Enhancing Security Risk Awareness in End-Users via Affective Feedback

A thesis submitted for the degree of Doctor of Philosophy (PhD)

by

Lynsay A. Shepherd

School of Arts, Media and Computer Games, Abertay University

August 2016

Declaration

Candidate's declarations:

I, Lynsay A. Shepherd, hereby certify that this thesis submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy (PhD), Abertay University, is wholly my own work unless otherwise referenced or acknowledged. This work has not been submitted for any other qualification at any other academic institution.

Signed.....

Date .....

Supervisor's declaration:

I, Jacqueline Archibald hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Doctor of Philosophy (PhD) in Abertay University and that the candidate is qualified to submit this thesis in application for that degree.

Signed.....

Date .....

Certificate of Approval

I certify that this is a true and accurate version of the thesis approved by the examiners, and that all relevant ordinance regulations have been fulfilled.

Signed.....

Date .....

Abstract

Background: Risky security behaviour displayed by end-users has the potential to leave devices vulnerable to compromise, despite the availability of security tools designed to aid users in defending themselves against potential online threats. This indicates a need to modify the behaviour of end-users, allowing them to consider the security implications of their actions online. Previous research has indicated affective feedback may serve as a successful method of educating users about risky security behaviours. Thus, by influencing end-users via affective feedback it may be possible to engage users, improving their security awareness.

Aims: Develop and apply knowledge of monitoring techniques and affective feedback, establishing if this changes users' awareness of risky security behaviour in the context of a browser-based environment.

Methodology: The methodology employs the use of log files derived from the monitoring solution, and information provided by users during the experiments. Questionnaire data was compared against log files and information provided during experiments, providing an overall quantitative approach.

Results: In the case of the log files and questionnaires, participants were found to have engaged in instances of risky security behaviours, which they were unaware of, and this indicated a low-level of awareness of risky security behaviour. Whilst the results indicate the affective feedback did not make a difference to behaviour during the course of the experiments, participants felt that the affective feedback delivered had an impact, raising their security awareness, encouraging them to learn about online security.

Conclusions: This body of research has made a novel contribution to the field of affective feedback and usable security. Whilst the results indicate the affective feedback made no difference to behaviour, users felt it had an impact on them, persuading them to consider their security behaviours online, and encouraging them to increase their knowledge of risky security behaviours. The research highlights the potential application of affective feedback in the field of usable security. Future work seeks to explore different ways in which affective feedback can be positioned on-screen, and how feedback can be tailored to target specific groups, such as children, or elderly people., with the aim of raising security awareness.

Acknowledgements

First and foremost, I'd like to thank my supervisors, Dr Jackie Archibald and Dr Ian Ferguson for providing guidance and support throughout the duration of the research project and the write-up.

Additionally, I'd like to thank the Scottish Funding Council, and the Scottish Informatics and Computer Science Alliance for funding the PhD research.

I would like to thank the many colleagues I've worked with across the various schools I've been part of in the last 4 years- SECAM, DBS, SET and AMG. Special thanks goes to those I worked with in the Defence Against the Dark Arts Department office- there's no such thing as too many cups of tea. Fact.

For providing an excellent musical soundtrack to the many late nights I had whilst writing up the thesis, I'd like to thank Bryan Adams, Keith Scott, Bruce Springsteen and the E-Street Band, the Goo Goo Dolls, and Jonathan Larson, amongst many, many others.

Last but not least, I'd like to thank my family and friends for their continued faith in me. I could not have done it without you.

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

1.1. Background

Risky security behaviour displayed by end-users has the potential to leave devices vulnerable to compromise (Li and Siponen 2011). Despite the availability of security tools designed to aid users in defending themselves against potential online threats (such as firewalls and virus scanners), these tools cannot stop users engaging in risky behaviour. This indicates a need to modify the behaviour of end-users, allowing them to consider the security implications of their actions online.

