable by their legitimate users. Also, emphasise the need to install hardware controls and educate users to tackle this malicious software by implementing best practices such as improving browser security and privacy settings and ensuring operating systems

and applications have the latest updates.

The author [118] defines spyware as a threat to the computer user and corporate and national security due to its privacy invasion and espionage behaviour. Spyware can exploit systems vulnerabilities and can be used by hackers to take advantage of computers. They act as a bot in a denial-of-service attack, which could be highly disruptive for both individual and corporate computer users and emphasise a need for educating the user as the first line of defence against this malicious software. However, it did not mention enough about what measures should be taken to create awareness among the users. Hence provide an opportunity to contribute to current research for user education and awareness against cyber threat.

2.3.3 Ransomware Threat and Notable Attacks

Ransomware is malicious software that secretly encrypts a user's data without obtaining permission from the user. It places barriers in the way of authorised access to user data. It prevents people from accessing their resources, which would be data [119]. A ransomware attack stands out from other types of malware since its effects cannot be undone. Once the data is encrypted, the only way to decode the user files is to utilise the key that was used to encrypt them in the first place. For the data to be decrypted, the attackers ask for payment in an anonymous form of currency, such as bitcoin [120]. The working procedure of the ransomware is shown **Figure 2.4**.

Figure 2.4: Ransomware Methodology [120]

The National Cyber Security Centre reported a rise in ransomware with evolving behaviour and increasingly sophisticated deployment methods. Ransomware has been found to be used as ransomware-as-a-service (RaaS)(NCSC, 2021)[9], which means criminals can pay a third party to deploy the ransomware on their behalf [121]. Ransomware can encrypt data and threaten to leak it online, increasing the risk for organisational that would have previously overcome attacks by storing backups and avoiding paying the ransom [15], (NCSC, 2021)[10]. Ransomware is identified as the U.K.'s most significant cyber security threat of 2021 [122], with amplification in the intensity and reach of the attacks (NCSC, 2021)[11]. Many sectors have been affected from January to November 2021, showing a 25% increase from the same period in 2020 [123]. The following are the most notable ransomware attacks in recent years.

- Examples of devastating ransomware strains include BlackMatter, which has been used to target U.S. critical infrastructure [124]. DarkSide RaaS targets critical infrastructure and uses phishing to gain initial network access before encrypting and stealing data [125].

- Norsk Hydro, the world's largest aluminium production company based in Norway was hit by ransomware LockerGoga in March 2019 [126], as a result of a phishing email opened by one of the employees [127]. The attack compromised 22,000 employees' computers working globally for the company and cost millions of pounds to recover from the breach [128].

- Another ransomware Conti has been increasingly used in over 400 attacks, including healthcare organisations. Conti is RaaS which obtains initial access to an organisation's networks through spear phishing, phone calls, stealing RDP credentials, malicious links, and downloadable software, among others. Which often take advantage of users lacking cyber security awareness [129]

- WannaCry: it is considered one of the deadliest ransomware to be developed [130]. This ransomware shut down multiple hospitals across the United Kingdom and Ukraine. The developers of Wannacry could detect the vulnerabilities

[9] https://www.ncsc.gov.uk/news/record-number-mitigated-incidents

[10] https://www.ncsc.gov.uk/blog-post/rise-of-ransomware

[11] https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat

of windows that were first discovered inside the United States National Security Agency. Symantec later suspected that the developers originated from a North Korean-linked group called Lazarus [131]. This ransomware is also one of the latest.

- Petya and NotPetya: launched after a week after the Wannacry outbreak. This ransomware is the confirmation of the new age of ransomware. Petya or NotPetya started with a tactic of sending a job application document via email in a pdf file format which is expected to be accessed by the company. NotPetya is the first ransomware that does not need spam emails or social engineering to infect and gain administrative access as long as there is a network connection between the devices [132].

  These are only a few examples of the multiple ransomware criminals use to extort money from organisations.

2.3.4 Humans as the Weakest Link

NIST cites ***people as the main facilitators of ransomware attacks***. End users were engaging in risky behaviour, administrators were configuring insecure systems, and developers were not educated in secure development practices [133]. CISA has identified spear phishing as a commonly used technique for gaining initial access to an information technology (I.T.) network. The attacker can pivot to an operational technology (O.T.) network [134]. Similarly, statistics show that the top four vulnerabilities allowing ransomware infections in 2020 were 'spam/phishing emails (54%) 'poor user practices' (27%), ***lack of cyber security training*** (26%), and weak passwords/access management (21%) [135]. Indeed, Sharma & Shanker (2022) indicated phishing which utilises social engineering, as the most common way to initiate an attack, and therefore people as the significant element in enabling ransomware attacks to occur [136]. Burita, *et al.* (2022) concluded from their research that to prevent phishing attacks, it was necessary to educate users on recognising the attack [137].

The COVID-19 pandemic in 2020 meant criminals could take advantage of an increase in homeworking and I.T. services moving the cloud in the UK (NCSC,

2021)[12]. Criminals carried out pandemic-themed social engineering attacks, E.g., a website purporting to track covid case numbers was also stealing users' Personally Identifiable Information (PII) [138]. Furthermore, the impact of COVID-19 on hospitals, governments and education made them more likely to pay ransoms to avoid further disruption to their systems [139]. The percentage of homeworkers in the U.K. doubled from 4.7 million to 9.9 million [140]. The percentage of attacks on homeworkers rose to 54% due to a lack of training on cyber security [110]. Georgiadou, *et al.* (2021) conducted research that discovered most homeworkers surveyed belonged to organisations that failed to provide security guidelines to their employees—indicating poor change management and security training procedures. They also found that 52% of devices used for accessing the company networks were homeworkers' own and not controlled by their I.T. department policies. At the same time, they were using unfamiliar cloud services and increasing their susceptibility to attack, with 1 in 5 homeworkers encountering a security threat (most of which were phishing attacks) [138]. This increase in home computer use and reliance on 'cloud' services has dispersed the traditional network perimeters of organisations, increasing their attack surface. Cyber-attacks on personal devices can enable attackers to access the company network to deploy sophisticated attacks, accessing company data or resources. They can also commandeer home worker's computers to attack other computers and networks [141]. Users do not view security as their primary focus when carrying out their day-to-day tasks and view safeguarding practices as complicated, inconvenient and a hindrance to their work. Leading users to perceive security compliance as a burden [142]).

Various governments across the globe recommend that organisations should educate their users, as this is fundamental to mitigating ransomware attacks. In the U.K., the National Cyber Security Centre (NCS) recommends educating users to prevent ransomware execution on devices (NCS, 2020)[13]. It has introduced the CyberFirst program, aimed at educating 11–17-year-olds in cyber security matters [143] and training school employees (NCSC, 2021)[14]. The Information Commissioner's Of-

[12] https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat

[13] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

[14] https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threat/ransomware-threat-methodology

fice (ICO) impresses the need for basic user awareness training in social engineering and phishing for data protection compliance regarding Ransomware [144]. The Australian Cyber Security Centre (ACSC) recommends training users on good security hygiene to mitigate ransomware attacks [145].

The U.S. government's Cyber Security and Infrastructure Security Agency (CISA) recommends training users to educate them on the dangers of visiting malicious websites [146] and the appropriate response to phishing emails [147]. The U.S. Department of Justice issued an inter-governmental report emphasising the relevance of training users on how attackers use social engineering techniques to attack networks (U.S. Department of Justice)[148]. NIST recommends training users regularly on policies and procedures. Plus, educating them on secure practices, such as using anti-virus software, only installing approved applications, and connecting to secure networks (NIST, 2022). Furthermore, the FBI's Internet Crime Complaint Centre (IC3) issued a joint advisory report from CISA, NSA, ACSC, and NCSC-UK recommending that users undergo awareness training on phishing and suspicious websites (IC3, 2021)[15].

Likewise, non-governmental bodies cite user awareness training as a prime mitigation step against ransomware. Mimecast stresses the importance of administering training that engages staff while gaining feedback and measuring success [149]. The Centre for Internet Security (CIS) suggests that training users to recognise malicious emails can limit the impact of ransomware by mitigating attacks [150]. KPMG recommends eLearning, which generally focuses on data protection, phishing, and cybercrime, tailoring the training to the user's role within the organisation [151]. The literature from these national cyber security centres of the U.K., U.S. and Australia identify ransomware as a global issue. However, current research focuses on ransomware challenges to the U.K. only.

Human Involvement in spreading ransomware is a key factor. Simple hard-coded software is useless. Ransomware could not spread and infect on its own. Human Involvement gives life to ransomware and the procedures of how ransomware infects devices. Humans create the ransomware software, and humans spread the virus. As previously stated, most acquisitions of ransomware are made due to a

[15] `https://www.ic3.gov/Media/News/2022/220209.pdf`

human falling for the spam email trick set by hackers. Social Engineering, which was previously discussed, also play a vital part since human use psychology to gain illegal motifs. Humans are also responsible for activating the malware since most ransomware activation happens when .exe files disguised as pdf or word files are executed. Cyber-criminals are also responsible for encrypting files inside the victim's device. Finally, once the trap is set, *Humans* are responsible for choosing whether to pay.

Human empowerment and information dissemination are key to knowing what ransomware is and how to fight the attacks. With proper education about the topic, humans can learn how to lessen at least these types of cyber-attacks using early-stage prevention. Finally, these preventions can only be done if the *Human* factor in the computing environment is willing enough to critically educate him or herself about the digital advancement of the different computing industries.

2.4 Game-Based Learning and User Awareness

One of the main objectives of this research is to use a game-based learning approach to design and develop a prototype, which can help users to educate and improve their understanding of the ransomware cyber security threat. The study showed that psychologist Jean Piaget's (1962) [152] cognitive development theory links the relationship between learning and playing techniques in human history back to thousands of years old strategy of learning. The evaluation of technologies and the advancement of user-friendly computers and smart devices has brought new opportunities for learning experiences through digital games [153]. The research [154] emphasises the need to consider game design elements as important factors to improve user motivation, which leads them to engage and educate. Therefore, the current research will focus on game-based learning and gamification to improve user awareness against Ransomware threat.

According to Association for UK Interactive Entertainment (UKIE, 2018), there are around 2.2 to 2.6 billion game audiences worldwide. It estimates that by the end of 2021, the demand for the game-based global software market will increase to nearly $138 billion. The ever-increased number of users' interest in the games and

improved I.T. structure has paved the way for educators and trainers to use games as an e-learning tool to educate users of any age on complex technical subjects. The research from [155] points out that motivation is an important factor in encouraging the learning process and considers game-based learning an effective way to make learning more fun for the learners as it enhances learners' engagement by allowing them to learn at their pace. However, the authors did not focus on any usability factors that can lead to improved user engagement and learning to achieve their education needs, hence providing an opportunity to consider the implementation of usability in the current thesis.

Games can be identified as a learning tool for many centuries and can be promoted as a skill development [156], e.g., Chess is used to improve strategic thinking. In contrast, Kriegsspiel can be seen as a popular war game developed by Persians in 1780 to improve military strategies for army officers. Game-based learning can also be adopted in curriculum development and innovative educational pedagogies and is acknowledged as an important education tool [157]. It emphasises the need for its adoption in modern educational curricula to improve learners' engagement, cognitive behaviour, and problem-solving skills. The main aim of the game-based learning technique is to act as a learning tool and "accomplishment of goals" [158], and this principle has been in common in both contexts, i.e. its historical usage and in modern education. Games are not one-size fits all solutions; their effectiveness relies on design objectives.

2.4.1 Educational Games for Ransomware

Much research has been done on ransomware, but not enough using games to educate people against ransomware attacks.

- Arachchilage & Hameed (2017) recognised the lack of cyber security-user-focused education and the insufficiency of phishing prevention tools. Recognising that the user is the 'weakest link' in cyber security, they set out to create a game focused on integrating self-efficacy into an educational game designed to prevent phishing attacks. They suggested increasing user knowledge by combining both conceptual and procedural to increase users' self-efficacy and change their behavioural response towards phishing. They believe that

good education games should enhance people's perception of threats and work with their behavioural drivers, teaching them how to respond rather than just warning them of threats. A limitation is that it is focused on identifying phishing URLs. Furthermore, the game design was proposed in the research, not implemented practically, or tested by game players to obtain feedback or research data resulting from the game's effect on players, their self-efficacy or their impact on cyber-security for the learner's organisation. They suggest that the government could implement the game, and future research includes new knowledge that security agencies and law enforcement could use to prevent crimes [159]. This motivates the current research to explore the opportunity to develop game-based learning for ransomware.

- Another previous study by Dion *et al.* [160] presented the conceptual framework for the gamification of ransomware education on the premise that negligent user actions can lead to successful cyber attacks. They also express the need for experienced programmers with secure development knowledge as an essential element for such a project. Plus, finding the balance between education and entertainment. Ensure it is not too complex or dull but not oversimplified to make it fun to play. In addition, to facilitate gameplay in poorer areas, the game could be compatible with less advanced technology. They also suggest that changes to the law of a region (in line with standards such as ISO/IEC 27001 and NIST CSF) could impact the adoption of educational training to comply with the law. The main limitation of this study was that the practical implementation of the game was not carried out. Instead, a prototype was presented [160]. Therefore, the current research will take this opportunity to develop a game to address ransomware awareness.

- Lika *et al.* [161] focused on teaching users about the NotPetya ransomware, which mainly targeted Ukraine in 2017- utilising the EternalBlue exploit, infecting computers initially through email attachments. They believed that the fix to prevent the ransomware from infecting computers was too complex for standard users. Implementing gamification would be necessary to educate users and a better way to prevent attacks. It created a storyline where the fix was referred to as a 'vaccine' that engaged the users while learning. The

game would also install the vaccine to NotPetya at the end of the gameplay. Lika *et al.* Conclude that the limitation of the study is that it is conceptual and practical implementation is lacking. So their suggestion for future work is for researchers to create and practically implement a similar game [161]. Also, this study does not mention how user experience can be embedded in the game design to improve user engagement. This motivates current research to explore usability in the proposed game design.

The review of the previous studies in this section informs that most of the research is done in the theoretical context with proposed future work of game implementation to tackle ransomware. Therefore current research will develop a game that engages the users with an entertaining storyline that will engage the player. A compelling storyline helps to set the context of the game and the challenges that the player will need to overcome during the game throughout the learning process [162].

2.4.2 Research Gap for Cyber Security Training

The need to be secure has never been felt so desperate before. Cyber security is rapidly evolving, and sophisticated threats are emerging daily. There is a dire need to create a culture of research and training to prepare professionals for future cyber security challenges. According to National Cyber Security Strategy 2016-2021 [163], the government aims to invest £1.9 billion in cyber security to make the U.K. secure and resilient against cyber threats. As a part of the national strategy, the government has introduced many training initiatives to create awareness among the public and businesses NCSC (2018).

With the opportunity to address cyber security training, research by [164] points out that the use of Serious Games with a purpose other than entertainment can be an effective tool to train users and cyber security professionals as it can make an impact on behavioural change through engagement. The study further concludes that using stories in game design can improve user engagement, which is achievable through an effective game design.

Chowdhury *et al.* [165] have noted that attacks are often successful due to human error- cognitive bias and lack of knowledge causing negligence or poor judgement.

However, organisations do provide cyber security training to employees to counteract this. However, the effectiveness of cyber security training has been questioned due to increased breaches. Criticisms have included lack of engagement, perceived time-cost, and unsuitability to individual's learning styles which is ineffective in influencing users' behaviour [165]. The effectiveness of security awareness training hinges on its delivery format, and simple but relevant game-based learning is an effective alternative to traditional linear training [166]. Game-based learning can effectively influence users' behaviour, incentivising them to carry out safeguarding activities, unlike traditional training, which fails to influence users' behaviour over time [142]. Most studies have found that game-based learning is more effective than traditional security training [167].

Table 2.1 shows a critical analysis of different related work of researchers, government and non-government organisations. All these studies support game-based learning as an effective awareness tool to improve user awareness. However, the discussion in the table shows the findings of these studies either suggest the conceptual frameworks without validation or lack practical implementation. To the best of the knowledge gained through the literature review. There was no fully functional game on ransomware threat. Therefore, the current thesis seizes this opportunity to address the gap in improving user awareness against malware using game-based learning. This novel game will be based on TTAT to improve user threat appraisal, coping appraisal and avoidance motivation behaviour, which will distinguish it from previous studies in terms of its theoretical model and design. The game Ransom*A*ware will target adult individual users and those in any organisational settings where cyber security training is a compliance.

Table 2.1: Related work & Research Gap

Related Work	**Year**	**Limitations and Research Gap**
Kuo-Chen Li *et al.* [155]	2010	The study is based on Motivation Driven Approach and suggests motivation as an important antecedent to drive user's motivation. However, the implementation of this game was to teach English only and required future work in cyber security domain to improve user motivation against malicious IT.
Fadi A. Aloul [109]	2012	Suggested a game as an effective training against phishing compared to traditional security training offered by organisations. However, this study does not provide any recommendations on the implementation of such a game.
Jemal Abawajy [166]	2014	The study emphasizes the need to review traditional security awareness training and recommends game-based learning as an effective and engaging solution to improve user awareness. However, the study does not provide any practical implementation guidelines.
La *et al.* [168]	2016	Proposed a theoretical game model for honeypot-enabled networks to defend against attackers. However, the work lacks implementation, and the discussion is only related to user motivation to deter such attacks.
Nader *et al.* [95]	2016	Discusses Social Bond Theory, which focuses more on the user's attitude towards compliance. However, the study does not address users' perceived threat and avoidance behaviour.

Abass *et al.* [169]	2017	Developed a game for Advanced Persistent Threats against cloud storage devices. However, this was just to analyse the behaviour of the attacks, not to create learning and awareness against these threats for end users.
Sedjelmaci *et al.* [170]	2017	The study proposed a game to detect anomalies in low-powered devices. The implementation of the game was in the form of a simulation to show the accuracy of the model for the network administrators rather than a learning tool for users.
Dion *et al.* [160]	2017	It was a conceptual framework to gamify ransomware learning. However, the limitation of this study was practical implementation due to a lack of knowledge of secure development.
Lei Cui *et al.* [73]	2018	Propose a game theory to be adopted for security and privacy issues in IoT-based applications. However, this was just a conceptualization. There was no practical implementation to address the security challenges.
Stamatios Papadakis [153]	2018	The study recommends a game development framework based on Self-determined theory to improve user motivation. However, the work lacks practical implementation and validation.
Lika *et al.* [161]	2018	The study recommends gamification to educate against ransomware. However, the full practical implementation is lacking and restricted to only a pop-up message.

NCSC, DMARC [171]	2018	This tool is made available to the public by National Cyber Security Centre UK to prevent untrusted emails. However, this is more of a technical solution to be implemented rather than an awareness or educational tool.
Yelena Petrykina *et al.* [142]	2021	The findings of this study report that security awareness training can be a burden for the user due to its complexity and recommends a usable gamified user awareness technique to improve the user's motivation against the threat. A security robot as a malware tool was introduced. However, this study has a number of limitations in terms of design and the game's theoretical model and requires future work to validate this idea.
Karzan & Siddeeq [167]	2021	The study provides a comparison of different security awareness formats, and its findings report that game-based learning is the most significant method to improve user motivation. However, these findings were more in the context of user motivation and were not applied to assess malicious IT behaviour.
Chowdhury *et al.* [165]	2022	The study recommends the adoption of game-based learning as a replacement for traditional security training to improve user engagement. However, the study does not propose any theoretical or practical implementation of the game design.

NCSC, Cyber Sprinters [172]	2023	National Cyber Security Centre UK has introduced a Cyber Sprinters initiative to improve cyber security awareness among children using game-based learning. However, this game aims to provide a very basic knowledge of cyber security. Its implementation lacks threat appraisal and coping appraisal against malicious IT. There is more opportunity to implement awareness of threat actors in this game. Also, this game does not provide awareness of the rising threat of ransomware.
Cyber Security Challenge UK [173]	2023	A non-government organisation, in a joint venture with National Crime Agency, UK, developed a simulation to introduce malware. However, this idea lacks full implementation and does not demonstrate the attack vector adopted by the attacker. Nor does it provide any awareness of how to stop such attack.

2.4.3 Mobile Game-Based Learning

The term "ubiquitous computing" was introduced in 1995 [174]. The power of computers has been transformed enormously and embedded into everyday smart objects such as smartphones, tablets, and wearable technologies [175]. The term ubiquity is also interchanged with the concept of the Internet of Things, 'Pervasive computing' or 'Invisible computing', but the whole idea is that these smart devices should have the capability to seamlessly interconnect and provide mobile support to users anytime and anywhere through information services. The research by [176] concludes that in an educational environment, trainers can benefit from the ubiquitous power of smart devices and can use mobile game-based learning as a tool in their curriculum design to introduce active learning. This can help learners to engage, motivate and reinforce their learning.

The motivation of this research thesis is to focus on game design prototypes for smartphones. This is mainly because of the fact [177] that smartphones have proliferated into our digital lives by using them for making phone calls, browsing, online banking, navigation, etc. In addition, young people carry more smartphones today than ever before. However, the author has not highlighted smartphones' size and processing limitations. Therefore, it is an opportunity to address this gap in the research thesis through a usable design which can run seamlessly and improve the learner experience.

According to market research and business intelligence portal Statista, global mobile traffic has been rising since 2015 and contributed 58.99% of the web traffic as of the second quarter of 2022 [178]. This means more and more people are using smartphones. The Office of National Statistics [179] release shows that 92% of the households in the U.K. have internet access and that smartphones are the most popular gadgets to connect online.

Mobile Applications & Blended Learning: Since the launch of Apple's iPhone in 2007 and the Android smartphone in late 2008, the global market of smartphones has grown heterogeneously [180]. Nowadays, smartphones contribute 84% of the overall global mobile phone sale. Android and iOS are the global leader in smartphone operating systems and has the largest app store [181]. Statista [182] reports there are 2.68 million free/premium apps available on the Google Play store from

2008 until September 2022, compared to Apple's 2.1 million apps. In contrast, the combined apps download of both apps' distribution platform was 50 billion until mid of December 2018, among which the most popular downloaded category are the Games. Based on the statistics about current growth and future trends of smartphones and apps, the research thesis seizes this opportunity to design a mobile game-based prototype to enhance user awareness against the ransomware threat.

Game-based learning is also seen as one of the elements of blended learning, which educators can adopt to flip the classroom to offer more active learning to students [183]. Higher education is embracing online learning in its curriculum design along with face-to-face delivery [184]. This allows learning in a wider context and opens learning opportunities for learners of all ages with better control over time and learning pace [185].

2.5 Summary

In this chapter, preliminary studies review existing literature on cyber security threats, cyber-physical systems, ransomware, and game-based learning, which was critically important to understand the challenging relationship between cyber technology and end users. Studies also explore the understanding of the most common attack vector that contributes to the lack of user awareness of the "Ransomware" threat, which was important to support the research question and objectives in the current research thesis. The literature review informs that previous research focused on implementing physical controls as a countermeasure to protect users against cyber-attacks and safeguard their confidentiality, integrity, and availability. However, preliminary studies identify the user as the weakest link and provide a way forward to improve user awareness against ransomware cyber security threat, which can be beneficial to prevent cyber-attacks. This research has been identified as a research gap as there is not enough research available on understanding user behaviour and the use of game-based learning in the field of Cyber Security to prevent cyber-attacks. This provides an opportunity to address this gap. Therefore, the researcher will contribute knowledge to develop a usable game-based learning prototype to enhance user education and awareness against cyber-threat ransomware.

Chapter 3

Research Methodology

3.1 Overview

This chapter provides details and justification of the research design and methodology followed in the current research to design and develop a game prototype to improve user awareness against the ransomware cyber security threat. It provides a further discussion of research paradigms and the justification of the research design process. It specifies the research philosophy, approach, methodologies and strategies adopted for data collection, analysis and interpretation during the study. This chapter also includes ethical issues implied by the current study. This chapter further introduced the inclusion of user-centred game development methodology, which is unique and will contribute to methodology in current research.

3.2 Research Design Process

The research design is more than a plan to answer the research question before data collection and analysis are performed; therefore, methodological coherence is critically important to consider during the research design process [186]. The research design does not guide the selection of any particular data collection methods or research approaches. However, it will be dependent on the research purpose. **Figure 3.1** shows the steps involve in the current research design process.

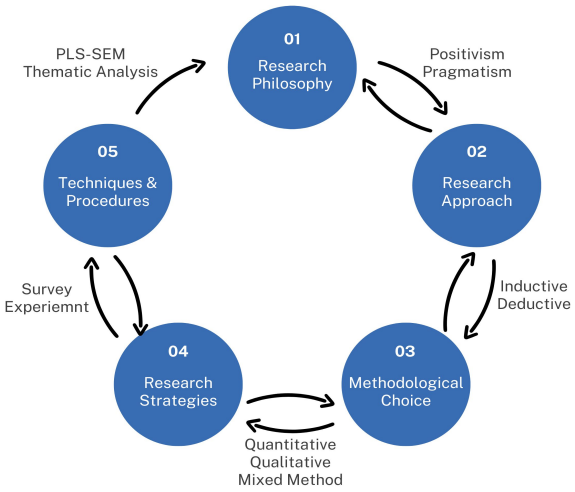

Figure 3.1: Research Design Process

3.3 Chosen Research Philosophies for The Current Thesis

A research paradigm is a set of philosophical assumptions [187] consisting of four components, i.e., ontology, epistemology, methodology and axiology, chosen by researchers that fit their research purpose [188]. Research philosophy is an assumption made by a researcher about the world, which underpins research strategy and data collection methods [189], as it can influence the research design; therefore, appropriate considerations are required for selecting research philosophy to produce quality research. Research philosophy is shown as the first step in **Figure 3.1**, as it creates researchers' beliefs methodically and serves as a stepping stone for later research phases.

Many research philosophies are popular in business and Information Systems studies [190]. However, [191] in his studies highlights that due to the broader domain of Information sciences, it is always beneficial to consider philosophical and theoretical issues related to chosen philosophy. To evaluate the suitability of the chosen research philosophies to answer the research question in the current thesis. **Table 3.1** discusses the strengths and limitations of the most common philosophies in the Information Systems Research context.

Table 3.1: Research Paradigms

Fundamental Beliefs	Research Philosophies or Paradigms			
	Positivism	Interpretivism	Pragmatism	Realism
Ontology	A researcher is independent of the studies and focuses on gaining factual knowledge. The research is based on objective criteria.	It is the opposite of positivism. The nature of reality is socially constructed and requires researcher input. This kind of research is based on subjective reality.	Reality can be objective and subjective—multiple views considered by research to interpret the reality of undertaking research (Goldkuhl, 2012).	The reality is objective. Knowledge is constructed through scientific assumptions and is independent of human beliefs and thoughts.
Epistemology	Research focuses on generalisation and views knowledge validity independent of its values and the researcher.	The researcher's view regarding knowledge construction is social and subjective.	Good knowledge can be a source of subjective and observable phenomena.	Knowledge credibility is seen as a source of observable phenomena.
Methodology	Quantitative research is adopted through structured surveys and interviews. The data is analysed through numeric and statistical techniques (Edirisingha, 2012).	Its nature is interpretive for subject understanding. Qualitative research is conducted through participants' observation, In-depth interviews and focus groups (Edirisingha, 2012).	It combines Positivism and Interpretivism and includes quantitative and qualitative research techniques (Morgan, 2014).	Historical analysis of pre-existing data, Reproductive Methodology and ethnographic studies.
Axiology	Research is value-free, and reality is objective.	Research is value bound. A small sampling is used from existing data is used for investigation.	The research considered both objective and subjective views to interpret results from values.	Research is value-laden, and reality is subjective.

3.4 Justification of The Chosen Approach

Research is an activity which helps to understand the behaviour of entities (also called phenomena) of the researcher's interest. These activities are methods or techniques used to create or understand knowledge. Hence researcher's choice of methods needs to be appropriate [192]. In order to make an informed decision regarding the justification of chosen research design for the current thesis, the author examines the context of different Information Systems paradigms shown in **Table 3.1** and discusses the nature of studies in the current thesis. There will be mainly two studies in current research.

- The *first study* reviewed TTAT [193] to understand the factors influencing individual users related to IT threat avoidance behaviour. TTAT model is adopted, and the hypotheses derived from this theory are used as a baseline to design a questionnaire for users' understanding of the perceived cyber security Ransomware threat. This empirical study identifies critical components required to include in the proposed Game mobile prototype for users' education. The gameplay approach is considered on the boundary of traditional and new research approaches as it projects more factual knowledge of the scenario. Therefore, study 1 will adopt the positivist approach, a more acceptable approach for current research [194].

- The *second study* empirically evaluates and validates the proposed Game design prototype and presents its findings. This study involves an experiment asking the participants to play a mobile game prototype for education and awareness against Ransomware cyber security threat. The respondents completed a pre & post-experiment questionnaire to evaluate the effectiveness of the mobile game prototype in enhancing users' motivation for learning Ransomware threat.

  Although the research assumptions inform the methodological choice, the essence of the research methodology depends on the research question. The authors' [195] arguments further rely on the question that research methodology is not just about collecting and interpreting data. It also explores theoretical perspectives of research [196]. Therefore, the researcher's justification of cho-

sen methodology is vital for translucent research design. In the current thesis, there were two options to opt for the research approach, i.e., (i) either through learning from an individual experience (by the researcher) or (ii) through a hypothesis (by someone). The empirical studies and perceived reality are part of the studies as this will help the researcher discover the reality. The studies in the current thesis are based on ontology belief to learn the existence of reality and therefore use positivism research philosophy to answer the research question [197].

The current thesis follows a three-step approach to find a solution to the problem of creating knowledge and awareness for the user against the Ransomware threat. The research will diagnose the problem in practice by adopting a framework. Design artefacts for designing a usable prototype, and then will develop a prototype for testing and validating the effectiveness of its implementation. The implementation results are essential in Information Systems research, which will be interpreted to add value to research further. Also, it is essential to mention that methodological choice [198] is critical for the research design process. It helps to draw a journey from start to end. However, it does not handle any particular situation or required tasks to reach the destination. Therefore, the chosen methodology should help achieve the research goal in a logical order [195].

Methods and techniques are also known as 'acting instructions', they include more explicit detailed steps to be carried out during the research and act as a tool for the researcher's guide to categorise and analyse the research data [195]. Once the research methodology is determined for the current research, it determines the suitability of data collection techniques through action or thinking techniques, which can be used to collect either already existing or new statistical data or qualitative data to answer the research question. Data collection techniques aim to generate, classify and analyse data. Therefore the selection of appropriate data classification techniques in the current thesis will depend on the meaning of the data extracted for the first and second studies. In the proceeding section, three possible research methodologies, i.e. Qualitative, Quantitative and Mixed research, will be examined before concluding the ones appropriate in the information systems research domain and also fit well for the research question in this thesis.

3.5 Choosing a Methodology for This Thesis

Research methodologies are classified according to their nature, among which quantitative and qualitative are the most popular approaches. The way quantitative research methods differentiate from qualitative is that it deals with structured data, which can be analysed for statistical analysis [199].

3.5.1 Quantitative Methodology

The research which adopts ***Quantitative*** methods can measure behaviours and trends of the sampling data but is limited to observed behaviour, which is more meaningful when measured using qualitative methods [200]. Data collected through the Quantitative method is quantified and aim at an objective, i.e., based on hard facts rather than a personal opinion [201]. In the current thesis, the goal of Study 1 is to empirically evaluate the elements of TTAT to include in the game design [202]. To determine the effect of exogenous variables on endogenous quantitative methodology is chosen to examine the relationship between different variables [203].

The purpose of the research approach is to find information from the collected data; therefore, the data collection and analysis process is supposed to be systematic and requires an appropriate selection of research approach to achieve the research aim [204]. The research methodology, if chosen correctly, embraces methods and processes that help address the research problem [205]. However, data collection through quantitative methods sometimes can take longer than the usual time scale to reach a large group. The current thesis will address this limitation using the online data collection method. Also, understanding target stakeholders is essential for meaningful data interpretation, which will be carefully considered while selecting appropriate research methods for this thesis.

The current thesis's *first study* will use a questionnaire survey strategy to collect quantitative data and test the hypothesis. However, to avoid single factor accounting for the majority of the covariance among the items, a statistical test, Harman's single-factor test, will measure common method bias [206]. Quantitative approaches interest positivist researchers due to being associated with objectivity [207]. During the *study 1* of the current research, the focus on collecting and analysing the data

will be to test the adopted theory of TTAT. Therefore quantitative research will use a deductive approach using a questionnaire survey [208]. The first study aims at investigating the key elements to be included in mobile game prototype to enhance user education and awareness against the cyber security threat. The positivist approach seems more relevant to answer the research question.

3.5.2 Qualitative Methodology

Qualitative research differentiates from quantitative from the perspective of studying social and cultural phenomena by the researcher in social sciences [209]. Qualitative research allows data collection through observations, fieldwork, experience and people's behaviours. As the data collection is non-numeric, it usually includes narrations, words and phrases, which allows the researcher to interpret them and find a solution to a problem in social, cultural and real-world situations [205], which might not be possible using numeric data in quantitative research [210].

Qualitative research is described as empirical research without numeric data [211]. Qualitative research, in contrast to quantitative research, is associated with subjectivity which interests interpretive researchers. Study 1, validates the objectivity in current research using statistical tests, which verify and validates the convergence of items and the hypotheses [203]. However, to validate the presence of TTAT elements through subjectivity, Qualitative analysis was performed in Study 2, to improve the credibility of the results [212]. The second study in the current thesis will aim to test a game prototype. Researchers use field or laboratory-based experiments, such as; semi-structured interviews, reading existing documentation, and thinking-aloud approaches for observations to collect qualitative data from actual participants based on the Interpretivism philosophy [207]. Qualitative data evaluation helps to understand the subject and social context of the phenomenon (game prototype) and tends to use an inductive approach and could have been an option to test the effectiveness of the elements of TTAT in game design [205]. Research using a qualitative approach can sometimes take longer due to the scope of the studies to understand the phenomenon and the hypothesis. However, as study 2 requires empirical evaluation of the game prototype, the qualitative analysis seems fitting for this purpose [213].

3.5.3 Multiple Methods of Research

Multiple methods research design can be classified into mixed methods research and Multimethod [214]. Mixed methods research design is a relatively new idea in information systems research. However, its roots can be found decades ago, when it was first used for physiological traits study [215]. Mixed method research design integrates qualitative and quantitative research methods [216]. It considers two philosophies, as the critical realists believe in the assumption that social conditions impact external objectivity [217]. Researchers typically use quantitative methods to investigate existing data and mix and match it with qualitative methods to probe further understanding of the data. This helps them to avoid any limitations associated with mono-method research. It also makes it more suitable to satisfy ontological and epistemological beliefs [218]. This type of research design can entail either an inductive and deductive approach together or one of them. However, this decision depends on the nature of the research question to solve the problem [219].

There are various ways through which mixed methods research can be carried out, using the logic of triangulation to improve the value of research findings using two different collection methods to understand the phenomena of study in more depth [220]. Mixed method research design is also seen as an approach to avoid biases from qualitative data, it allows the convergence of quantitative and qualitative data to analyse and evaluate any contradictory findings, but it can lead to repeating the whole process. It can result in a phenomenal increase in time usage to repeat the process until desired results are achieved [215]. When used in the explanatory sequential mixed model, mixed method research design can allow qualitative data output into quantitative data. However, the whole research process can be daunting due to the unequal size of the sample and the further investigation of quantitative data.

Mixed-method research uses a pragmatic philosophical assumption that diverse data can lead to a more robust understanding of the problem [221]. Inquiry strategies are usually concurrent and sequential and adopt open-ended and close-ended questions as data collection methods. Data findings are mixed at different stages of data analysis and evaluation [221]. Due to the scope of the mixed-method ap-

proach, Study two of the current thesis adopts a mixed-method approach as; (i) In phase 1, the quantitative analysis assesses the usability of the game design prototype. Initially "Thinking-aloud" usability test was considered for testing the user experience of the game design. Usability experts recommend a "Thinking-aloud" qualitative test to understand the user's cognitive behaviour related to design [222]. This test requires setting up a lab to record user responses to the design in a live environment [223]. However, as the data was collected for the current research during the COVID-19 pandemic, complying with UK government regulations of social distancing restrictions onsite live tests were impossible (Office, 2020)[1]. Therefore, the author decided to adopt the System Usability Scale (SUS) questionnaire [224] to assess subjective satisfaction with the Ransom*A*ware game design. SUS is another popular quantitative approach recommended in the field of usability [225]. Then statistical analysis using SPSS was performed to measure the game's effectiveness to evaluate the extent to which the game has helped users improve awareness against the ransomware cyber security threat, whereas (ii) In phase 2, the study selected a qualitative approach to evaluate elements of TTAT embedded in game design empirically. The data was collected through semi-structured interviews, a technique used to evaluate the subjective satisfaction of TTAT elements empirically.

3.6 Research Strategy & Data Collection Techniques

Data gathering is a critical phase for any research since, for every research question, a researcher intends to procure a valid data collection approach to answer the questions [226]. With many researchers using data collection as part of the study, researchers devised two techniques: Primary and Secondary Data Collection.

The *Primary data* collection technique includes collecting first-hand or raw data and is transformed into cohesive information relating to the Research [227], [228]. The current research aims to improve user awareness against a cyber security threat

[1]https://www.gov.uk/government/publications/full-guidance-on-staying-at-home-and-away-from-others

using game-based learning, a relatively new phenomenon it relies on ontology belief. Therefore primary data collection was the preferred choice for the purpose. Primary data are gathered for multiple reasons, and these reasons include the following:

- Answer a peculiar or distinctive research question
- A solution to a particular problem or hypothesis
- Validation or Negation of a Theory

Primary data collection should be systematically and purposely defined in the research objectives by identifying the population and other sources from which data will be acquired and the necessary steps for data collection [227]. Study one of the current research is based on the TTAT model and aims to validate its elements empirically. The research thesis employs a quantitative research method and uses a questionnaire for data collection. Questions are based on understanding the Technology Threat Avoidance Theory (TTAT) adoption model to assess which elements to include in the game prototype. A pilot and the main studies were conducted using a questionnaire for data collection. The purpose of the pilot study was to test the hypothesis at the preliminary phase and save time and effort to avoid any unforeseen problems before it can be implemented in the main studies more precisely or to review the need to add a new hypothesis or drop an existing one [229].

A questionnaire is an effective tool for data collection [230]. Data collected through questionnaires can be quantitative or qualitative. However, it depends on the nature of the questions included in the survey questionnaire, e.g. if questions are open-ended, that encompasses qualitative analysis techniques. In contrast, close-ended questions will entail quantitative analysis for interpretations. The main study questionnaire was designed to assess respondents' perception of the likely harm a Ransomware cyber-attack can cause them. This questionnaire includes constructs of Technology Threat Avoidance Theory (TTAT), which is a proven theory that explains individual user behaviour, which leads to avoidance motivation against the threat [141]. Likert style questionnaire is adopted using a scale from 1-5, with scale 1 being "Strongly Disagree" and scale 5 as "Strongly Agree". The questionnaire was published online for respondents to collect their responses. The focus of the First

Study will include a questionnaire based on the Likert scale, which helps measure the opinions, beliefs and attitudes of the respondents/individuals [231] and yields reliable data for the researcher for effectively accurate measuring of statistical data.

Secondary data collection involves collecting, identifying and interpreting data primarily gathered by another researcher, organisation or research conducting body [228]. These data were collected in the past and are mainly not intended for the same research paper on which the researcher is currently focusing [227]. Although published data relevant to the researcher's study could be considered secondary, there are a few trusted secondary data sources, such as government publications, technical and trade journals and business reports. However, considering data suitability and adequacy are essential factors in answering a research question [201]. Therefore author decided to collect primary data for current research. Furthermore, the current research required subjective satisfaction with the game design. Therefore, primary data collection was a more suitable choice for this thesis.

3.7 Game Development Methodology Challenge

The current research aims to develop a usable game prototype to create awareness against the ransomware cyber security threat. This process involves carefully considering the design and development procedures to adopt so the game can meet its intended outcomes. Agile is one of the development methodologies which has been in use in software development processes due to its ability to focus more on product development [232]. It has also recently emerged as a popular methodology for developing commercial games as it offers flexibility to accept requirements changes for quick product delivery [233]. Although [234] suggests, agile has evolved to address the human and social aspects of emerging technologies and address the usability of the product design. However, this requires rigorous interaction with stakeholders to achieve this goal. Whereas [235] suggests that agile methodology can also be beneficial in the modelling aspect of the game. However, it requires more adoption in game development yet.

In contrast, the Waterfall is a sequential methodology [236] and is suitable for

those development projects for which requirements are clear before the development proceeds. The current research empirically validates elements of TTAT to include in the game design during study 1, intending to improve user avoidance motivation against the ransomware cyber security threat, which sets the requirements clearly to develop a game for the current research. Therefore waterfall methodology seems to be more suitable for the current game design. However, [237], in his philosophical viewpoint of the waterfall methodology, suggests there is not one methodology that can meet the game design requirement in the context of game development engineering and human interaction design. Emphasise the need for a hybrid methodology.

The current research also aims to implement usability during game development to produce a user-centred design. Previous researches focus more on theoretical knowledge [141] or the design methodology to improve aesthetics [238]. However, [239] argues that a user-centred design is a process which is more than aesthetics. He presents a methodology based on five layered models to implement UI/UX for digital products such as contemporary web applications.

As suggested by [237], no one methodology is fit for all to support the development and usability of the product design. Therefore in the current research, the author has decided to choose a hybrid methodology based on (i) Waterfall, which can support the game development process from the developer context and (ii) James Garrett's design methodology for the user-centred design to focus on user experience. However, the challenge was that the elements of User Experience [239] methodology focus more on web applications' usability and has tested beyond the web design. In the current research, this methodology is revisited and adapted for the game design. The current thesis proposed a unified methodology called UXD based on the amalgamation of Waterfall and some elements of James Garrett's user experience. The design and development of game design and development in the current research design will follow this model to deliver an efficient and robust design.

3.8 Data Collection and Analysis

The current research involves primary data collection to answer the research question. The research implied two studies in the research design process to collect data. A questionnaire was designed using a Likert-style scale of 1 to 5 based on the proven theoretical model of TTAT to carry out Study 1. The research adopted a quantitative data analysis approach to the data collected through a questionnaire using PLS-SEM [240]. However, before proceeding with data collection, it was critically important to carry out the measurement validation. Therefore Cronbach's alpha and Composite reliability tests will be performed to ensure items are closely related as a group [241]. The current research adopted SmartPLS software, and descriptive statistics was run to assess the item's internal consistency [242]. The model validation was conducted based on [203]. The multicollinearity test was run to avoid data biases [243]. To ensure all constructs have sufficient discriminant validity, cross-loadings of items will be examined to ensure they have a higher correlation in their own construct [203]. The findings of Study 1 are reported in Chapter 4.

Study 2 implied a mixed-method approach. First quantitative analysis was adopted to evaluate the game design's usability empirically. This phase required the practical involvement of the respondents to play the game. After playing the game, the respondents were asked to participate in the System Usability Scale (SUS) test [225]. The data collected through SUS was quantitatively analysed, and the results significantly confirmed user satisfaction with game usability. Pre & post-test questionnaires then followed this to assess the effectiveness of the game design for its intended audience. The quantitative analysis of these results reports significant results confirming subjective satisfaction with the game, i.e., the game helped users to improve their awareness against the ransomware cyber security threat.

Secondly, qualitative analysis was adopted to validate the elements of TTAT in game design empirically. The respondents who participated in the gameplay were invited to provide feedback on elements of TTAT embedded in game design. Study 2 implied the semi-structured interview technique due to its usefulness in understanding users' perspectives [244], [245]. The study aims to get user feedback on TTAT elements implemented in the game; therefore, the semi-structured interview

was considered suitable for current studies. Data collected through the interviews were qualitatively analysed using thematic analysis. This technique was found suitable for current studies to identify themes related to TTAT elements [212]. Nvivo, a qualitative analysis tool, was adopted to generate themes from the interview data [246]. The findings were consistent with elements of TTAT, and the results of this study are reported in Chapter 4.

3.9 Research Ethics in The Current Thesis

The current research involves data collection from human participants using a questionnaire and semi-structured interviews. Like any other research, [51] considers ethics an important component of the research design process. The current research does not intend to collect any personal information related to the individual and ensure data anonymity (ICO, 2021)[2]. There is no physical interaction with any individual. All respondents are within the age range of 18-55 and do not include any vulnerable participants. The current research has been granted ethical approval from the research and ethics committee to adhere to Brunel University research ethics regulations. This research aims to promote knowledge and truthfulness and ensure to avoidance of errors (Integrity) during data collection and evaluation to maximise data accuracy. The research will also aim to utilise collected data only for its intended purpose (Privacy) and will not expose (Confidentiality) it for any purpose other than the purpose of the research question.

3.10 Summary

Research methodology is critically important for any research and requires the researcher to have a rigorous understanding of the research design process to answer the research question. Therefore, the appropriate selection of philosophical stance, research approach, research strategy and technique required careful consideration. In this chapter, different research philosophies and beliefs are critically appraised,

[2]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

and their strengths and weakness are discussed to justify chosen philosophy to answer the research question of this thesis. The studies in the current thesis are based on ontology belief to learn the existence of reality and use positivism research philosophy to answer the research question.

The research approaches are discussed in detail to choose the one which fits well to find information from the collected data. The deductive approach has been selected as the current research focuses on collecting and analysing data to be tested via the adopted TTAT theory. This chapter critically discussed different research methods, i.e., Quantitative, Qualitative and mixed methods. *Study 1* employed quantitative research methods to empirically validate which elements of TTAT to include in the game design. In *Study 2*, the quantitative analysis method also empirically validates usability and game effectiveness. Therefore SPSS and SEM-PLS have been chosen as data analysis tools for statistical analysis. Whereas thematic analysis is performed using qualitative data gathered through semi-structured interviews. Lastly, this chapter also discussed the importance of research ethics and how it will be considered to achieve truthfulness, confidentiality, integrity and privacy in current research.

Chapter 4

Data Collection and Analysis

4.1 Overview

This chapter reports on the findings and analysis of *Study 1*. The Technology Threat Avoidance Theory (TTAT) is examined to understand the factors influencing individual users related to IT threat avoidance behaviour. It is used as a baseline to design a questionnaire for users' understanding of the perceived threat. This empirical study is used to identify critical components required to include in the game for users' education against ransomware. A pilot study is conducted first before the main study. The results are critically evaluated before a conclusion is drawn.

4.2 Theoretical Foundation

According to the Cyber Risk Management (CyRiM) report, global ransomware attacks could cost businesses almost 200bn [247]. This report highlights the exponentially growing contagious cyber security threat ransomware to ICT and its severe threat to the global economy. Businesses' dependency on technology is rapidly growing to automate and improve business operations and compete in the global market, which means its users are more vulnerable to cyber threats than ever [247]. Therefore, it is critically essential for technology to serve its moral purpose. If compromised by the malicious threat, this could jeopardise IT and users, by compromising their privacy, confidentiality, and availability. Ransomware generally compromises

users' security via emails. It requires user action to execute before it encrypts users' files, takes the computer hostage and demands to pay ransom in return for decrypting their data [248]. The report further emphasises the need to develop an effective response strategy as an essential part of business operations. So the strategy could improve their cyber defence against this malicious software and avoid any business interruption due to unavailability caused by this cyber threat which could seriously impact business continuity. The UK National Cyber Strategy 2022 has set out a plan to support the growth of the cyber security sector [249], emphasises the need for cyber resilience and recommends spending on user education as an effective cyber-defence tool.

In this thesis, to design a prototype which can enhance users' motivation through education and awareness against the cyber security threat ransomware, a theoretical model is adopted from a proven Technology Threat Avoidance Theory (TTAT). The purpose of TTAT is to understand the behaviour of individual users to avoid any malicious IT threat [141]. However, this is imperative to understand that threat avoidance and threat adoption are qualitatively two different phenomena [250]. Therefore in this thesis, we will first distinguish the difference between these two concepts and then elaborate TTAT more to see how it can be effectively used to determine the impact of IT threat avoidance behaviour of the user. TTAT is depicted from the Cybernetic theory framework [251] and coping theory to deal effectively with IT threats. It helps to understand two cognitive processes of users, i.e., 'Threat Appraisal' when users acknowledge the presence of an IT threat and are conscious of its malicious consequences [252]. This process of acquiring knowledge and apprehension through thinking further leads to another cognitive process of 'Coping Appraisal', which makes the user believe in his ability to succeed against his IT threat perception by taking appropriate preventive measures to avoid malicious threats [141]. TTAT basis on the argument that the user's motivation can lead to avoiding malicious IT if he is conscious of the threat and believes in avoiding it using appropriate measures. If such measures are not believed to be adequate to avoid threats, it can lead the user to Emotion-Focused Coping [141]. Therefore TTAT theory will be adopted in this research thesis to understand human behaviour in coping with ransomware cyber security threat and will make informed choices for contribution

to improved used education and awareness against malicious threats.

To safeguard against cyber threats, only users' adoption behaviour, i.e., implementation of physical controls such as firewalls, intrusion detection and Intrusion prevention systems and antiviruses, will not be a robust solution to address this issue. The user would also need to demonstrate avoidance behaviour [253]. The combination of both user avoidance and adoption behaviour can lead to the practice of a practical security approach for safeguarding against malicious threats. The current research adopts the TTAT model to depict IT users' threat avoidance and adoption behaviour in the context of ransomware cyber security threat [141]. This is achieved by considering the user's perspective of the IT threats, i.e. if the user does not perceive Ransomware malware as a threat. The user may not choose to opt for adoption behaviour by not considering the need for any physical control to tackle this malicious IT threat. This understanding of human behaviour perception will lead to the design of a prototype which will improve user motivation and awareness against malicious cyber threats.

4.3 Research Model and Hypotheses Development

The research model shown in **Figure 4.1** is adopted from the (Liang & Xue, 2010) TTAT variance model and hypothesises that it is the Avoidance Motivation that determines users' Avoidance Behaviour against cyber security threat ransomware. Moreover, avoidance motivation is affected by a perceived threat, i.e., the extent to which users view ransomware as a threat. Furthermore, the perceived threat is influenced by two antecedents, i.e., perceived severity (the degree of damage caused by the ransomware threat) and perceived susceptibility (the subject's belief of likely harm by the ransomware threat) and the interaction of both elements. According to the [141] model, the user's Avoidance motivation against the ransomware is also positively determined by the following constructs, i.e., Safeguard-effectiveness, and Self-Efficacy and negatively mediated by the interaction of Safeguard effectiveness and Perceived Threat.

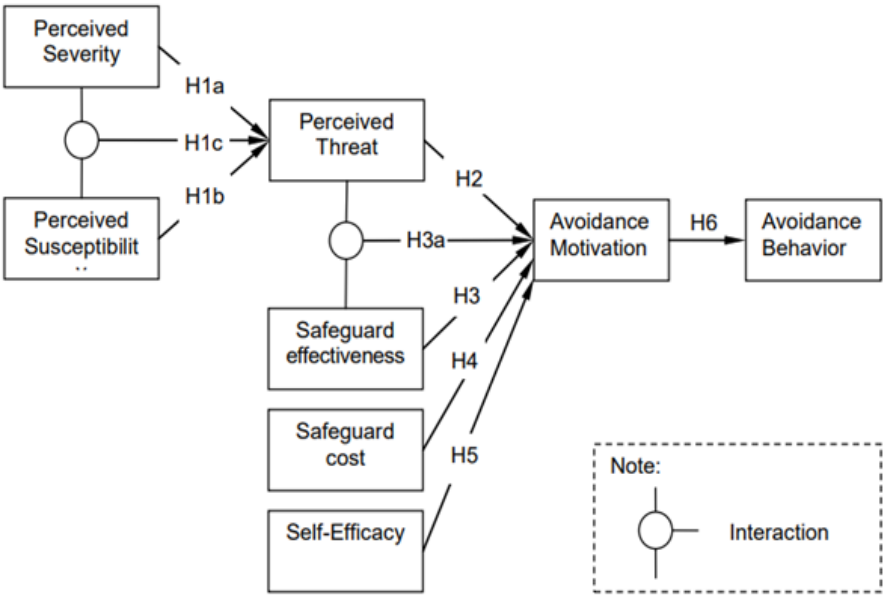

Figure 4.1: Research Model [141]

- Following the [141] TTAT model, perceived severity contributes to the user's threat perception. It is defined as the degree of the user's perception of negative consequences caused by the threat. In contrast, perceived susceptibility is proposed as a subjective belief of being negatively harmed by the malware threat, which can contribute to the user's threat perception. Previous studies in the field of health psychology conducted by [254] and [250] posit that an individual's motivation to prevent illness will increase with higher perceived susceptibility and severity. In the context of IT security, this idea is supported by [255]. The current research aims to improve user awareness against the cyber security threat of ransomware using game-based learning. Users will encounter malicious/non-malicious emails shown by planets and bear the consequences of their selections based on their actions. The wrong decision-making can encrypt users' spaceships, further losing points or lifelines. This process will teach users the perceived susceptibility of being attacked and likely harmed by Ransomware cyber security threat, which will positively affect threat perception. Based on the above argument, hypotheses H1a and H1b are adapted from TTAT [141].

  ***H1a**: Perceived severity of being attacked by ransomware positively affects perceived threat.*

***H1b**: Perceived susceptibility of being attacked by ransomware positively affects perceived threat.*

- TTAT model views threat perception as an interaction of perceived susceptibility and severity. The threat is conceptually considered a risk [256]. Its level in information security is determined by its likelihood and severity, which means the combined effect of perceived susceptibility and severity will be meaningful for the threat perception, and the absence of any one of them will have a negative effect on the perceived threat. This is very similar to the idea that the computer's purpose is just for entertainment instead of storing or processing sensitive information. The user's risk assessment outcome will determine whether the individual will consider cyber security threat malicious or will not be threatened. Therefore, current research adopts Hypothesis H1c, which is in line with the previous study of [141].

  ***H1c**: Perceived susceptibility and perceived severity have a positive interaction effect on perceived threat.*

- According to the theory of motivation [257], human actions require motivation to achieve specific needs. The theory distinguishes 'security' as one of the human needs essential for survival and more control of their lives. Therefore [141] argues that malicious IT can be a painful experience for the user. The TTAT model views a positive relationship between the degree of threat and the user's motivation to thwart it. The current research suggests that while Ransomware cyber security threat can result in taking control of a user's machine, understanding its severe consequences to an individual's privacy can motivate the user to avoid ransomware. Therefore, in the context of current research, Hypothesis H2 is adopted from TTAT [141].

  ***H2**: Perceived threat positively affects avoidance motivation*

- Once the individual perceives the threat [141] TTAT model suggests that this will initiate the users' coping appraisal process. The individual will evaluate the effectiveness, feasibility and confidence of the selected safeguard measure to avoid IT threat. According to [141], TTAT defines safeguard effectiveness

as a subjective assessment of the individual that how useful it can be considered to avoid IT threat. The concept of safeguard effectiveness is derived from the theory of behaviour change [258], a model presented by [254]. The current study suggests game-based learning adoption as an awareness tool against ransomware cyber security threat and hypothesises that its effectiveness can motivate individuals to avoid a cyber attack. Based on this argument Hypothesis H3 is adopted from TTAT [141].

***H3**: Safeguard effectiveness positively affects avoidance motivation*

- According to [141] TTAT model, the relationship between perceived threat and avoidance motivation can be negatively moderated by safeguard effectiveness. However, using safeguard measures reflects the user's control over the threat, leading the user to perform avoidance motivation. However, [141] argues that an individual can be complacent in avoiding threat if he feels any antivirus software will reduce the effect. In contrast, a malware threat avoidance model [259] based on the TTAT model proposed a positive relationship between perceived threat and avoidance motivation. However, the hypothesis did not appear to be significant. Hence current research will consider [141] Hypothesis. Therefore, the argument suggests the adoption of TTAT's Hypothesis H3a [141].

  ***H3a**: Perceived threat and safeguard effectiveness have a negative interaction effect on avoidance motivation*

- Safeguard cost is associated with the user's physical and cognitive efforts required to adopt a safeguard measure, such as money, time, inconvenience, and comprehension [141]. The absence of these characteristics can make the user less eager to develop motivation. According to studies [254] related to health behaviour, the user is less likely to develop any avoidance motivation if the cost outweighs the benefits. In the context of IT security, a similar study by [255] identified that the cost of home wireless network security affected the decision of users to develop avoidance motivation. The current research aims to design a game-based learning against ransomware cyber security threat and will implement time limitations for the user to complete the learning activity.

A previous study [259] implemented timeboxing in studies in line with the [141] proposition. Therefore, based on this argument, current research adopt the Hypothesis H4 from TTAT [141].

***H4**: Safeguard cost negatively affects avoidance motivation*

- Self-efficacy is an individual's confidence in taking the safeguard measure and is considered an essential element contributing to a user's avoidance motivation [141]. The previous research conducted by [258] and [260] also examined an individual's security behaviour. Their findings also suggested that a user's self-confidence influences a user to develop avoidance motivation. Therefore, higher self-efficacy in adopting the safeguard measure will likely increase the user's avoidance motivation. The current research aims to embed a reward mechanism in game design. The user will earn points on a successful attempt to thwart ransomware cyber security threat and will be awarded a title on completion of the game based on expertise achieved. Hence current research hypothesises H5 [141].

  ***H5**: Self-efficacy positively affects avoidance motivation*

- According to [141], the user's intention to use safeguards in the context of IT security is defined as its avoidance motivation. This idea is further confirmed by a study [261] that a user's behaviour intention is a cognitive change driven by avoidance motivation. In the current research, user engagement will be driven through the implementation of lifeline, bonus rewards and consequences of losing points for any wrong decision. Therefore, current research supports the adoption of Hypothesis H6 [141].

  ***H6**: Avoidance motivation positively affects the avoidance behaviour of using the safeguard*

4.4 Methodology - Study 1

4.4.1 Data Collection

A survey was conducted to test the model for this study. The respondents were mainly colleagues, friends, and working professionals, who were contacted outside their work hours. The target audiences were 18-55 years and selected based on their minimum daily internet usage of 1-5 hours. Prior to data collection, this research was granted ethics approval by the University's research ethics committee. In addition, to adhere to General data protection regulations [262] and Data Protection Act [263], a participant information sheet was included in the questionnaire to provide the explicit purpose of the data collection. A survey instrument was created online, and respondents were asked to consent before proceeding with the questionnaire. Response to all instruments was made compulsory to avoid any missing data. A total of 153 respondents completed the questionnaire. The demographics related to the sample selected for current research are shown in the **Table 4.1**;

Table 4.1: Participant's Demographics

Gender	Number
Male	87
Female	66
Age	
Under 18	0
18-23	51
24-34	37
35-45	39
45-55	26
Education	
Undergraduate	107
Postgraduate	46
Internet Usage Per Day	
less than 3 hours	21
4 to 7 hours	57
8 to 10 hours	14
10 plus hours	8

4.4.2 Measurement Development

The current research developed measurements based on previous relevant literature and the theoretical TTAT model presented by [141]. All constructs were adopted from [141] model, and items for each variable were adapted to assess which elements of the TTAT model can be implemented in game design to improve user awareness against the ransomware cyber-attack. The questionnaire designed for this purpose includes eight constructs of the TTAT model *(P_Sus, P_Sev, P_Thr, S_eff, S_Cos, S_Eff, A_Mot, A_Beh*).

- The measure of Perceived Susceptibility (*P_Sus*) is in line with [141] and the previous studies conducted by [264]. It is in context to investigate whether

users believe ransomware to be a malicious threat. If the user considers ransomware a threat, it will convince the user to avoid it. Otherwise, users will not take any action as they do not see it as a threat. To measure the user's Perceived Susceptibility (*P_Sus*) to the ransomware cyber security threat. The *P_Sus* construct was designed with four items, as shown in **Appendix A**.

- The measurement of Perceived Severity (*P_Sev*) was developed in line with [141] and previous research on privacy by [265] and a study on the rise of malware by [266]. Perceived Severity (*P_Sev*) is a second construct influencing a user's threat perception as defined by [141]. The purpose of this variable in this research is to determine the extent to which users can consider the consequences of being compromised by the ransomware cyber security threat. Increasing *P_Sev* leads to higher threat perception, improving the user's avoidance motivation. *P_Sev* construct was designed using six questions, as shown in **Appendix A**.

- The measurement of Perceived Threat (*P_Thr*) was also developed in line with [141]. The original idea of *P_Thr* was based on cybernetic theory [267], which reflects users' relation between the current state and the undesired end state. However, in the context of IT. The TTAT propose that *P_Thr* is also caused by the combination of user perception of being susceptible to malicious threat and the magnitude of its negative impact on the user. The current research aims to determine user avoidance behaviour which is also determined by the perceived threat. Therefore, find it helpful to examine antecedents that contribute to *P_Thr*. Based on this idea, the *P_Thr* construct was designed with three questions, as shown in **Appendix A**.

- The measurement of Safeguard effectiveness (*S_eff*) is based on the [141] model and [264] literature. It is the third construct influencing users' avoidance of the cyber security threat as defined by the [193] TTAT model. The purpose of this variable in current research is to determine the user's belief that the chosen countermeasure against the ransomware cyber security threat is effective. *S_eff* construct was designed using four questions, as shown in **Appendix A**.

- The measurement of Safeguard Cost (*S_Cos*) was developed in line with the [141] theoretical model. The authors link it with the user's physical and cognitive efforts. They believe that if (*S_Cos*) outweighs the perceived effectiveness of the chosen safeguard, this can result in a barrier against a user's motivation to thwart a ransomware attack. The construct will measure how *S_Cos* can influence the user's decision against threat reduction. *S_Cos* construct is designed using three questions, as shown in **Appendix A**.

- The measurement of Self-Efficacy (*S_Eff*) was developed is consistent with the previous theory of [117] and [141]. TTAT model derived by [193] examines the role of safeguarding measures (Self-efficacy, Safeguard costs, Safeguard Effectiveness) and considers them an essential factor that arbitrates in users' threat avoidance motivation. In the current research, the safeguarding measure 'Self-Efficacy' *(S_Eff)* is included as one of the constructs to examine its impact on the user's avoidance motivation against a cyber security threat. *S_Eff* construct was designed with six questions, as shown in **Appendix A**.

- The measurement of Avoidance Motivation (*A_Mot*) was developed in line with previous research by [261] on behavioural intention and according to the TTAT model derived by (Liang & Xue, 2010), when user perceived threat and copping appraisal is high, this will improve user motivation to avoid the threat. Therefore, the (*A_Mot*) construct is included in this research. Its elements will determine the level of user avoidance motivation against the ransomware cyber-attack, as this variable is directly influenced positively or negatively by perceived threat and safeguarding measures. This variable will help to determine the impact on user behaviour. The questionnaire includes three elements of the *A_Mot* construct, as shown in **Appendix A**.

- The measurement of Avoidance Behaviour (*A_Beh*) is also consistent with [141]. The TTAT model explains how the amalgamation of the user's perceived susceptibility to the malicious threat and its severity constitutes user threat perception, enabling users to evaluate coping appraisal using safeguard measures[141]. The outcome of this phenomenon will lead the user to two

differing coping options, which means the user will either take action against the threat (problem-focused coping) or not do anything (emotion-focused coping). The current research aims to measure the change in user behaviour. Hence construct Avoidance Behaviour (*A_Beh*) has been included in the questionnaire with two elements to assess user's behaviour as shown in the figure **Appendix A**.

A pilot study (empirical research) was conducted with 15 respondents. The purpose was to elicit respondents' feedback and ensure the questionnaire's validity and reliability ahead of the main studies [229]. Based on the feedback, some of the item's wording was revised and some questions were removed. The final questionnaire shown in **Appendix A** measures eight elements (constructs) of TTAT, it consists of three items of p_sus, three items of p_sev, three items of p_thr, three items of s_eff, three items of p_cos, five items of s_Eff, three items of a_mot and two items of a_beh. The constructs were evaluated using a Likert-style questionnaire using a scale from 1-5 [268], with a scale of 1 being "Strongly Disagree" and a scale of 5 as "Strongly Agree".

4.5 Data Analysis and Results - Study 1

In *Study 1*, the research aims to test the hypotheses and validate the measurements and the research model. It adopts Partial Least Squares structural equation modeling (PLS-SEM) using SmartPLS 3.0. The PLS-SEM is a quantitative analysis technique which has recently gained considerable attention in the field of management information systems discipline [240] as it has the ability to utilise smaller sample sizes and handle multiple regression analysis [269]. Previous studies by [240] and [270] report that it is valuable for exploratory research. Study 1 requires analysis of multiple constructs to validate elements of TTAT empirically. Therefore the use of PLS-SEM is found suitable for the current studies.

4.5.1 Measurement Validation

Table 4.3 provides a Summary of the various statistical tests performed for the instrument measurement validation and the model validation. All constructs listed in the table were adopted from the previous study by [141]. Data analysis was performed in two steps: *(1)* Measurement validation, and *(2)* Research model Testing.

For the *measurement validation*: After the data was collected, ***Harmanś single-factor*** test was performed to investigate the concern that there is any possible presence of Common Method Bias (CMB)/Common Method Variance (CMV) in the instrument [206]. The test results shows, seven factors have emerged, which explains 76.291% of the total variance, while the most considerable variance explained by one factor was 28.854, as this value is less than 50%, according to [271] this means CMB/CMV is not a severe concern in our studies. **Table 4.2** represents the values of the test.

Table 4.2: Harman's single-factor

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %	Total	% of variance	Cumulative %
1	7.214	28.854	28.854	7.214	28.854	28.854	4.000	15.998	15.998
2	4.215	16.860	45.714	4.215	16.860	45.714	2.950	11.801	27.799
3	1.906	7.625	53.339	1.906	7.625	53.339	2.753	11.010	38.809
4	1.659	6.636	59.975	1.659	6.636	59.975	2.726	10.905	49.714
5	1.610	6.439	66.414	1.610	6.439	66.414	2.683	10.730	60.444
6	1.322	5.287	71.701	1.322	5.287	71.701	2.078	8.314	68.758
7	1.148	4.591	76.291	1.148	4.591	76.291	1.883	7.533	76.291
8	0.898	3.590	79.882						
9	0.700	2.800	82.682						
10	0.649	2.595	85.277						
11	0.615	2.459	87.736						
12	0.472	1.889	89.625						
13	0.449	1.797	91.422						
14	0.381	1.525	92.948						
15	0.335	1.341	94.289						
16	0.296	1.183	95.472						
17	0.270	1.082	96.554						
18	0.216	0.863	97.417						
19	0.173	0.694	98.110						
20	0.152	0.607	98.718						
21	0.129	0.517	99.235						
22	0.074	0.298	99.533						
23	0.045	0.181	99.714						
24	0.039	0.157	99.872						
25	0.032	0.128	100.000						

To further validate *measurement*: **descriptive statistics** were performed using SPSS. The values of Skewness and Kurtosis were examined to ensure the normal distribution of all items. If values of both measures are in the range of (-2 to +2), [272] suggest this represents the normality. At the same time, coefficients of reliability tests i.e., Cronbach's alpha (α) and Composite reliability (CR) were performed. The purpose of conducting these tests was to evaluate the internal consistency reliability of the instrument to determine research model reliability. **Table 4.3** shows the results of α for the constructs as; (P_Sus = 0.7, P_Sev = 0.7, P_Thr = 0.85, S_eff = 0.93, S_Cos = 0.92, S-Eff = 0.85, A_Mot = 0.92 and A_Beh = 0.84), these findings are within the recognised scale of 0.7 as recommended by [241] and [273]. While the test results of CR for all the constructs are well above the [203] recommended scale of 0.7. These results indicate that measurement items of each construct have good reliability.

Table 4.3: Normality, reliability, and discriminant validity.

Constr.	Items	Mean	Std.	Kurtosis	Skewness	Loading	α	CR	AVE
P_Sus	Q2	3.72	0.87	0.54	-0.54	0.706	0.7	0.82	0.6
	Q3	3.23	1.11	-0.52	-0.35	0.762			
	Q4	3.65	0.99	0.80	-0.83	0.851			
P_Sev	Q8	3.88	0.78	0.24	-0.37	0.766	0.7	0.83	0.61
	Q9	3.74	0.85	-0.19	-0.25	0.805			
	Q10	3.82	0.78	0.13	-0.25	0.774			
P_Thr	Q12	4.08	0.75	0.32	-0.61	0.867	0.85	0.91	0.77
	Q13	4.05	0.71	-0.29	-0.29	0.893			
	Q14	4.03	0.76	-0.49	-0.32	0.871			
S_eff	Q17	4.39	0.72	1.90	-1.47	0.935	0.93	0.96	0.88
	Q18	4.42	0.70	1.76	-1.49	0.946			
	Q19	4.44	0.68	1.99	-1.69	0.935			
S_Cos	Q21	2.56	0.94	0.22	1.33	0.936	0.92	0.95	0.86
	Q22	2.47	0.93	0.85	1.35	0.945			
	Q23	1.90	1.10	0.50	1.21	0.893			
S-Eff	Q24	4.09	0.72	-0.38	-0.34	0.764	0.85	0.9	0.63
	Q26	4.24	0.62	0.27	-0.38	0.88			
	Q27	4.19	0.62	0.94	-0.49	0.854			
	Q28	2.79	1.30	-1.14	0.50	0.747			
	Q29	2.45	1.68	-1.56	0.49	0.723			
A_Mot	Q30	4.24	0.66	1.90	-1.12	0.937	0.92	0.95	0.86
	Q31	4.24	0.61	1.27	-0.53	0.949			
	Q32	4.27	0.64	1.36	-0.92	0.893			
A_Beh	Q33	4.12	0.55	1.40	-0.65	0.941	*0.84	0.92	0.86
	Q34	4.14	0.52	1.88	-0.10	0.91			

To test the *model validity*: the current research assessed ***convergent validity*** (on the basis of Average variance extracted - **AVE**) and ***discriminant validity*** based on the Fornell & Larcker criterion [203], i.e., (1) "the square root of each construct's AVE should be the highest among all correlative constructs" and (2) "cross-loading, each item should have the highest loading in its own construct". *Structural equation modeling* (SEM) analysis was conducted using smartPLS. Results reported in **Table 4.4** show, items have much higher factor loading than cross-loadings, and the AVE square root shown in **Table 4.5** is greater than its cross-correlations with other constructs. These results indicate that all constructs have sufficient discriminant validity, for any items for which cross-loading was less than 0.6 were dropped for further analysis. At the same time, **Table 4.3** shows that the value of AVE is ranged from 0.6 to 0.88. According to [203], this satisfies all the conditions for convergent validity. Thus, the model shows adequate reliability and convergent and discriminant validity.

Table 4.4: Cross-loading

	A_Beh	A_Mot	S_Cos	S_eff	P_Sev	P_Sus	P_Thr	S_Eff
Q33	**0.941**	0.543	-0.079	0.338	0.115	0.125	0.433	0.275
Q34	**0.910**	0.441	-0.055	0.229	0.091	0.116	0.363	0.199
Q30	0.503	**0.937**	-0.195	0.615	-0.053	0.090	0.497	0.377
Q31	0.518	**0.949**	-0.274	0.583	0.031	0.084	0.517	0.368
Q32	0.469	**0.893**	-0.152	0.478	0.096	0.184	0.558	0.411
Q21	-0.026	-0.201	**0.936**	-0.278	0.220	0.199	0.116	0.163
Q22	-0.044	-0.232	**0.945**	-0.323	0.201	0.226	0.005	0.108
Q23	-0.141	-0.187	**0.893**	-0.243	0.257	0.190	0.100	0.055
Q17	0.333	0.604	-0.263	**0.935**	-0.100	0.149	0.374	0.210
Q18	0.276	0.538	-0.349	**0.946**	-0.025	0.167	0.382	0.168
Q19	0.264	0.557	-0.256	**0.935**	0.057	0.215	0.407	0.255
Q8	-0.021	-0.023	0.323	-0.112	**0.766**	0.152	0.212	0.218
Q9	0.007	-0.079	0.167	0.013	**0.805**	0.179	0.235	0.150
Q10	0.236	0.132	0.108	0.020	**0.774**	0.159	0.286	0.123
Q2	0.034	0.113	0.131	0.263	0.113	**0.706**	0.192	0.284
Q3	0.087	-0.051	0.202	-0.005	0.120	**0.762**	0.156	0.200
Q4	0.156	0.172	0.189	0.153	0.221	**0.851**	0.288	0.391
Q12	0.390	0.475	0.051	0.439	0.183	0.226	**0.867**	0.448
Q13	0.414	0.507	0.065	0.341	0.272	0.225	**0.893**	0.484
Q14	0.340	0.501	0.079	0.319	0.363	0.301	**0.871**	0.561
Q24	0.173	0.274	-0.056	0.215	0.074	0.316	0.405	**0.764**
Q26	0.207	0.361	-0.017	0.226	0.227	0.341	0.440	**0.880**
Q27	0.270	0.388	-0.025	0.271	0.119	0.272	0.429	**0.854**
Q28	0.216	0.328	0.282	0.114	0.176	0.338	0.530	**0.747**
Q29	0.148	0.279	0.333	0.041	0.213	0.328	0.487	**0.723**

Table 4.5: Fornell-Larcker criterion

	A_Beh	A_Mot	S_Cos	S_eff	P_Sev	P_Sus	P_Thr	S_Eff
A_Beh	**0.926**							
A_Mot	0.536	**0.927**						
S_Cos	-0.073	-0.225	**0.925**					
S_eff	0.312	0.605	-0.307	**0.939**				
P_Sev	0.113	0.025	0.242	-0.026	**0.782**			
P_Sus	0.13	0.127	0.222	0.188	0.209	**0.775**		
P_Thr	0.433	0.565	0.075	0.413	0.318	0.289	**0.877**	
S_Eff	0.26	0.415	0.118	0.225	0.204	0.397	0.572	**0.796**

Further, the results reported in **Table 4.4** and **4.5** have been confirmed by the test of the ***Heterotrait-Monotrait (HTMT) Ratio*** [274] for the model evaluation [240]. The HTMT analysis is shown in **Table 4.6** which reports that the HTMT values of all the constructs are less than the suggested threshold of 0.85 [274]. Thus, it provides confidence that the discriminant validity results of the two previous techniques are valid.

Table 4.6: Heterotrait-monotrait ratio (HTMT)

	A_Beh	A_Mot	S_Cos	S_eff	P_Sev	P_Sus	P_Thr	S_Eff
A_Beh								
A_Mot	0.607							
S_Cos	0.086	0.242						
S_eff	0.345	0.65	0.33					
P_Sev	0.169	0.144	0.324	0.114				
P_Sus	0.157	0.192	0.28	0.238	0.283			
P_Thr	0.512	0.639	0.094	0.469	0.399	0.354		
S_Eff	0.298	0.465	0.218	0.25	0.275	0.496	0.672	

Further, a ***multicollinearity*** test was conducted, and variance inflation factor (***VIF***) values were examined. This test was conducted to evaluate any multicollinearity issue [275], which can occur because of errors caused by high correlation among the latent variables [276] and can result in undermining the statistical significance of an independent variable. The items were standardised to minimise any multicollinearity issues. The results of the test are included in **Table 4.7**, which

shows VIF < 5 for all the variables and is in the acceptable range as suggested by [277].

Table 4.7: Multicollinearity Test

VIF (Collinearity Statistics)									R	
	A_Beh	A_Mot	S_Cos	S_eff	P_Sev	P_Sus	P_Thr	S_Eff	R^2	R^2 Adj.
A_Beh	- -	- -	- -	- -	- -	- -	- -		0.29	0.28
A_Mot	1	- -	- -	- -	- -	- -	- -	- -	0.52	0.51
S_Cos	- -	1.18	- -	- -	- -	- -	- -	- -	- -	- -
S_eff	- -	1.4	- -	- -	- -	- -	- -	- -	- -	- -
P_Sev	- -	- -	- -	- -	- -	- -	1.05	- -	- -	- -
P_Sus	- -	- -	- -	- -	- -	- -	1.05	- -	0.15	0.14
P_Thr	- -	1.74	- -	- -	- -	- -	- -	- -	- -	- -
S_Eff	- -	1.5	- -	- -	- -	- -	- -	- -	- -	- -

The above statistical test results show reliable values of convergent and discriminant validity, hence supporting the validity and reliability of the instrument and research model.

4.5.2 Model Testing

Figure 4.2 shows the model testing results. The model accounts for 21 per cent of the variance in p_thr, 55 per cent in a_mot, and 29 per cent in a_beh. According to the hypothesis, the p_thr is significantly determined by p_sev ($b = 0.26, p < 0.01$) and p_sus ($b = 0.21, p < 0.05$), thus supporting hypotheses H1a and H1b. According to [278], these results show that p_sus and p_sev influence on users a_mot is fully mediated by a p_thr. The model shows users' a_mot is significantly determined by p_thr ($b = 0.25, p < 0.05$), s_eff ($b = 0.31, p < 0.05$) and s-Eff ($b = 0.23, p < 0.01$). These results support Hypothesis H2, H3 and H5. At the same time, 'Interaction effect 2' between p_thr and s_eff is found ($b = -0.12, p < 0.05$). This result is significant and is in line with the findings of [141]. Thus support Hypothesis H3a. And then a_mot ($b = 0.54, p < 0.01$) influences a_beh significantly. Thus support hypothesis H6. However two results were found insignificant. The 'Interaction effect

1' H1c, between p_sus and p_sev is found ($b = 0.25, p > 0.05$) but it is in line with findings of [141]. However, the only result found insignificant and opposed to the TTAT finding is safeguard cost ($b = -0.14, p > 0.05$). Thus, current research does not support Hypothesis H4.