1.1.1. Risky security behaviour

What constitutes risky behaviour is not necessarily obvious to all end-users and therefore, it can be difficult to recognise. Examples of behaviour which could be perceived as risky include: interacting with a website containing coding vulnerabilities (Hadnagy 2011), downloading data from unsafe websites (Fetscherin 2009) or, creating weak passwords/sharing passwords with colleagues (Stanton 2005) (Payne and Edwards 2008).

A number of studies have been conducted, in an attempt to define and categorise risky security behaviour. In 2012, a taxonomy was developed by Padayachee (2012) to categorise compliant security behaviours whilst investigating if particular users had a predisposition to adhering to security behaviour. The results of the research highlighted elements which may influence security behaviours in users e.g. extrinsic motivation, identification, awareness and organisational commitment.

Another study was documented in a 2005 paper by Stanton et al. (2005). Interviews were conducted with IT and security experts, in addition to a study involving end-users in the US, across a range of professions. The findings produced a taxonomy, consisting of 6 identified risky behaviours: intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance and basic hygiene.

These taxonomies present an abstract model of risky security behaviours. This piece of research seeks to explore a subset of such behaviours, which can be found within the context of a browser-based environment. Risky behaviours in this context may include visiting social media websites, revealing too much information online, and choosing a poor password. Vulnerable areas where users may place themselves at risk are discussed in more detail in section 2.2. There are a number of potential threats users may encounter when browsing the internet, and the following section provides an overview of further risks.

1.1.2. Potential threats

Whilst browsing the web, end-users may find themselves exposed to various security threats. Should users choose to download pirated films or software, in addition to breaking the law, they are also engaging in risky security behaviour, placing their system at risk. There is the potential for files from an unverified source to contain viruses or malware (Fetscherin 2009).

Poorly constructed websites featuring coding vulnerabilities also pose a risk to end-users. Generally, users are unaware of the existence of such flaws. If an application contains vulnerabilities, users may expose themselves to an attack by simply visiting a site e.g. users may fall victim to an XSS attack or a session hijacking attempt. Social engineering attempts are also closely linked to technology flaws. Often, users divulge too much information about themselves on social networking sites (Kaspersky Lab 2013). An attacker could gather this information to produce a directed attack against a user e.g. sending the victim an email containing a malicious link about a subject they are interested in (Hadnagy 2011). Sending a user an email of this type is known as a phishing attack. The malicious link contained within the email may link to a site asking users to enter information e.g. bank account details. As such, many average-users would fail to identify a phishing email, potentially revealing private information (Schechter et al. 2007) (Kaspersky Lab a) 2013).

Owing to the number of attacks directed towards users, various browser-based tools have been developed, with the intention of educating users, reducing the likelihood that they become a victim of an attack. The tools developed span a number of years, indicating that this is still a growing problem, and that perhaps a different approach to user feedback is needed. This research project seeks to explore the potential role affective feedback can have in educating users regarding security awareness in the context of a browser-based environment.

1.1.3. Affective feedback

Affective feedback is defined as "*the process of using technology to help people achieve and maintain specific internal states*" (McDarby et al. 2004) i.e. using signals to alter user behaviour. There are a number of affective feedback techniques which can be implemented in an attempt to alter a user's behavioural state. These include the use of virtual human characters, avatars, textual content (Dehn and Van Mulken 2012) as cited in (Jameson and Riedl 2011), and the use of colour and sound (McDarby et al. 2004) to influence state. Specifically, Dehn and Van Mulken (2012) state that *"...the simple question as to whether an animated interface agent improves human–computer interaction does not appear to be the appropriate question to ask. Rather, the question to ask is: what kind of animated agent used in what kind of domain influence what aspects of the user's attitudes or performance...*".

Avatars provide affective feedback and have been seen to be beneficial in educational environments (McDarby et al. 2004) (Robison et al. 2009) (Hall et al. 2005). Textual information with the use of specific words also has the potential to alter a user's state/behaviour e.g. a password may be described as "weak" and this can encourage them to create a stronger password (Ur 2012). Colour is also often utilised, with green or blue used to imply a positive occurrence, with red indicating a negative outcome (Ur 2012).