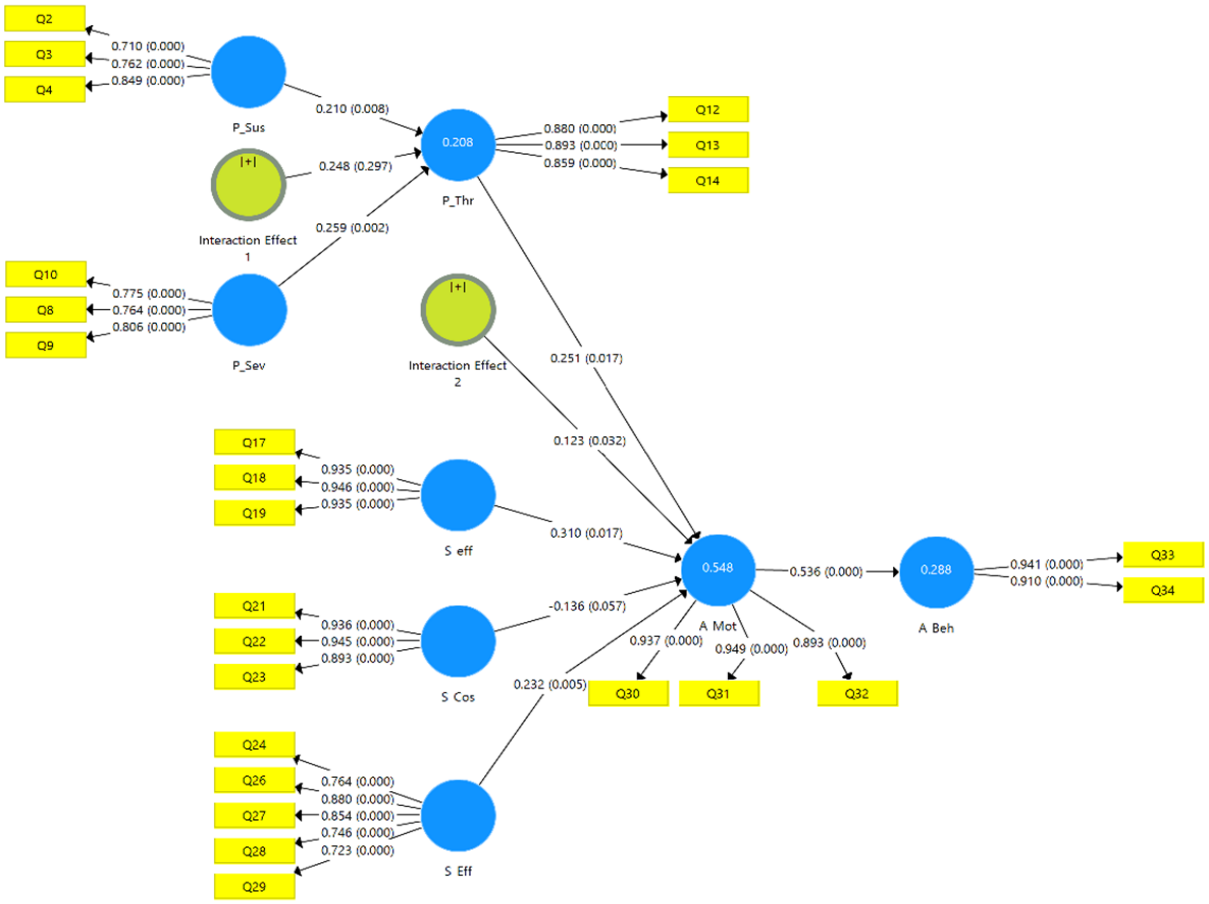

Figure 4.2: Structural Model Path Coefficients

Table 4.8: Hypotheses Results

Hypothesis	Path	Beta Coeff.	*T*-Value	*P*-Value	Results
H1a Perceived severity of being attacked by ransomware positively affects perceived threat	P_Sev → P_Thr	0.259	3.1	0	Supported
H1b Perceived susceptibility of being attacked by ransomware positively affects perceived threat.	P_Sus → P_Thr	0.21	2.67	0.01	Supported
H2 Perceived threat positively affects avoidance motivation.	P_Thr → A_Mot	0.251	2.36	0.02	Supported
H3 Safeguard effectiveness positively affects avoidance motivation	S_eff → A_Mot	0.232	2.85	0.01	Supported
H4 Safeguard cost negatively affects avoidance motivation	S_Cos → A_Mot	−0.136	1.87	0.06	Not Supported
H5 Self-Efficacy positively affects the avoidance behaviour of using the safeguard	S_Eff → A_Mot	0.232	2.85	0.01	Supported
H6 Avoidance motivation positively affects the avoidance behaviour of using the safeguard	A_Mot → A_Beh	0.536	7.3	0	Supported
H1c Perceived susceptibility and perceived severity have a positive interaction effect on perceived threat	Interaction Effect 1 P_Sus × P_Sev → P_Thr	0.248	1.03	0.31	Not Supported
H3a Perceived threat and safeguard effectiveness have a negative interaction effect on avoidance motivation	Interaction Effect 2 P_Thr × S_eff → A_Mot	-0.123	2.17	0.03	Supported

4.6 Discussion

The current study empirically investigated the factors affecting users' motivation to avoid ransomware cyber security threat through game-based learning. TTAT model, derived from [141], was validated using questionnaire data, and analysis was performed using PLS_SEM. The analysis results show a significant change in users' motivation to avoid ransomware cyber security threat (55%) and avoidance behaviour (29%). These results explain that users must be motivated to avoid the ransomware cyber security threat. The change in avoidance behaviour requires an individual to acknowledge that the ransomware exists and a user's belief that it is avoidable. These findings are in line with the findings of Liang & Xue TTAT model, which focuses on computer security behaviour and malware, but contrary to findings from a previous study [259], which was more on the behaviour of online social network users. As the current study aims to improve users' awareness of ransomware threat, present research findings will be considered significant. In addition, the results supported hypotheses H1a & H1b, as the perceived severity of being compromised by ransomware positively influenced the individual's threat perception. This means the user must be conscious of being attacked by ransomware and its severe consequences of being compromised to develop threat perception. This is in line with the findings of [141] TTAT model and a previous study [279].

Further results showed that once the user's threat perception was developed, the user evaluated three cognitive factors (S_eff, S_Cos, and S-Eff) to assess the effectiveness of safeguard measures against ransomware avoidance motivation. The result in the preceding section supports the first safeguard measure (S_eff), hypothesised as H3. It positively influenced the use of game-based learning as an engaging and user-friendly measure for a user's avoidance motivation against ransomware threat. The second safeguard measure (S_Cos) is hypothesised as H4. It negatively influences an individual's avoidance motivation. The result of H4 is insignificant and is opposed to the previous study [141]. This is because ransomware is a new phenomenon, and its impact is far more significant than any traditional malware. Losing access to data is more critical for the user today than time investment and control cost. The result of H2 indicates that because of the consequences of ransomware, once the user

perceives ransomware as a threat, it motivates the user to avoid it. This finding is in line with [141] TTAT. The third safeguard measure (S-Eff), which is hypothesised as H5, also has a positive influence on avoidance motivation. As more individuals learn and understand the ransomware threat through game-based learning, more users will be confident in avoiding it. The results support the hypothesis and are in line with previous findings of [141] and [280].

The current study also tested the interaction effect between p_thr and s_eff, hypothesised as H3a and negatively influences users' avoidance motivation against the ransomware threat. This is in line with previous findings of Liang & Xue [141] TTAT. In contrast, hypothesis H1c is the interaction between p_sus and p_sev. The results are in line with previous findings of [279] and [141]. This interaction was explained as a moderate phenomenon by Liang & Xue in the context of a game virus.

In contrast, current research aims at ransomware cyber security threat. Its implications are far more than any other virus as users are more exposed to smart Internet-connected devices. The current research findings show that the interaction between perceived susceptibility and perceived severity is in line with previous findings of [281] in the security behaviours of smartphone users.

4.7 Research Implications

Post Covid-19 has shifted the world towards more digitisation. Cyber-physical systems are an integral part of our digital lives. Businesses, local governments, and critical health services are facing the Internet more than ever in the modern world. With more exposure to online services, the pandemic has changed the cyber security landscape, bringing more challenges for organisations to safeguard their critical assets against cyber-attacks [282]. NCSC (2021) has reported ransomware as the most significant among many other cyber threats in recent years. It is almost certain that it will grow further and continue to jeopardise the security of individuals, organisations, and critical infrastructure. Much existing literature focuses on cyber resilience in the organisational context, where security is much more a compliance

requirement to have an information security management system in place to adhere to regulatory requirements such as (ISO27001) [283], (GDPR) [284] or similar [285]. This forces organisations to form policies in line with their information governance strategy and make it mandatory for their employees to follow them to achieve security. This approach is contrary to the user's security behaviour in individual settings, where the response to any cyber threat is voluntary, and its decision depends on the perception of the threat by the individual.

The current research addresses this gap by adopting the [141] TTAT model, which focuses on two aspects of the individual's security behaviour, i.e., (1) threat appraisal and (2) coping behaviour. Individuals must acknowledge the presence of malicious threats and their possible consequences. This leads to the user's copping behaviour in which the individual assesses the effectiveness of safeguard measures (S_eff, S_Cos and S_Eff) to thwart the malicious threat. Both factors will develop user avoidance motivation, resulting in a change in behaviour against the malicious threat.

There are two key contributions to the literature; *Firstly*, current research findings identify that statistical results of safeguard cost are insignificant in the context of user perception of the safeguard cost to ransomware threat. This finding contradicts the original finding of the TTAT model of [141] and [279]. The previous studies explain that p_thr is determined by p_sev and P_sus in the malicious IT context and the combined effect of the p_thr and s_cost in the IT security context [255]. While ransomware is a relatively new phenomenon and malicious compared to other families of malware [110], attackers use novel tactics to compromise the security of computer systems. According to [141], s_cos is the user's physical and cognitive effort. Study 1 in current research proposes game-based learning to improve users' motivation against the ransomware cyber security threat and considers a time-based storyline an essential characteristic of the game. Therefore, findings of current studies suggest that as soon as an individual perceives ransomware susceptibility, it is evident that the user will develop a threat perception to its security. This user perception of the threat will be enough for a user to develop motivation to thwart ransomware without considering the safeguard cost.

Secondly, current research findings empirically tested and supported the relation-

ship between game effectiveness and user. Cyber security education is a complex domain due to its technical nature and changing landscape. The current research identified game-based learning as an educational tool to address the gap in cyber security education. The model testing results show that users believe game-based learning is user-friendly and will improve awareness against ransomware. Therefore, in current research, the usability factor is considered an essential factor in the game design framework, which will help the users enjoy game playing and improve their awareness against ransomware threat [286]. Users have been flooded with information due to the heterogeneous connectivity of computers. With the rise of cyber-physical systems, the relationship between humans and IoT devices requires reliability. The user is considered the first line of defence against malware attacks. Therefore, designing and developing game-based learning for ransomware is a contribution. This is contrary to original studies by [141], which considered safeguard effectiveness as a subjective assessment and the user's intention or ability to use hardware as an effective tool against malicious IT.

In Summary, the current research studied the TTAT model. It validated the hypotheses leading to critical components required to include in the proposed Game for users' awareness against ransomware cyber security threat.

4.8 Implications for Practice

The current research examines individuals' avoidance behaviour to thwart ransomware cyber security threat. Whether an individual user requires security for their device or in sitting in an organisational context, security is the responsibility of each stakeholder as a collective effort. The current studies target individuals in both contexts. Since the Internet users and the integration of technologies in our lives is increasing exponentially. Attackers exploit humans as the weakest link to execute successful security breaches and gain an advantage in the lucrative cyber crime market. There is a dire need to address the new challenges these technologies pose to secure our future [198]. It has been seen that it needs a high level of expertise to write malicious code, but it takes only **ONE** click to activate ransomware. Therefore, findings from current research inform the design and development of

game-based learning tool to upskill individuals against ransomware cyber security threat. The game will aim to develop user motivation against the ransomware malware and will lead to a change in user avoidance behaviour against it.

The current research endorses education and awareness of ransomware cyber security threat using game-based learning. The findings drawn from the current research suggest that user motivation can be developed through threat perception and coping appraisal. The research informs these findings to design and development of the game design. It suggests that game-based learning against ransomware threat will provide a positive learning experience for individuals to develop their avoidance motivation when they are in voluntary settings, and security consideration is their choice rather than compliance. The current research suggests the game will interact with users based on a storyline, which will help users engage and develop awareness against the ransomware cyber security threat. The research also informs usability as an essential element to be considered in the game design. So users can engage in learning in a friendly manner. The game will be available for individual users at no cost to benefit learning and education against ransomware threat to a broader body of knowledge. The rapid digital transformation has made people use more smart devices than ever. Individuals spend more time online with constant connectivity to the Internet, and more people are using smart devices than ever before. The current research findings target these individuals to improve their security and awareness of the rising ransomware threat through a usable approach.

The current research also recommends that commercial organisations include game-based learning in their information security awareness program. It suggests this as an opportunity to replace traditional theoretical knowledge tests with more interactive learning. For an organisation to comply with statutory, legal and regulatory requirements, Game-based learning can effectively make users aware of the rising ransomware threat. No matter how expensive hardware is in place, security awareness in any organisation requires a hybrid approach to educate staff against the changing landscape of cyber security threats. Also, as security is the responsibility of everyone in any organisation, the current research suggests adopting Game-based learning to develop their avoidance motivation against the ransomware threat. The current research also suggests it is vital for organisations to consider the security

challenges posed by a large number of the remote workforce because of the pandemic, which has emerged new business models [110]. Criminals are exploiting vulnerabilities in smart home devices due to individuals' poor cyber hygiene practices. The current research also targets organisations to prioritise the security awareness of their employees working from home and suggests the adoption of Game-based learning as an effective tool to develop their avoidance motivation against ransomware in a user-friendly and engaging manner. Organisations should embed game-based learning in their security awareness training programmes, which should frequently run for each stakeholder during their employment.

Current research aims to upskill users through education and awareness of ransomware cyber security threat using game-based learning [287]. The research findings will eventually play an important role in promoting cyber security awareness. This can help overcome skills shortages in cyber security and enhance career opportunities in the domain. Therefore, current research also suggests using game-based learning as an opportunity for future research for school-going pupils to motivate them to learn about ransomware awareness. Engagement through game-based learning can make them enthusiastic cyber experts and help to fill the gap in future cyber roles. Security and privacy can be achieved through the collaboration of different entities. However, this research will contribute knowledge related to Ransomware awareness to the user through a usable approach [288].

4.9 Summary

The chapter concludes with *Study 1* to investigate which elements of the TTAT model should be included in the game design, which can help to address users' awareness of the ransomware cyber security threat. The aim was to investigate how users' avoidance motivation can be developed to thwart ransomware attack. The analysis performed on data collected from 153 respondents shows that P_Sus, P_Sev, S_eff, S_Cos, and S_Eff influence user motivation against ransomware cyber security threat and change individual behaviour towards its awareness. As technology is becoming more sophisticated, there is a rise in more organised cyber-attacks. Organisations are struggling to develop an effective Cyber security strategy to cope

with cyber security threats. This is mainly because more user awareness is required in the cyber security domain. The UK Government is intended to invest £1.9 billion as a part of the National Cyber Security strategy plan 2016. The research findings inform a novel technique to develop game-based learning to address ransomware cyber security awareness. The current research findings can benefit individuals and organisations by adopting an interactive way to educate and make aware individuals using game-based learning, which can engage users in a user-friendly manner.

Chapter 5

Ransom*A*ware Game Design & Development

5.1 Overview

This Chapter focuses on designing and developing a usable Game Design prototype to improve user education awareness against ransomware threat. There are two essential things to consider in the design phase.

(i) To implement user experience to achieve usability in game design.

(ii) To implement elements of TTAT from a development point of view.

The study focuses on the principles of game design to achieve usability. For this purpose, personas, MoSCoW analysis, task analysis, user stories and wireframe techniques are used to understand the user interaction with the system. The findings of chapter 4 suggest that elements of TTAT, i.e., P_Sus, P_Sev, S_eff, S_Cos, S-Eff, A_Mot, and A_Beh, should be included in the game design framework to improve users' avoidance motivation against ransomware cyber security threat. The open-source Android mobile application development tool MIT App inventor is adopted as a platform to design and develop a usable solution based on the findings reported in chapter four. The study will also report consideration of usability factors, which are critically important for an efficient design.

5.2 Usability – User Experience for User-Centred Design

For a game design to be successful for its intended audience, the study first focuses on the importance of user experience UX [289]. Implementing UX is beyond design aesthetics and the product's functional requirements [290]. From the user's perspective, it is not just about completing the task accurately and efficiently, which is the goal of product design anyways. However, it is the experience which they want to enjoy while completing the tasks [239]. Therefore, for a design to stay ahead in a competitive digital market, the product designer must include usability in the design, empowering them to interact with the product efficiently and effectively [291].

The game design in this study emphasises user-centred design (UCD) [292] to address the user experience. It considers the context of user requirements, i.e., the elements to be included in the game design. To thoroughly map these requirements in the design for an optimised solution that can add value to the user's experience and help the research achieve its aims [265]. For this purpose number of design solutions are generated during different phases of the design representing abstract to concrete design concepts. The study proposes U*X*D Methodology based on Waterfall and an adapted version of Jesse James Garret's methodology to implement UCD for the game design prototype.

The current research aims to develop a usable game which is user-centred design, a design which can map product objectives into user needs [293]. The game development process involves coding, which requires a software development process to implement the game requirements. Previous studies recommend agile methodology due to its agility [232] or waterfall methodology if the product requirements are precise [236]. A review of different UX frameworks [293] focuses more on the social theoretical context and is not empirically validated in game development. However, studies [294] propose a hybrid approach to address game development and usability in design. Considering that no single framework could address the development and usability process for the game design, current research finds this opportunity to present a new unified methodology based on Waterfall and James Jarrett's method-

ology, shown in **Figure 5.1**.

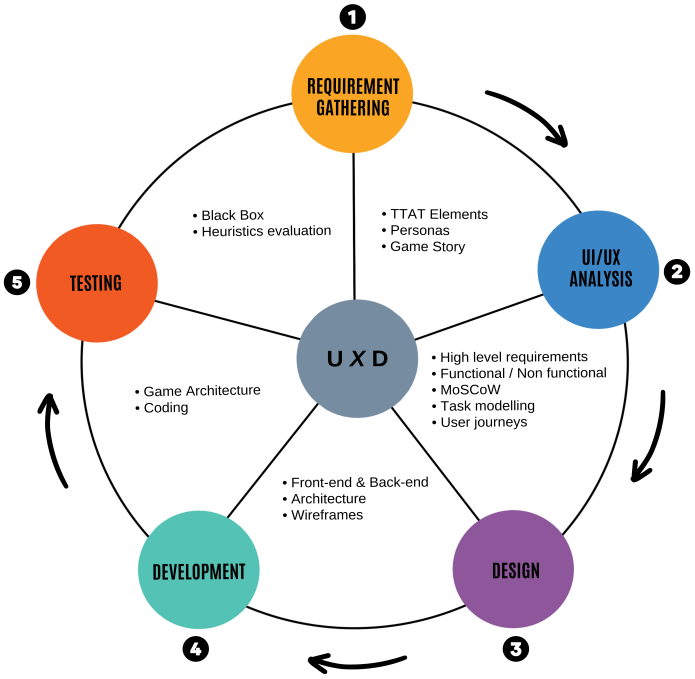

Figure 5.1: Unified User Experience Development Methodology

Requirements Gathering; The game design process defines product (Game) goals/objectives and user needs at an abstract level [295]. This phase is critical for understanding the user behaviour, level of technology and the, subject awareness, background, demographic, and psychographics facts [295]. This helps determine the target user and their needs related to the product. The findings from chapter 4 related to elements of TTAT to include in the game design will be input in this phase.

The main questionnaire adopted for data collection in chapter 4 of this research thesis was targeted at colleagues/friends. These target users will play the proposed mobile game for education and awareness against the cyber security threat of ransomware. During the UX design process, the game content design and the Information architecture would require a critical understanding of the explicit intent of user interaction with the game. For this purpose, the Personas shown in **Figure 5.2** represent fictional characters [296]), which will help the designer understand the user behaviour, needs, goals and the application flow. The personas will allow the designer to focus on user needs at each application design level to avoid thinking of

making a design for himself. This is achieved by dividing the user groups of similar needs into either a smaller group or a segment based on demographic and psychographics criteria, which is one of the first steps for implementing UX for the target users.

Figure 5.2: User Personas [297]

5.3 Story Behind Ransom*A*ware

Storytelling is an essential part of a game design to engage users [298]. Memorable characters are integral to any story to improve user interaction and player-centred learning [299]. Therefore, the game Ransom*A*ware is based on a story with some memorable characters.

The game aims to make users aware of possible threats and decrease their vulnerability against ransomware. It starts with an introduction to the users, and they find themselves in a spaceship flying through space. They come across unknown planets and are prompted with messages. These messages appear in an email format and are either genuine or malicious. The users can 'ACCEPT' or 'REJECT' these messages, directly influencing their success or demise. This critical decision will not be straightforward or easy to make, depicting real-life encounters with malicious emails. The correct judgements will earn points, while incorrect judgement will cost lives and points. The game is made visually engaging for the user by them being virtually present in an interactive cockpit. Memorable characters like the space shuttle scanning the user's space rocket and allowing safe passage or hacking

it into lockdown and making it inaccessible let them taste real-life vulnerability.

This game will continue until the users have completed their flight over eight planets. It will give them six opportunities to assess their abilities and recognise and avoid possible threats of falling prey to ransomware. A time limit will push the users to make decisions quickly, which brings daily life into perspective as a regular user spends only a few seconds or less to decide their fate which might lead to encrypted files and data lost or stolen. At the end of the gameplay, the users will get feedback to evaluate their awareness.

Game Instructions

The users are familiarised with the working of the Ransom*A*ware game by the following instructions;

The game starts with the user virtually present in the spaceship flying through space. The running score, lifeline and time are visual at all times. A planet is seen approaching, and a user is prompted with a message. The message urges the user to believe its genuineness, giving it a limited time to respond with "ACCEPT" or "REJECT", resulting in the alien spaceship scanning your rocket and moving forward with one of the following scenarios.

If a message is genuine:

- By selecting "**REJECT**", you are made aware of your wrong choice and lose 10 points.
- By selecting "**ACCEPT**", you are made aware of your right decision and are awarded 10 points.

If a message is malicious:

- By selecting "**REJECT**", you defeat the malicious alien and earn 10 points.
- By selecting "**ACCEPT**", the malicious alien ship hacks your spaceship, and you are left with two options to either decide to "**Pay Ransom**", which will reduce one of your lives or to "**Call Helpline**", which will reduce your time by 10 seconds.

This will continue until you either run out of time, limited to 180 seconds, or run out of lives which are 3 in total. The game will end if you go through all six planets or reach 100 points. After the game ends, a feedback message will be displayed. This feedback gives you personalised instructions depending on your final score to help you improve your awareness against relevant ransomware Cyber Security threat.

Table 5.1: RansomAware Training Rewards

Points	Reward
90 - 100	Gold
70 - 80	Silver
50 - 60	Bronze
0 - 50	No Award

5.4 Game Design High-Level Requirements

UI/UX Analysis: At this stage, the game design prototype must meet the high-level user/product requirements to include the elements of TTAT in the game design. The following requirements are mapped with TTAT elements reported in study 1 as;

- A User-centred design (UCD) to provide usability to its users.
- Promote education and awareness against the cyber security threat of ransomware to its users.
- Game to make the user understand the *Identification* of ransomware threat and its likely **harm/risk** - *(P_Sus))/P_Thr*
- Game to introduce user, **consequences (CIA)** of a ransomware attack or the danger of ransomware attack - *(P_Sev)/ P_Thr.*
- The game is **user-friendly**, allowing the user to proceed without difficulties/advance to the next level - *(S_eff).*

- Improve user **engagement** to seamlessly complete the gameplay (find it helpful, exciting role play or challenges) and improve their awareness and knowledge of computer security against ransomware - *(S_eff)*.
- Game to promote feasibility so users can make a timely, cost-effective and appropriate decision during play - *(S_Cos)*.
- Game to help the user build their **confidence** (lifeline or points gain) to educate against how to prevent ransomware cyber attack - *(S-Eff)*.
- The game aims to help users with problem-focused coping by improving their Avoidance_Motivation and Behaviour against the cyber threat ransomware. This will be assessed using overall game results to see how effectively the game has helped users with an understanding of ransomware *Threat Appraisal and Coping Appraisal*.

5.5 Functional and Non-Functional Requirements

UI/UX Analysis: Functional requirements are essential in development projects in order to detail each specific system function that the application must be capable of performing [300]. They are a list of required operations that can be measured and evaluated to verify their successful implementation in a project. Equally important, however, are also non-functional requirements, which describe how the system will perform its required operations, for example, in terms of quality, performance and design or development constraints [301]. Since non-functional requirements are non-tangible and usually relative and subjective, they can be harder to measure and evaluate, as [302] highlight.

In the context of research, the game storyline and the high-level game design requirements include elements of TTAT which will determine the functional and non-functional requirements to be considered during game design. However, to consider the scope of the design and development work, MoSCoW Analysis is performed to prioritise these requirements [295]. It is beneficial for development projects to avoid any Scope Creep, which can result in project delays [303]. Therefore to ensure timely delivery of the Ransom*A*ware game, requirements were analysed to prioritise

the functionalities embedded during the development process. [304]. **Figure 5.3** provides details of the MoSCoW prioritisation technique applied to the requirements of the Ransom*A*ware, showing the requirements which will be included in the game design process and recommendations for future iteration.

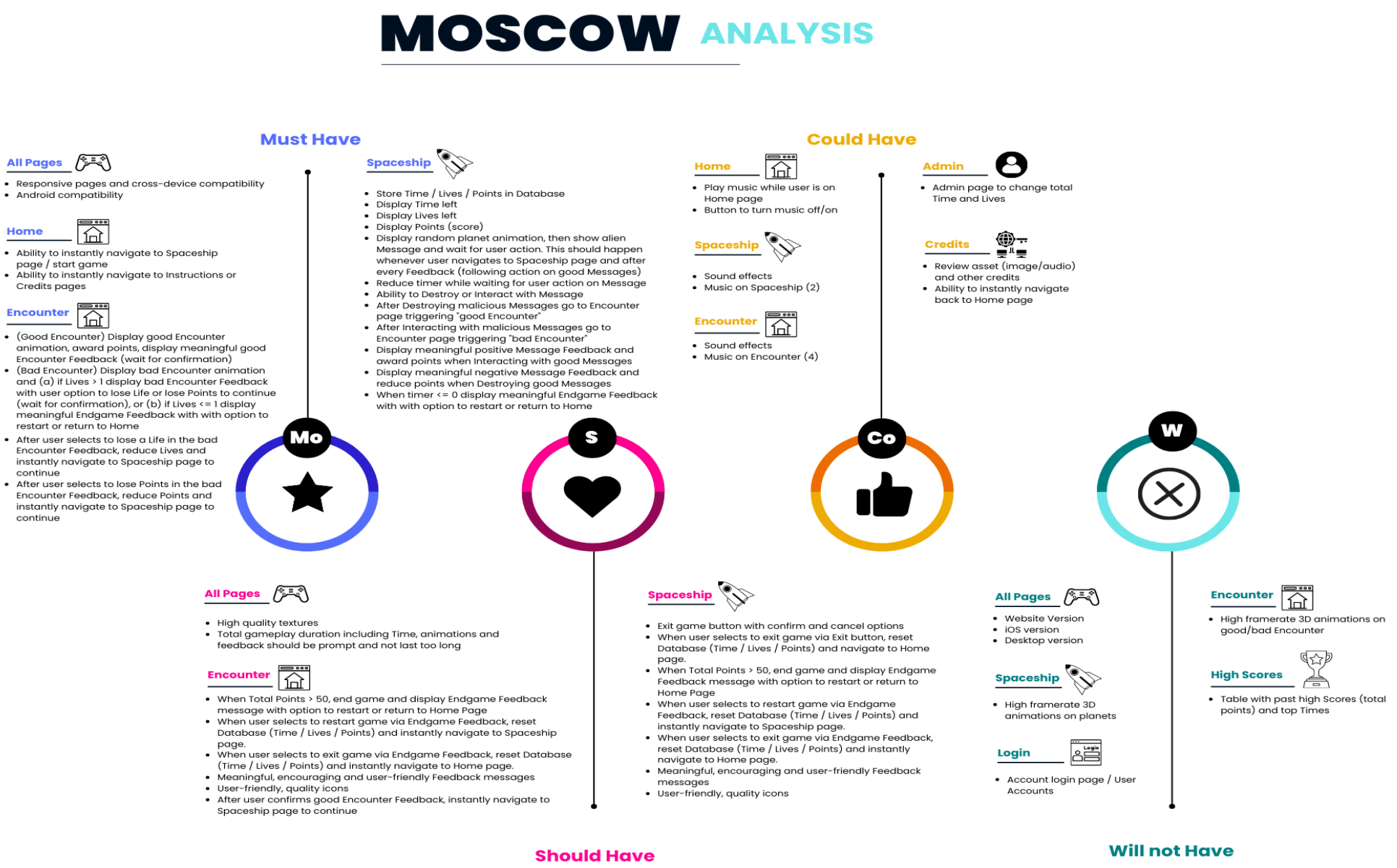

Figure 5.3: MoSCoW Analysis

5.6 Task Modelling to Achieve Usability

UI/UX Analysis: Various Task Modelling exercises and User Journeys were created to transform the identified User Needs into application architecture and navigation [305]. Together with the proposed User Personas, these can demonstrate how different users will achieve their tasks and goals while interacting with the application. As [306] states, task maps (showing all steps involved in a particular user task) can get very complicated, especially in complex projects. Hence, the focus must be placed on the most critical tasks in achieving each goal. Furthermore, adding extra functionality usually comes at the cost of usability due to increased system complexity [307]. Task Models / User Journeys can depict how easily users can achieve their goals and maintain the balance between complexity and usability.

5.6.1 Task Model 1 - Read Game Instructions

Opening the Game Ransom*A*ware takes the users to the Home screen. User press the "Read Instructions" button. This navigates the user to the Read Instructions pages. Selecting the "Back to Home" button will take the user to the Home screen.

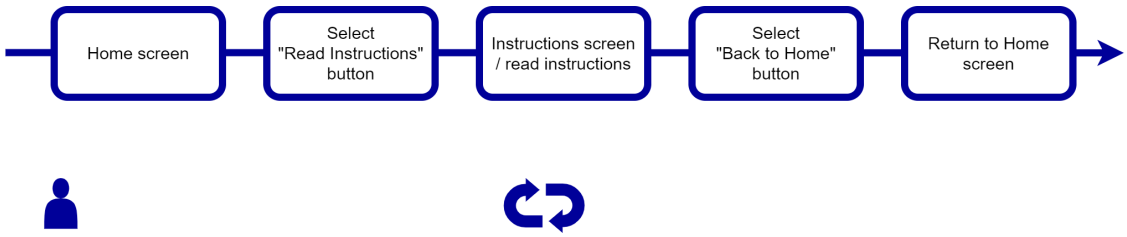

Figure 5.4: Read Game Instructions

5.6.2 Task Model 2 - Delete or Interact with The Alien Message

From the Home screen. The user clicks on the "Play Game" button. The game starts with the user onboard the spaceship. The planets displayed messages and prompted the user to make the decision. The user goes through a complex evaluation (Legit-

imate sender address?/ Professional wording?/ Requests private information/ Has attachments?/ Unsolicited communication?/ Other criteria) as to whether accept or delete the message. Depending on the user's action, the spaceship dashboard will be updated with a reward or penalty.

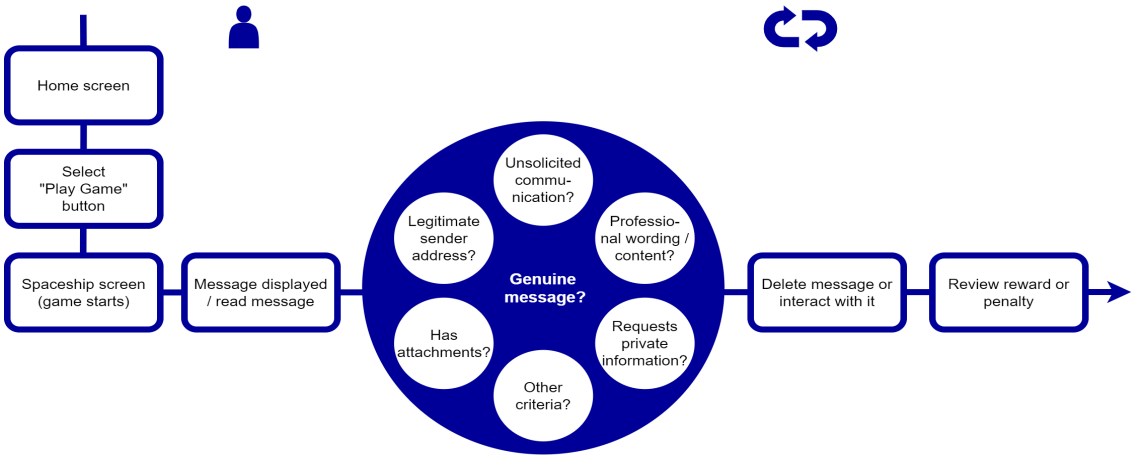

Figure 5.5: Delete or Interact

5.6.3 Task Model 3 - Exit a Game

From the Home screen, the user selects the "Play Game" button and onboard the spaceship. If a user needs to exit the game at any point. The user clicks the "Exit Game" button from the spaceship dashboard. This will prompt a message, asking the user to confirm the game exit. Once the exit option is confirmed, this will take the user back to the home screen.

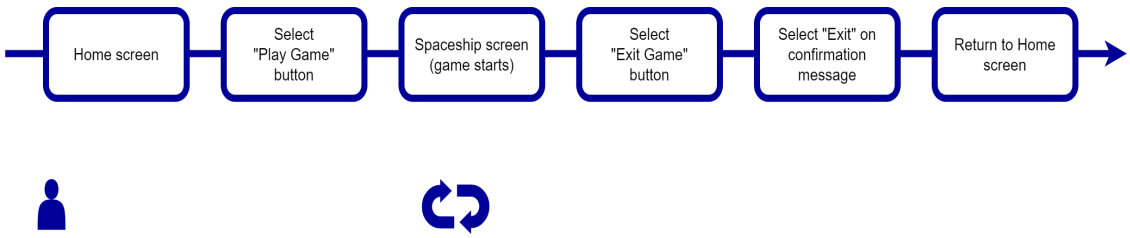

Figure 5.6: Exit a game

5.7 User Journeys to Implement Usability

UI/UX Analysis: User Journeys is another UX analysis technique that provides a user's walkthrough [308] on how the user performs a task and identifies any opportunity to optimise the user's experience [309]. In the context of game design, journey maps were utilised to visualise the user's experience with the Ransom*A*ware game design.

5.7.1 User Journey 1 - Time, Score and Feedback Review

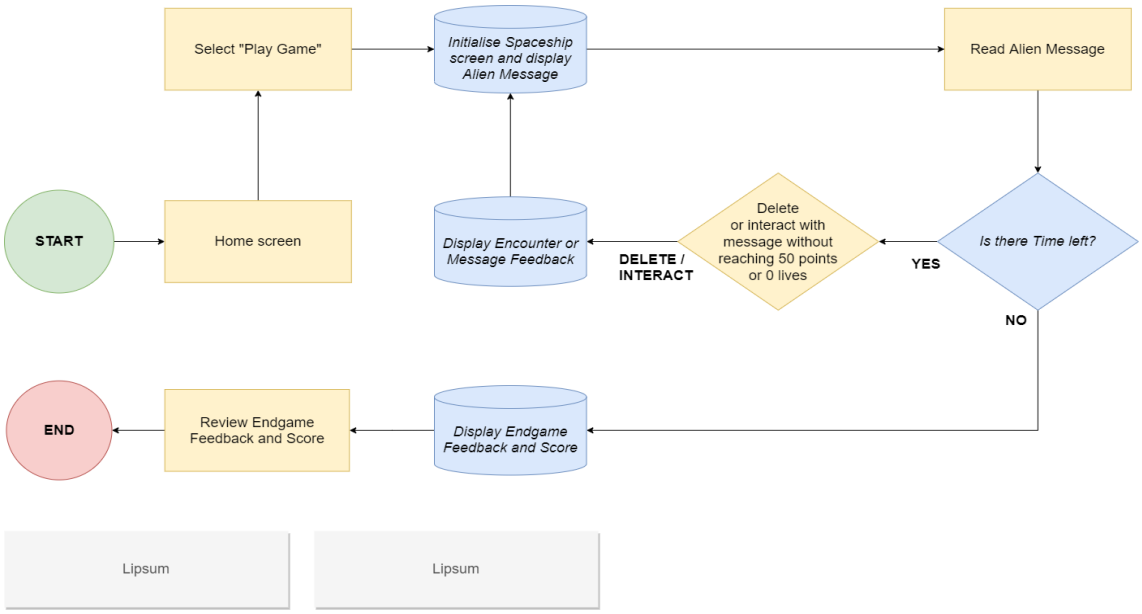

Figure 5.7: User Journey 1

The following abbreviations will be used to translate the map.

S: start, A: user action, D: user decision, SA: system process, SD: system decision, E: End

S

> A: Home screen

> A: Select "Play Game."

> SA: Spaceship screen/display message

> A: Read the message

> SD: Is there time left?

(No) > Connection to "SA: Display Endgame feedback and score."

(Yes) > Connection to "A: Read the message."

> D: Delete or interact with messages without reaching 50 points or 0 lives

> Connection back to "A: View message."

> SA: Display Endgame feedback and score

> A: Review Endgame feedback and score

> E

5.7.2 User Journey 2 - Pay Ransom

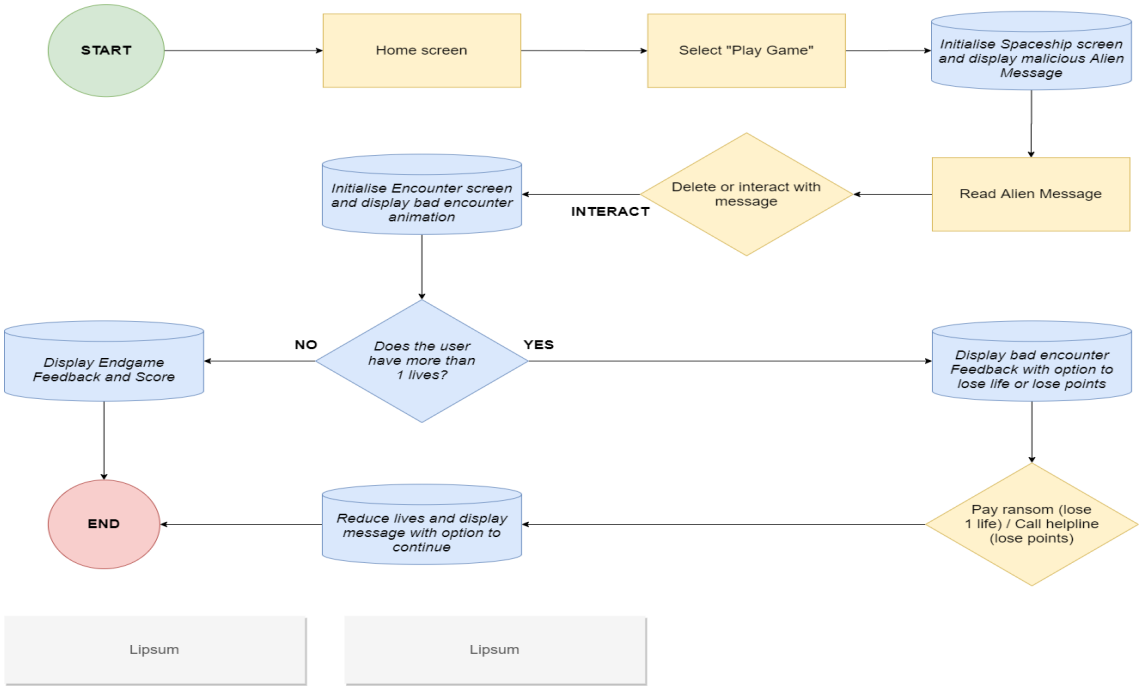

Figure 5.8: User Journey 2

S

> A: Home screen

> A: Select "Play Game."

> SA: Spaceship screen/display malicious message

> A: Read the message

> D: Delete / interact?

(Interact) > SA: Encounter screen/display bad encounter

> SD: Does the user have more than one life?

(yes) > SA: Display bad Encounter Feedback with the option to lose life or points

> D: Pay the ransom

> SA: Reduce points and display feedback with the option to continue

> E

(no) > SA: Display Endgame feedback and score

> E

5.7.3 User Journey 3 - Delete Good Message

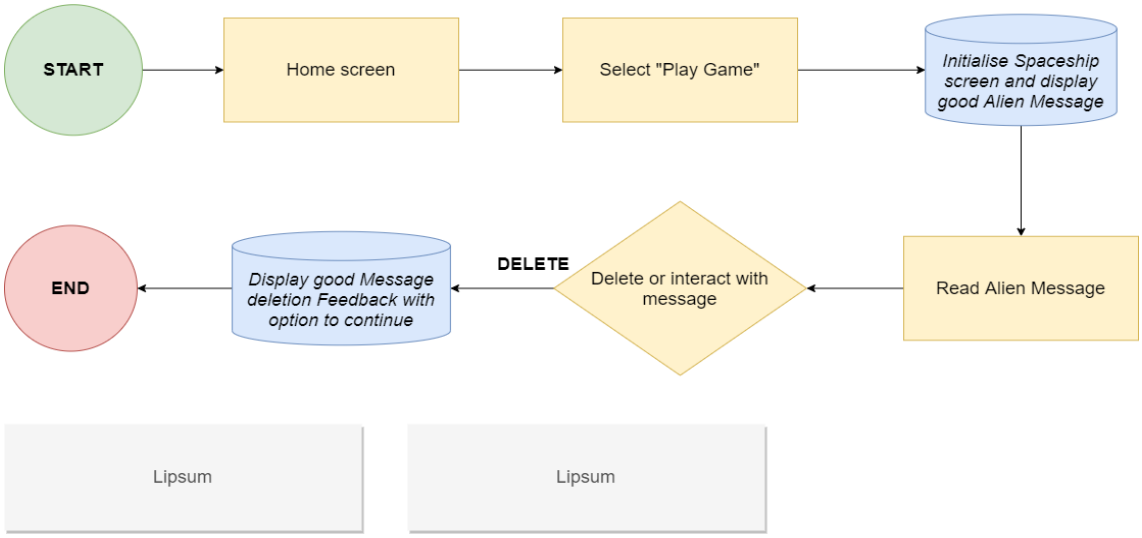

Figure 5.9: User Journey 3

S

> A: Home screen

> A: Select "Play Game."

> SA: Spaceship screen/display good message

> A: Read the message

> D: Delete / interact?

(Delete) > SA: Display good message deletion feedback with the option to continue

> E

5.8 Game Ransom*A*ware Architecture

Design Phase: The architecture is concerned with the system design from the developer's context. It links the design and requirements [310]. **Figure 5.10** shows the structural components of the Ransom*A*ware game design. The current research aims to develop a Ransom*A*ware game using on MIT App Inventor platform. From the developer context, The game can run on a personal computer or an Android-based smartphone. The game architecture allows the developer to conceptually and logically view the design before proceeding to the development phase [310]. The architecture is divided into two layers showing how usability and elements of TTAT will communicate in the front and back-end of the game to make an efficient and effective design.

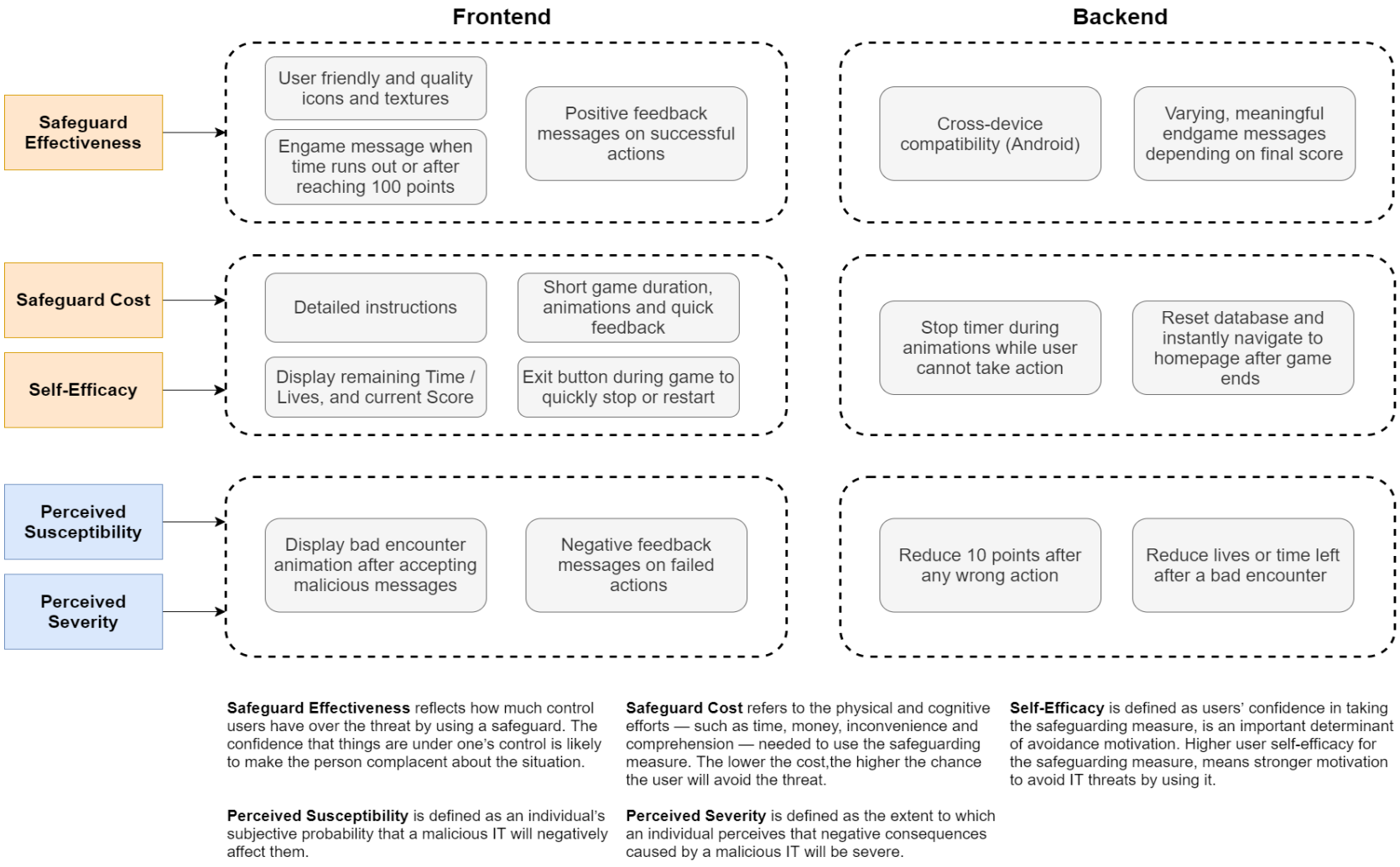

Figure 5.10: Ransom*A*ware Architecture

5.9 Wireframes Walkthrough of Ransom*A*ware

Design effectiveness and efficiency are essential for usability [311]. Wireframes are important in designing digital interactions and applications and were used to present the layout of various screens in the Ransom*A*ware app. As [312] mention, from the early stages of design, wireframes can save time and expenses by effectively expressing ideas and connecting back-end concepts to the front end. Although wireframe design can require experience and skill to accomplish, which implies a learning curve, it can aid with communicating elaborate functionality in high detail. The wireframes **Figure 5.11-14** illustrate the proposed Ransom*A*ware game components and design structure.

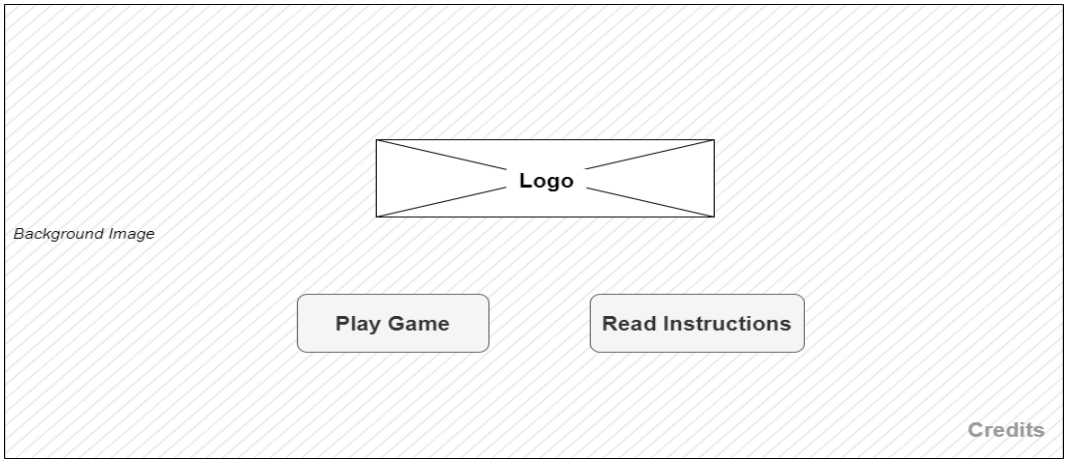

Figure 5.11: Homepage

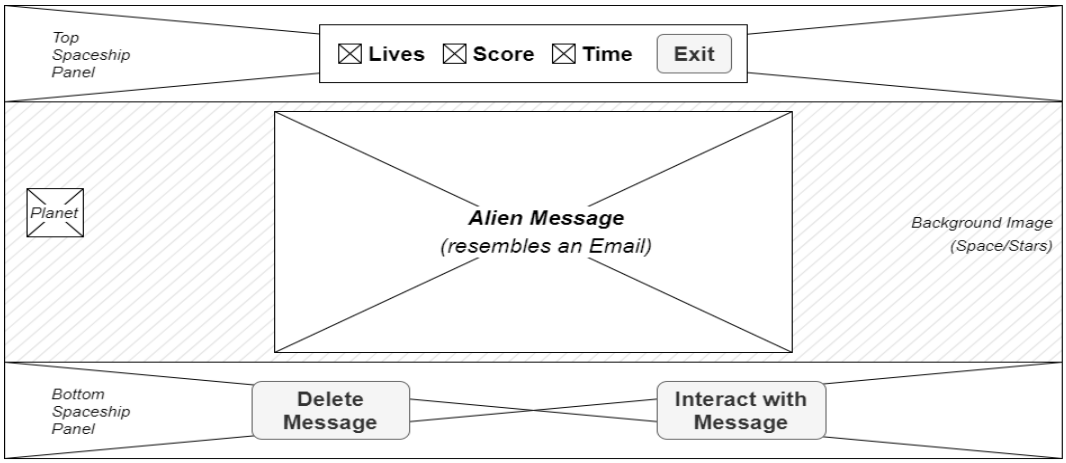

Figure 5.12: Spaceship Alien Message

Figure 5.13: Feedback Message

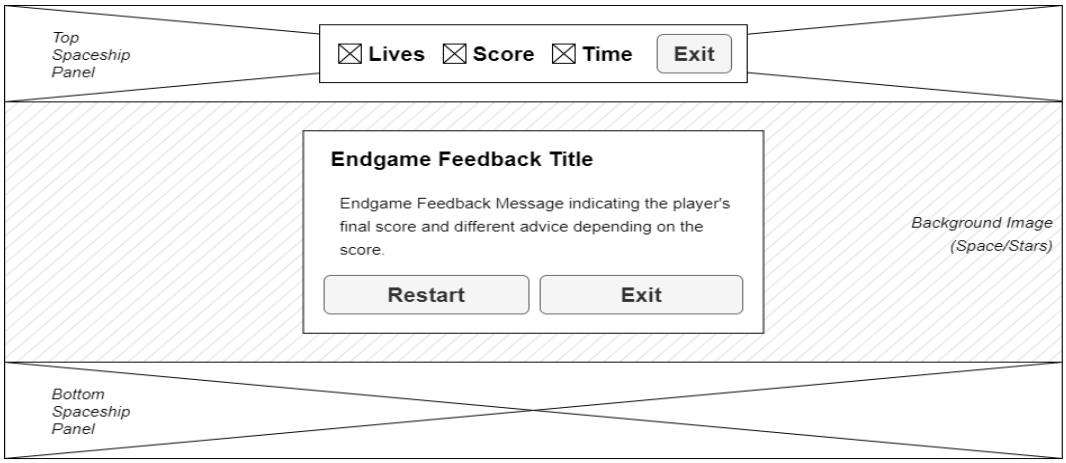

Figure 5.14: Spaceship EndGame Message

5.10 Game Development Phase

The current study adopted MIT App Inventor to develop a Ransom*A*ware game. It is a platform focused on quickly building mobile applications in a drag-and-drop interface, initially developed by Google in 2009 [313]. The project was moved to MIT in 2011, where it is still housed and has received tremendous popularity and numerous updates. As [314] notes, App Inventor promotes digital literacy by enabling developers to focus on programming logic for their app rather than code syntax. App Inventor allows for fast, iterative design without in-depth programming knowledge while promoting continuous application testing using built-in blocks representing

programming concepts such as functions, event listeners or logical and mathematical operators [315]. The walkthrough snippets below show the development process of the Ransomware Game.

Figure 5.15: Ransom*A*ware Home Screen

Snippet 1: Ransom*A*ware Live Dashboard

Figure 5.16: Ransom*A*ware Dashboard

The Ransom*A*ware application uses global variables to keep track of player' lives' (a counter that gets reduced after wrong decisions and indicates the end of the game when it reaches zero), total points so far (the player score), remaining time until the game ends and the 'alien message' to be displayed next. The code blocks demonstrated in **Figure 5.17** handle these global variables via three procedures:

- 'get_db_values' is called when the game starts and sets the aforementioned global variables with starting values: 3 lives, 0 points, 180 seconds of game time remaining and a random number from 0 to 19 for the first message to be displayed (out of a pool of 20 messages)

- 'store_values_in_db' is called at various points during the game after player decisions, storing the values of these variables in the database, from where they can be read or updated later in any application screen

- 'set_stats_values' is called again after player decisions and uses the lives, points and time variables to update in-game indicators that instantly inform the player of their values during the duration of a game

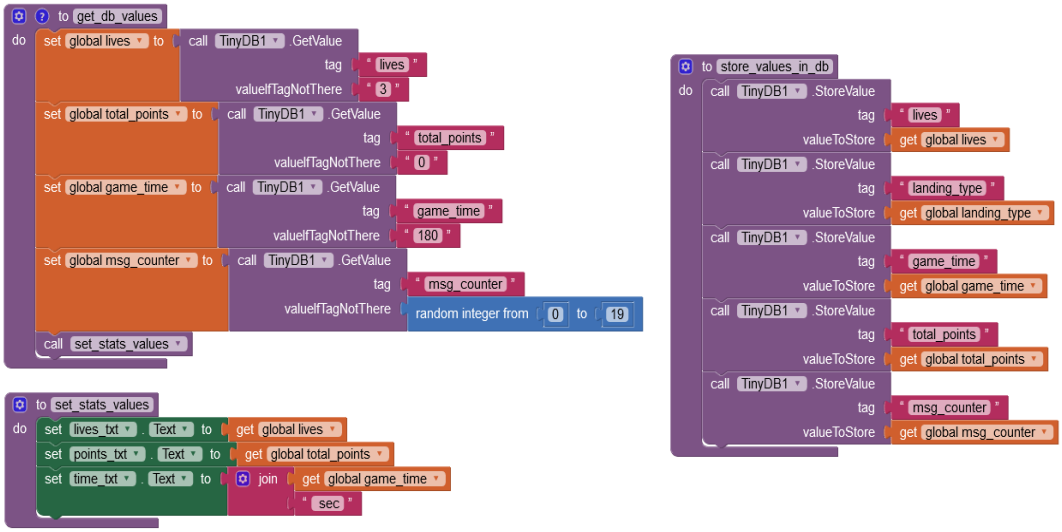

Figure 5.17: Utilising global variables for key status indicators

Snippet 2: Control Planet Animations

The planet to be displayed each time is selected randomly from a pool of 8 potential planets of the solar system. The animation displays nine images of the planet in quick succession, a process controlled via the 'planet_animation_clock' timer. An indicative approaching planet animation can be seen in **Figure 5.18**.

The 'initScreen' procedure in **Figure 5.19** is automatically called when the player starts the game and enters the spaceship cockpit screen. It is responsible for setting and displaying key in-game indicators and also initiate the 'showMessage' procedure. 'showMessage' first checks if the player's score has reached 100,

Figure 5.18: Approaching planet animation

showing the player a rewarding endgame message. If not, it stops the time, enables the 'planet_animation_clock' timer, which sets off the animation of an approaching planet, and hides the player 'Accept' and 'Reject' message controls. After the planet animation, the 'display_msg' procedure is called to display an alien message on the screen.

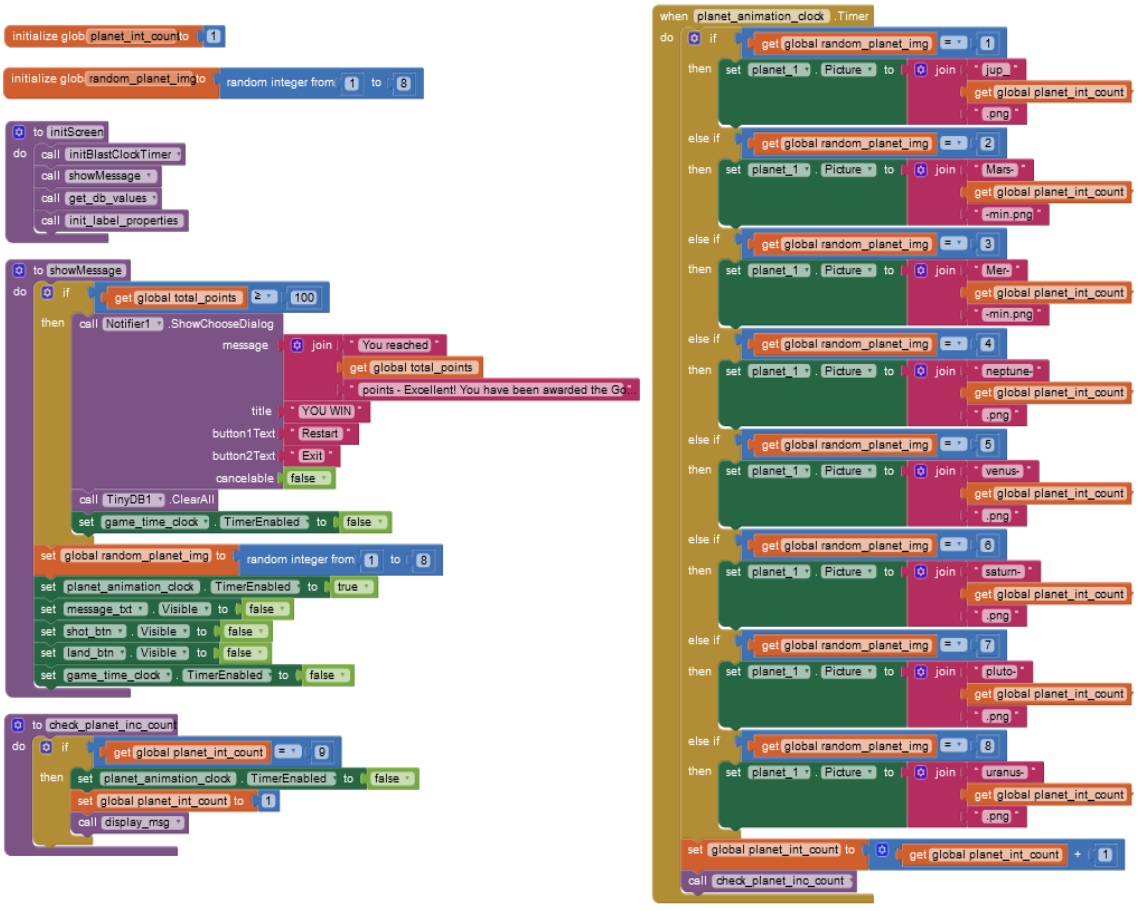

Figure 5.19: Control planet animations

Snippet 3: Display Alien Message and Increase Message Counter

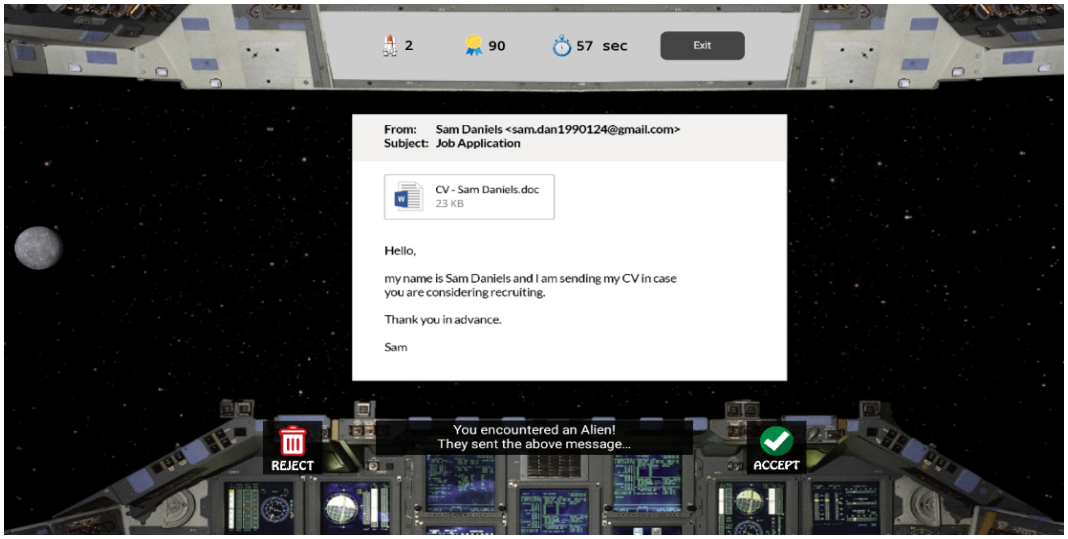

Figure 5.20: Display alien message

The 'inc_msg_counter' procedure, ' display_msg', increases the message counter by one before displaying the message. The message counter is used to determine the file name of the message image. This way, a new message is displayed every time the procedure is called following the planet animation. After the message has been displayed, the 'Accept' and 'Reject' buttons appear on the screen to allow the player to take action depending on the message. The game timer also starts running at this point until the player makes a decision.

The 'display_msg' procedure displays an alien message on the screen. The message to be displayed is selected based on the global variable 'msg_counter', which holds a number from 0 to 19 and has been initialised with a random number in this range when the game starts. The procedures controlling this behaviour are demonstrated in **Figure 5.21**.

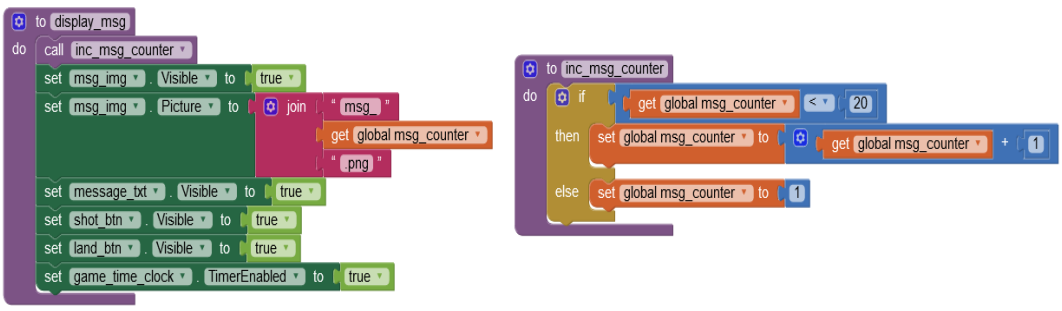

Figure 5.21: Display alien message and increase message counter

Snippet 4: Decrease Game Time while the Game Time Clock Timer is Enabled

The 'game_clock_timer' becomes enabled after the message has been displayed. Every timer used in the application runs every second until disabled, executing all routines and commands in its block.

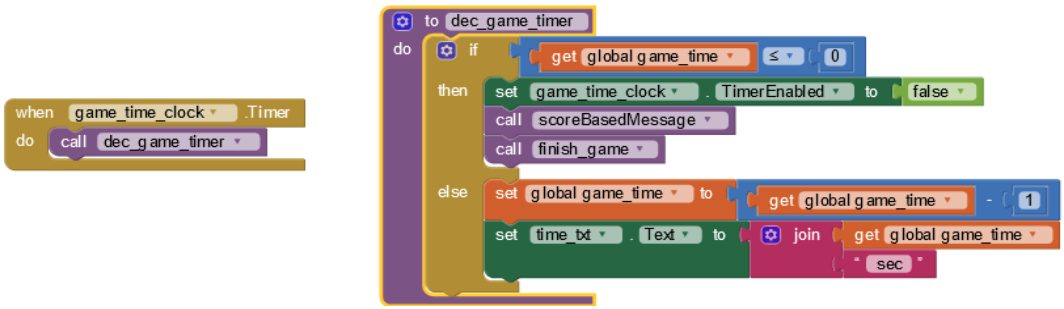

Figure 5.22: Game timer procedure

The 'game_clock_timer' calls the 'dec_game_timer' procedure, which decreases the value of the 'game_time' global variable by one, and updates the on-screen text displaying the remaining time with its value. If the 'game_time' reaches zero, the endgame message notification is displayed (*see Snippet 7*) through the 'scoreBasedMessage' procedure, and the 'finish_game' procedure is called to end the game.

Snippet 5: Determine What Happens After a User Clicks on Accept Message Button

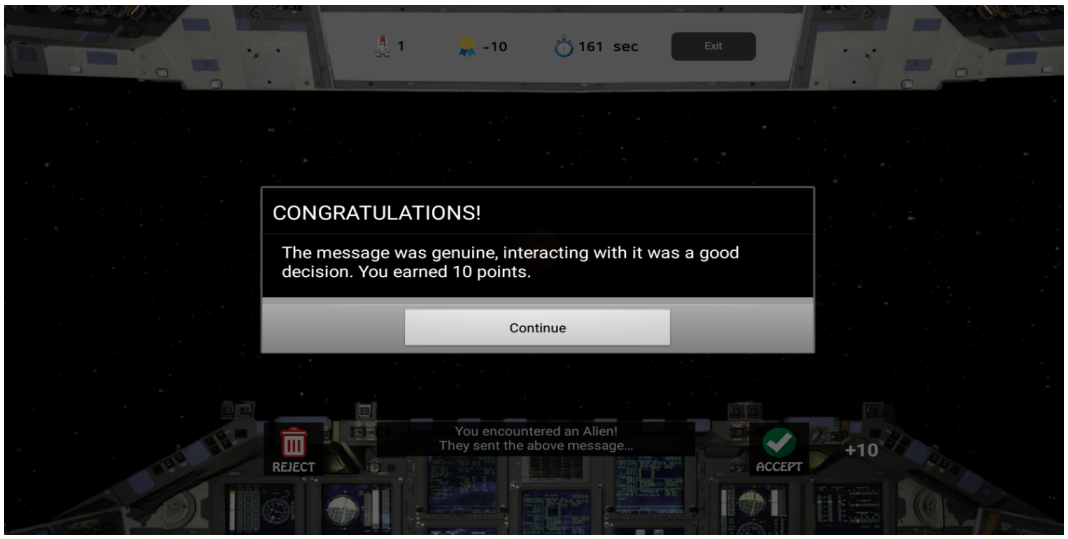

Figure 5.23: Notification Displayed After Accepting a Genuine Alien's Message

Whenever an alien message is displayed, the user is presented with the option to accept or reject it based on its content, as explained in Snippet 3, **Figure 5.20**. The 'Accept' button triggers the 'land_btn' code block, shown in **Figure 5.24**. The 'land_btn' code block stops the time by disabling the 'game_time_clock' timer and hides the alien message. Afterwards, it will do the following depending on the type of message displayed:

- If the message is malicious, the 'bad_landing' procedure is called, which will update the global variable 'landing_type' to 'bad_landing' to store the fact that the player accepted the malicious message. The 'bad_landing' procedure will initiate a new application screen that will display a relevant animation to the user (*see Snippet 6*).
- If the message were genuine, a feedback message would be displayed on the screen, informing the user of their correct decision. This is demonstrated in **Figure 5.23**.

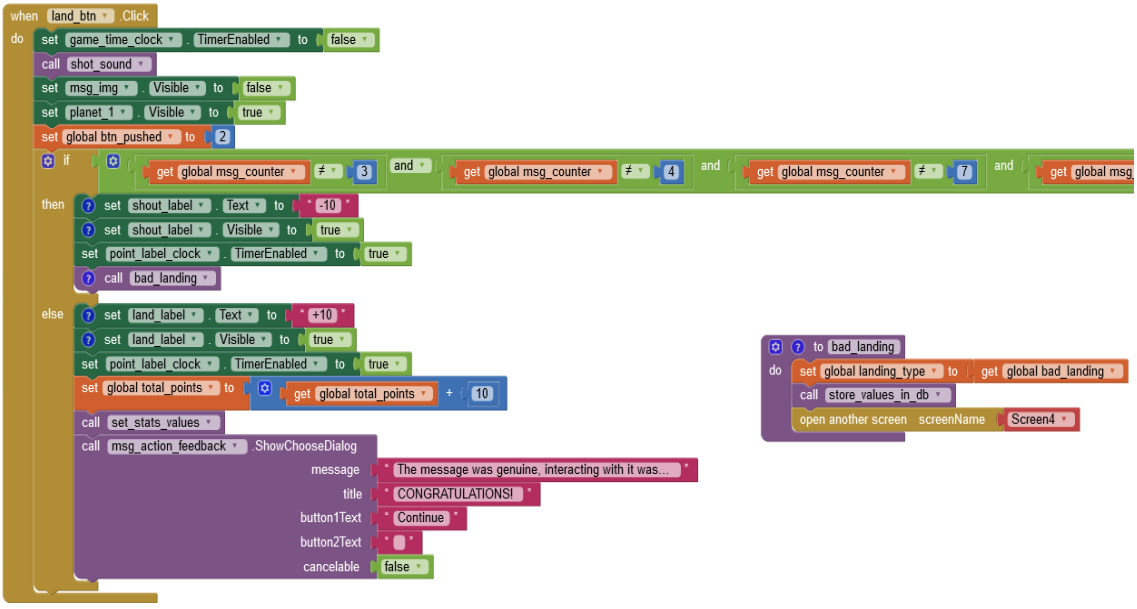

Figure 5.24: The land button code block executed when the user accepts an alien message

Snippet 6: Display Good or Bad Landing Sequence

After the player selects the 'Accept' or 'Reject' button on a malicious message, a new screen is initiated to display a relevant animation. After the new screen

loads, an initial animation shows an alien ship scanning the player's spaceship. Afterwards, if the player's decision is correct, a 'good_landing' animation is initiated, showing the player's spaceship defeating the alien ship. If the decision is wrong, a 'bad_landing' animation is initiated, and the alien ship is shown to attack the player's spaceship. To check if the player's decision was correct or wrong, the code checks the global variable 'landing_type', which was set earlier, as explained in Snippet 5. The procedures controlling this behaviour are demonstrated in **Figure 5.26**. The stages of the alien ship scanning the player spaceship and indicative screenshots of the good and bad animation sequences are demonstrated in **Figure 5.25**, **5.27** and **5.28**.

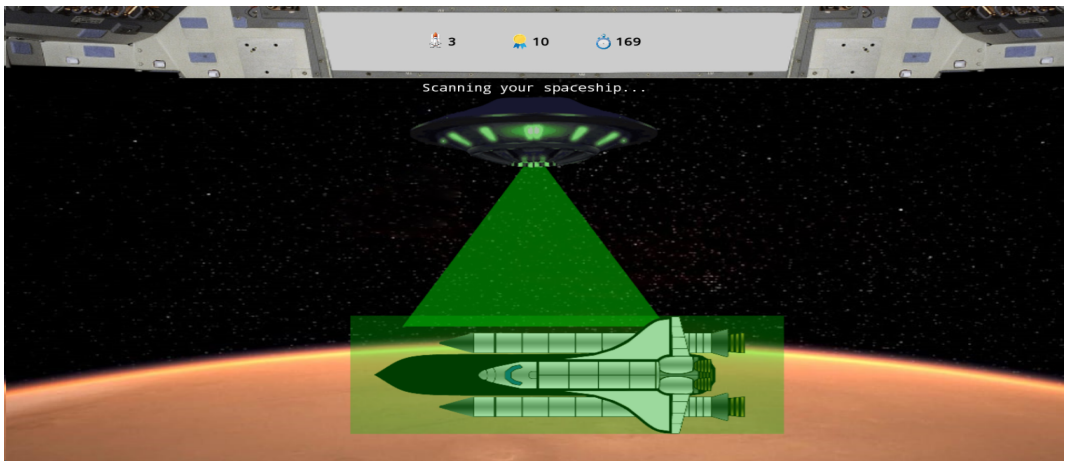

Figure 5.25: Animation of Alien ship scanning the player

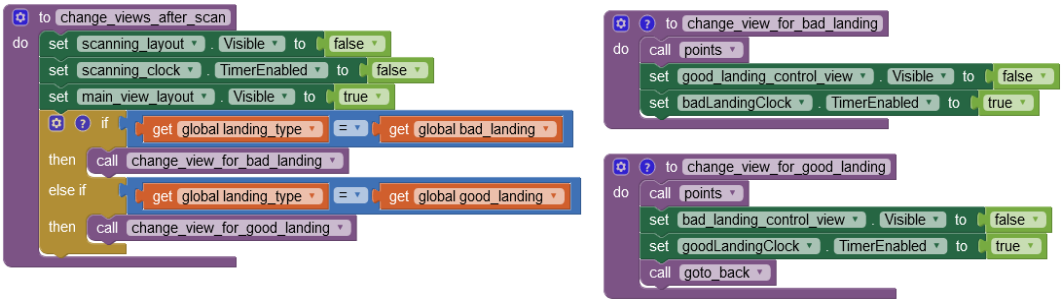

Figure 5.26: Procedures controlling the display of the good or bad alien animation sequence

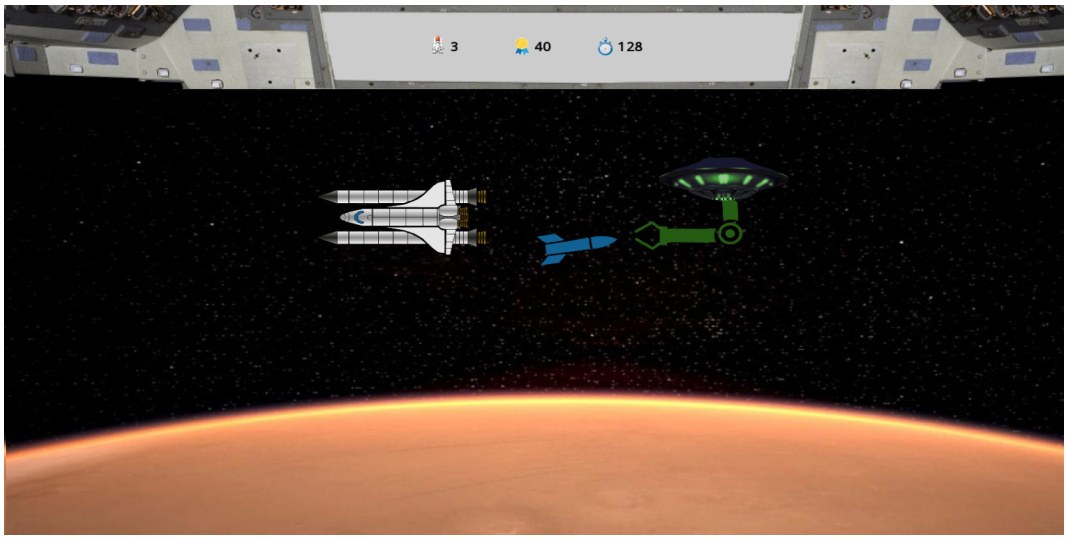

Figure 5.27: Player defeating the Alien

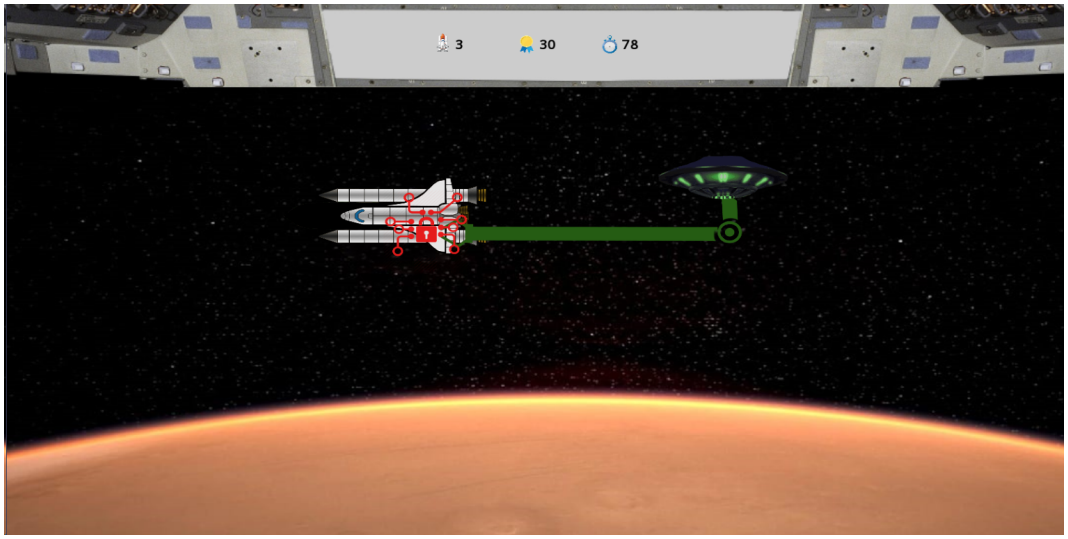

Figure 5.28: Alien ship attacking the player depicting successful Ransomware Attack

Snippet 7: Display Endgame Notification Depending on the Score

The 'dec_game_timer' procedure discussed in Snippet 4 earlier checks if the time has reached zero. If yes, it calls the 'scoreBasedMessage' procedure, which will determine the endgame message depending on the player's final score, and store it in the 'scoreMessage' global variable. The 'finish_game' procedure is called afterwards to display the endgame message stored in the 'scoreMessage' global variable on the screen, inform the player of their performance and advise them on actions to improve. The 'finish_game' and 'scoreBasedMessage' procedures discussed above are shown on **Figure 5.29**.

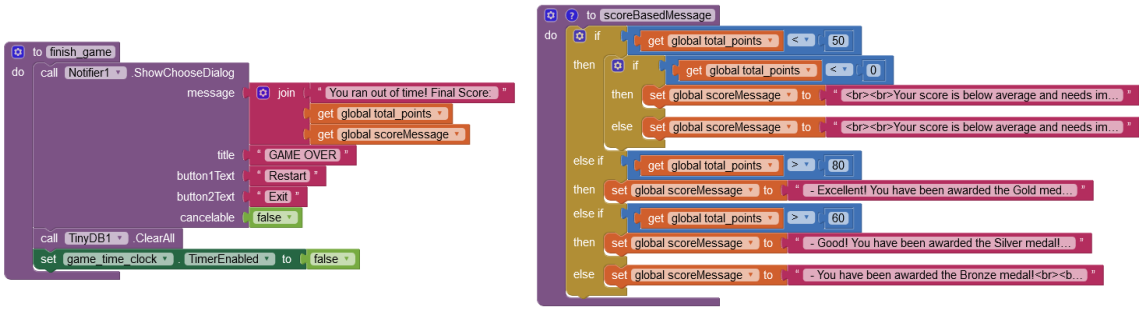

Figure 5.29: Procedures determining and displaying the endgame message

The endgame message also allows the player to restart or exit the game. Finally, the 'finish_game' procedure clears all variables stored in the database to prepare it for a new game.

Indicative endgame messages, depending on various final scores, can be seen in Figure **5.30, 5.31** and **5.32**.