Previous research has indicated affective feedback may serve as a successful method of educating users about risky security behaviours (McDarby et al. 2004) (Robison et al. 2009) (Hall et al. 2005). Users' attitudes regarding risky security behaviour must be modified in a bid to keep them safer online. Thus, by influencing end-users via affective feedback it may be possible to engage users into changing their behaviour.

To further the argument for use of affective feedback Wixon (2011) discusses its benefits but also calls for more studies into the role of affective computing, placing emphasis on the need for empirical data. This is an argument also put forward by Beale and Creed (2009) in their overview of emotional simulations. Additionally, it has been highlighted that users may interact with machines for greater periods of time if a computer appears to respond to their emotions (Robison et al. 2009), indicating that affective feedback would be an appropriate route to take when getting users to consider security mechanisms which are in place on machines. In turn, this may encourage users to reduce their risky security behaviours online.

1.2. Project aim

The issues identified throughout the previous section lead to the following research aims, and subsequently, the overall research question.

The research aim:

Develop and apply knowledge of monitoring techniques and affective feedback, establishing if this changes users' awareness of risky security behaviour in the context of a browser-based environment.

The research objectives:

- Consider the current awareness of risky security behaviours in end-users and examine differing affective feedback techniques
- Develop a user monitoring system for use within a browser-based environment
- Develop prototype software containing affective feedback agents
- Construct an experimental design to address the research question
- Quantify the difference in awareness in end-users using statistical analysis and draw conclusions

The overall research question:

“Is it possible to enhance security risk awareness in end-users via dynamically provided affective feedback?”

1.3. Project tasks

The project has been split into several phases which are outlined below:

- **Phase one- literature review**
    - Investigate current awareness of risky security behaviours in end-users
    - Examine differing affective feedback techniques

- **Phase two- preparatory work**
    - Restrict the scale of the research and focus specifically on a browser-based environment
    - Establish a monitoring system for a browser-based environment
    - Develop prototype software containing affective feedback agents
    - Create an experimental design to address the research question

- **Phase three- experimental work**

    - Utilise several affective and non-affective feedback agents within a browser-based environment

    - Evaluate the effectiveness of each of these agents via user trials

    - Quantify the difference in awareness using statistical analysis and draw conclusions

1.4. Dissertation structure

The subsequent section of the thesis, Chapter 2, contains the literature review. This section aims to provide an overview of the security issues end-users may face when browsing the internet, alongside a definition of risky security behaviours users may engage in whilst online. The role of affective feedback will be investigated, with examples of how it has been used in the past, notably in scenarios requiring the use of learning tools.

This project seeks to utilise affective feedback in the context of a web browser. In recent times, a number of tools have been created to assist users in learning about staying safe and secure whilst browsing the web. Previous research will be analysed, providing a critique of methods developed in an attempt to keep users safer online. Solutions created to reduce specific types of attack will be discussed, highlighting plausible issues these tools fail to resolve.

The project will focus on the development of a tool for a web browser, specifically Mozilla's Firefox browser, and an overview of the software will be included within Chapter 4. A number of prototype extensions were developed prior to creating the final tool and these will be outlined in this section, providing a rationale and a purpose as to why each of these smaller tools was created.

By outlining the background of the project in the literature review, and by revealing various tools which could be suitable for targeting such a problem, the research goal is outlined in Chapter 3. This covers the key issues, the research question and the way in which the project seeks to address the problem, and how a result is achieved. Chapter 5 will then go on to discuss the final implementation of the monitoring solution and Chapter 6 outlines the delivery of the affective feedback system.

Following on from this, Chapter 7 will discuss the methodology and the experimental design, outlining the implementation of the project, in terms of the experiments conducted, the rationale behind the experiments, and details of the software and hardware used to capture the experimental data.

The results section, Chapter 8, will detail the results gained from the experiments, prior to the discussion and analysis of the findings in Chapter 9. Chapter 10 seeks to provide an evaluation of the results gained, considering future work which could be undertaken. Finally, conclusions will be drawn as to whether end-user security awareness can be improved via the use of affective feedback, potentially improving overall system security.

Chapter 2. Literature Review

This section documents previous research, providing an overview of the security issues users face when browsing the internet, and the risky security behaviours they may inadvertently engage in. Subsequently, there will be an examination of what is classed as risky security behaviour within the scope of a web browser, and a comparison of ways in which previous studies have attempted to measure the perception of risk in users is included. Various monitoring solutions utilised will also be covered and there will be a discussion regarding Mozilla's Firefox browser as this piece of software is integral to the project. The literature review will conclude with an overview of tools which have recently been designed to help users online, in terms of security, highlighting the key problems with traditional security tools and advice. By reviewing the literature, this will illustrate potential areas for research into affective feedback.

2.1. Security issues users face

Whilst users are browsing the web, there are a number of security issues they may potentially be subjected to. In addition to breaking the law, should users download illegal files such as pirated movies or software, they are also engaging in risky security behaviour, placing their system at risk. The files downloaded may contain viruses or malware (Fetscherin 2009).

Interaction with websites featuring coding vulnerabilities is also risky and users are generally unaware of such flaws (Imperva 2016). If an application is poorly constructed, users may expose themselves to an attack by simply visiting a site e.g. vulnerability to cross-site scripting (XSS) attacks or session hijacking. XSS attacks are common on the web and may occur where users have to insert data into a website e.g. a contact form. Attacks related to social engineering are also linked to technology flaws. Often, users divulge too much information about themselves on social networking sites (Kaspersky Lab 2013) e.g. it is possible to extract geolocation data from a specific Twitter account to establish the movements of a user. Such patterns have the potential to highlight the workplace or home of a user. An attacker could target a user, gathering the information shared to produce a directed attack against the victim e.g. sending the victim an email containing a malicious link about a subject they are interested in (Hadnagy 2011). Sending a user an email of this type is known as a phishing attack (a spear phishing attack when it is targeted towards specific users). The malicious link contained within the email may link to a site asking users to enter information such as bank account details. As such, many average-users would fail to identify a phishing email, potentially revealing private information (Kaspersky Lab a) 2013) (Schechter et al. 2007). The rise in spear phishing attacks has led the FBI to warn the public regarding this issue (FBI 2013).

Perhaps one of the most common risky security behaviours involves poor password hygiene. There can be a trade-off between the level of security of a password provides and its usability (Payne and Edwards 2008). Passwords which are shorter are less secure however, they are easier for users to remember and are therefore usable. Users may also engage in the practice of sharing passwords. When Stanton et al. (2005) interviewed 1167 end-users in devising a taxonomy of risky behaviours, it was found that 23% of those interviewed shared their passwords with colleagues. 27.9% of participants wrote their passwords down.

These are just a sample of the attacks users may be subjected to whilst browsing the web on a daily basis. Owing to these types of attacks, there is a need to utilise tools to educate users regarding risky security behaviours. Potentially, such attacks could be incorporated into a model, and subsequently translated into a monitoring solution, and an affective feedback system.

2.2. Risky security behaviour

Prior to discussing risky security behaviour, the differences between security and privacy should be defined, in the context of this research project. Security is expectation end-users have that their data will be held safely, an in appropriate format e.g. if a website holds a password, it should be salted and hashed. Privacy is the expectation that users should be able to control who they share their data with.

There have been several attempts to categorise behaviours displayed by users which could be classified as risky (summarised in Table 1). Papers contained within this table were chosen as they present a number of different ways to classify security behaviours, which could be applied to the context of a browser-based environment. Such attempts include a 2005 paper by Stanton et al. (2005). Following interviews with both security experts and IT experts, and a study involving end-users in the US, across a range of professions, a taxonomy of 6 behaviours was created: intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance and basic hygiene.