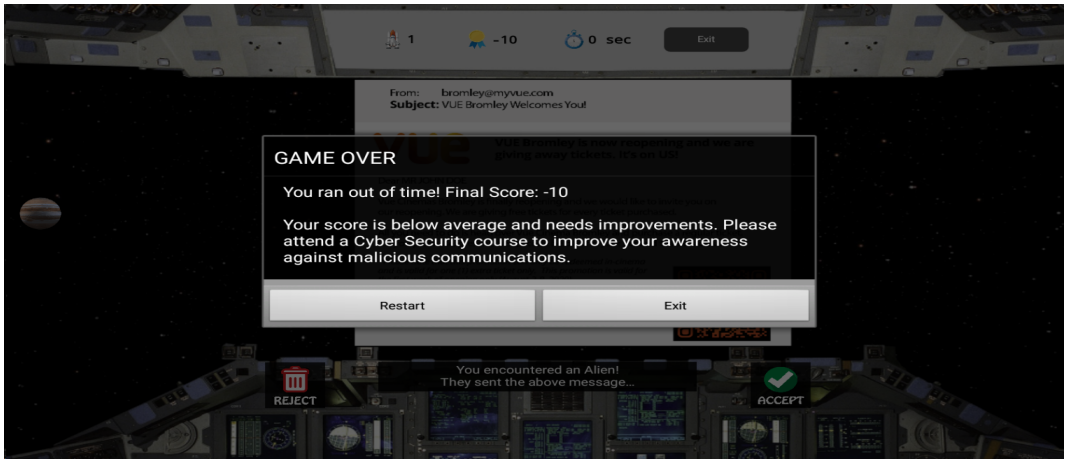

Figure 5.30: Endgame feedback message for a final score of 10

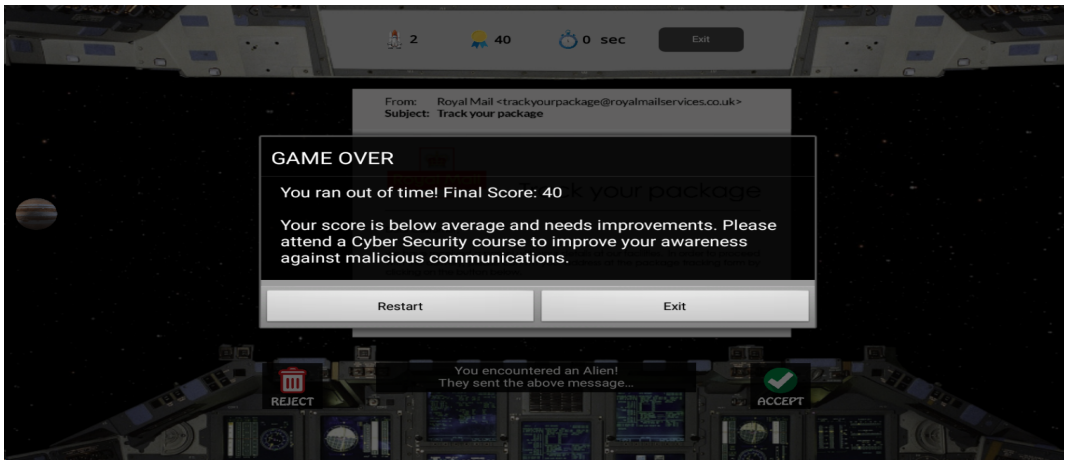

Figure 5.31: Endgame feedback message for a final score of 40

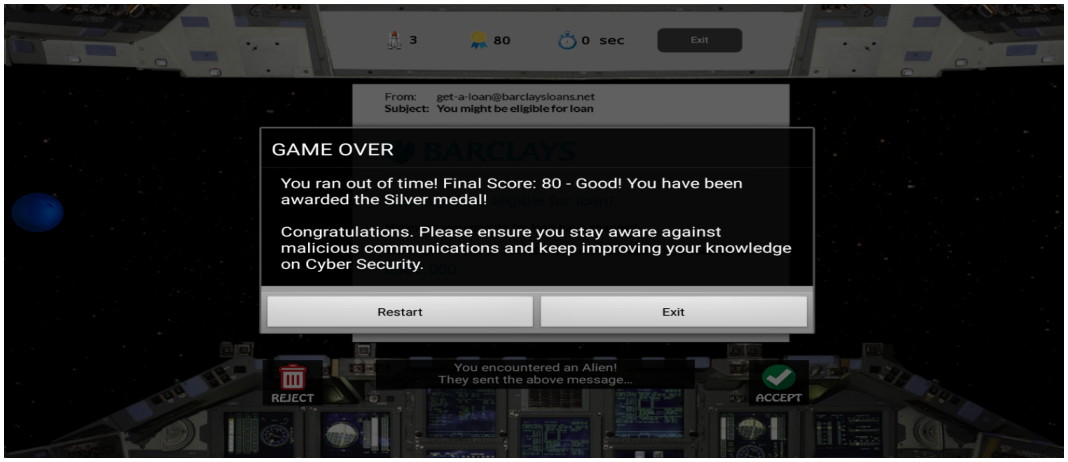

Figure 5.32: Endgame feedback message for a final score of 80

5.11 Developers Testing Ransom*A*ware

As [316] analysed, testing is vital in a development project to identify problems, fix them, and improve quality. Various testing techniques exist and aim to test usability, performance, functionality, integration and other areas, potentially involving developers and users depending on each technique. [316] Further note that these testing techniques are categorised between Black Box and White Box testing, which test the system's external and internal behaviour. In contrast, Grey Box testing can be used to test both. From the development context, to ensure coding is free of errors, the code was thoroughly reviewed using the Black box technique. The heuristic technique was used to analyse user engagement with the Ransom*A*ware game [317]. The testing at this step was performed from the developer's context.

The next chapter will provide detailed empirical testing of the game design.

5.12 Summary

The chapter concludes with designing and developing a working game called Ransom*A*ware. The current research aims to improve user awareness of ransomware using game-based learning. The design and development process adopted a Unified User Experience Development Methodology (U*X*D). This methodology offers a rigorous process to implement user experience in the game design, underpinned with development methodology to follow from the developer context to ensure an efficient and effective game is delivered which is fit for its purpose. The game architecture was also examined to ensure elements of TTAT are successfully embedded, so they can effectively communicate between the front and back-end of the game.

Chapter 6

Ransom*A*ware Testing and Evaluation

6.1 Overview

Chapter Six: This chapter evaluates the Ransom*A*ware game introduced in Chapter 5 of this research thesis. The Ransom*A*ware is a game developed using the MIT App Inventor emulator and based on the TTAT of (Liang & Xue) [141]. This is *Study 2* of the current research. It adopts a mixed-method approach to evaluate the game empirically. It includes four steps evaluation process, i.e., (i) a pre-experiment questionnaire to assess the user's understanding of the cyber security threat ransomware, (ii) Gameplay - Ransom*A*ware, aiming to improve user awareness against ransomware cyber security threat, followed by usability test using System Usability Scale (SUS) questionnaire to assess user's satisfaction of the game design, (iii) Post-experiment questionnaire to evaluate the Ransom*A*ware effectiveness in improving user education and awareness against the ransomware and (iv) Semi-structured interviews. The study employs both the pilot and the main study. The subsequent section of this chapter will provide a discussion on data collection techniques, experimental design, results analysis and chapter summary.

6.2 Feasibility Study 2 of The Current Research

Two studies were designed in the current thesis. Study 1 in Chapter 4 reports TTAT elements, i.e., perceived severity, perceived susceptibility, perceived threat, Safeguard effectiveness, Safeguard cost, and Self-Efficacy, are critically important to be included in the game design to motivate users against the malicious IT ransomware. The findings show user's avoidance motivation is significantly determined by the user's perceived threat ($b = 0.25, p < 0.05$), which is significantly determined by perceived susceptibility ($b = 0.21, p < 0.05$) and perceived severity ($b = 0.26, p < 0.01$). Similarly, coping appraisal using safeguard measures, i.e., safeguard effectiveness ($b = 0.31, p < 0.05$), self-efficacy ($b = 0.23, p < 0.01$) and the interaction of safeguard effectiveness and perceived threat ($b = -0.12, p < 0.05$) significantly influence user motivation and user's avoidance behaviour is significantly determined by avoidance motivation ($b = 0.54, p < 0.01$). These findings are in line with the previous studies of Liang & Xue [141]. The model explains 55% variance in user avoidance motivation and 29% in avoidance behaviour, which is significant and supported by previous studies [240], [141]. Thus, these findings were input into Chapter 5 to be implemented during the Ransom*A*ware game design and development. Whereas Chapter 6 presents Study 2 of the current thesis, which evaluates game Ransom*A*ware and validates that the findings of Chapter 4 are successfully embedded in the game design.

To determine the feasibility of current studies, a pilot study was conducted. The aim was to assess any changes required to improve the Ransom*A*ware game design ahead of the main studies [229]. The current studies evaluate user satisfaction with the game Ransom*A*ware during a pilot study through conducting a usability test. The game evaluation is important at this stage because it aims to improve user awareness of the ransomware cyber threat through user engagement. To assess whether game-based learning achieves its purpose, i.e., the participant finds the game a usable solution to their learning needs against the cyber security threat ransomware. Therefore, user satisfaction is an important part of the game evaluation during the pilot study. This will help the research studies assess if any improvement is required to the Ransom*A*ware design prototype.

An experimental process was set up as part of the evaluation process. Users were asked to play the game, followed by semi-structured interviews to assess their satisfaction with the game design. Thematic analysis was employed to assess users' opinions collected through semi-structured interviews [318]. The pilot study included pre-test and post-test in addition to subjective satisfaction to evaluate any change to user's knowledge and awareness against the ransomware cyber security threat. Findings from usability experts [319] and [320] suggest that most usability problems can be identified with fewer users. Therefore, the current pilot study employed 15 participants to test user satisfaction with the Ransom*A*ware game design. Before the pilot study was conducted, the participants were briefed about the purpose and procedure of the test.

The pilot studies included experimental evaluation of the game-designed prototype and employed a mixed-method data collection approach. The quantitative data collection approach was employed to analyse data collected during the pre-test, post-test and System Usability Scale (SUS) [225]. The SUS usability questionnaire was set up using a 5-point Likert style to assess the usability of the Ransom*A*ware game. The qualitative data collection technique was employed during semi-structured interviews to ensure TTAT elements are embedded in the Ransom*A*ware design [321]. SUS consists of 10 questions, the initial data collection through the questionnaire reported some difficulty in the interpretation of Question 8, i.e., '*I found the RansomAware game very cumbersome to use*' due to the word 'cumbersome' by some non-native English participants [225]. This word was replaced with the word 'inconvenient', so participants from wider society can easily interpret all the questions to provide robust feedback related to game design usability. The average SUS score of 73.53 was reported during the pilot study, which is acceptable for any usability test, as suggested by industry experts [322].

6.3 Study 2 - System Usability Scale Test

The main studies employed a sample of 30 participants to test user satisfaction with the Ransom*A*ware game design. Although people between the ages of 18-25 are reported to be more vulnerable to phishing [323], however as ransomware is

a threat to individuals and businesses [323], the scope of current studies is in the wider context for both, i.e., individual users and professionals. Therefore sample respondent size was chosen within the range of 18-55 from a wider discipline of society. This includes individual home users, University graduates, and working professionals from a range of professions who have experience with smart devices such as mobile phones, tablets and internet usage. Ethical approval was granted before the pilot study, and participants were administered through MS Teams due to COVID restrictions on face-to-face meetups. Participants' demographics are shown in **Table 6.1.**

Table 6.1: Participants' demographics

Measure	Item	Amount
Gender	Male	19
	Female	11
Age	18-25	7
	26-35	12
	36-55	11
Smart device	Mobile	17
	Tablet	4
	Computer	9
Internet Usage per day	1-3	3
	4-6	14
	7 or more	13

6.4 Data Collection Procedure

The current main studies aim to evaluate the effectiveness of the game 'Ransom*A*ware' in improving users' education and awareness against the ransomware cyber security threat and require participants to involve in a practical task. Due to covid restrictions and safety considerations of the participants, it was decided to conduct an online test. The participants were carefully selected to ensure they could access the internet, a smart device, or a computer.

Study 2 consists of four phases, which required the users to participate in a pre-test questionnaire in the *first phase*. The questionnaire was designed on the latest guidelines of the national cyber security centre UK (NCSC, 2021) on ransomware awareness. It consisted of 10 questions to assess users' awareness of ransomware cyber security. In the *second phase*, the participants were given 15 minutes to play the Ransom*A*ware game. The game was designed and developed based on the TTAT framework as a part of the current studies to improve users' education against the ransomware cyber security threat. The participants were offered remote online support if anyone needed help setting up the game or had any other queries. After

completing the gameplay, users were requested to complete the 'System Usability Scale' questionnaire [224] to evaluate the user's satisfaction of the Ransom*A*ware design. In the *third phase*, users completed a post-test questionnaire of 10 questions designed on NCSC guidelines on ransomware awareness. The results from the first and third phases were compared to assess the effectiveness of Ransom*A*ware gameplay on users' awareness of the ransomware cyber security threat. The *fourth phase* was optional. Users were requested to participate in semi-structured interviews. This approach was useful in eliciting more information from the respondents on their subjective satisfaction with the game Ransom*A*ware.

6.5 Data Collection Instrument

The main studies adapted John Brooke's system usability scale (SUS), as shown in **Figure 6.2** to evaluate the user's satisfaction with Ransom*A*ware the game design. SUS was developed by [225] and is considered a reliable and low-cost measure to assess the design's usability. The scale consists of 10 questionnaire items, which are used to evaluate the user's satisfaction with Ransom*A*ware design, with a focus on the appropriateness of game design for its purpose [225]. While the game Ransom*A*ware aims to improve user awareness against ransomware cyber security threat, usability is an important factor for the game design to provide users with a seamless experience to engage in their learning against the threat. If users find the game difficult to play or fail to complete the game activity provided, this will compromise the purpose of the game design prototype. Hence SUS usability test was carried out in the main study to ensure the game design fits its purpose in the context of user awareness of the cyber security threat ransomware.

Several authors also support the idea of a usability test [324], defining usability as a prime goal for a product design and recommending a user-based evaluation to assess the design's usability. Therefore, the SUS evaluation questionnaire is adopted during the main study to assess the usability consideration in Ransom*A*ware game design. The idea of user-based usability evaluation criteria is also considered an effective method by the international organisation for standardisation ISO-9241-11 framework on user's perception of design effectiveness and satisfaction for its con-

text [325]. Therefore the main study employed SUS questionnaire to evaluate the user interaction with the game Ransom*A*ware [324]. In comparison to other usability measures, such as Computer System Usability Questionnaire (CSUQ) and Questionnaire for User Interface Satisfaction (QUIS), SUS is found to be a reliable usability measure for smaller sample sizes [326]. Moreover, when compared with other usability questionnaires, i.e., (SUMI) by [327] and (WAMMI) [328], SUS appears to be superior in assessing usability.

Table 6.2: System Usability Scale (SUS) questionnaire, Adapted from [224]

	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
1. I think I would like to use the Ransom*A*ware game frequently.	☐	☐	☐	☐	☐
2. I found the Ransom*A*ware game unnecessarily complex.	☐	☐	☐	☐	☐
3. I thought the Ransom*A*ware game was easy to use.	☐	☐	☐	☐	☐
4. I think I would need the support of a technical person to use this Ransom*A*ware game.	☐	☐	☐	☐	☐
5. I found that the various functions in this Ransom*A*ware game were well integrated.	☐	☐	☐	☐	☐
6. I thought there was too much inconsistency in this Ransom*A*ware game.	☐	☐	☐	☐	☐
7. I imagine most people would learn to use this Ransom*A*ware game very quickly.	☐	☐	☐	☐	☐
8. I found the Ransom*A*ware game very inconvenient to use.	☐	☐	☐	☐	☐
9. I felt very confident using the Ransom*A*ware game.	☐	☐	☐	☐	☐
10. I needed to learn many things before I could get going with this Ransom*A*ware game.	☐	☐	☐	☐	☐

6.6 Experimental Protocol Design

This main study aims to evaluate the 'Ransom*A*ware' game to improve users' education and awareness against the ransomware cyber security threat. The *Study 2* protocol consists of four phases. This requires the participants to participate in a pre-test questionnaire, which will then be followed by a *gameplay* Ransom*A*ware. The users will be asked to complete the '*System Usability Scale*' questionnaire to evaluate their subjective measurement of the Ransom*A*ware game. Then, users will complete a post-test. The purpose of the pre and post-test is to evaluate the effectiveness of the Ransom*A*ware design for its purpose. *Study 2* concludes with semi-structured interviews of the participants. The study requires participants to follow the instructions in the order shown in **Figure 6.1**.

Instructions for Participants	
Phase 1	**Pre-Test** The test will provide ten different cyber security questions relevant to Ransomware cyber threat. You need to answer each question on a scale of 1-5 with 1 = "Strongly Agree", 2 = "Agree", 3 = "Neutral", 4 = "Disagree", and 5 = "Strongly Disagree". This test requires PC access and will run online using a browser. Click on the link to proceed with the test.
Phase 2	a) **Game Play** You will be given 15 minutes to complete the Ransom*A*ware game. The study recommends that the participant read the 'instructions' manual to be fully aware of the game's rules before proceeding with gameplay. Click on the link to proceed with gameplay. Note: Remote online assistance will be provided to set up the environment if required. b) **System Usability Scale (SUS)– Questionnaire** To evaluate the subject's satisfaction with the RansomAware game, the user will complete SUS questionnaire. Click on the link to proceed with the questionnaire.
Phase 3	**Post-Test** The test will provide you 10 different cyber security questions relevant to Ransomware cyber threat. You need to answer each question on a scale of 1-5 with 1=" Strongly Disagree ", 2= "Disagree", 3 = "Neutral", 4 = "Agree", and 5 = "Strongly Agree". This test requires you access to a PC and will run online using a browser. Click on the link to proceed with the test.
Phase 4	To test the game through the Internationally accepted model TTAT. You are requested to participate in a semi-structured interview. For those who will confirm their availability, Team's invite will be sent to them.

Figure 6.1: Instructions for Participants

6.7 System Usability Scale Test Results

The main study adapted System Usability Scale (SUS) questionnaire items from [224] to assess subjective satisfaction with the Ransom*A*ware game design. The questionnaire consists of 10 items on a Likert scale of 1-5. All these items belong to one construct, measuring usability. This usability test aims to ensure Ransom*A*ware game serves its purpose, is effective for its stakeholders, and is efficient in playing and satisfying users' learning needs against ransomware cyber security threats [224]. Therefore do not require running cronbach's alpha. SUS determines the design's usability on the overall score rather than on the measurement of individual items. All questions were mandatory for the participants to respond to; once SUS questionnaire data was collected from all participants, data was analysed based on the following criteria.

1. Results of odd questions Q1, 3, 5, 7 and 9, subtract 1 from the score.
2. Results of even questions Q2, 4, 6, 8 and 10, subtract their value from 5.
3. SUM up the score of all 10 items from steps 1 & 2 to get the total SUS raw score.
4. Multiply the total SUS raw score with a value of 2.5 to obtain the final SUS score.

Table 6.3 shows that 30 respondents completed the SUS questionnaire during the main study. The minimum SUS score achieved by an individual is 75. In contrast, the maximum SUS score by an individual is 97.5, with the overall average SUS score of 87.58, which is well above the required usability score, i.e., the benchmark of 68 suggested by [322]. This means respondents are well satisfied with the usability of Ransom*A*ware, and no improvements are required to the game design.

Table 6.3: Individual participant's SUS Score

Participant ID	SUS Score	Participant ID	SUS Score	Participant ID	SUS Score
1	75	11	90	21	85
2	87.5	12	90	22	97.5
3	82.5	13	85	23	82.5
4	90	14	92.5	24	87.5
5	92.5	15	90	25	92.5
6	82.5	16	80	26	92.5
7	87.5	17	85	27	82.5
8	90	18	92.5	28	92.5
9	80	19	92.5	29	80
10	85	20	92.5	30	92.5
	Average Score				87.58

To verify and validate SUS results. Table 6.4 reports the validation of the results obtained through the System Usability Scale (SUS) [224]. The respondents in this survey include individual users and professionals from different industries, which also includes responses from working professionals from the user experience & design domain. The 'Mean' of the results shows respondents agreed with the questions asked in the survey. However, where the 'Mean' result is less, this is not related to any negative correlation, but this is mainly due to the nature of the questions asked, e.g., Q2, Q4, Q6, Q8 and Q10 are in similar direction, asking users whether they were dissatisfied with the game and the responses are in the same direction. Similarly, Q1, 3, 5, 7 and 9 were in one direction hence reporting high 'Mean'. The idea of the directions of these questions is supported by John Brooke in his System Usability Scale [224] to ensure that respondents make an effort to read each question before they can answer it [225]. To further validate these responses, Table 6.4 also reports the standard deviation, which is in an acceptable range of data variation of $\pm$1SD.

Table 6.4: SUS Mean and SD

Questions		Mean	Std. Deviation
Q1	I think I would like to use the RansomAware game frequently.	4.33	0.479
Q2	I found the RansomAware game unnecessarily complex.	1.47	0.507
Q3	I thought the RansomAware game was easy to use.	4.5	0.509
Q4	I think I would need the support of a technical person to use this RansomAware game.	1.47	0.507
Q5	I found that the various functions in this RansomAware game were well integrated.	4.5	0.509
Q6	I thought there was too much inconsistency in this RansomAware game.	1.17	0.379
Q7	I imagine most people would learn to use this RansomAware game very quickly.	4.3	0.466
Q8	I found the RansomAware game very inconvenient to use.	1.57	0.679
Q9	I felt very confident using the RansomAware game.	4.63	0.49
Q10	I needed to learn many things before I could get going with this RansomAware game.	1.57	0.504

6.8 Pre & Post Tests Results Analysis

The main study conducted *Paired-Sample t-Test* to measure the results obtained from the *pre-test* and *post-test*. This statistical test aimed to determine the effectiveness of gameplay for improved user awareness against the cyber security threat ransomware. Paired-Samples t-Test compares the mean from the pre-test and *post-test* to detect any statistically significant differences between the *pre-test* and post-test results [329]. The main study test the following hypotheses.

- Null Hypothesis (**H0**): Ransom*A*ware game will not improve user awareness against ransomware cyber security threat.
- Alternative Hypothesis (**H1**): Ransom*A*ware game will improve user awareness against ransomware cyber security threat.

The main study tested 30 participants to determine the effectiveness of gameplay 'Ransom *A*ware' for improving user awareness against the cyber security threat ransomware. They were given 15 minutes to play the Ransom*A*ware game and complete pre and post-test questionnaires. The study computes the results of pre and post-tests using the SPSS statistical tool at a 95% confidence interval and finds that the *post-test* (μ = 3.103, SD = .1520) is found to be statistically significantly

greater than the *pre-test* (μ = 2.983, SD= .1642), t(29) = -5.410 with p-value (< .001). The results suggest that while the p-value is less than .05, it thus supports the *Alternative Hypothesis (**H1**)*, i.e., the game 'Ransom*A*ware' design fulfils its purpose and is an effective tool for improving user awareness against the ransomware cyber security threat.

6.9 Pre & Post Test Results Validation

To validate the pre & post-test results, calculated through Paired-Sample t-Test. The assumption of the normality test was carried out in SPSS using *One-Sample Kolmogorov-Smirnov (K-S Test)*. It is a parametric test procedure to ensure the differences between each pre-test and post-test score are normally distributed, i.e., the frequency distribution of our data fits the normal distribution [329]. For this purpose, we checked the p-value of the test to see whether the p-value was less than 0.05 or greater. If the p-value is less than 0.05, then there is a significant deviation from normal distribution and data is not normally distributed. However, if the p-value is greater than 0.05, this is assumed to be normally distributed. Our K-S Test results reported p < .001 for the pre-test and p = .003 for the post-test, these values show normality test is not met. These findings suggest that Paired-Sample t-Test can be biased. [329] suggests this issue can be resolved with an increase in the sample. While study 2 involves subjective satisfaction with the game design, which involves usability testing, the smaller sample is recommended for testing purposes [319]. Therefore, the current study employed an alternative solution suggested by [329], a non-parametric test called Wilcoxon signed-rank test. This test has fewer assumptions than parametric tests and is useful for small data sets. Thus, the main study performed Wilcoxon signed-rank Test in SPSS. The results in **Table 6.5** show p < 0.01 (less than 0.5), indicating a statistical difference between the pre-test and post-test. This means game Ransom*A*ware has effectively improved user awareness against the cyber security threat ransomware, thus rejecting the null hypothesis.

Table 6.5: Hypothesis Test Summary

Null Hypothesis	Test	Sig.[a,b]	Decision
The median of differences between Average_PreT and Average_PostT equals 0	Related-Samples Wilcoxon Signed Rank Test	0 .	Reject the null hypothesis.
a. The significance level is .050.			
b. Asymptotic significance is displayed.			

6.10 Thematic Analysis to Confirm Elements of TTAT

In phase 4 of *study 2*, fifteen respondents agreed to participate in the semi-structured interviews. The aim was to get their feedback on the Ransom*A*ware game to validate that elements of TTAT are embedded in the game design framework. The current study chooses thematic analysis to perform metadata analysis on the interview data. Thematic analysis is reported as a widely used qualitative approach due to its flexibility, usefulness, and beyond psychology studies [212]. While thematic analysis allows to identify of themes from rich data and predict various aspects related to the research, therefore, current studies analyse qualitative analysis using thematic analysis using the following steps recommended by [212];

1. The aim of selecting primary data through the semi-structured interview was to answer the research question and empirically validate the presence of TTAT elements in the Ransom*A*ware game. Therefore, the participant's responses are carefully read a few times to get familiarisation with the data.

2. The current studies use NVivo software due to its ability to handle and analyse any unstructured qualitative data. It adopts an Inductive thematic analysis approach to identify codes from the data. See **Table 6.6**.

3. Responses were examined and reviewed to identify as many themes as possible or patterns as possible in the data.

4. Themes were reviewed and aligned with research question themes using a deductive approach. The aim was to evaluate their effectiveness in the Ransom*A*ware game. See **Table 6.6**.

Semi-structured interviews were conducted to validate the elements of TTAT employed in the game prototype. The **Table 6.6** provides a summary of the thematic analysis performed. **Figure 6.2** shows themes and the codes identified from the respondents' quotes.

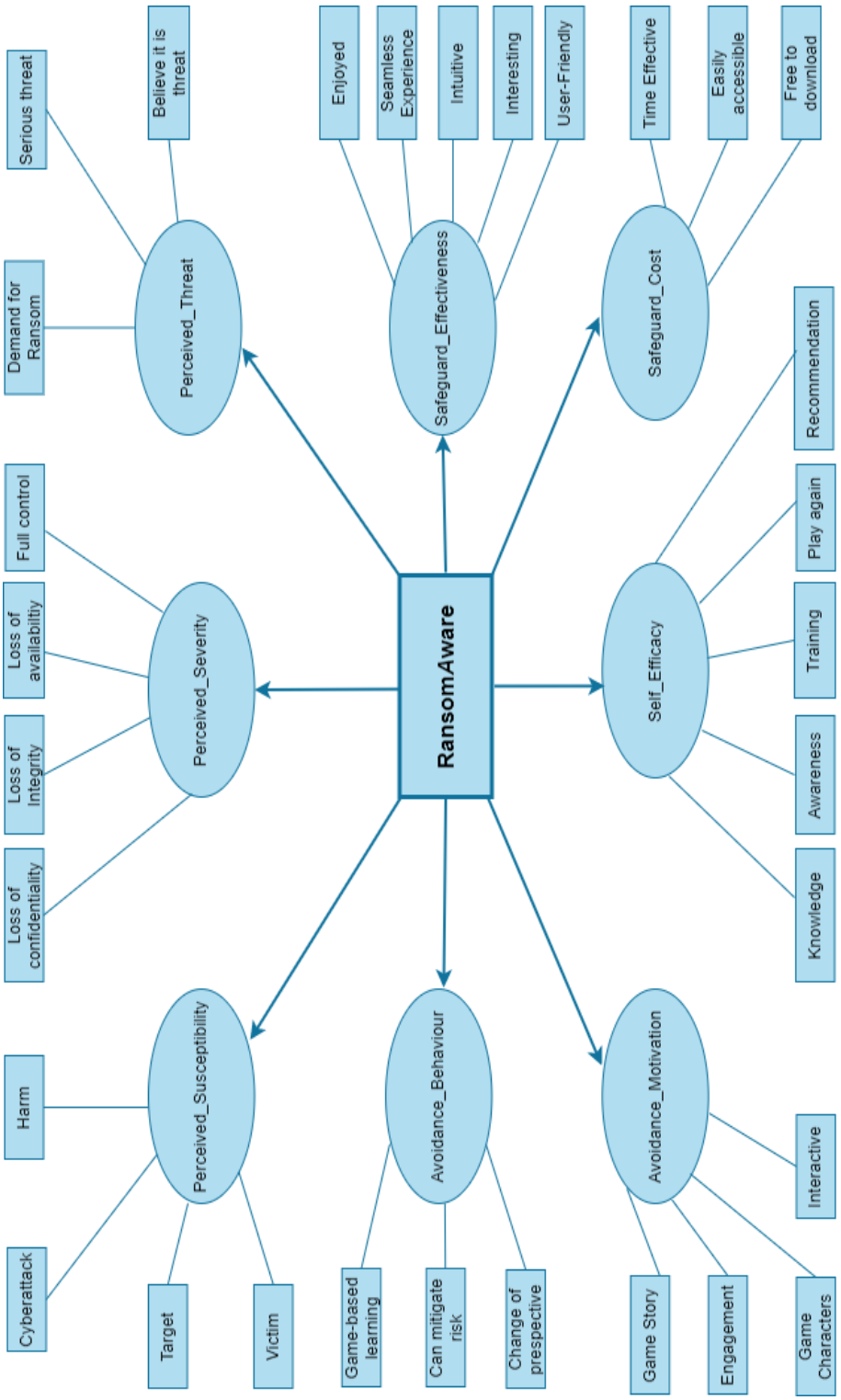

Figure 6.2: Themes and codes

Table 6.6: Thematic Analysis

Themes	**Codes**	**Respondents Quotes**
P_Sus	Victim, Target, Under cyberattack, Likely harm	*"I spend much time with emails and on social media with known and unknown people. I can be a victim of the ransomware."* *"Considering how cyber security threats are evolving, the attackers use more advanced ways to attack. I think I can be the target of cyber security threat ransomware."* *"Where we benefit a lot from the digital revolution, at the same time, it brings many cyber security challenges. Ransomware is an emerging phenomenon. I can be exposed to this cyber security threat."*
P_Sev	Loss of confidentiality, Loss of Integrity, Loss of availability, Full control	*"After playing the RansomAware game, I understand that ransomware can compromise my privacy by accessing my data."* *"Wow, I learnt that once the ransomware attack is successful, the attacker has full control of my data and can do anything with it."* *"My PC has everything from my old pictures to work-related data. I never thought that someone could use ransomware to take control of it."*

Continued on next page

Table 6.6 – continued from previous page

Themes	Codes	Respondents Quotes
P_Thr	Demand for ransom, Serious threat, Believe it is a threat	*"I heard a lot about computer viruses in the past, but until I played the RansomAware game, I was never sure about the malicious nature of the ransomware, which can take any computer machine hostage and demand the money to release."* *"After playing ransomware game and learning its consequences, I believe this is a serious threat to computer security."* *"I use emails to exchange work-related documents. After playing RansomAware game, I believe it is a security threat to computer users."*

Continued on next page

Table 6.6 – continued from previous page

Themes	Codes	Respondents Quotes
S_eff	Enjoyed, Seamless Experience, Intuitive, Interesting, User-friendly	*"Overall, I enjoyed playing the game. It was a very interesting way to learn about a complex cyber threat, ransomware. The game was pretty straightforward to use. It was a seamless experience. I liked the way how the game was based on the story. It helped me to engage. It was useful to make informed decisions."* *"The game story engaged me. The design is intuitive and easy to navigate. I found it an effective way to learn ransomware."* *"The game was interesting and engaging, giving enough development opportunity while keeping you on realistic edge as who has time to read these sorts of emails."* *"Interesting story. I learnt complex cyber security in a friendly manner. This game approach is much better than traditional multiple-choice theoretical information security training."*

Continued on next page

Table 6.6 – continued from previous page

Themes	Codes	Respondents Quotes
P_Cos	Time effective, Easily accessible, Free to download	*"The game was different from traditional hourly long training. I finished playing the game within the given time. It is time effective. I believe this is worth considering for ransomware awareness training."* *"It was a great experience with RansomAware. I was able to download it on my PC and mobile phone. The game is accessible, which means learning can happen on the go."* *" I love playing online games and believe they are good for human cognitive behaviour. My experience with RansomAware was awesome, you know why? Because it was easy to use and free to download."* *"I played a RansomAware game on my mobile phone while going to a friend's house. This was an interesting experience. I believe it is a usable and interactive design."*

Continued on next page

Table 6.6 – continued from previous page

Themes	Codes	Respondents Quotes
S-Eff	Knowledge, Awareness, Training, Play again, Recommendation	*"I would say game-based learning is fun. It boosted my confidence. I will consider replaying if needed again and will surely recommend this game to my family and friends."* *"The game helped me with critical thinking to make the right decision. I feel more confident and aware of the malicious nature of ransomware attacks. I believe game-based learning is a good way forward to refresh your knowledge and will play again. Considering cyber security is an essential part of our lives, I will recommend the RansomAware game to my friends and family to benefit from it."* *"The scoring system was quite encouraging. If needed, I will replay this game as a refresher training and recommend others too."* *" I scored a bronze award for my points earned, which is not bad but shows me I need to up my game if I want to be completely safe. Overall, I would recommend this game to everyone."* *I felt confident by earning points during gameplay. RansomAware game helped me to build my confidence to thwart ransomware threat."*

Continued on next page

Table 6.6 – continued from previous page

Themes	Codes	Respondents Quotes
A_Mot	Game Story, Engagement, Game Characters, Interactive	*"I successfully achieved Gold reward at the end of the game-play and believed the game-story and the design was an important element which contributed to my interest and knowledge awareness against the ransomware cyber security threat."* *"The idea of points award was motivational at the same time deduction of marks created a deterrence to improve my attention to detail."* *"The game-based learning was an enjoyable experience for learning about the malicious ransomware threat. I liked the spacer and the alien characters."*
A_Beh	Game-based learning, Can mitigate risk, Change of Perspective	*"The game story and design aspects of the game were very well integrated, which created my interest and helped me to achieve my goal of improving awareness against the ransomware cyber security threat. I believe the likelihood of ransomware attack can be mitigated."* *"It is not impossible to stop ransomware. The game RansomAware has changed my perspective."* *"I will adopt ransomAware game to enhance my avoidance behaviour against ransomware threat."*

Perceived Susceptibility (P_Sus), Perceived Severity (P_Sev), Perceived Threat (P_Thr), Safeguard effectiveness (S_eff), Safeguard cost (S_Cos), Avoidance Motivation (A_Mot), Avoidance Behaviour (A_Beh).

6.11 Discussion on TTAT Themes

This section provides a discussion on each theme presented in **Table 6.6**.

- **Perceived_Susceptibility (P_Sus)**

In the context of current research, P_Sus is described as being conscious of the ransomware cyber security threat. The aim of embedding this element in the game design was to create a realisation of ransomware. The respondents acknowledged that playing Ransom*A*ware, the game has helped them to understand the likely harm of ransomware. From the respondent's statement below.

"I spend much time with emails and on social media with known and unknown people. I can be a victim of the ransomware."

The game Ransom*A*ware adopted phishing and spear phishing as a technique to demonstrate the ransomware attack. This helped the respondent realise how he interacts with different people using emails as a mode of communication in their digitally driven life. Where digital interaction through emails is robust and convenient, malicious emails can compromise a user's security through malicious content. While playing the game, Ransom*A*ware made the user understand the Identification of ransomware threat through malicious emails. In another statement by the user;

"Considering how cyber security threats are evolving, the attackers use more advanced ways to attack. I think I can be the target of cyber security threat ransomware."

The digital revolution drives our life today, and technology is integral to our social system. While moving towards smart cities and infrastructure, the landscape of cyber security is changing too. The exponential increase of social computing is threatened by evolving cyber risks, paralysing these systems from access by legitimate stakeholders living in a cyber-physical-social system. The game Ransom*A*ware helps the individual to perceive a threat by introducing a story based on legit and non-legit emails and the consequences associated with user actions on dealing with

such emails that he can subject to ransomware attacks.

"Where we benefit a lot from the digital revolution, at the same time, it brings many cyber security challenges. Ransomware is an emerging phenomenon. I can be exposed to this cyber security threat."

- **Perceived_Severity (P_Sev)**

In the context of current research, P_Sev is defined as the extent to which a Ransomware attack can be considered a negative impact on an individual. Some participants have made the statements below highlighting that users acknowledged the severity of their data being compromised by cyber-attack ransomware.

"After playing the RansomAware game, I understand that ransomware can compromise my privacy by accessing my data"

"Wow, I learnt that once the ransomware attack is successful, the attacker has full control of my data and can do anything with it."

"My PC has everything from my old pictures to work-related data. I never thought that someone could use ransomware to take control of it."

The game Ransom*A*ware adopts a storyline to make the user aware of the malicious nature of the ransomware cyber-attack. The player encounters a character called 'Alien Ship' and interprets whether the email message is genuinely based on the user's cognitive behaviour. If the decision-making is not right, then it will lead the user to bear the consequences of losing one lifeline and being locked by the ransomware. This helped the users understand that once their machine is locked and remotely controlled by the attacker, it can give full access to their data and compromise their confidentiality, integrity and availability, as shown from the themes that emerged from the statements above.

- **Perceived_Threat (P_Thr)**

The current research adopted game-based learning for user engagement and

awareness against ransomware cyber-security threat. The theme, 'Demand for ransom' emerged from one participant's statement below. This is based on the fact that the game story introduces a malicious message. If the user interacts with that message and accepts it, this leads to the user's 'Spaceship' being hijacked by the 'Alien' and prompts two options for the user to select one. Suppose the user selects the 'Pay ransom' option. In that case, this will reduce one lifeline, or the user can select an alternative option, i.e., 'Call Helpline', which will penalise the user by reducing the time to play the game by 10 seconds. This helped the user to recognise ransomware as a serious threat to its computer security.

"I heard a lot about computer viruses in the past, but until I played the RansomAware game, I was never sure about the malicious nature of the ransomware, which can take any computer machine hostage and demand the money to release."

"After playing ransomware game and learning its consequences, I believe this is a serious threat to computer security."

A statement below, from one of the participants, emerges a theme 'Believe it is a threat'. The finding shows that the game story adopts malicious email as an attack vector in the Ransom*A*ware game, which has helped the participant perceive ransomware as a cyber security threat to its security.

"I use emails to exchange work-related documents. After playing RansomAware game, I believe it is a security threat to computer users."

- **Safeguard_effectiveness (S_eff)**

It is defined as a subjective assessment to perceive the usefulness of the safeguarding measure, which can help to reduce the IT threat. The current research adopted gamed-based learning to safeguard users against the ransomware cyber security threat through awareness and training using a Ransom*A*ware game. The themes that emerged from the statements below show that participants enjoyed playing the Ransom*A*ware game. It was a usable experience for them to navigate.

The game story successfully engaged the audience to help them become aware of the cyber security threat of ransomware. Moreover, game-based learning was appreciated as an effective security training tool compared to conventional theoretical training adopted by organisations.

"Overall, I enjoyed playing the game. It was a very interesting way to learn about a complex cyber threat, ransomware. The game was pretty straightforward to use. It was a seamless experience. I liked the way how the game was based on the story. It helped me to engage. It was useful to make informed decisions."

"The game story engaged me. The design is intuitive and easy to navigate. I found it an effective way to learn ransomware."

"The game was interesting and engaging, giving enough development opportunity while keeping you on realistic edge as who has time to read these sorts of emails."

"Interesting story. I learnt complex cyber security in a friendly manner. This game approach is much better than traditional multiple-choice theoretical information security training."

- **Safeguard_Cost (S_Cos)**

It is defined as a user's physical and cognitive efforts to decide whether the cost justifies the effectiveness of the safeguard measure. If it does, then it leads to developing user avoidance behaviour. In the current research, the Ransom*A*ware game adopts the storyline, which is a time constraint. The user is supposed to respond to events generated in a given time 15 minutes before the game ends. This helps the user to improve their decision-making, so they can make informed choices to improve their awareness against the ransomware. The statement below from the participant emerges the theme ' time Effective'. This finding shows that participants found the Ransom*A*ware game an effective tool to get awareness against the ransomware threat.

"The game was different from traditional hourly long training. I finished playing the game within the given time. It is time effective. I believe this is worth considering for ransomware awareness training."

Similarly, in the statement below, the participant mentions the game being 'Easily accessible' for the user. The Ransom*A*ware game is compatible with smartphones and PCs, which makes it a usable and effective tool for the user to improve their awareness against the ransomware cyber security threat anytime and anywhere.

"It was a great experience with RansomAware. I was able to download it on my PC and mobile phone. The game is accessible, which means learning can happen on the go."

In other statements below, findings highlight the theme 'Free to download', which refers to the safeguard effectiveness of the game Ransom*A*ware for an individual user. While large corporates have budgets for staff training, the cost could be a barrier to user training against cyber security threats in individual user settings. Therefore participants acknowledge the usefulness of the game.