Padayachee (2012) provides a breakdown of compliant security behaviours whilst investigating if certain users had a predisposition to adhering to security behaviour. A taxonomy was developed, highlighting elements which may influence security behaviours in users e.g. extrinsic motivation, identification, awareness and organisational commitment. The paper acknowledges the taxonomy does not present a complete overview of all possible motivational factors regarding compliance with security policies. Despite this, it may provide a basis as to how companies could start to improve their security education, with a view to gaining the attention of end-users.

A trade-off exists between the usability of passwords and the level of security they provide (Payne and Edwards 2008). Usable passwords are easier for users to remember however, this can mean they are short and therefore less secure. Users may also engage in questionable behaviour regarding passwords. Other researchers have explored the usability of passwords and have acknowledged the difficulties end-users experience in choosing a password. Researchers noted that *"length requirements alone are not sufficient for usable and secure passwords"* (Shay et al. 2016). A 2015 paper concurs with this argument, recognising the issues users may have in creating complex passwords which will stand against malicious cracking tools (Al-Ameen, Wright and Scielzo. 2015).

Another of these categories is related to how users perceive technology flaws, e.g. vulnerability to XSS attacks or session hijacking, whereby users may inadvertently reveal information to untrusted websites (Table 1.- naïve mistakes). Potentially, just visiting a webpage containing flaws such as XSS is enough to place the end-user at risk. Social engineering can also be considered to fall into the naïve mistake category listed in Table 1: e.g. an attacker could potentially clone a profile on a social networking site and use the information to engineer an attack against a target (e.g. via the malicious link technique) (Hadnagy 2011). Such attacks can be facilitated by revealing too much personal information on social networking sites (Balduzzi 2011).

Downloading illegal files such as music/software can be classed as risky behaviour: in addition to breaking the law, users are potentially exposing their system to viruses or malware that the downloaded files may contain (Fetscherin 2009).

Table 1 - comparison of terminology describing risky security behaviours

Stanton, J.M. et al. (2005)	**Padayachee,K.** (2012)	**Payne, B. and Edwards, W** (2008)	**Balduzzi, M.** (2011)	**Hadnagy, C.** (2011)	**Fetscherin, M.** (2009)	**Herath, T. and Rao, H.R.** (2009)	**Bubas et al.** (2008)	**Milne, Labrecque and Cromer (2009)**	**Willison and Warkentin** (2013)
Intentional destruction: intention to harm IT resources in a company	Amotivation	-	-	-	-	-	-	-	Formation of behavioural intention to abuse. Computer abuse. Undetected abuse.
Detrimental misuse: using IT for inappropriate purposes	Amotivation	-	-	-	Downloading illegal files	-	Sharing files which may be malicious	-	Formation of behavioural intention to abuse. Computer abuse. Undetected abuse.
Dangerous tinkering: accidentally configuring IT resources with security flaws	-	-	-	-	-	-	-	-	-
Naïve mistakes: user doesn't realise their behaviour is flawed	-	Passw-ord usability	Sharing too much on social netwo-rks	Sharing too much on social networks	-	-	Privacy violation awareness	Saving passwords, revealing private information to untrusted sites, password usability	-
Aware assurance: wants to protect company IT systems-recognises security issues.	Extrinsic motivation	-	-	-	-	Intrinsic motivation: perceived effectiveness	-	-	-
Basic hygiene: user is educated about security issues and adheres to security policies	Extrinsic and intrinsic motivation	Passw-ord usability	-	-	-	Extrinsic motivation: social pressures	-	-	-

A paper by Bubas et al. (2008) analysed and modelled a number of factors which are related to online security behaviour and privacy behaviour online. The paper notes that "*computer security is becoming an increasingly more complex problem owing to the amounts and types of information that have to be secured and types of threats to computer systems*". To investigate the issue, a survey was developed to ascertain how the habits and assumptions of internet users could help in producing a list of known behaviours. The following factors (beliefs) which can lead to engagement in risky behaviours were discussed-

- F1- conscientiousness in the maintenance of the operating system, upgrading of the internet browser and use of antivirus and antispyware programs.

- F2- engagement in risky and careless online activities with lack of concern for personal online privacy.

- F3- disbelief that privacy violations and security threats represent possible problems.

- F4- lack of fear regarding potential privacy and security threats with no need for change in online behaviour.

In particular, the factor 2 was of the most interest because it links directly to risky security behaviours. The survey confirmed a list of known risky security behaviours such as visiting untrustworthy sites, sharing files via peer-to-peer networks, or simply believing that the user was not at risk of a privacy violation. These factors also correlated with the fact that people who engage in such behaviours and beliefs are more likely to have a virus/malware infection on their home computer. These people are also more likely to have suffered from a loss of data on their personal computer.

A paper by Milne, Labrecque and Cromer (2009) also investigated the area. One particular study investigated both risky behaviours and protective behaviours, then compared these with self-efficacy. The paper highlights that depending on the demographic and the self-efficacy of the end-user, this causes different types of behaviour to be exhibited online. 449 people participated in the web-based study. During the survey, participants were asked if they had engaged in specific risky behaviours online, drawn from previous research into risky behaviours (LaRose and Rifon (2007), and a previous paper by Milne, Rohm and Bahl, (2004)).

Specific risky security behaviours users were asked about in the survey included using revealing private email addresses to register for contests on websites, passwords consisting of dictionary words, and accepting unknown friends on social networking sites. The most common risky behaviour which participants admitted to was allowing the computer to save passwords, in which 56% of participants admitted to this.

Willison and Warkentin (2013) performed an empirical review relating to staff members within a company who purposely engage with malicious use of computers. By exploring previous research, they were able to understand security issues which may occur within companies, and discern threats. By understanding the thought processes of the potential offender, they were able to consider how the role of self-efficacy was linked to deterring the offender from committing computer misuse, or more seriously, a crime. Work conducted by Willison and Warkentin (2013) is based upon Straub and Welke's (1998) security action cycle. In extending this model, they looked at 3 areas which are potential motives: criminal justifications and deterrence, expressive and instrumental motives and deterrence, and injustice and disgruntlement as motives. Research found that there was a link between these motives, and that understanding motives behind computer misuse could lead to further research projects regarding how to tackle the issue.

This section has outlined various attempts to categorise behaviour. However, when exploring risky security behaviours, the perception of risk which the end-user possesses must be taken into consideration. Further work is outlined in the following section in an effort to quantify behaviours and to measure perception of risk. This indicates there is still a need to investigate end-user behaviour and awareness.

2.3. Measuring perception of risk

It can be hard for the user to recognise their security behaviour as risky. A number of techniques have been used to gauge the perception of risk (summarised in Table 2). Papers presented in the table have been chosen as they present research regarding perception of risky behaviour which may apply to the context of a browser-based environment. Farahmand et al. (2009) explored the possibility of using a psychometric model originally developed by Fischoff et al. (1978) in conjunction with questionnaires, allowing a user to reflect on their actions and gauge their perception, providing a qualitative overview. Such an approach could be utilised in this research project.

Farahmand, Atallah and Spafford (2013) investigated models of risk perception in relation to incentives. To achieve this, a revised model based upon the work of Fischhoff et al. (1978) was developed. During the extension of this model 42 US-based information security executives were interviewed to determine how incentives (e.g. motives for adhering to a policy) and risk perception can help inform security decisions. The paper cites Schneier (2008) and the possible areas where reality of risk could diverge from perception of risk. These areas include: the severity of the risk, the probability of the risk, the magnitude of the costs, how effective the countermeasure is at mitigating the risk, and the tradeoff itself. Results from the study highlight a number of key areas which managers in a company should consider when encouraging employees to consider risk perception. These areas include making security part of the work environment, and having an understanding of perception of risk and values.

Takemura (2011) also used questionnaires when investigating factors determining the likelihood of workers complying with information security policies defined within a company, in an attempt to measure perception of risk. Participants were asked a hypothetical question regarding whether or not they would implement an anti-virus solution on their computer if the risk of them getting a virus was 10%, 20% and so-on. Results revealed that 52.7% of users would implement an antivirus solution if the risk was only 1% however, 3% of respondents still refused to implement antivirus, even when the risk was at 99% which displays a wide range of attitudes towards risk perception. The study concluded that risk perception was a psychological factor with the potential to influence problematic behaviours.