" I love playing online games and believe they are good for human cognitive behaviour. My experience with RansomAware was awesome, you know why? Because it was easy to use and free to download."

"I played a RansomAware game on my mobile phone while going to a friend's house. This was an interesting experience. I believe it is a usable and interactive design."

- **Self-Efficacy (S-Eff)**

It is defined as an important user's belief, which helps them determine the safeguard measure's effectiveness. From the statements below, findings show participants feel more confident after playing the Ransom*A*ware game. It has helped the user to improve their awareness against ransomware cyber security threat, and the theme 'Recommendation' highlights their confidence in the game to play and recommend others.

"I would say game-based learning is fun. It boosted my confidence. I will consider replaying if needed again and will surely recommend this game to my family and friends."

"The game helped me with critical thinking to make the right decision. I feel more confident and aware of the malicious nature of ransomware attacks. I believe game-based learning is a good way forward to refresh your knowledge and will play again. Considering cyber security is an essential part of our lives, I will recommend the RansomAware game to my friends and family to benefit from it."

In other statements below, participants stated that while making the right decision to identify a malicious attack. The Ransom*A*ware game encouraged them through the points-earning feature, which helped them to boost their confidence against ransomware awareness. Similarly, in another statement, the participant appreciated the reward base strategy adopted by Ransom*A*ware. Once the user completes the game in a given time, the game prompts feedback to the user and awards a medal to determine its level of expertise in awareness against the ransomware. This is evident from the findings that this approach helped users improve their confidence that the Ransom*A*ware game can help them thwart the ransomware cyber security attack.

"The scoring system was quite encouraging. If needed, I will replay this game as a refresher training and recommend others too."

" I scored a bronze award for my points earned, which is not bad but shows me I need to up my game if I want to be completely safe. Overall, I would recommend this game to everyone."

"I felt confident by earning points during gameplay. RansomAware game helped me to build my confidence to thwart ransomware threat."

- **Avoidance Motivation (A_Mot)**

It encourages users to save themselves from IT threats by taking appropriate safeguards. In the context of current studies, the research aimed to design and develop a prototype that should be user-friendly and engage users to improve their avoidance motivation against the ransomware cyber security threat. The statement below from

the participant emerges the theme 'Game Story', highlighting how Ransom*A*ware game has helped users create interest and engagement to develop avoidance motivation against ransomware cyber security threat. Similarly, other statements made by the participants mention the 'engagement' and 'interactivity' themes, which emerged due to the game story. This has helped the user's interest in engaging with the ransomware awareness process. Furthermore, considering intuitive design during game development helped the user with a seamless learning experience.

"I successfully achieved Gold reward at the end of the game-play and believed the game-story and the design was an important element which contributed to my interest and knowledge awareness against the ransomware cyber security threat."

User engagement was paramount for user learning against ransomware. Therefore, it was important during game design to include those elements that can help users develop avoidance motivation. For this purpose, the Ransom*A*ware game offers its users to earn points for any right decision-making against the malicious attack or for losing life or points as a deterrence to improve their decision-making against the cyber security threat ransomware. From the statement below, the participant acknowledged that the game storyline helped the user to improve its avoidance motivation against the ransomware cyber security threat.

"The idea of points award was motivational at the same time deduction of marks created a deterrence to improve my attention to detail."

The statement below from the participant highlights the theme of 'Game Characters'. Ransom*A*ware is based on the storyline, which uses different characters to improve user interaction and engagement. The user onboard the spaceship encounters email messages from different solar system planets. These pop-up messages are a combination of genuine or malicious email messages. The user's analysis of the situation helps the user to make the decision, either 'REJECT' or 'ACCEPT' these messages. The spacer scans the user's spaceship to evaluate the user's decision-

making. If the decision was wrong, then the 'Alien' character was used to demonstrate how the attacker hijacked the user's spaceship and got complete control of the spaceship. The participant's statement acknowledges how using different game characters helped users engage and improve their avoidance motivation.

"The game-based learning was an enjoyable experience for learning about the malicious ransomware threat. I liked the spacer and the alien characters."

- **Avoidance Behaviour (A_Beh)**

In the context of current research, A_Beh is defined as the extent to which the user is motivated to thwart ransomware cyber security after playing a Ransom*A*ware game as a safeguard measure. The current research adopted the TTAT model to design and develop a game called Ransom*A*ware. The game was based on a user-centred design to provide usability to its users and promote user awareness against ransomware cyber security threat. One participant's statement below highlights the theme 'can mitigate ransomware'. This acknowledges that the game Ransom*A*ware was user-friendly, useful for its purpose and helped users develop awareness against the ransomware cyber security threat. After playing the game, user avoidance behaviour against ransomware is changed. Users feel game-based learning can help to mitigate ransomware risk to its security.

"The game story and design aspects of the game were very well integrated, which created my interest and helped me to achieve my goal of improving awareness against the ransomware cyber security threat. I believe the likelihood of ransomware attack can be mitigated."

The statement below from the participant highlights the theme 'Change of Perspective'.This is in the context of the user's belief about preventing ransomware attacks before playing the Ransom*A*ware game. Furthermore, playing the game has improved user awareness, which helped users develop enough avoidance motivation and behaviour against the ransomware cyber security threat. From the statements

below, it is evident that Ranom*A*ware game-based learning is appreciated. Participants are willing to adopt this game to enhance their avoidance behaviour against the ransomware cyber security threat.

"It is not impossible to stop ransomware. The game RansomAware has changed my perspective."

"I will adopt ransomAware game to enhance my avoidance behaviour against ransomware threat."

The discussion and synthesis of the thematic analysis indicate that the Ransom*A*ware game has helped users to identify ransomware as a threat and its possible consequences. The users believe that due to their interaction with technology, they can be susceptible to a ransomware attack. Most respondents showed concern about losing access to their data due to a ransomware attack and acknowledged that such an attack could be severe and result in taking full control of their data. This confirms the user's suscepbilitity to ransomware threat [141]. However, at the same time, users reported that the Ransom*A*ware game is a fun way to learn. They found it an effective safeguard against the ransomware threat. Users enjoyed playing the Ransom*A*ware game and found it user-friendly. Users appreciated the game's intuitiveness and acknowledged that this helped them engage with learning. They reported that game design is effective, making the ransomware complex cyber security threat a seamless learning experience. This confirms the perceived effectiveness, an element of TTAT in the game [141].

The users also acknowledged that they found Ransom*A*ware accessible on their phones, allowing them to learn on the go and at their own pace. They also commended the game time effectiveness, which allowed them to judge in a given time, similar to real-world situations when they have to differentiate between malicious and non-malicious emails. This acknowledges the TTAT element perceived cost related to the Ransom*A*ware game [141]. From the respondent's quotes, it is evident that the reward feature embedded in the game Ransom*A*ware helped the users to gain confidence through earning points. Users acknowledged that they feel more aware of the ransomware threat after playing the game and are confident of thwarting ransomware. This shows that the game develops users' self-efficacy, the presence

of another element of the TTAT in the game (Liang & Xue, 2010).

The user comments also stated that they liked the storyline of the Ransom*A*ware and the characters used. Their interaction with these characters made them engage with learning fully and thus developed an avoidance motivation against the ransomware. Users commended game-based learning and mentioned that Ransom*A*ware changed their perspective on ransomware. They feel more aware of the ransomware threat and believe this learning can help them mitigate its future risks. This confirms the presence of avoidance motivation and behaviour elements of the TTAT in Ransom*A*ware game [141]. **Figure 6.3** shows word cloud emerges from the thematic analysis performed. The discussion and analysis of the semi-structured interviews empirically validate that the findings suggested by study 1 in chapter 4 are successfully embedded in the game design.

Figure 6.3: Word Cloud

6.12 Summary

In this chapter, *Study* 2 of the research chapter was concluded. The study aimed to empirically evaluate the usability of the Ransom*A*ware game and elements of TTAT embedded in the game to assess its effectiveness in improving user awareness against the ransomware cyber security threat. This study was carried out in two stages; (1) To evaluate the usability of the game Ransom*A*ware, quantitative analysis was performed to report the findings of the SUS usability test followed by a t-test. The statistical test validates that the findings are significant and support the hypothesis that the Ransom*A*ware game offers usability to its users. Whereas in stage (2), Qualitative analysis was adopted to analyse user's satisfaction with the Ransom*A*ware game, thematic analysis was performed to validate the effectiveness of TTAT elements embedded in the Ransom*A*ware game. Next, chapter 7 provides a further discussion of the results and research implications.

Chapter 7

Discussion of the Findings

7.1 Overview

Chapter Seven: This chapter discusses the results obtained from two studies conducted for the current research. First, it focuses on the empirical findings of *Study 1*, which is about elements of TTAT to include in the Ransom*A*ware design. The aim is to improve user awareness against the ransomware cyber security threat, along with a discussion on the research model based on TTAT and the hypothesis formation, followed by theoretical validation of the research model. Then the discussion will proceed on the empirical findings of *Study 2*, which includes practical validation of the usability and the elements of TTAT implemented during game design and development to assess user satisfaction with the game design. Furthermore, this chapter will discuss the implication and contributions of the current research.

7.2 Discussion on Findings of Study 1 & 2

The current research aims to improve user awareness against the cyber security threat ransomware using game-based learning and designed two studies to achieve its research objectives. The findings reported by both studies are theoretically and practically validated. Chapter 4 reports the findings of *Study 1*, which is based on the TTAT. It explains the individual's behaviour against the malicious IT threat. Ransomware is a kind of malware that can greatly impact the confidentiality, integrity

and availability of an individual's data, as well as the organisational IT network. Therefore in this study, elements of TTAT are critically evaluated to determine which factors can influence the users' IT avoidance behaviour to thwart ransomware cyber security threat. TTAT define 'Threat Appraisal' and 'Coping Appraisal' as two cognitive processes which act as oxidants to enhance user avoidance motivation against malicious IT. The current research is based on ontology belief and adopts positivism to gain factual knowledge. Therefore, it adopted elements of TTAT to set up a questionnaire for users' understanding of the perceived threat of ransomware, its malicious consequences and user willingness to adopt preventive measures. The empirical study is then conducted to identify critical components of TTAT required to include in the proposed Game Design for users' education against ransomware.

The current research adopts TTAT theoretical model and uses a deductive approach to develop hypotheses. It hypothesises that the user's avoidance behaviour against the ransomware is driven by the user's avoidance motivation, which is determined by the user's 'Threat Appraisal,' i.e. when the user perceives its susceptibility to ransomware, which can vary and depends on the user exposure to technology. The more the user is dependent on technology, the more it will be prone to risks like ransomware and its perceived severity, i.e., the extent to which a ransomware attack can compromise a user's privacy. This depends on the user's risk analysis, data classification and the purpose of using the computer machine. If the usage is personal, the ransomware attack on personal data may not have a high impact compared to if the machine holds critical classified organisational data, which is subject to compliance or other regulatory requirements. This means 'P_Sus' and 'P_Sev' will have a multiplicative impact on the 'Threat appraisal'. The absence of one of the elements means the user's avoidance motivation against ransomware will be subject to change if 'Threat appraisal' is not acknowledged as high risk.

The model further hypothesises that 'Threat appraisal' stimulates the user's 'Coping appraisal,' i.e., the user considers taking safeguard effectiveness measures such as 'S_eff', S_Cos' and 'Self-Eff' to develop their motivation against the ransomware threat. In the current research, once a user perceives ransomware as a threat, the user must be motivated enough to believe that preventive measure is useful to stop it. If the benefit of adopting a measure against the threat outweighs its cost and

the user is confident to adopt a preventive measure, this will enhance user avoidance motivation. The study also examined the interaction between p_sus and p_sev to see its effect on the perceived threat of ransomware. Moreover, the relationship between perceived threat and safeguard effectiveness was also examined to see how their combined interaction affects users' avoidance motivation against ransomware.

A survey was conducted to a sample size of 153 to validate the TTAT model empirically. Respondents from wider backgrounds, from individual home computer users to working professionals, were included in the survey. To comply with research ethics, personal data was not collected, and working professionals' organisation details were not sought. However, as phishing is the most common factor used by ransomware attackers, as reported by [330], respondents' selection criteria were based on their access to the Internet. The survey included all eight constructs of TTAT, i.e., P_Sus, P_Sev, P_Thr, S_eff, S_Cos, S-Eff, A_Mot and A_Beh. In order to evaluate their effectiveness against ransomware threat. Therefore these elements to be included in the game design, study-1 adopted quantitative analysis to theoretically validate the research model and test the hypothesis, using the (PLS-SEM) statistical test. While ransomware is a new phenomenon, the features of PLS-SEM make it a valuable technique for data analysis for any exploratory research [240].

The findings of *Study 1* revealed that elements of TTAT (P_Sus, P_Sev, P_Thr, S_eff, S_Cos, S-Eff, A_Mot and A_Beh) are important to consider in the Ransom*A*ware design. These elements can enhance the effectiveness of game-based learning and can improve user awareness against ransomware threats. These findings were input to Chapter 5, which focuses on the design and development of the Ransom*A*ware game. The suggested elements of TTAT are implemented in the game story during the Ransom*A*ware design and development process reported in Chapter 5.

Study 2 of the current research is reported in chapter 6. It aims to evaluate the effectiveness of the Ransom*A*ware game. The findings of this study empirically validate two important objectives of this research, i.e., *How to implement user experience to achieve usability.* Usability improves user satisfaction with the game design. The current study reveals it is not about improving the design aesthetics and implementing the functional requirements correctly, which is the expectation

from the end-product for its stakeholder to accomplish the task. An intuitive design is more than that. Therefore, the current study focuses on user experience design principles [331],[332] to deliver user-centred design to engage its users. While game design involves the design and development process, it was critically important to consider that game meets the research aim, i.e., it should be able to improve user awareness against ransomware cyber security threat. For this purpose, the design phase started with refining the Ransom*A*ware game goals/objectives using different UX approaches. MoSCoW analysis was performed to manage the game's requirements and use of Personas to align users' needs, behaviour, and experience to the game functionality. So game Ransom*A*ware can satisfy users' need to improve their awareness of the ransomware threat.

Ransomware is a complex phenomenon. The current research aims to make a usable learning tool for the users, which can simplify their learning and engage them to improve their awareness against the ransomware cyber security threat. Therefore Ransom*A*ware game adopts a story with memorable characters to create an interest and make learning fun for the users. Ransom*A*ware also uses visuals to improve users' interaction with the game, so users can have a seamless playing experience and improve their awareness against the ransomware cyber security threat. While usability consideration was one factor in improving users' engagement and learning, at the same time, it was also important to validate that the elements of TTAT are successfully embedded in the Ransom*A*ware game design so as to promote user awareness against the ransomware cyber security threat. The Ransom*A*ware game can help the user identify the consequence of ransomware attack. It demonstrates how attackers use phishing as an attack vector to deceive users and take control of their machine and data as a hostage through a remote command and control mechanism.

Moreover, demands virtual currency as a ransom help users improve their decision-making to differentiate between good and bad emails, so they can make an informed decision on whether to accept or reject phishing emails. This phenomenon is similar to our daily life experience while interacting with emails, and sometimes users fall prey to malicious emails due to hasty decisions. Therefore to address this issue, the Ransom*A*ware game is time-based, i.e., the user must complete the game within 15

minutes before the game finishes. This game feature promotes feasibility and improves user cognitive behaviour against malicious attacks. The Ransom*A*ware game encourages users to learn through its intuitive design and enhances users' awareness against the ransomware cyber security threat. At the same time, it is important to consider improving user motivation during gameplay. Therefore game offers points as a reward to users for their correct actions and awards medals on completing the game, along with feedback to evaluate its learning level. This can be useful in an organisational setting to boost employees' information security training against ransomware cyber threat. It can also motivate an individual to enhance their learning against ransomware.

To empirically validate usability and elements of TTAT in the Ransom*A*ware game. An experimental protocol was set up, a pilot study was conducted before the main studies, and a sample size of 30 respondents was selected to participate in the gameplay, as suggested by previous usability studies [319]. A small sample is more efficient in performing usability tests. It is not only the cost-effective way to collect data, but it can also help to identify any usability issues [320]. However, this selection was based on the criteria of respondents having access to smart devices and internet usage. This was because current research aims to improve user awareness against the cyber security threat ransomware, which uses emails as a prime carrier to penetrate users' machines. *Study 2* adopted a mixed methods methodology to assess the game's effectiveness. Quantitative analysis was performed to evaluate the usability test and subjective satisfaction of the game, followed by qualitative analysis to confirm elements of TTAT in the Ransom*A*ware game helps in improving user education and awareness against the cyber security threat.

7.3 Reliability and Validity of Study 1 & 2 Results

Study 1 adopted (PLS-SEM) to conduct quantitative analysis. The consideration of using this methodology was suggested by findings reported in the studies by [240] and [274]. PLS-SEM has recently gained popularity in the social sciences due to its

ability to evaluate the measurement of latent variables and the relationship between them. While *Study-1* includes a sample size of 153, the statistical power of PLS-SEM makes it an ideal methodology option to handle the current research sample size and demonstrate convergence behaviour [274]. Study 1 adopted TTAT constructs, i.e., (p_sus, p_sev, p_eff, p_cost, s-eff, p_thr, a_mot and a_beh) of a previous study conducted by [141] in a Likert-style questionnaire and performed a number of statistical tests to validate instrument and the model. Results are reported in Chapter 4.

The instrument adopted in *Study 1* includes both independent (p_sus, p_sev, p_eff, p_cos, s-eff) and dependent variables (p_thr, a_mot and a_beh). TTAT of [141] suggests user's avoidance behaviour against malicious IT is determined by its avoidance motivation which is further determined by a perceived threat and coping appraisal. In the context of current research, elements of TTAT are adopted. This is to assess to what degree a user's avoidance behaviour against the ransomware cyber security threat can be influenced by its avoidance motivation. Furthermore, it is determined by the extent to which a user can be susceptible to a ransomware attack and its perception of the level of severity ransomware may cause to its security.

Moreover, the combined effect of these two elements determines whether users consider ransomware a threat. The *Study-1* further includes items related to safeguard effectiveness to assess whether the user will find the proposed game an effective remedy against the ransomware attack. The game will be a feasible solution for the user to perceive avoidability against Ransomware. The user will be confidently able to use it, as the game would not require any technical expertise compared to traditional hardware solutions against ransomware threat.

Study 1 validates the research model and the hypotheses. The study employed PLS-SEM. The statistical findings of the research model explain a 55% variance in user motivation to avoid ransomware cyber security threat and 29% in avoidance behaviour to thwart ransomware attack. These findings are significant and align with the previous findings of [141], which focused on computer security. The current study aims to improve user awareness against ransomware, a relatively new phenomenon that compromises user security; therefore, the findings of the current studies are considered significant. *Study 1* adopts the deductive approach to develop

the hypothesis from the existing theory [141]). The findings revealed significant results for hypotheses H1a ($b = 0.26, p < 0.01$) and H1b ($b = 0.21, p < 0.05$). These results show that users perceive being likely harmed by the ransomware, and perceived ransomware impact can be severe. These findings are important for the current research as it aims to improve user awareness against ransomware. The research cannot achieve its intended aim without users not considering ransomware as a cyber security threat and its consequences H2 ($b = 0.25, p < 0.05$). Thus, the current research supports the findings of H1a, H1b and H2 are in line with previous research conducted by [141].

The statistical findings also support the hypotheses H3 ($b = 0.31, p < 0.05$), and H5 ($b = 0.23, p < 0.05$). These results indicate users' coping appraisal. This means that once a user perceives ransomware as a threat, that encourages the user to take safeguard measures. The results of H3 & H5 positively influence the user to adopt game-based learning as an effective tool against ransomware. This enhances the user's belief that the game will provide enough awareness against the ransomware and boost their confidence to thwart it. The finding H4 ($b = -0.14, p > 0.05$) shows that H4 negatively influences user avoidance motivation against ransomware. This finding is insignificant and opposed to the previous study by [141] TTAT. In the context of current studies, this finding reveals that in any successful ransomware attack, the attacker demands a ransom to be paid in virtual currency, which is high in value and can have a huge impact on the user. Therefore, the repercussions of the attack outweigh the safeguard control's cost.

The current study also examined the interaction effects of the perceived threat of ransomware and game as safeguard effectiveness. The statistical findings H3a ($b = -0.12, p < 0.05$) reveal that this interaction negatively influences the user's ransomware avoidance motivation. This finding indicates significant results and supports the findings of [141] TTAT's model. The results of H3a suggest that in current studies, to enhance user avoidance motivation against ransomware. Threat appraisal of the ransomware and the game's effectiveness as a coping appraisal are important contributors to the user's avoidance motivation. When a user perceives susceptibility to ransomware and its severe impact on their security, this acknowledgement of threat appraisal and the effectiveness of the Ransom*A*ware can influence

users' avoidance motivation against ransomware.

The second interaction between perceived susceptibility and perceived threat represents Hypothesis H1c ($b = 0.25, p > 0.05$). This is the second hypothesis which is not supported by current studies. However, this finding is in line with the previous study by [141]. This finding is statistically insignificant because this hypothesis was developed by [141] based on previous studies of health beliefs. However, the results were insignificant when this hypothesis was applied in the context of malicious IT by [141] and [280]. Similarly, when this hypothesis was tested in current research in the context of ransomware, the results were also found insignificant. This could be mainly because ransomware is the latest cyber security threat, considered more sophisticated in its design and the user's inability to tackle it due to its malicious nature. The ransomware repercussions are also far more than any traditional virus. When users perceive high susceptibility to ransomware, this will have a strong relationship with its severity and vice versa. Therefore, the current research findings do not support hypothesis H1c. This finding also aligns with a previous study [281]. *Study-1* supports hypothesis H6 ($b = 0.54, p < 0.01$), the statistical findings show that users' avoidance motivation significantly impacts avoidance behaviour against the ransomware cyber security threat. The statistical findings from the empirical study confirm the measurement and research model validation to determine elements of TTAT to be included in the game.

Study 2 of the current research adopts a mixed-methods approach to evaluate Ransom*A*ware effectiveness empirically. The research design process includes quantitative analysis to measure the user's satisfaction with Ransom*A*ware. An experimental protocol was set up to collect data in four steps. During phase 1: Users were requested to participate in a *pre-test* consisting of 10 questions based on the National Cyber Security Centre UK guidelines on cyber security awareness. The aim was to analyse users' understanding of ransomware cyber security before they proceeded with gameplay. The questionnaire assessed only user knowledge in the cyber security domain. Therefore, Cronbach's alpha was not applicable to validate the instrument, contrary to the *study-1* questionnaire, which included number of variables and constructs required validation. In phase 2: Users were given 15 minutes to play the Ransom*A*ware game, followed by a usability test to measure users'

satisfaction with the Ransom*A*ware. The current study adapts the System Usability Scale (SUS) questionnaire from [225]. This test was important for the current study to ensure that Ransom*A*ware achieves its design goals to meet the user's ransomware awareness needs. The SUS usability is supported by previous studies by [324], [325] and is considered a reliable test for small sample sizes by [326]. Thirty respondents participated in the usability test. The findings of SUS report that the lowest SUS score achieved by an individual is 75, and the maximum score is 97.5, with an overall average score of 87.58. These results are well above the required usability threshold of 68 recommended by [322], indicating that participants are satisfied with the game design. However, to validate the SUS results, each question's Mean and Standard Deviation was measured, and the overall findings suggest an acceptable data variation. All results are presented in Chapter 6.

In phase 3 of *Study 2*, participants were asked to complete the post-test, consisting of 10 questions based on National Cyber Security Centre UK guidelines on cyber security ransomware. The current study adopts a deductive approach for hypothesis formation and aims to assess whether Ransom*A*ware gameplay helped the user to improve their awareness of ransomware. The study collected data from 30 respondents to determine the effectiveness of the Ransom*A*ware game. *Paired-Sample t-Test* was employed, "It compares the mean from the *pre-test* to the mean from the *post-test* to detect if there is any statistically significant difference between the results". The statistical findings report that results from *post-test* (μ = 3.103, SD = 0.1520) are significantly greater than the pre-test (μ = 2.983, SD= 0.1642), t(29) = -5.410 with p-value $<$ 0.001 thus supports the hypothesis that Ransom*A*ware game has helped the user to improve their awareness against the ransomware cyber security threat. One-Sample Kolmogorov-Smirnov (K-S Test), a parametric test to check the normality, was used to validate these results. The findings of the K-S Test report that the p-value of the pre-test and post-test are less than 0.05, which means data is not normally distributed [329]. This indicates biasedness in Paired-Sample t-Test results which can be removed by increasing the sample size. However, as study 2 aims to evaluate the usability of Ransom*A*ware, all previous studies suggest a small sample size for usability tests [326] and [224]. Therefore, the current study opts alternative non-parametric statistical test called the *Wilcoxon signed-rank* rec-

ommended by [329] for smaller data sizes. The test findings reveal $p < 0.01$. This indicates there was a statistical difference between *pre-test* and *post-test* results. Hence validates user satisfaction with the Ransom*A*ware game design.

The second important part of *Study 2* was to empirically validate the elements of TTAT. These elements were employed during the game design and development phase reported in Chapter 5. The current study adopts thematic analysis, which is considered a useful and flexible method for qualitative analysis compared to grounded theory, as reported by [212]. As the current study aims to validate TTAT elements, the inductive and deductive analysis approach was followed to identify themes from qualitative data collected and discuss how it relates to elements of TTAT. The participants who played the Ransom*A*ware game in phase 3 were requested to participate in the semi-structured interview during phase 4 of the protocol. Study 2 validates usability in ransom*A*ware game design and the game's effectiveness in improving users' awareness against the ransomware cyber security threat. However, to avoid any biases in the findings and ensure the quality and trustworthiness of the findings [223], a qualitative data analysis approach was selected to answer the research question, i.e., to validate elements of the TTAT elements successfully embedded in Ransom*A*ware game. A semi-structured interview is a most widely used technique in qualitative research due to its flexibility and ability to provide rich information from its respondents [321]. While gaining an open response from the respondents, the current study ensures compliance with any ethical issues and collects data relevant to the research question only, i.e., it gains only a user view of the Ransom*A*ware game.

Fifteen respondents agreed to take part in the semi-structured interviews. These interviews were conducted individually with these participants. The current study adopts NVivo for analysing the unstructured data collected through semi-structured interviews. Thematic analysis was performed to identify codes and themes that emerged from data to answer the research. The findings are validated through inductive and deductive thematic analysis approaches. Thematic analysis reports some interesting findings which highlight themes that emerged and confirms the effectiveness of TTAT elements embedded in the Ransom*A*ware game. This confirms Ransom*A*ware effectiveness in improving users' awareness against ransomware

with much feedback on usable, interactive and engaging design, and users feel more confident after playing the game.

7.4 Implications of The Current Research

The current research findings suggest that Ransom*A*ware game significantly improves user awareness against the ransomware cyber security threat. The TTAT presented by previous studies [141] theoretically validates the individual's security behaviour. However, current research fills the gap of previous studies. It empirically validates the proposed Ransom*A*ware game for both, i.e. individuals and those in the organisational settings to thwart ransomware cyber security threat. This study will benefit individuals and those in organisational settings. The game Ransom*A* can empower them to improve their awareness of ransomware and handle such cyber threats in future.

Firstly, the current research results demonstrate that user avoidance behaviour against the ransomware cyber security threat is determined by avoidance motivation, the user's acknowledgement of the ransomware as a threat, and the user's perception of its severity and susceptibility to it. Secondly, developing a coping appraisal (s_eff, s_cos and s_Eff) is an antecedent to determine user avoidance motivation against the ransomware cyber security threat. These hypotheses are statistically significant and are in line with previous studies conducted by [141].

However, results from current research did not support hypothesis H4, i.e., Safeguard costs negatively affect avoidance motivation against ransomware. To explain this, TTAT mainly reports on computer users' security behaviour, whereas current research focuses on the cyber social model. The interaction between users and technology is more complex than ever before, making it challenging to preserve its security. Ransomware, in particular, is a novel concept which has emerged as the most malicious malware due to its ability to exploit humans as the weakest link. The repercussion of a ransomware attack is far more than any traditional malware. A ransomware attack is remotely controlled by the attacker, making the personal or organisational data inaccessible until a high-value ransom is paid in virtual currency.

Even then, it may result in critical data loss and bad publicity. Therefore the finding of the current research reveals that the high cost of safeguard will not influence users' avoidance motivation against the ransomware cyber security threat. Threat appraisal of the ransomware will be enough to influence the avoidance motivation of the user. This finding is a theoretical implication of current research.

In recent years there has been a rise in remote home working due to the pandemic, which has had a lasting effect on the number of employees working from home, increasing the security risks. Additionally, there has been a rise in ransomware as a Service (RaaS) [121]. It has been well documented that any ransomware attack will involve a substantial financial loss for an organisation, whether through paying the ransom to release the encrypted data, loss of profit from operational disruption, or fines incurred through data breaches. Furthermore, a high cost is involved for companies spending on information security compliance [333]. Most individuals depend on their home devices to organise and complete necessary tasks in their daily lives. The cost of installing any safeguarding measure is always considerably less financially and personally compared to a possible ransomware attack.

So, it is assumed that for both organisations and individuals, there is a question that the organisation would want to avoid the ransomware threat. Thus, in the context of current research, the cost of the safeguard measure will outweigh its benefits. Therefore, findings do not support hypothesis H4 and contribute to the theoretical implication of current research.

Humans are the most important component of the cyber social system, interacting with technology in individual or organisational settings. Therefore, the success and effectiveness of organisational cyber security compliance is pivotal to user awareness. The current research endorses cyber security training based on Ransom*A*ware game to improve the user's awareness against the ransomware cyber security threat. To ensure the confidentiality, integrity, and reliability of the cyber social system, Sowe *et al.* [334] have stated that security is the responsibility of every stakeholder in the digital ecosystem and its engagement is critical to preserve the security [335]. The current research informs senior management, policy and decision-makers in any organisation to design their information security programmes based on game-based learning. This can replace traditional theoretical training and help organisations

mitigate the risks of ransomware cyber security attack. Individual users can also benefit from the relationship between Ransom*A*ware game as safeguard effectiveness and the usability of the game design, which can develop their self-efficacy. The current research findings suggest that individuals in an independent setting may not consider the importance of cyber security due to its complex nature. Therefore game-based learning using Ransom*A*ware can help individuals to understand the severity of ransomware cyber security threat and improve their avoidance motivation against it in an interactive way through intuitive design, which can influence user learning through engagement.

7.5 Methodology Contribution in The Current Research

The current research provided a valuable methodology that contributed to developing a Ransom*A*ware game, which developers and designers can incorporate in future to design a usable game and follow a development process to deliver an efficient design. Two challenges in the current research were overcome during the design and development of the Ransom*A*ware game reported in Chapter 5.

The first methodological challenge was choosing the right game development methodology for the game as it involves coding. Likewise, any other software product, Ransom*A*ware, requires a software development life cycle. The literature in Chapter 5 reported that Agile and Scrum methodologies have been quite popular in developing efficient game design due to their ability to deliver working applications robustly through constant rigorous interaction with their stakeholders. This is normally managed by getting users' feedback at each stage of development and is more suitable for commercial product development. However, these methodologies were unsuitable for developing Ransom*A*ware game as they require several iterations, back and forth with users during the development process.

In contrast, the Waterfall methodology is more suitable for the development projects when product requirements are clear initially and do not require constant interaction with stakeholders. Therefore, the current research adopted Waterfall

to follow ransomware's software development life cycle. However, to address the implementation of usability in the game Ransom*A*ware, these traditional methodologies focus more on the software development process and only the aesthetics of the application design. In contrast, the user experience design is more than that and requires a rigorous set of activities to deliver a user-centred design.

Therefore, the second methodological challenge was selecting the right design methodology for the game design, which can focus on usability to meet the current research objective to improve ransomware awareness through usable game-based learning. To address this challenge of creating user experience in the Ransom*A*ware game design. Games Garrett's methodology on elements of user experience was reviewed. This methodology is quite popular for usable web solutions. However, the gaming concept is beyond web applications and requires more user engagement and interaction. Therefore this challenge was exploited into an opportunity, and a new framework based on adapted elements of user experience and Waterfall called the Unified U*X*D model was proposed. Ransom*A*ware game is designed and developed on this model and empirically validated in *Study 2*.

This proposed methodology is unique, which can allow future design researchers and developers to map their requirements for an efficient end product. The new proposed methodology unifies the set of activities which can guide the product designers and the developers to collaborate and deliver a user-centred design. Although game design and development are two different processes, it is one product in the user's view. Therefore, the proposed framework can allow product designers and developers to synchronise their work in an agile fashion without the need for stakeholder involvement at each stage of the development. The proposed unified framework can be adopted for organisations to deliver small projects with a more efficient delivery time, as it simultaneously allows usability and game development implementation. The current research aimed to design and develop an education and awareness game on ransomware threat. This means the proposed design and development methodology can benefit organisations involved in making educational games to deliver a usable design which can motivate users and provide fun learning [336]. The proposed unified model allows synchronisation between designer and developer, thus allowing the organisations to impact society to deliver educational games quicker. The

commercials in educational games can fast track design and development of usable games and quickly reach the market with their end-product to stay competitive, which can also benefit them monetarily.

7.6 Practical Contribution in The Current Research

This study can significantly contribute to the academic body of knowledge on the gamification of cyber security training in various areas such as government, healthcare, and education. This will help some of the most susceptible organisations to ransomware to lower the risk of succumbing to an attack.

Ransom*A*ware is a practical contribution addressing the knowledge gaps mentioned in the previous section. It is a working game that can be played as opposed to a theoretical description of a game. It also has an engaging storyline and interactivity to captivate users, thus increasing their knowledge and altering their behaviour regarding ransomware threats. The study makes a practical contribution to the ability of organisations to combat the threat of ransomware. By producing a game that can be used by organisations such as the government, healthcare providers or schools/higher education/cyber trainers to train people on practical methods to avoid facilitating a ransomware attack. The government bodies dedicated to tackling cyber crime should raise awareness of the training among organisations and encourage them to deploy it throughout their organisations. A nationwide campaign and events, such as school visits, to publicise the training.

The current research suggests, within organisations, the Ransom*A*ware game training can be deployed as part of the organisation's Information Security Management System (ISMS) in accordance with the ISO/EIC 27001:2017 standard Annex A, control objective "*A.7.1.2: To ensure that employees and contractors are aware of their information security responsibilities.*" [283]. This can help the organisations to fulfil their mandatory responsibility under the subsection "*A.7.2.2: Information security awareness, education and training for employees and contractors.*", [283].

As mentioned in ISO/EIC 27002:2017 [337], ' information security awareness, education and training programmes' are essential for ensuring that staff and contractors understand the policies and objectives of the ISMS, relevant to their roles and responsibilities and tailored to their skill levels. Furthermore, that training should help them comprehend why it is important that they need to adhere to the

policies and how their actions can affect the organisation (ISO/EIC, 2017). For this reason, the Ransom*A*ware game training can benefit all staff and contractors working with the organisation to help organisations ensure a high level of comprehension and efficacy.

Ransomware is a complex threat, and researchers [338] theorised that cyber security training could be difficult for a non-technical staff member. There is also a potential risk of delivering 'dry' training material that does not motivate the user and inhibits the learning process. The current study can inform that the Ransom*A*ware game would have the potential to engage the user through its story and interactivity thoroughly with the knowledge that could easily be transferred to their working practices. They could learn at their own pace while getting immediate feedback. Additionally, deploying the game would be low cost for the organisation and entail less physical risk, making it more accessible than traditional training [338]. Ransom*A*ware game-based learning can be a more cost-effective method of training than traditional training methods, making it a more attractive training type for an organisation to adopt. Game-based learning has been successfully utilised in other industries, such as aviation and medicine, to train professionals [339]. Similarly, [340] confirmed that game-based learning positively affects school students' engagement and satisfaction and supports remote teaching methods adopted due to Covid-19 [340], which may be another consideration in case of future outbreaks.

The Ransom*A*ware game could be included with other IT or security-related training activities or as a standalone training exercise. The game aims to be accessible and relevant to all individual roles and responsibilities, plus understandable for all skill levels, as per the ISO recommendations. It is recommended that staff are tested after the training to confirm that they have adequately understood and assimilated the knowledge delivered (ISO/EIC, 2017). Ransom*A*ware game, through its interactive game story, adopts the mechanism of earning points and awarding users based on their final score. This can help organisations meet the requirements of compliance required in the field of cyber security as recommended by (ISO/EIC, 2017).

The Ransom*A*ware game can be distributed at least yearly, and the best practice would be to repeat the training throughout the year. The game would be updated

to reflect any policy changes impacting the organisation's training requirements if required. This will ensure the training is kept current and delivered as new employees and contractors start working for the organisation or move into new roles within the organisation. It shall be working in support of the organisation's policies and security controls for information security management so it is closely aligned with the objectives of the organisation's security awareness programme, which would include campaigns with events and various media distributed throughout the organisation. The game itself can be accessed online and downloaded onto various devices. This will be easy to access for employees and contractors working in the office or remotely at home or elsewhere. To help address the issues that organisations face with the training staff, considering the increase in post-COVID homeworking practices, which has been shown to increase the risk of a security incident for the organisation.

These could be the main beneficiaries of game-based learning:

- The governing bodies of organisations should decide to deploy the training and send a clear and consistent message to the organisation as such, emphasising the importance of the training and also, monitoring the deployment of the game and providing persistent communication on the organisation's progress with the training and its effect on cyber security. The game-based learning delivered throughout the organisation will help them meet standards and compliance requirements and lower security risks which could impact the organisation, such as data breaches which could result in the organisation incurring fines and reputational damage.

- Managers should encourage their staff to undertake the training and monitor their participation and results. They should set goals and regular check-ins with staff to facilitate learning and remove any hurdles that may prevent them from participating in the training—providing them with time to do the training and engaging with employees regarding the training and subject matter.

- The Ransom*A*ware game-based learning can help strengthen security and compliance, providing management persistence with supporting it in the long term. Managers' targets should incorporate measurement of their promotion of the game among staff, the training results and the progression of staff's knowl-

edge. It can mitigate the risk of a ransomware attack on business operations to avoid disruption. This will help the managers meet their business objectives and enhance the company's reputation and profits.

- HR managers should draw out organisation-wide training schedules which ensure cyber training that incorporates the game is undertaken regularly, at least once a year or when a major change requires re-educating employees. Participation should be stipulated as a requirement for employment, in which case the game would be updated to reflect policy changes. The game-based learning would make the onboarding process easier, in which HR is required to deliver security and policy training to new employees. Contractors should also be included. It would enhance the trainee experience of assimilating knowledge and saving time by replacing dry induction training and classroom-based learning with game-based learning. HR should also provide contact points for the participants to get further information and training materials.

- The IT department would also benefit from game-based training to supplement any policies and procedures it needs to convey to the organisation's employees. Making this easier, quicker, and more cost effective than traditional training. By delivering the information through this method, which is engaging and easy to assimilate for learners, they will see an increase in beneficial security-related behaviours from staff members. The effect will be fewer security incidents for them to address, less downtime, recovery, and less damage to the organisation.

- Individuals can benefit from the knowledge conveyed through the Ransom*A*ware game and the enjoyment of playing the game. Plus, a sense of self-efficacy concerning security matters will lead to efficient handling of security issues and avoidance of time-consuming and costly security incidents which would otherwise have disrupted their work. As many individuals run most of their personal lives on devices connected to the internet, they will experience increased security and reduced disruption by utilising the knowledge gained in circumventing attacks.