San-José and Rodriguez (2011) used a multimodal approach to measure perception of risk. In a study of over 3000 households with PCs connected to the internet, users were given an antivirus program to install which scanned the machines on a monthly basis. The software was supplemented by quarterly questionnaires, allowing levels of perception to be measured and compared with virus scan results. Users were successfully monitored via the use of a number of security indicators. These security indicators (SI.) included:

- SI. 1 Tools and security measures indicator- comparison of an optimal set-up vs. the current set-up of the end-user.

- SI. 2 Security behaviour and habits indicator- viewing end-user behaviour when browsing the web, or opening emails/attachments e.g. do users scan email attachments with an antivirus tool before opening them?

- SI. 3 E-trust indicator- users' subjective perception of security whilst browsing the web.

- SI. 4 Malware incidents indicator- percentage of computers in the study which contained malware following a scan.

- SI. 5 Computers at high risk indicator- percentage of devices which contained a potentially high risk malware incident.

- SI. 6 Computers with high dissemination indicator- takes users behaviour into consideration- does the device contain a malicious file which has the potential to be shared across other machines? To provide an example, if an end-user utilises messaging services and is communicating with others, there is the potential for the malicious file to be sent to someone else.

Taking the indicators into account, results showed that the antivirus software created a false sense of security and that users were unaware of how serious certain risks could be. Additionally, in this study, it was highlighted that the installation of security tools is necessary, but more needs to be done in relation to end-users. The authors suggest end-users should be provided with technical education about threats and insecure behaviours. This would supplement active and passive methods of defending against threats.

Labunets et al. (2013) conducted a small-scale experiment to compare the effectiveness and perception of two differing risk-based methods: visual methods (CORAS, a method for security risk analysis) and textual methods (Security Requirements Engineering Process-SREP). 28 participants were split into 4 groups, and were asked to carry out a number of tasks relating to a Smart Grid application scenario (an electricity network-based scenario) e.g. groups had to identify security threats and requirements. During this process, they also had to answer a questionnaire relating to the methods they were testing. Additionally, the experimental process was also supplemented by interviews with participants in order to determine influences which lead to the effectiveness of the tools.

Analysing the interviews and the questionnaires, results from this study concluded that when identifying threats in the Smart Grid scenario, the visual method is more effective. Conversely, in extracting security requirements of a system, the text-based method performs better than the visual method. However, in relation to perception and intention in end-users, the participants preferred the visual method.

Hibshi, Breaux and Broomell (2015) investigated risk perception whilst eliciting security requirements. Networks consist of a number of devices and set-ups, all of which interact with each other, therefore analysts looking after such a system must have a level of risk perception to consider the number of security requirements needed for a complex system. The results discuss the results from two user surveys carried out, looking at the way in which security risks are perceived and how decisions are made by analysts in relation to changing threats and requirements. Several areas were identified are priorities when considering security environments: requirements composition (overall combination of security requirements for a complex system), requirements ambiguity (conflicting requirements from different parts of a complex system), requirements completeness (have all requirements for the system been met?) and distributed knowledge (the number of people who have an overall understanding of the system).

During the study containing security vignettes *("scenarios comprised of discrete factors that contribute to human judgment"*), 174 participants were exposed to 64 of these vignettes, alongside 2 threat scenarios. Results of the study proved the approach developed allowed for the effective elicitation of security requirements, and measure security adequacy ratings, which in turn can help inform the risk perception levels of the analyst.

Ng, Kankanhalli and Xu (2009) examined the use of a health belief analogy when explaining the perception of risk in terms of cyber security. The perception of falling ill was directly related to a) the perceived susceptibility of falling ill and b) how severe the illness is perceived to be. When translated to the field of cyber security, it was discovered these factors along with perceived benefits, perceived barriers, cues to action, general security orientation and self-efficacy can help to determine the riskiness of user behaviour. Experiments were conducted with an example based upon email attachments. It was concluded that users' security behaviour could be determined via perceived susceptibility, perceived benefits, and self-efficacy.