7.7 Summary

This chapter discusses the findings of *Study 1* performed in current studies. In *Study 1*, a theoretical model was developed based on the TTAT. This model was empirically tested to evaluate the effectiveness of elements of TTAT to be included in Ransom*A*ware. The model was validated using quantitative data analysis. The statistical findings supported all the hypotheses in line with the previous study conducted by Liang & Xue except H4, for which the findings of the current research were not significant to support the negative effect of safeguard cost on avoidance motivation. This reveals its findings in the context of Ransomware phenomena which is relatively new in the cyber security domain. Whereas the discussion in *Study 2* provides an empirical evaluation of the game design, the respondents were asked to play the game. The results were quantitatively analysed to test the usability of the Ransom*A*ware game. The current research findings supported the usability embedded in the game design. This was further followed by semi-structured interviews to empirically confirm elements of TTAT embedded in the game, qualitative analysis was performed, and results were validated through thematic analysis. The current study contributes to theoretical, methodological and practical implications. It suggests how individuals and organisations can benefit from game-based learning to improve their user education against ransomware cyber security threat. It endorses the inclusion of game-based learning in cyber security awareness programmes for organisations, so the decision and policymakers can benefit from it to mitigate risks of cyber-attacks to their organisations and for the individuals to take control of their security intuitively.

Chapter 8

Conclusion and Future Recommendations

8.1 Conclusion

This chapter provides a conclusion derived from the research thesis. It makes future recommendations on how the proposed, Ransom*A*ware game can be put into practice Cyber Security Management Framework for effective user awareness against ransomware. Finally, this chapter also identifies research limitations and opportunities for future work to extend the findings of this research. The current research aimed to develop a usable security approach for user awareness against ransomware cyber security threat. Ransomware is malware which takes a user's machine hostage, encrypts all the files, and prevents a legitimate user from accessing its device unless a ransom is paid in the form of virtual currency in exchange for decryption by criminals (NCSC, 2020). There is no guarantee that data will be restored even if the payment is made. NCSC and Cyber Crime Agency UK advise users not to pay criminals any extortion to these criminals [341]. There have been some previous studies on computer security. However, ransomware is a new phenomenon, and the user has been identified as the weakest link, which the attacker exploits. The current research found this as a gap in addressing user awareness challenges about ransomware. The principal contribution of the current research is the game prototype design, enabling users to improve their awareness against the rising ran-

somware cyber security threat. Two studies were conducted in the current research to contribute to the research gap identified. The summary of the research objectives achieved is presented in the section below.

- Objective 1:

  Critically appraise the cyber-social model to explore the challenging relationship between cyber-technology and end users.

  This objective of the current research was addressed in Chapter 2. It provides a literature review on the cyber social system, the rise of cyber security threats and the anatomy of ransomware. Moreover, it discusses the need for game-based learning in the cyber security domain to address the research gap related to user awareness against the cyber security threat ransomware. A detailed overview of the cyber social system is presented in this chapter, which identifies humans as an integral part of the Cyber-Physical Systems (CPSs). With the rise of the Internet of things, CPSs have emerged as a smart solution to revolutionise human lives. By 2023 the internet will connect 5.1 billion Internet users and 29.3 billion devices [342]. The literature on smart (homes, cities, healthcare, grids and disaster management) was reviewed to explore how Internet-connected cyber-physical systems have become part of the cyber social system. This relationship benefits humans with its efficient and robust solutions for day-to-day operations and supporting critical infrastructure. The ability of these cyber-physical systems to share data requires constant internet connectivity. However, this makes them vulnerable to cyber-attacks. As a result, these systems' confidentiality, integrity and availability can be compromised. Literature informs that due to the broader societal capabilities of cyber-physical systems, the reliable relationship between humans and the cyber social system can only be safeguarded through cyber resilience. This informs human awareness of the cyber security threats to be paramount to mitigate these risks.

- Objective 2:

  Critically identify factors contributing to the lack of user awareness of the "Ransomware" threat.

  To address objective 2 of the current research, chapter 2 also explored different cyber security threats and narrowed the review to ransomware malware. Ransomware has been identified as the most severe threat to the UK, reported by NCSC. Individuals and organisations are at constant risk of being exploited by cyber criminals. National Cyber Security Strategy, UK (Office, 2022) reports that ransomware attacks continue to become even more sophisticated and damaging. In this chapter, the social engineering technique, phishing/spear phishing, has been identified as one of the most widely attack-vector used by attackers to deceive humans. The criminals send phishing emails to trick users by asking them to reveal their personal information. The literature review further informs that security is the responsibility of everyone, thus emphasising the need for user awareness to combat such cyber security attacks. After presenting a detailed overview of the cyber social system, and a discussion on changing landscape of cyber security, ransomware has been identified as an emerging cyber threat, which exploits user lack of awareness of phishing emails. This means ransomware requires user action to execute. Thus, the literature review in current research determines that cyber security is not just a technical problem. There is a dire need to improve user awareness of the evolving ransomware cyber security threat. Considering cyber security is a complex domain, improving user awareness of ransomware phenomena was daunting. The literature in the current thesis informs that game-based learning has been widely used as a teaching pedagogy to motivate and engage users in their learning. Its usage is also common in other fields of society, such as military training, driving hazard perception, flight simulation and others. However, no literature on the practical use of game-based learning for ransomware was available. Therefore, this opportunity has been identified as a research gap in the current thesis, and this chapter concluded intending to address ransom awareness for the user through the design and development of a usable game prototype.

- Objective 3:

  Design a usable game-based prototype to improve user awareness of ransomware

  To achieve objective 3 of the current research. In this thesis, the research aims to improve user awareness of the Ransomware cyber security threat using game-based learning. In Chapter 5, there were two critical goals to consider during the design and development phase of the game; (i) The findings reported by Chapter 4 on how elements of TTAT to embed in the Ransom*A*ware game (ii) A usable game to enhance the user engagement of the ransomware awareness. The game design and development process adopted a unified U*X*D model. This chapter introduces the game story and the memorable characters involved. Several techniques were adopted, such as; High-level requirements, User Personas, MoSCoW analysis, Task modelling, User Journeys, Game Architecture design and wireframes to implement usability and elements of TTAT in the design. Several design artefacts are included to provide a walk-through of the steps taken during the game's development and the design outcome.

- Objective 4:

  Empirically evaluate the effectiveness of a game-based prototype to assess awareness of ransomware.

  To achieve objective 4 of the current research. In the current thesis following tasks were performed; (1) To confirm the Ransom*A*ware usability, and (2) to confirm the effectiveness of TTAT elements successfully embedded in the game design. In Chapter 6, the study employed experimental procedures to collect primary data and adopted a mixed-method approach to analyse data. To empirically evaluate the usability of the game design, users were invited to play Ransom*A*ware. The results were validated using quantitative analysis. The statistical findings report significant results confirming the usability of the game design. To empirically validate the presence of elements of the TTAT in the game design. Study 2 employed thematic analysis to perform qualitative analysis. The findings of the thematic analysis were synthesised which validates that elements of TTAT are successfully embedded in the game design.

The current research aimed at developing a usable game design based on the internationally accepted TTAT model. The findings reported in this thesis confirm the user's satisfaction with the Ransom*A*ware game and empirically validate the effectiveness of the user learning against the ransomware cyber security threat.

8.2 Contributions of the Thesis

The research in this thesis addressed user awareness of ransomware cyber security threat using game-based learning. The thesis provides significant contributions in the following areas:

- Theoretical Contribution - The findings of the current research inform that ransomware is a new phenomenon, and users' consideration of the safeguard cost outweighs when it comes to mitigating ransomware attack. Also, game-based learning was identified as a gap to address the complex domain of cyber security.
- Methodology Contribution - Proposed a unified methodology called U*X*D to support the game development process and the implementation of user experience systematically in the design.
- Practical Contribution - Designed and developed a working game Ransom*A*ware. which is a novel concept to the author's best of knowledge. The game was empirically evaluated to ensure it achieves its intended outcomes.

8.3 Research Limitations

The research presented in the thesis aimed to develop a usable solution to improve user awareness against the ransomware threat, which is identified as a significant threat to the UK. Like all research studies, this research also has some limitations. One limitation is that the study demographics represent only the UK population, while ransomware shows increased globalised trends in recent years. The current

research findings can not be generalised as the cyber social system is complex, particularly in the post-covid world is more technology driven. The literature review suggests that humans are the weakest link in a cyber social system. Even though a sample was recruited from individual home computer users and those in the organisational setting, this does not represent the population of general computer users. Therefore author suggests careful considerations should be made while generalising current research findings to a wider context. Another limitation of the current study is that it is based on the Technology Threat Avoidance Theory (TTAT), which focuses more on the cognitive behaviour of the user related to malicious IT concepts. The current research considers two domains of cognitive behaviour, i.e., threat appraisal and coping appraisal, to test the proposed game. Though, this theory was empirically validated through game-based learning in the context of ransomware awareness. There are several other social elements (culture, language) than these domains, which the research can be further extended, but was considered out of scope for the current thesis. Ransomware is malware which needs an attack vector to transport. The literature in the current thesis informs humans as the main facilitators of ransomware attacks. It identifies phishing, insecure configurations, weak passwords, and insecure software development are the main enablers of ransomware attacks. Among all these, phishing is reported as the most common cause of ransomware attacks. The research in the current thesis only addresses the gamification of phishing techniques to improve user awareness of ransomware. It was quite challenging and overwhelming to accommodate all the ransomware attack vectors in the game design due to their different attack philosophies. Thus future research can be conducted to explore this opportunity with different attack vectors.

Another limitation of this research was the use of a game development platform. MIT App Inventor was chosen due to its ability to offer an online development environment and visual block programming to build an Android-based App. This platform is quite popular for developing mobile games to solve real-world problems. Although the game Ransom*A*ware was successfully developed using the MIT App inventor and later empirically tested to meet its objective. However, the tool did not allow the creation of a high-fidelity prototype and restricted the author with limited functionalities of the tool. In any development environment, if a platform

allows more freedom for bespoke applications, this can bring more innovation to the product.

8.4 Future Research

The findings of the current thesis provide contributions related to theory, methodology and practice reported in Chapter 7. The limitations of the current research pose challenging opportunities for future researchers. Potential enhancements for future research are conceivable.

- National Artificial Intelligence strategy July 2022, set outs UK ambitions towards automation of different public sectors including education. This can be an opportunity and motivation for future developers to enhance the automation of Ransom*A*ware through embedding a trained AI model. Which can enable Ransom*A*ware to make more smart decisions such as; Generating contents of new phishing emails automatically, and predicting messages based on the user's learning needs i.e., the messages that the user is more likely to fail or recognise as a legitimate message. User success rate based on types of malicious emails e.g., attachments, and links.

- Developing a Ransom*A*ware game using the MIT App inventor tool was an interesting experience for the author. However, at the same time, it was a daunting task to implement a game story with memorable characters. The findings of the game development experience in the current thesis inform researchers to explore more innovative game development environments, such as Android Studio or similar development platforms, that can allow design innovation to improve or commercialise the Ransom*A*ware game prototype.

- The future iteration of the game can include cross-platform compatibility to run on iOS and android platforms. The game can be integrated into the database, allowing the user to view the history of tests taken, particularly past scores and track improvement with performance test statistics, e.g., how much it took to complete.

- The findings show that ransomware is a global issue and is continuously increasing. The cyber security agencies from the United Kingdom, Unites States, and Australia have made a joint task force to unify their strengths and reduce the impact of ransomware. National government advisory bodies of the UK, US and Australia (NCSC-UK, CISA, NSA and ACSC) have recommended user awareness training to mitigate its risks. Users, organisations and critical infrastructure are connected through cyber-physical systems and are more at risk of ransomware attacks. This is an opportunity for future research to collect data globally so that research can benefit in a wider context.

- The research presented in this thesis presented a game prototype based on phishing that helped the users improve their learning of ransomware to thwart it. The future iteration of this game could be further extended and include other ransomware attack vectors. The game-based learning can be integrated into cyber security training programmes. It can be extended to more audiences, such as software developers and IT administrators, to improve their awareness of the importance of secure software development and configurations to mitigate the risks of ransomware.

From the suggestions presented for the future road map, it can be seen that there are still more opportunities to enhance user awareness through Ransom*A*ware, especially with the support of professional game development platforms. There is also an opportunity to reach a global audience, so they can benefit from this research. However, the research presented in this thesis has provided a strong foundation for future research towards enhancing user awareness of the contemporary ransomware issue in the cyber security domain.

References

[1] Yuchong Li and Qinghui Liu. "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments". In: *Energy Reports* 7 (2021), pp. 8176–8186.

[2] Roger A. Grimes. "Future of Ransomware". In: *Ransomware Protection Playbook*. 2022, pp. 261–272.

[3] Christopher Kuner et al. "The rise of cybersecurity and its impact on data protection". In: *International Data Privacy Law* 7.2 (2017), pp. 73–75.

[4] Kim-Kwang Raymond Choo. "The cyber threat landscape: Challenges and future research directions". In: *Computers & security* 30.8 (2011), pp. 719–731.

[5] Cheerala Rohith and Ranbir Singh Batth. "Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War Between Nations and its Repercussion". In: *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*. 2019, pp. 640–645. DOI: 10.1109/ICCIKE47802.2019.9004236.

[6] Kelce S Wilson and Müge Ayse Kiy. "Some fundamental cybersecurity concepts". In: *IEEE access* 2 (2014), pp. 116–124.

[7] Olufunsho I. Falowo et al. "Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents (December 2022)". In: *IEEE Access* (2022), pp. 1–1. DOI: 10.1109/ACCESS.2022.3231847.

[8] Saman Taghavi Zargar, James Joshi, and David Tipper. "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding At-

tacks". In: *IEEE Communications Surveys Tutorials* 15.4 (2013), pp. 2046–2069. DOI: 10.1109/SURV.2013.031413.00127.

[9] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. "A Survey of Man In The Middle Attacks". In: *IEEE Communications Surveys Tutorials* 18.3 (2016), pp. 2027–2051. DOI: 10.1109/COMST.2016.2548426.

[10] Gowthamaraj Rajendran et al. "Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures". In: *2019 International Carnahan Conference on Security Technology (ICCST)*. 2019, pp. 1–6. DOI: 10.1109/CCST.2019.8888399.

[11] Kathleen Hall Jamieson. *Cyberwar: how Russian hackers and trolls helped elect a president: what we don't, can't, and do know*. Oxford University Press, 2020.

[12] Tasnuva Mahjabin et al. "A survey of distributed denial-of-service attack, prevention, and mitigation techniques". In: *International Journal of Distributed Sensor Networks* 13.12 (2017), p. 1550147717741463.

[13] Steve Mansfield-Devine. "DDoS goes mainstream: how headline-grabbing attacks could make this threat an organisation's biggest nightmare". In: *Network Security* 2016.11 (2016), pp. 7–13.

[14] Panos Kostakos et al. "Catchem: A Browser Plugin for the Panama Papers using Approximate String Matching". In: *2017 European Intelligence and Security Informatics Conference (EISIC)*. IEEE. 2017, pp. 139–142.

[15] Usman Javed Butt et al. "Ransomware Threat and its Impact on SCADA". In: *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*. 2019, pp. 205–212. DOI: 10.1109/ICGS3.2019.8688327.

[16] Shou-Ching Hsiao and Da-Yu Kao. "The static analysis of WannaCry ransomware". In: *2018 20th international conference on advanced communication technology (ICACT)*. IEEE. 2018, pp. 153–158.

[17] Qian Chen and Robert A Bridges. "Automated behavioral analysis of malware: A case study of wannacry ransomware". In: *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE. 2017, pp. 454–460.

[18] Jim Isaak and Mina J. Hanna. "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection". In: *Computer* 51 (8 Aug. 2018), pp. 56–59. ISSN: 0018-9162. DOI: 10.1109/MC.2018.3191268.

[19] Julia E Sullivan and Dmitriy Kamensky. "How cyber-attacks in Ukraine show the vulnerability of the US power grid". In: *The Electricity Journal* 30.3 (2017), pp. 30–35.

[20] Yingmeng Xiang, Lingfeng Wang, and Nian Liu. "Coordinated attacks on electric power systems in a cyber-physical environment". In: *Electric Power Systems Research* 149 (2017), pp. 156–168.

[21] Lawrence J Trautman and Peter C Ormerod. "Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach". In: *Am. UL Rev.* 66 (2016), p. 1231.

[22] Hicham Hammouchi et al. "Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time". In: *Procedia Computer Science* 151 (2019), pp. 1004–1009.

[23] Aaron Perzanowski and Jason Schultz. *The end of ownership: Personal property in the digital economy*. MIT Press, 2016.

[24] Emily McReynolds et al. "Toys that listen: A study of parents, children, and internet-connected toys". In: *Proceedings of the 2017 CHI conference on human factors in computing systems*. 2017, pp. 5197–5207.

[25] Emmeline Taylor and Katina Michael. "Smart toys that are the stuff of nightmares". In: *IEEE Technology and Society Magazine* 35.1 (2016), pp. 8–10.

[26] Johnny Botha, Marthie Grobler, and Mariki Eloff. "Global data breaches responsible for the disclosure of personal information: 2015 & 2016". In: *European Conference on Cyber Warfare and Security*. Academic Conferences International Limited. 2017, pp. 63–72.

[27] Samuel Greengard. "The new face of war". In: *Communications of the ACM* 53.12 (2010), pp. 20–22.

[28] David Kushner. "The real story of stuxnet". In: *ieee Spectrum* 50.3 (2013), pp. 48–53.

[29] Steven Furnell, Pete Fischer, and Amanda Finch. "Can't get the staff? The growing need for cyber-security skills". In: *Computer Fraud & Security* 2017.2 (2017), pp. 5–10.

[30] Daniel Pedley et al. *Cyber security skills in the UK labour market 2020*. 2020.

[31] Hussain Aldawood and Geoffrey Skinner. "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review". In: *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. 2018, pp. 62–68. DOI: 10.1109/TALE.2018.8615162.

[32] Madeline Carr. "Public–private partnerships in national cyber-security strategies". In: *International Affairs* 92.1 (2016), pp. 43–62.

[33] Hans de Bruijn and Marijn Janssen. "Building cybersecurity awareness: The need for evidence-based framing strategies". In: *Government Information Quarterly* 34.1 (2017), pp. 1–7.

[34] Joe Kim. "Cyber-security in government: reducing the risk". In: *Computer Fraud & Security* 2017.7 (2017), pp. 8–11.

[35] Jose M Such et al. "Basic cyber hygiene: Does it work?" In: *Computer* 52.4 (2019), pp. 21–31.

[36] Government. *Procurement Policy Note 09/14: Cyber Essentials scheme certification - GOV.UK*. https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification. 2016.

[37] Parliament. *Cyber crime and security*. https://commonslibrary.parliament.uk/cyber-crime-and-security/. 2017.

[38] Maria Bada, Angela M Sasse, and Jason RC Nurse. "Cyber security awareness campaigns: Why do they fail to change behaviour?" In: *arXiv preprint arXiv:1901.02672* (2019).

[39] NCSC. *CF-Annual-Report-2020-21-Final-Version.pdf*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ncsc.gov.uk/files/CF-Annual-Report-2020-21-Final-Version.pdf. 2020.

[40] Chris Ensor. "Investing in UK Cyber Talent". In: *ITNOW* 58.2 (2016), pp. 58–59. DOI: 10.1093/itnow/bww054.

[41] DCMS. *New online challenge will test teenagers' cyber security skills - GOV.UK*. https://www.gov.uk/government/news/new-online-challenge-will-test-teenagers-cyber-security-skills. 2017.

[42] Saleh AlDaajeh et al. "The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education". In: *Computers & Security* (2022), p. 102754.

[43] Michelle Goddard. "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact". In: *International Journal of Market Research* 59.6 (2017), pp. 703–705.

[44] IT Governance. *The GDPR (General Data Protection Regulation) — IT Governance*. https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation. 2018.

[45] Audrey Guinchard. "Our digital footprint under Covid-19: should we fear the UK digital contact tracing app?" In: *International Review of Law, Computers & Technology* 35.1 (2021), pp. 84–97.

[46] UK Government. *Data protection: The Data Protection Act - GOV.UK*. https://www.gov.uk/data-protection. 2018.

[47] Alan Calder. *EU GDPR: a pocket guide*. IT Governance Ltd, 2018.

[48] Eugenia Politou, Efthimios Alepis, and Constantinos Patsakis. "Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions". In: *Journal of cybersecurity* 4.1 (2018), tyy001.

[49] David J Hand. "Aspects of data ethics in a changing world: Where are we now?" In: *Big data* 6.3 (2018), pp. 176–190.

[50] Luís M. Pedroso et al. "How can GDPR fines help SMEs ensuring the privacy and protection of processed personal data". In: *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*. 2021, pp. 1–6. DOI: 10.23919/CISTI52073.2021.9476620.

[51] John Mingers. "Combining IS research methods: towards a pluralist methodology". In: *Information systems research* 12.3 (2001), pp. 240–259.

[52] Stephen Hart et al. "Riskio: A serious game for cyber security awareness and education". In: *Computers & Security* 95 (2020), p. 101827.

[53] Hilary Collins. *Creative research: the theory and practice of research for the creative industries*. Bloomsbury Publishing, 2018.

[54] Diego Romaioli. "A generative sequential mixed methods approach using quantitative measures to enhance social constructionist inquiry". In: *Journal of Mixed Methods Research* 16.2 (2022), pp. 207–225.

[55] Theophilus Azungah. "Qualitative research: deductive and inductive approaches to data analysis". In: *Qualitative research journal* (2018).

[56] Niklas Luhmann. *Social systems*. stanford university Press, 1995.

[57] Talcott Parsons and Edward A. Shils. *Toward a General Theory of Action*. Routledge, July 2017. ISBN: 9781351301527. DOI: 10.4324/9781351301527.

[58] Yuchen Zhou et al. "Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities". In: *IEEE Communications Surveys & Tutorials* 22.1 (2019), pp. 389–425.

[59] Edward R Griffor et al. *Framework for cyber-physical systems: volume 1, overview*. National Institute of Standards and Technology, June 2017. DOI: 10.6028/NIST.SP.1500-201.

[60] flaticon. *"smart city icons" created by Freepik - Flaticon*. https://www.flaticon.com/search?word=smart%20city. 2022.

[61] Ray Y Zhong et al. "Intelligent manufacturing in the context of industry 4.0: a review". In: *Engineering* 3.5 (2017), pp. 616–630.

[62] Alessandro Quarto et al. "IoT and CPS applications based on wearable devices. A case study: Monitoring of elderly and infirm patients". In: *2017 IEEE Workshop on Environmental, Energy, and Structural Monitoring Systems (EESMS)*. IEEE. 2017, pp. 1–6.

[63] David Nunes, Jorge Sá Silva, and Fernando Boavida. *A Practical Introduction to Human-in-the-loop Cyber-physical Systems*. John Wiley & Sons, 2018.

[64] Wolfgang Bohm et al. "4th International Workshop on Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC'18)". In: IEEE, Apr. 2018, pp. 1–2. ISBN: 978-1-5386-7468-0. DOI: 10.1109/EITEC.2018.00005.

[65] Eric Ke Wang et al. "Security issues and challenges for cyber physical system". In: *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*. IEEE. 2010, pp. 733–738.

[66] Berkeley. *Cyber-Physical Systems - a Concept Map*. https://ptolemy.berkeley.edu/projects/cps/. (Accessed on 12/05/2022). 2018.

[67] Siddhartha Kumar Khaitan and James D McCalley. "Design techniques and applications of cyberphysical systems: A survey". In: *IEEE Systems Journal* 9.2 (2014), pp. 350–365.

[68] Shafiq ur Rehman and Volker Gruhn. "An approach to secure smart homes in cyber-physical systems/Internet-of-Things". In: *2018 Fifth International Conference on Software Defined Systems (SDS)*. IEEE. 2018, pp. 126–129.

[69] Rosslin John Robles and Tai-hoon Kim. "Applications, systems and methods in smart home technology: A". In: *Int. Journal of Advanced Science And Technology* 15 (2010), pp. 37–48.

[70] Jordi Mongay Batalla, Athanasios Vasilakos, and Mariusz Gajewski. "Secure smart homes: Opportunities and challenges". In: *ACM Computing Surveys (CSUR)* 50.5 (2017), pp. 1–32.

[71] United Nations. *68% of the world population projected to live in urban areas by 2050, says UN — UN DESA — United Nations Department of Economic and Social Affairs*. https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html. 2018.

[72] Hadi Habibzadeh et al. "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities". In: *Sustainable Cities and Society* 50 (2019), p. 101660.

[73] Lei Cui et al. "Security and privacy in smart cities: Challenges and opportunities". In: *IEEE access* 6 (2018), pp. 46134–46145.

[74] Mohd Abdul Ahad et al. "Enabling technologies and sustainable smart cities". In: *Sustainable cities and society* 61 (2020), p. 102301.

[75] Dolf Gielen et al. "The role of renewable energy in the global energy transformation". In: *Energy Strategy Reviews* 24 (2019), pp. 38–50.

[76] Silvia H Bonilla et al. "Industry 4.0 and sustainability implications: A scenario-based analysis of the impacts and challenges". In: *Sustainability* 10.10 (2018), p. 3740.

[77] Mohammad Esmalifalak et al. "Detecting Stealthy False Data Injection Using Machine Learning in Smart Grid". In: *IEEE Systems Journal* 11 (3 Sept. 2017), pp. 1644–1652. ISSN: 1932-8184. DOI: 10.1109/JSYST.2014.2341597.

[78] Xinghuo Yu and Yusheng Xue. "Smart grids: A cyber–physical systems perspective". In: *Proceedings of the IEEE* 104.5 (2016), pp. 1058–1070.

[79] Ramasamy Mariappan, PV Narayana Reddy, and Chang Wu. "Cyber physical system using intelligent wireless sensor actuator networks for disaster recovery". In: *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*. IEEE. 2015, pp. 95–99.

[80] Niranjan Suri et al. "Exploiting smart city IoT for disaster recovery operations". In: *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. IEEE. 2018, pp. 458–463.

[81] Kwok Tai Chui et al. “Disease diagnosis in smart healthcare: Innovation, technologies and applications”. In: *Sustainability* 9.12 (2017), p. 2309.

[82] Stephanie B Baker, Wei Xiang, and Ian Atkinson. “Internet of things for smart healthcare: Technologies, challenges, and opportunities”. In: *Ieee Access* 5 (2017), pp. 26521–26544.

[83] R Shantha Mary Joshitta and L Arockiam. “Device authentication mechanism for IoT enabled healthcare system”. In: *2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)*. IEEE. 2017, pp. 1–6.

[84] Kefei Mao et al. “Security enhancement on an authentication scheme for privacy preservation in ubiquitous healthcare system”. In: *2015 4th International Conference on Computer Science and Network Technology (ICCSNT)*. Vol. 1. IEEE. 2015, pp. 885–892.

[85] Jyri Rajamäki, Julia Nevmerzhitskaya, and Csaba Virág. “Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF)”. In: *2018 IEEE Global Engineering Education Conference (EDUCON)*. IEEE. 2018, pp. 2042–2046.

[86] Jing Zeng et al. “A survey: Cyber-physical-social systems and their system-level design methodology”. In: *Future Generation Computer Systems* 105 (2020), pp. 1028–1042.

[87] Alex Pentland, Alexander Lipton, and Thomas Hardjono. *Building the New Economy: Data as Capital*. MIT Press, 2021.

[88] David Sousa Nunes, Pei Zhang, and Jorge Sá Silva. “A survey on human-in-the-loop applications towards an internet of all”. In: *IEEE Communications Surveys & Tutorials* 17.2 (2015), pp. 944–965.

[89] Rossouw Von Solms and Johan Van Niekerk. “From information security to cyber security”. In: *computers & security* 38 (2013), pp. 97–102.

[90] Stephen Hinde. “Security surveys spring crop”. In: *Computers & Security* 21.4 (2002), pp. 310–321.

[91] Gurpreet Singh Matharu, Priyanka Upadhyay, and Lalita Chaudhary. "The internet of things: Challenges & security issues". In: *2014 International Conference on Emerging Technologies (ICET)*. IEEE. 2014, pp. 54–59.

[92] Rajesh Kumar Goutam. "Importance of cyber security". In: *International Journal of Computer Applications* 111.7 (2015).

[93] Srijoy Dutta and Rohan Mathur. "Cybersecurity—An integral part of STEM". In: *IEEE 2nd Integrated STEM Education Conference*. IEEE. 2012, pp. 1–4.

[94] Steve M Hawkins, David C Yen, and David C Chou. "Disaster recovery planning: a strategy for data security". In: *Information management & computer security* (2000).

[95] Nader Sohrabi Safa, Rossouw Von Solms, and Steven Furnell. "Information security policy compliance model in organizations". In: *computers & security* 56 (2016), pp. 70–82.

[96] Edward Humphreys. "Information security management standards: Compliance, governance and risk management". In: *information security technical report* 13.4 (2008), pp. 247–255.

[97] Erastus Karanja. "The role of the chief information security officer in the management of IT security". In: *Information & Computer Security* (2017).

[98] NIST. *Risk Management — NIST*. `https://www.nist.gov/risk-management`. 2022.

[99] Andy Taylor et al. *Information Security Management Principles British Computer Society*. BCS, 2020.

[100] Mamoona Humayun et al. "Cyber security threats and vulnerabilities: a systematic mapping study". In: *Arabian Journal for Science and Engineering* 45.4 (2020), pp. 3171–3189.

[101] Mike Chapple and David Seidl. *CompTIA Security+ Study Guide*. Eight. Wiley, 2021.

[102] Christopher Hadnagy. *Social engineering: The art of human hacking*. John Wiley & Sons, 2010.

[103] Joseph M Hatfield. "Social engineering in cybersecurity: The evolution of a concept". In: *Computers & Security* 73 (2018), pp. 102–113.

[104] DCMS. *Cyber security breaches survey 2022 - GOV.UK*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022. 2022.

[105] NCSC. *Phishing attacks: defending your organisation - NCSC.GOV.UK*. https://www.ncsc.gov.uk/guidance/phishing. 2018.

[106] Tzipora Halevi, Nasir Memon, and Oded Nov. "Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks". In: *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)* (2015).

[107] Hussain Aldawood and Geoffrey Skinner. "Educating and raising awareness on cyber security social engineering: A literature review". In: *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*. IEEE. 2018, pp. 62–68.

[108] Antonio Scarfo. "New security perspectives around BYOD". In: *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications*. IEEE. 2012, pp. 446–451.

[109] Fadi A Aloul. "The need for effective information security awareness". In: *Journal of advances in information technology* 3.3 (2012), pp. 176–183.

[110] Usman Javed Butt et al. "Cloud and Its Security Impacts on Managing a Workforce Remotely: A Reflection to Cover Remote Working Challenges". In: *Cybersecurity, Privacy and Freedom Protection in the Connected World*. Springer, 2021, pp. 285–311.

[111] Mohammed N Alenezi et al. "Evolution of malware threats and techniques: a review". In: *International journal of communication networks and information security* 12.3 (2020), pp. 326–337.

[112] Ralph Langner. "Stuxnet: Dissecting a cyberwarfare weapon". In: *IEEE Security and Privacy* 9 (3 May 2011), pp. 49–51. ISSN: 15407993. DOI: 10.1109/MSP.2011.67.

[113] Thomas M Chen and Saeed Abu-Nimeh. "Lessons from stuxnet". In: *Computer* 44.4 (2011), pp. 91–93.

[114] Siobhan Gorman and Julian E Barnes. "Cyber combat: Act of war". In: *The Wall Street Journal* 31 (2011), p. 2011.

[115] Seguin Patrick. *What is Spyware? — Spyware Definition — Avast*. https://www.avast.com/c-spyware. 2022.

[116] Malwarebytes. *What is Spyware — Spyware Removal and Protection — Malwarebytes*. https://www.malwarebytes.com/spyware. 2023.

[117] Deborah R Compeau and Christopher A Higgins. *Computer Self-Efficacy: Development of a Measure and Initial Test*. 1995, pp. 189–211.

[118] Roger Thompson. "Why spyware poses multiple threats to security". In: *Communications of the ACM* 48.8 (2005), pp. 41–43.

[119] Umara Urooj et al. "Ransomware detection using the dynamic analysis and machine learning: A survey and research directions". In: *Applied Sciences* 12.1 (2021), p. 172.

[120] Pavol Zavarsky, Dale Lindskog, et al. "Experimental analysis of ransomware on windows and android platforms: Evolution and characterization". In: *Procedia Computer Science* 94 (2016), pp. 465–472.

[121] Per Håkon Meland, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. "The Ransomware-as-a-Service economy within the darknet". In: *Computers & Security* 92 (2020), p. 101762.

[122] Kingsley Hayes. "Ransomware: a growing geopolitical threat". In: *Network Security* 2021.8 (2021), pp. 11–13. ISSN: 1353-4858. DOI: https://doi.org/10.1016/S1353-4858(21)00089-1. URL: https://www.sciencedirect.com/science/article/pii/S1353485821000891.

[123] Florin Zandit. *Chart: The Industries Most Affected by Ransomware — Statista*. https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/. 2021.

[124] CISA. *BlackMatter Ransomware — CISA*. https://www.cisa.gov/uscert/ncas/alerts/aa21-291a. 2021.

[125] CISA. *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks — CISA*. https://www.cisa.gov/uscert/ncas/alerts/aa21-131a. 2021.

[126] Thomas Miller et al. "Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems". In: *International Journal of Critical Infrastructure Protection* 35 (2021), p. 100464. ISSN: 1874-5482. DOI: https://doi.org/10.1016/j.ijcip.2021.100464. URL: https://www.sciencedirect.com/science/article/pii/S1874548221000524.

[127] Joe Slowik. *Spyware-Stealer-Locker-Wiper-LockerGoga-Revisited.pdf*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.dragos.com/wp-content/uploads/Spyware-Stealer-Locker-Wiper-LockerGoga-Revisited.pdf?utm_referrer=https://www.dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/. 2020.

[128] Bill Briggs. *Hackers hit Norsk Hydro with ransomware. The company responded with transparency — Transform*. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/. 2019.

[129] CISA. *Conti Ransomware — CISA*. https://www.cisa.gov/uscert/ncas/alerts/aa21-265a. 2022.

[130] Savita Mohurle and Manisha Patil. "A brief study of wannacry threat: Ransomware attack 2017". In: *International Journal of Advanced Research in Computer Science* 8.5 (2017), pp. 1938–1940.

[131] Josh Fruhlinger. "What is WannaCry ransomware, how does it infect, and who was responsible". In: *CSO Online* 30 (2018).

[132] Usman Javed Butt, Maysam F Abbod, and Arvind Kumar. "Cyber threat ransomware and marketing to networked consumers". In: *Handbook of research on innovations in technology and marketing for the connected consumer*. IGI Global, 2020, pp. 155–185.

[133] Bill Fisher, William Barker, and Karen Scarfone. *Getting Started with Cybersecurity Risk Management Ransomware*. en. 2022-02-23 05:02:00 2022. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934365.

[134] CISA. *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems — CISA*. https://www.cisa.gov/uscert/ncas/alerts/aa20-205a. 2020.

[135] Statista. *Leading cause of ransomware infection 2020 — Statista*. https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/. 2022.

[136] Nikhil Sharma and Ravi Shanker. "Analysis of Ransomware Attack and Their Countermeasures: A Review". In: *2022 International Conference on Electronics and Renewable Systems (ICEARS)*. IEEE. 2022, pp. 1877–1883.

[137] Ladislav Burita, Ivo Klaban, and Tomas Racil. "Education and Training Against Threat of Phishing Emails". In: *International Conference on Cyber Warfare and Security*. Vol. 17. 1. 2022, pp. 7–18.

[138] Anna Georgiadou, Spiros Mouzakitis, and Dimitris Askounis. "Working from home during COVID-19 crisis: a cyber security culture assessment survey". In: *Security Journal* 35.2 (2022), pp. 486–505.

[139] Craig Beaman et al. "Ransomware: Recent advances, analysis, challenges and future research directions". In: *Computers & Security* 111 (2021), p. 102490.

[140] ONS. *Homeworking in the UK – regional patterns - Office for National Statistics*. https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/homeworkingintheukregionalpatterns/2019to2022. 2022.

[141] Huigang Liang, Yajiong Lucky Xue, et al. "Understanding security behaviors in personal computer usage: A threat avoidance perspective". In: *Journal of the association for information systems* 11.7 (2010), p. 1.

[142] Yelena Petrykina, Hadas Schwartz-Chassidim, and Eran Toch. "Nudging users towards online safety using gamified environments". In: *Computers & Security* 108 (2021), p. 102270.

[143] NCSC. *Record number of cyber incidents mitigated as NCSC... - NCSC.GOV.UK*. https://www.ncsc.gov.uk/news/record-number-mitigated-incidents. 2021.

[144] ICO. *Ransomware and data protection compliance — ICO*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ransomware-and-data-protection-compliance/. 2022.

[145] ACSC. *2021-010: ACSC Ransomware Profile - Conti — Cyber.gov.au*. https://www.cyber.gov.au/acsc/view-all-content/advisories/2021-010-acsc-ransomware-profile-conti. 2021.

[146] CISA. *Conti Ransomware — CISA*. https://www.cisa.gov/uscert/ncas/alerts/aa21-265a. 2021.

[147] CISA. *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks — CISA*. https://www.cisa.gov/uscert/ncas/alerts/aa21-131a. 2021.

[148] DoJ. *U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov — OPA — Department of Justice*. https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov. 2021.

[149] Mimecast. *State of Email Security — Mimecast*. https://www.mimecast.com/state-of-email-security/. 2021.

[150] CIS. *7 Steps to Help Prevent & Limit the Impact of Ransomware*. https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware. 2022.

[151] *The changing shape of ransomware*. https://kpmg.com/dp/en/home/insights/2021/04/the-changing-shape-of-ransomware.html.

[152] Pierre Corbeil and Dany Laveault. "Validity of a simulation game as a method for history teaching". In: *Simulation & Gaming* 42.4 (2011), pp. 462–475.

[153] Stamatios Papadakis. "The use of computer games in classroom environment". In: *International Journal of Teaching and Case Studies* 9.1 (2018), pp. 1–25.

[154] Jim Buckley et al. "A gamification–motivation design framework for educational software developers". In: *Journal of Educational Technology Systems* 47.1 (2018), pp. 101–127.

[155] Kuo-chen Li et al. "Designing game-based learning framework-a motivation-driven approach". In: *2010 10th IEEE International Conference on Advanced Learning Technologies*. IEEE. 2010, pp. 215–216.

[156] Meihua Qian and Karen R. Clark. "Game-based Learning and 21st century skills: A review of recent research". In: *Computers in Human Behavior* 63 (2016), pp. 50–58. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2016.05.023. URL: https://www.sciencedirect.com/science/article/pii/S0747563216303491.

[157] Roslina Ibrahim and Azizah Jaafar. "Educational games (EG) design framework: Combination of game design, pedagogy and content modeling". In: *2009 international conference on electrical engineering and informatics*. Vol. 1. IEEE. 2009, pp. 293–298.

[158] J.Michael Spector and Pål I. Davidsen. "Creating engaging courseware using system dynamics". In: *Computers in Human Behavior* 13.2 (1997), pp. 127–155. ISSN: 0747-5632. DOI: https://doi.org/10.1016/S0747-5632(97)80002-7. URL: https://www.sciencedirect.com/science/article/pii/S0747563297800027.

[159] Nalin Asanka Gamagedara Arachchilage and Mumtaz Abdul Hameed. "Integrating self-efficacy into a gamified approach to thwart phishing attacks". In: *arXiv preprint arXiv:1706.07748* (2017).

[160] Yap L Dion, Abigail A Joshua, and Sarfraz N Brohi. "Negation of ransomware via gamification and enforcement of standards". In: *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence*. 2017, pp. 203–208.

[161] Reyner Aranta Lika et al. "NotPetya: cyber attack prevention through awareness via gamification". In: *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*. IEEE. 2018, pp. 1–6.

[162] Nikolaos Pellas and Stylianos Mystakidis. "A Systematic Review of Research about Game-based Learning in Virtual Worlds." In: *J. Univers. Comput. Sci.* 26.8 (2020), pp. 1017–1042.

[163] *National Cyber Security Strategy 2016 to 2021 - GOV.UK*. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. (Accessed on 12/05/2022).

[164] Maurice Hendrix, Ali Al-Sherbaz, and Bloom Victoria. "Game based cyber security training: are serious games suitable for cyber security training?" In: *International Journal of Serious Games* 3.1 (2016).

[165] Nabin Chowdhury, Sokratis Katsikas, and Vasileios Gkioulos. "Modeling effective cybersecurity training frameworks: A delphi method-based study". In: *Computers & Security* 113 (2022), p. 102551.

[166] Jemal Abawajy. "User preference of cyber security awareness delivery methods". In: *Behaviour & Information Technology* 33.3 (2014), pp. 237–248.

[167] Karzan Hussein Sharif and Siddeeq Yousif Ameen. "A Review on Gamification for Information Security Training". In: *2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI)*. IEEE. 2021, pp. 1–8.

[168] Quang Duy La et al. "Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things". In: *IEEE Internet of Things Journal* 3.6 (2016), pp. 1025–1035. DOI: 10.1109/JIOT.2016.2547994.

[169] Ahmed A. Alabdel Abass et al. "Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage". In: *IEEE Access* 5 (2017), pp. 8482–8491. DOI: 10.1109/ACCESS.2017.2691326.

[170] Hichem Sedjelmaci, Sidi Mohamed Senouci, and Tarik Taleb. "An Accurate Security Game for Low-Resource IoT Devices". In: *IEEE Transactions on Vehicular Technology* 66.10 (2017), pp. 9381–9393. DOI: 10.1109/TVT.2017.2701551.

[171] *Mail Check - NCSC.GOV.UK*. https://www.ncsc.gov.uk/information/mailcheck. (Accessed on 05/12/2023). 2018.

[172] NCSC. *CyberSprinters - NCSC.GOV.UK*. https://www.ncsc.gov.uk/collection/cybersprinters. (Accessed on 05/12/2023). 2023.

[173] CS. *Intro to Malware - Cyber Games UK*. https://cybergamesuk.com/malware. (Accessed on 05/12/2023). 2023.

[174] Roy Want et al. "An overview of the PARCTAB ubiquitous computing experiment". In: *IEEE personal communications* 2.6 (1995), pp. 28–43.

[175] Michael Friedewald and Oliver Raabe. "Ubiquitous computing: An overview of technology impacts". In: *Telematics and Informatics* 28.2 (2011), pp. 55–65.

[176] Catherine Marinagi, Christos Skourlas, and Petros Belsis. "Employing ubiquitous computing devices and technologies in the higher education classroom of the future". In: *Procedia-Social and Behavioral Sciences* 73 (2013), pp. 487–494.

[177] Diane J Cook and Sajal K Das. "Pervasive computing at scale: Transforming the state of the art". In: *Pervasive and Mobile Computing* 8.1 (2012), pp. 22–35.

[178] Statista. *Global mobile traffic 2022 — Statista*. https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/. 2022.

[179] ONS. *Internet users, UK - Office for National Statistics*. https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020. 2021.

[180] Gartner. *Gartner Says Worldwide Sales of Smartphones Returned to Growth in First Quarter of 2018*. https://www.gartner.com/en/newsroom/press-releases/2018-05-29-gartner-says-worldwide-sales-of-smartphones-returned-to-growth-in-first-quarter-of-2018. 2018.

[181] Stacy Golmack. *Current Trends And Future Prospects Of The Mobile App Market — Smashing Magazine*. https://www.smashingmagazine.com/2017/02/current-trends-future-prospects-mobile-app-market/. 2017.

[182] Statista. *Google Play Store: number of apps 2022 — Statista*. https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/. 2022.

[183] Christine Elizabeth Holbrey. "Kahoot! Using a game-based approach to blended learning to support effective learning environments and student engagement in traditional lecture theatres". In: *Technology, Pedagogy and Education* 29.2 (2020), pp. 191–202. DOI: 10.1080/1475939X.2020.1737568. eprint: https://doi.org/10.1080/1475939X.2020.1737568. URL: https://doi.org/10.1080/1475939X.2020.1737568.

[184] Anupama Roy and Mike Sharples. "Mobile Game Based Learning: Can it enhance learning of marginalized peer educators?" In: *International Journal of Mobile and Blended Learning (IJMBL)* 7.1 (2015), pp. 1–12.

[185] Thomas Connolly and Mark Stansfield. "Using Games-Based eLearning Technologiesin Overcoming Difficulties in Teaching Information Systems". In: *Journal of Information Technology Education: Research* 5.1 (2006), pp. 459–476.

[186] Becky Wai-Ling Packard and Paul F Conway. "Methodological choice and its consequences for possible selves research". In: *Identity* 6.3 (2006), pp. 251–271.

[187] John Mingers. "The contribution of systemic thought to critical realism". In: *Journal of Critical Realism* 10.3 (2011), pp. 303–330.

[188] Egon G Guba, Yvonna S Lincoln, et al. "Competing paradigms in qualitative research". In: *Handbook of qualitative research* 2.163-194 (1994), p. 105.

[189] M Saunders and P Lewis. "Doing research in business and management: an essential guide to planning your project.[online] Available at:¡ http://library. wur. nl". In: *WebQuery/clc/2036357¿[Accessed 15 Jul. 2014]* (2012).

[190] Maryam Alavi and Patricia Carlson. "A review of MIS research and disciplinary development". In: *Journal of management information systems* 8.4 (1992), pp. 45–62.

[191] Geoff Walsham. "Interpretive case studies in IS research: nature and method". In: *European Journal of information systems* 4.2 (1995), pp. 74–81.

[192] Imre Lakatos. *The methodology of scientific research programmes: Volume 1: Philosophical papers*. Vol. 1. Cambridge university press, 1980.

[193] Huigang Liang and Yajiong Xue. "Avoidance of information technology threats: A theoretical perspective". In: *MIS quarterly* (2009), pp. 71–90.

[194] Robert D Galliers and Frank F Land. "Choosing appropriate information systems research methodologies". In: *Communications of the ACM* 30.11 (1987), pp. 901–902.

[195] Jan Jonker and Bartjan W Pennink. "The essence of methodology". In: *The Essence of Research Methodology*. Springer, 2010, pp. 21–41.

[196] David E Gray. "Theoretical perspectives and research methodologies". In: *Doing research in the real world* 3 (2014), pp. 15–38.

[197] Rafael Gonzalez and Ajantha Dahanayake. "A concept map of information systems research approaches". In: *the Proceedings of the 2007 IRMA International Conference, Vancouver*. 2007.

[198] Nerida Hyett, Amanda Kenny, and Virginia Dickson-Swift. "Methodology or method? A critical review of qualitative case study reports". In: *International journal of qualitative studies on health and well-being* 9.1 (2014), p. 23606.

[199] Carl Martin Allwood. "The distinction between qualitative and quantitative research methods is problematic". In: *Quality & Quantity* 46.5 (2012), pp. 1417–1429.

[200] Shoshanna Sofaer. "Qualitative methods: what are they and why use them?" In: *Health services research* 34.5 Pt 2 (1999), p. 1101.

[201] Kevin McCusker and Sau Gunaydin. "Research using qualitative, quantitative or mixed methods and choice based on the research". In: *Perfusion* 30.7 (2015), pp. 537–542.

[202] SYLVAN Wallenstein, Christine L Zucker, and Joseph L Fleiss. "Some statistical methods useful in circulation research." In: *Circulation Research* 47.1 (1980), pp. 1–9.

[203] Claes Fornell and David F Larcker. "Evaluating structural equation models with unobservable variables and measurement error". In: *Journal of marketing research* 18.1 (1981), pp. 39–50.

[204] Earl R Babbie. *The practice of social research*. Cengage learning, 2020.

[205] Mohamed Al Kilani and Volodymyr Kobziev. "An overview of research methodology in information system (IS)". In: *Open Access Library Journal* 3.11 (2016), pp. 1–9.

[206] Marta Pinzone et al. "Effects of 'green' training on pro-environmental behaviors and job satisfaction: Evidence from the Italian healthcare sector". In: *Journal of Cleaner Production* 226 (July 2019), pp. 221–232. ISSN: 09596526. DOI: 10.1016/j.jclepro.2019.04.048.

[207] Martin Brett Davies and Nathan Hughes. *Doing a successful research project: Using qualitative or quantitative methods*. Bloomsbury Publishing, 2014.

[208] Vishal Arghode. "Qualitative and Quantitative Research: Paradigmatic Differences." In: *Global Education Journal* 2012.4 (2012).

[209] Wendy Bussen and Michael D Myers. "Executive information system failure: a New Zealand case study". In: *Journal of Information Technology* 12.2 (1997), pp. 145–153.

[210] Bonnie Kaplan and Joseph A Maxwell. "Qualitative research methods for evaluating computer information systems". In: *Evaluating the organizational impact of healthcare information systems*. Springer, 2005, pp. 30–55.

[211] Keith F Punch and Alis Oancea. *Introduction to research methods in education*. Sage, 2014.

[212] Virginia Braun and Victoria Clarke. "Using thematic analysis in psychology". In: *Qualitative research in psychology* 3.2 (2006), pp. 77–101.

[213] André Queirós, Daniel Faria, and Fernando Almeida. "Strengths and limitations of qualitative and quantitative research methods". In: *European journal of education studies* (2017).

[214] Pär J Ågerfalk. *Embracing diversity through mixed methods research*. 2013.

[215] Donald T Campbell and Donald W Fiske. "Convergent and discriminant validation by the multitrait-multimethod matrix." In: *Psychological bulletin* 56.2 (1959), p. 81.

[216] Alan Bryman. "Integrating quantitative and qualitative research: how is it done?" In: *Qualitative research* 6.1 (2006), pp. 97–113.

[217] Abbas Tashakkori and Charles Teddlie. *Putting the human back in "human research methodology": The researcher in mixed methods research*. 2010.

[218] Jeffrey A Greene, Roger Azevedo, and Judith Torney-Purta. "Modeling epistemic and ontological cognition: Philosophical perspectives and methodological directions". In: *Educational Psychologist* 43.3 (2008), pp. 142–160.

[219] Jo Reichertz. "4.3 Abduction, deduction and induction in qualitative research". In: *A Companion to* (2004), p. 159.

[220] Donna M Mertens and Sharlene Hesse-Biber. *Triangulation and mixed methods research: Provocative positions*. 2012.

[221] Michael D Fetters, Leslie A Curry, and John W Creswell. "Achieving integration in mixed methods designs—principles and practices". In: *Health services research* 48.6pt2 (2013), pp. 2134–2156.

[222] Jakob Nielsen. "Estimating the number of subjects needed for a thinking aloud test". In: *International journal of human-computer studies* 41.3 (1994), pp. 385–397.

[223] T Kallio and A Kaikkonen. "Usability testing of mobile applications: A comparison between laboratory and field testing". In: *Journal of Usability studies* (2005), pp. 23–28.

[224] John Brooke. *SUS: A 'Quick and Dirty' Usability Scale*. June 1996. DOI: 10.1201/9781498710411-35.

[225] Brooke J. "SUS: a retrospective". In: *Journal of usability studies,* 8 (2 2013), pp. 29–40.

[226] M Sandelowski. "Combining qualitative and quantitative sampling, data collection, and analysis techniques in mixed-method studies". en. In: *Res. Nurs. Health* 23.3 (June 2000), pp. 246–255.

[227] Joop J Hox and Hennie R Boeije. "Data collection, primary versus secondary". In: (2005).

[228] Victor Oluwatosin Ajayi. "Primary sources of data and secondary sources of data". In: *Benue State University* 1.1 (2017), pp. 1–6.

[229] Edwin van Teijlingen and Vanora Hundley. *Edwin R. van Teijlingen and Vanora Hundley.* 2002.

[230] Hamed Taherdoost. "What is the best response scale for survey and questionnaire design; review of different lengths of rating scale/attitude scale/Likert scale". In: *Hamed Taherdoost* (2019), pp. 1–10.

[231] Tomoko Nemoto and David Beglar. "Likert-scale questionnaires". In: *JALT 2013 conference proceedings.* 2014, pp. 1–8.

[232] André Godoy and Ellen F Barbosa. "Game-Scrum: An approach to agile game development". In: *Proceedings of SBGames* (2010), pp. 292–295.

[233] Alina Mihaela Dima and Maria Alexandra Maassen. "From Waterfall to Agile software: Development models in the IT sector, 2006 to 2018. Impacts on company management". In: *Journal of International Studies* 11.2 (2018), pp. 315–326.

[234] Rashina Hoda, Norsaremah Salleh, and John Grundy. "The rise and evolution of agile software development". In: *IEEE software* 35.5 (2018), pp. 58–63.

[235] Fabio Petrillo and Marcelo Pimenta. "Is agility out there? Agile practices in game development". In: *Proceedings of the 28th ACM International Conference on Design of Communication.* 2010, pp. 9–15.

[236] Sundramoorthy Balaji and M Sundararajan Murugaiyan. "Waterfall vs. V-Model vs. Agile: A comparative study on SDLC". In: *International Journal of Information Technology and Business Management* 2.1 (2012), pp. 26–30.

[237] Erik Bethke. *Game development and production.* Wordware Publishing, Inc., 2003.

[238] Robin Hunicke, Marc LeBlanc, Robert Zubek, et al. "MDA: A formal approach to game design and game research". In: *Proceedings of the AAAI Workshop on Challenges in Game AI.* Vol. 4. 1. San Jose, CA. 2004, p. 1722.

[239] Jesse James Garrett. *The elements of user experience : user-centered design for the Web and beyond*. 2011, p. 172. ISBN: 9780321683687.

[240] Joe F Hair Jr et al. "Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research". In: *European business review* (2014).

[241] Ned Kock and Jacques Verville. "Exploring free questionnaire data with anchor variables: An illustration based on a study of it in healthcare". In: *International Journal of Healthcare Information Systems and Informatics* 7 (1 Jan. 2012), pp. 46–63. ISSN: 15553396. DOI: 10.4018/jhisi.2012010104.

[242] Ken Kwong-Kay Wong. "Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS". In: *Marketing Bulletin* 24.1 (2013), pp. 1–32.

[243] Edward R. Mansfield and Billy P. Helms. "Detecting Multicollinearity". In: *The American Statistician* 36 (3a Aug. 1982), pp. 158–160. ISSN: 0003-1305. DOI: 10.1080/00031305.1982.10482818.

[244] Anne Galletta. *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication*. Vol. 18. NYU press, 2013.

[245] Hanna Kallio et al. "Systematic methodological review: developing a framework for a qualitative semi-structured interview guide". In: *Journal of Advanced Nursing* 72 (12 Dec. 2016), pp. 2954–2965. ISSN: 03092402. DOI: 10.1111/jan.13031.

[246] Nancy L. Leech and Anthony J. Onwuegbuzie. "Beyond constant comparison qualitative data analysis: Using NVivo." In: *School Psychology Quarterly* 26 (1 Mar. 2011), pp. 70–84. ISSN: 1939-1560. DOI: 10.1037/a0022711.

[247] Daffron J. et al. *Bashe attack Global infection by contagious malware*. 2019. URL: http://irfrc.ntu.edu.sg/Research/cyrim/Pages/Home.aspx.

[248] Xin Luo and Qinyu Liao. "Awareness Education as the Key to Ransomware Prevention". In: *Information Systems Security* 16 (4 Sept. 2007), pp. 195–202. ISSN: 1065-898X. DOI: 10.1080/10658980701576412.

[249] *National Cyber Strategy 2022 - GOV.UK*. https://www.gov.uk/government/publications/national-cyber-strategy-2022.

[250] Andrew J Elliot, Andreas B Eder, and Eddie Harmon-Jones. "Approach–avoidance motivation and emotion: Convergence and divergence". In: *Emotion Review* 5.3 (2013), pp. 308–311.

[251] Norbert Wiener. *Cybernetics: Control and Communication in the Animal and the Machine*. 1948.

[252] "Cybernetic and General-System Approaches to Urban and Regional Research: A Review of the Literature". In: *Environment and Planning A: Economy and Space* 2 (4 Dec. 1970), pp. 369–408. ISSN: 0308-518X. DOI: 10.1068/a020369.

[253] DWP. *Security Standard Firewall Security (SS0 13)-Department for Work and Pensions*. chrome-https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/882768/dwp-ss013-security-standard-firewall-security-v1.5.pdf. 2020.

[254] Nancy K Janz and Marshall H Becker. "The health belief model: A decade later". In: *Health education quarterly* 11.1 (1984), pp. 1–47.

[255] Irene Woon, Gek-Woo Tan, and R Low. "A protection motivation theory approach to home wireless security". In: (2005).

[256] Richard Baskerville. "Risk analysis as a source of professional knowledge". In: *Computers & Security* 10.8 (1991), pp. 749–764.

[257] A. H. Maslow. "A theory of human motivation." In: *Psychological Review* 50 (4 July 1943), pp. 370–396. ISSN: 1939-1471. DOI: 10.1037/h0054346.

[258] Albert Bandura. "Self-efficacy mechanism in human agency." In: *American Psychologist* 37 (2 1982), pp. 122–147. ISSN: 0003-066X. DOI: 10.1037/0003-066X.37.2.122.

[259] Ehinome Ikhalia. "A malware threat avoidance model for online social network users". PhD thesis. Brunel University London, 2017.

[260] Boon Yuen Ng, Atreyi Kankanhalli, and Yunjie (Calvin) Xu. "Studying users' computer security behavior: A health belief perspective". In: *Decision Support Systems* 46 (4 Mar. 2009), pp. 815–825. ISSN: 01679236. DOI: 10.1016/j.dss.2008.11.010.

[261] Viswanath Venkatesh et al. *User Acceptance of Information Technology: Toward a Unified View*. 2003, pp. 425–478.

[262] Information Commissioner's Office ICO. "The principles - Guide to the General Data Protection Regulation (GDPR)". In: (2021). URL: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.

[263] Gov UK. *Data protection - GOV.UK*. 2018. URL: https://www.gov.uk/data-protection.

[264] Jacqueline R Saleeby. "Health beliefs about mental illness: An instrument development study". In: *American Journal of Health Behavior* 24.2 (2000), pp. 83–95.

[265] H Jeff Smith, Sandra J Milberg, and Sandra J Burke. "Information privacy: Measuring individuals' concerns about organizational practices". In: *MIS quarterly* (1996), pp. 167–196.

[266] Kurt Thomas and David M Nicol. "The Koobface botnet and the rise of social malware". In: *2010 5th International Conference on Malicious and Unwanted Software*. IEEE. 2010, pp. 63–70.

[267] Norbert Wiener. *Cybernetics or Control and Communication in the Animal and the Machine*. MIT press, 2019.

[268] Harry N Boone, Jr Associate Professor, and Deborah A Boone Associate Professor. *Number 2 Article Number 2TOT2*. 2012. URL: http://www.joe.org/joe/2012april/tt2p.shtml[8/20/20129:07:48AM].

[269] Jan-Michael Becker et al. "Discovering unobserved heterogeneity in structural equation models to avert validity threats". In: *MIS quarterly* (2013), pp. 665–694.

[270] Marko Sarstedt et al. "Partial least squares structural equation modeling (PLS-SEM): A useful tool for family business researchers". In: *Journal of Family Business Strategy* 5 (1 Mar. 2014), pp. 105–115. ISSN: 18778585. DOI: 10.1016/j.jfbs.2014.01.002.

[271] Philip M Podsakoff et al. "Common method biases in behavioral research: a critical review of the literature and recommended remedies." In: *Journal of applied psychology* 88.5 (2003), p. 879.

[272] Meghan K Cain, Zhiyong Zhang, and Ke-Hai Yuan. "Univariate and multivariate skewness and kurtosis for measuring nonnormality: Prevalence, influence and estimation". In: *Behavior research methods* 49.5 (2017), pp. 1716–1735.

[273] Jum C. Nunnally. *Psychometric Theory*. McGraw-Hill, 1978.

[274] Jörg Henseler, Christian M Ringle, and Marko Sarstedt. "A new criterion for assessing discriminant validity in variance-based structural equation modeling". In: *Journal of the academy of marketing science* 43.1 (2015), pp. 115–135.

[275] Michael Patrick Allen. "The problem of multicollinearity". In: *Understanding regression analysis* (1997), pp. 176–180.

[276] Mansour Alraja. "Frontline healthcare providers' behavioural intention to Internet of Things (IoT)-enabled healthcare applications: A gender-based, cross-generational study". In: *Technological Forecasting and Social Change* 174 (2022), p. 121256.

[277] Aiken L. S. and S.G West. *Multiple regression: Testing and interpreting interactions.* Sage Publications, 1991.

[278] Reuben M Baron and David A Kenny. "The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations." In: *Journal of personality and social psychology* 51.6 (1986), p. 1173.

[279] Gamagedara Arachchilage and Nalin Asanka. "Security awareness of computer users: A game based learning approach. Brunel University, School of Information Systems". In: *Computing and Mathematics* (2012).

[280] Asanka Gamagedara Arachchilage Nalin. *Security Awareness of Computer Users: A Game Based Learning Approach*. 2012.

[281] Amit Das and Habib Ullah Khan. "Security behaviors of smartphone users". In: *Information & Computer Security* (2016).

[282] NCSC. *Annual Review 2021 Making the UK the safest place to live and work online*. 2021.

[283] BSI. *Bibliographic Info :: BSOL British Standards Online - BS EN ISO/IEC 27001:2017 Information technology. Security techniques. Information security management systems. Requirements*. https://bsol.bsigroup.com/Bibliographic/BibliographicInfoData/000000000030347472. 2017.

[284] *The GDPR (General Data Protection Regulation) — IT Governance*. https://www.itgovernance.co.uk/data-protection-dpa-and-eu-data-protection-regulation.

[285] *Data protection: The Data Protection Act - GOV.UK*. https://www.gov.uk/data-protection.

[286] Sumaira Shafiq and Tamim A Khan. "Role & value of usability in educational learning via game based apps". In: *International Journal of Scientific and Technology Research* 7.11 (2018), pp. 70–77.

[287] Kellie E Kercher and Dale C Rowe. "Risks, rewards and raising awareness: training a cyber workforce using student red teams". In: *Proceedings of the 13th annual conference on Information technology education*. 2012, pp. 75–80.

[288] Sultan Al-Sharif et al. "White-hat hacking framework for promoting security awareness". In: *2016 8th IFIP international conference on new technologies, mobility and security (NTMS)*. IEeE. 2016, pp. 1–6.

[289] Desney S. Tan et al. *Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems : 2011 proceeding, Vancouver, BC, Canada - May 07-12, 2011*. ACM Press, 2011. ISBN: 9781450302685.

[290] KwanMyung Kim and Kun-Pyo Lee. "Two types of design approaches regarding industrial design and engineering design in product design". In: *DS 60: Proceedings of DESIGN 2010, the 11th International Design Conference, Dubrovnik, Croatia*. 2010.

[291] Foraker Labs. *Usability First - Introduction to User-Centered Design — Usability First*. https://www.usabilityfirst.com/about-usability/introduction-to-user-centered-design. 2015.

[292] Usability Gov. *User-Centered Design Basics — Usability.gov*. https://www.usability.gov/what-and-why/user-centered-design.html. 2022.

[293] Vanisri Nagalingam and Roslina Ibrahim. "User experience of educational games: a review of the elements". In: *Procedia Computer Science* 72 (2015), pp. 423–433.

[294] Erik Bethke. *Game Development and production*. Wordware Publishing, Inc., 2003.

[295] Jesse James Garrett. *The elements of user experience*. unknown, 2022.

[296] Rikke Friis Dam and Teo Yu Siang. *Personas – a simple introduction*. Dec. 2022. URL: https://www.interaction-design.org/literature/article/personas-why-and-how-you-should-use-them.

[297] *This Person Does Not Exist - Random AI Face Generator*. https://this-person-does-not-exist.com/en. 2022.

[298] Josiah Lebowitz and Chris Klug. *Interactive storytelling for video games: A player-centered approach to creating memorable characters and stories*. Taylor & Francis, 2011.

[299] Tracey Fullerton. *Game Design Workshop: A Playcentric Approach to Creating Innovative Games*. 3rd. CRC Press, 2014.

[300] Kajal Claypool and Mark Claypool. "Teaching software engineering through game design". In: *ACM SIGCSE Bulletin* 37.3 (2005), pp. 123–127.

[301] Martin Glinz. "On non-functional requirements". In: *15th IEEE international requirements engineering conference (RE 2007)*. IEEE. 2007, pp. 21–26.

[302] Lawrence Chung et al. *Non-functional requirements in software engineering*. Vol. 5. Springer, 2012.

[303] Marijn Janssen, Haiko Van Der Voort, and Anne Fleur van Veenstra. "Failure of large transformation projects from the viewpoint of complex adaptive systems: Management principles for dealing with project dynamics". In: *Information Systems Frontiers* 17.1 (2015), pp. 15–29.

[304] Katherine Bradbury et al. "Developing digital interventions: a methodological guide". In: *Evidence-Based Complementary and Alternative Medicine* 2014 (2014).

[305] Pistoia Alliance. *Task Modelling*. 2020.

[306] Tom Gross. *UCProMo—Towards a User-Centred Process Model*. 2016. DOI: 10.1007/978-3-319-44902-9_19.

[307] Rachel Harrison, Derek Flood, and David Duce. "Usability of mobile applications: literature review and rationale for a new usability model". In: *Journal of Interaction Science* 1.1 (2013), pp. 1–16.

[308] Tharon Howard. "Journey Mapping: A Brief Overview". In: *Communication Design Quarterly Review* 2 (3 2014), pp. 10–13.

[309] Joe J. Marquez, Annie Downey, and Ryan Clement. "Walking a Mile in the User's Shoes: Customer Journey Mapping as a Method to Understanding the User Experience". In: *Internet Reference Services Quarterly* 20 (3-4 Oct. 2015), pp. 135–150. ISSN: 1087-5301. DOI: 10.1080/10875301.2015.1107000.

[310] Ian Sommerville. *Engineering software products*. Pearson London, 2020.

[311] Maria Rauschenberger et al. "Efficient measurement of the user experience of interactive products. How to use the user experience questionnaire (UEQ). Example: Spanish language version". In: (2013).

[312] Sutipong Sutipitakwong and Pornsuree Jamsri. "Pros and cons of tangible and digital wireframes". In: *2020 IEEE Frontiers in Education Conference (FIE)*. IEEE. 2020, pp. 1–5.

[313] Jeff Gray et al. "Teaching CS principles with app inventor". In: *Proceedings of the 50th Annual Southeast Regional Conference*. 2012, pp. 405–406.

[314] Shaileen Crawford Pokress and José Juan Dominguez Veiga. "MIT App Inventor: Enabling personal mobile computing". In: *arXiv preprint arXiv:1310.2830* (2013).

[315] Siu-Cheung Kong and Harold Abelson. *Computational Thinking Education*. 2019.

[316] Maneela Tuteja, Gaurav Dubey, et al. "A research study on importance of testing and quality assurance in software development life cycle (SDLC) models". In: *International Journal of Soft Computing and Engineering (IJSCE)* 2.3 (2012), pp. 251–257.

[317] David Pinelle, Nelson Wong, and Tadeusz Stach. "Heuristic evaluation for games". In: ACM Press, 2008, p. 1453. ISBN: 9781605580111. DOI: 10.1145/1357054.1357282.

[318] Michele J McIntosh and Janice M Morse. "Situating and constructing diversity in semi-structured interviews". In: *Global qualitative nursing research* 2 (2015), p. 2333393615597674.

[319] Robert A. Virzi. "Refining the Test Phase of Usability Evaluation: How Many Subjects Is Enough?" In: *Human Factors: The Journal of the Human Factors and Ergonomics Society* 34 (4 Aug. 1992), pp. 457–468. ISSN: 0018-7208. DOI: 10.1177/001872089203400407.

[320] Jakob Nielsen and Thomas K. Landauer. "A mathematical model of the finding of usability problems". In: ACM Press, 1993, pp. 206–213. ISBN: 0897915755. DOI: 10.1145/169059.169166.

[321] Nicholas Clifford et al. *Key methods in geography*. Sage, 2016.

[322] Usability Gov. *System Usability Scale (SUS) — Usability.gov*. https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.. 2022.

[323] Steve Sheng et al. "Who falls for phish?" In: ACM Press, 2010, p. 373. ISBN: 9781605589299. DOI: 10.1145/1753326.1753383.

[324] Nigel Bevan. "Usability is quality of use". In: *Advances in Human Factors/Ergonomics*. Vol. 20. Elsevier, 1995, pp. 349–354.

[325] BSI. *BS EN ISO 9241-11:2018(en), Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts*. https://bsol.bsigroup.com/PdfViewer/Viewer?pid=000000000030412057. 2018.

[326] Tullis T.S. and Stetson J.N. "A comparison of questionnaires for assessing website usability. In Usability professional association conference". In: June 2004, pp. 1–12.

[327] Jeff Sauro and James R. Lewis. "When designing usability questionnaires, does it hurt to be positive?" In: ACM, May 2011, pp. 2215–2224. ISBN: 9781450302289. DOI: 10.1145/1978942.1979266.

[328] Jurek Kirakowski, Nigel Claridge, and Richard Whitehand. "Human centered measures of success in web site design". In: *Proceedings of the Fourth Conference on Human Factors & the Web*. 1998.

[329] Andy Field. *Discovering Statistics Using SPSS*. 3rd ed. Sage, 2009.

[330] CISA. *2021 Trends Show Increased Globalized Threat of Ransomware — CISA*. https://www.cisa.gov/uscert/ncas/alerts/aa22-040a. 2022.

[331] Tara Matthews, Tejinder Judge, and Steve Whittaker. "How do designers and user experience professionals actually perceive and use personas?" In: *Proceedings of the SIGCHI conference on human factors in computing systems*. 2012, pp. 1219–1228.

[332] Patrick Faller. *What Are User Personas and Why Are They Important? — Adobe XD Ideas*. https://xd.adobe.com/ideas/process/user-research/putting-personas-to-work-in-ux-design/. 2019.

[333] Lena Y Connolly and David S Wall. "The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures". In: *Computers & Security* 87 (2019), p. 101568.

[334] Sulayman Sowe et al. "Cyber-Physical Social Systems: Getting People into the Loop". en. In: (2016-01-01 00:01:00 2016).

[335] Regner Sabillon, Victor Cavaller, and Jeimy Cano. "National cyber security strategies: global trends in cyberspace". In: *International Journal of Computer Science and Software Engineering* 5.5 (2016), p. 67.

[336] Carlo Perrotta et al. *The NFER Research Programme Game-based learning: latest evidence and future directions*. 2013. ISBN: 978-1-908666-60-4. URL: www.nfer.ac.uk.

[337] BSI. *Bibliographic Info :: BSOL British Standards Online -BS EN ISO/IEC 27002:2017 Information technology. Security techniques. Code of practice for information security controls*. https://bsol.bsigroup.com/Bibliographic/BibliographicInfoData/000000000030347481. 2017.

[338] Jin-Ning Tioh, Mani Mina, and Douglas W Jacobson. "Cyber security training a survey of serious games in cyber security". In: *2017 IEEE Frontiers in Education Conference (FIE)*. IEEE. 2017, pp. 1–5.

[339] Devottam Gaurav et al. "Empirical Study of Adaptive Serious Games in Enhancing Learning Outcome". In: *International Journal of Serious Games* 9.2 (2022), pp. 27–42.

[340] Woo-Hyun Lee, Han-Moi Shim, and Hyung-Gi Kim. "Effect of Game-based Learning using Live Streaming on Learners' Interest, Immersion, Satisfaction, and Instructors' Perception". In: *International Journal of Serious Games* 9.2 (2022), pp. 3–26.

[341] Action Fraud. *RansomAware — Action Fraud*. https://www.actionfraud.police.uk/campaign/ransomaware. (Accessed on 05/13/2023). 2018.

[342] Cisco. *Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper - Cisco*. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. (Accessed on 05/13/2023). 2020.

Appendix A

Table A.1: Study 1 Questionnaire

Constr.	Q's	Construct measurements
P_Sus	Q2	Ransomware is a kind of software, which is malicious in nature.
	Q3	It is high likely that my computer will be compromised by Ransomware in the future.
	Q4	It is true that Ransomware malware cannot install in my PC without my consent.
	Q5	It is likely that I can be easily trap by malicious ransomware attack.
P_Sev	Q6	It is likely that Ransomware cyber-attack will not encrypt files from my computer.

Continued on next page

Table A.1 – continued from previous page

Constr.	Q's	Construct measurements
	Q7	Ransomware cyber-attack if not countermeasure, can cause a severe threat to the security of my computer.
	Q8	Ransomware cyber-attack can take control of my data from remote computer and will make it unavailable for me.
	Q9	Ransomware is a kind of malicious cyberattacks, which demands for Ransom (virtual currency) in return of user data to release.
	Q10	Ransomware cyber-attack can compromise privacy and confidentiality of my data.
	Q11	It is likely Ransomware can compromise the integrity of my data.
P_Thr	Q12	I feel Ransomware is a kind of cyber-attack, which can be threaten to myself.
	Q13	Ransomware is a kind of cyber-attack, controlled by remote attacker; it could be harmful to keep the computer turned ON while it is under attack.
	Q14	I feel Ransomware is a kind of cyber-attack, which can threat to my personal computer security.
	Q15	I feel Ransomware is a kind of cyber-attack, which can threat to my computer network security.
	Q16	I feel Ransomware is a kind of cyber-attack, which can threat to my data.
S_eff	Q17	I believe game based learning can be a user friendly useful tool to educate myself against cyberattack Ransomware.
	Q18	I think Game based learning will be an effective tool to engage and educate me against the Ransomware cyberattack.
	Q19	I believe Game Based Learning tool will improve my education and awareness against techniques used by Ransomware

Continued on next page

Table A.1 – continued from previous page

Constr.	Q's	Construct measurements
	Q20	I do not think game based learning will allow me usability to improve my education and awareness against the Ransomware cyber threats.
S_Cos	Q21	It is time-consuming task to find a time to learn how to play game for Ransomware education and awareness.
	Q22	It is expensive to spend on game based learning for education and awareness against Ransomware cyber security threat.
	Q23	It is not feasible for me to get access to a computer or smart device to educate myself against cyber security threat Ransomware.
S_Eff	Q24	If I have the right knowledge, I can thwart Ransomware cyber-attack.
	Q25	If I have the resources available, I can learn how to identify Ransomware cyber threat.
	Q26	I can learn quickly if help is available to educate about Ransomware cyber-attack.
	Q27	If I do not have the right knowledge, I cannot thwart Ransomware cyber-attack.
	Q28	Ransomware is a sophisticated cyber threat; I don't think I can learn how to stop it.
	Q29	Due to changing landscape of cyber security, I do not think education and awareness will help me to thwart Ransomware cyber-attack.
A_Mot	Q30	I would like to adopt Game based learning tool to educate myself against the Ransomware cyberattack because it enhances user learning engagement.

Continued on next page

Table A.1 – continued from previous page

Constr.	Q's	Construct measurements
	Q31	I will adopt Game based learning because it is a way to motivate me to educate against Ransomware cyber threat.
	Q32	I will adopt Game based learning because it will allow me to educate against Ransomware cyber threat at my own learning pace.
A_Beh	Q33	I will adopt Game based learning because education and awareness against Ransomware cyber threat will help me to avoid any compromise to my computer security.
	Q34	I will adopt Game based learning because education and awareness against Ransomware cyber threat will help me to avoid any compromise to my information Privacy.

Appendix B

Table B.1: Themes and Codes

Themes	**Codes**	**Respondents Quotes**
P_Sus	Victim, Target, Under cyberattack, Likely harm	*"I spend much time with emails and on social media with known and unknown people. I can be a victim of the ransomware."* *"Considering how cyber security threats are evolving, the attackers use more advanced ways to attack. I think I can be the target of cyber security threat ransomware."* *"Where we benefit a lot from the digital revolution, at the same time, it brings many cyber security challenges. Ransomware is an emerging phenomenon. I can be exposed to this cyber security threat."*
P_Sev	Loss of confidentiality, Loss of Integrity, Loss of availability, Full control	*"After playing the RansomAware game, I understand that ransomware can compromise my privacy by accessing my data."* *"Wow, I learnt that once the ransomware attack is successful, the attacker has full control of my data and can do anything with it."* *"My PC has everything from my old pictures to work-related data. I never thought that someone could use ransomware to take control of it."*

Continued on next page

Table B.1 – continued from previous page

Themes	Codes	Respondents Quotes
P_Thr	Demand for ransom, Serious threat, Believe it is a threat	*"I heard a lot about computer viruses in the past, but until I played the RansomAware game, I was never sure about the malicious nature of the ransomware, which can take any computer machine hostage and demand the money to release."* *"After playing ransomware game and learning its consequences, I believe this is a serious threat to computer security."* *"I use emails to exchange work-related documents. After playing RansomAware game, I believe it is a security threat to computer users."*

Continued on next page

Table B.1 – continued from previous page

Themes	Codes	Respondents Quotes
S_eff	Enjoyed, Seamless Experience, Intuitive, Interesting, User-friendly	*"Overall, I enjoyed playing the game. It was a very interesting way to learn about a complex cyber threat, ransomware. The game was pretty straightforward to use. It was a seamless experience. I liked the way how the game was based on the story. It helped me to engage. It was useful to make informed decisions."* *"The game story engaged me. The design is intuitive and easy to navigate. I found it an effective way to learn ransomware."* *"The game was interesting and engaging, giving enough development opportunity while keeping you on realistic edge as who has time to read these sorts of emails."* *"Interesting story. I learnt complex cyber security in a friendly manner. This game approach is much better than traditional multiple-choice theoretical information security training."*

Continued on next page

Table B.1 – continued from previous page

Themes	Codes	Respondents Quotes
P_Cos	Time effective, Easily accessible, Free to download	*"The game was different from traditional hourly long training. I finished playing the game within the given time. It is time effective. I believe this is worth considering for ransomware awareness training."* *"It was a great experience with RansomAware. I was able to download it on my PC and mobile phone. The game is accessible, which means learning can happen on the go."* *" I love playing online games and believe they are good for human cognitive behaviour. My experience with RansomAware was awesome, you know why? Because it was easy to use and free to download."* *"I played a RansomAware game on my mobile phone while going to a friend's house. This was an interesting experience. I believe it is a usable and interactive design."*

Continued on next page

Table B.1 – continued from previous page

Themes	Codes	Respondents Quotes
S_Eff	Knowledge, Awareness, Training, Play again, Recommendation	*"I would say game-based learning is fun. It boosted my confidence. I will consider replaying if needed again and will surely recommend this game to my family and friends."* *"The game helped me with critical thinking to make the right decision. I feel more confident and aware of the malicious nature of ransomware attacks. I believe game-based learning is a good way forward to refresh your knowledge and will play again. Considering cyber security is an essential part of our lives, I will recommend the RansomAware game to my friends and family to benefit from it."* *"The scoring system was quite encouraging. If needed, I will replay this game as a refresher training and recommend others too."* *" I scored a bronze award for my points earned, which is not bad but shows me I need to up my game if I want to be completely safe. Overall, I would recommend this game to everyone."* *I felt confident by earning points during gameplay. RansomAware game helped me to build my confidence to thwart ransomware threat."*

Continued on next page

Table B.1 – continued from previous page

Themes	Codes	Respondents Quotes
A_Mot	Game Story, Engagement, Game Characters, Interactive	*"I successfully achieved Gold reward at the end of the game-play and believed the game-story and the design was an important element which contributed to my interest and knowledge awareness against the ransomware cyber security threat."* *"The idea of points award was motivational at the same time deduction of marks created a deterrence to improve my attention to detail."* *"The game-based learning was an enjoyable experience for learning about the malicious ransomware threat. I liked the spacer and the alien characters."*
A_Beh	Game-based learning, Can mitigate risk, Change of Perspective	*"The game story and design aspects of the game were very well integrated, which created my interest and helped me to achieve my goal of improving awareness against the ransomware cyber security threat. I believe the likelihood of ransomware attack can be mitigated."* *"It is not impossible to stop ransomware. The game RansomAware has changed my perspective."* *"I will adopt ransomAware game to enhance my avoidance behaviour against ransomware threat."*

Perceived Susceptibility (P_Sus), Perceived Severity (P_Sev), Perceived Threat (P_Thr), Safeguard effectiveness (S_eff), Safeguard cost (S_Cos), Avoidance Motivation (A_Mot), Avoidance Behaviour (A_Beh).