Hill and Donaldson proposed a methodology to integrate models of behaviour and perception (Hill and Donaldson 2015). The research attempted to assess the perception of security the system administrator possesses, and create a trust model which reduces the threat from malicious software. The methodology engaged system administrators whilst developing the threat modelling process, and quantified risk of threats, essentially creating a triage system to deal with issues.

Ur et al. (2016) investigated the correlation between users' perceptions of password strengths and their actual strength on smartphones. The research employed the use of an online study to measure users' thoughts on password strength and memorability, and their understanding of potential attacks. This data was compared against to users' perceptions regarding how passwords would fare against password cracking attacks. Comparing the data, allowed for the perception of risky behaviours to be determined. Outcomes highlighted serious misconceptions regarding dictionary passwords, and common passwords, and generally users didn't understand attacks.

Table 2 - comparison of methods used for measuring perception of risky behaviour

Technique	Description
Psychometric model (Farahmand 2009) (Fischoff 1978) Farahmand, Atallah and Spafford (2013)	Used the models to determine characteristics relating to gauging perception of security and privacy risks.
Questionnaires (Fischoff 1978) (Takemura 2011) (Ur 2016) Hibshi, Breaux and Broomell (2015) Labunets et al. (2013)	Subjects were assigned questionnaires to allow them to reflect on their perception of risk.
	Used to determine the likelihood of workers complying with information security policies.
	Used quarterly questionnaires to gauge perception of risk. Compared these to anti-virus scan results.
	Used to gauge perceptions on the strength and memorability of smartphone passwords.
	Used to gauge security requirements of a complex system.
Technology-based (San-José and Rodriguez 2011)	Installed antivirus software on over 3000 internet connected PCs which were scanned on a monthly basis.
Health belief model (Ng, Kankanhalli and Xu 2009)	The model was used as an analogy to explain perception of risk.
Threat model (Hill and Donaldson 2015)	Utilised system administrators and quantified risk to produce a triage system
Interviews (Labunets et al. 2013)	Determine effectiveness of visual and textual risk-based methods.

Thus far, background research has identified a number of security issues the end-user may be subjected to whilst browsing the web. Attempts have been made to categorise such behaviour, and measure the perception of risk which the end-user may possess. These sections have highlighted that it can be difficult for the end-user to recognise that their behaviour is placing them, and their devices at risk. This suggests that end-users require some form of security education. A number of tools have previously been developed in attempt to improve end-user security awareness (discussed in detail in the following section, and to raise perception of risk. These tools developed span a number of years, and yet some of them still present issues when raising security awareness. Such issues suggest a different approach is required. Affective feedback has been used in academic environment to aid students in learning. Owing to the use of affective feedback in this environment, it is plausible it could be utilised and applied to the domain of security awareness and education.

2.4. Tools created to help users in terms of security

2.4.1. Keeping users safe and preventing attacks

2.4.1.1. Password tools

Many users participate in risky security behaviour, particularly when it involves passwords, as highlighted by Stanton et al. (2005). A number of attempts have been made to understand the problems users face when dealing with passwords, with tools developed to aid users. Furnell et al. (2006) conducted a study, to gain an insight into how end-users deal with passwords. The survey found that 22% of participants said they lacked security awareness, with 13% of people admitting they required security training. Participants also found browser security dialogs confusing and in some cases, misunderstood the warnings they were provided with. The majority of participants considered themselves as above average in terms of their understanding of technology, yet many struggled with basic security. As a result of confusion in end-users, a number of studies have been conducted in an attempt to improve users' security awareness in terms of passwords.

Bicakci et al. (2009) explored the use of using graphical passwords built into a browser extension, based on the notion that humans are better at memorising images than text. The aim of the software developed was to make passwords more usable, decreasing the likelihood of users engaging in risky security behaviour. Participants could select 5 points on an image with a grid overlay to produce a password, which was compared against previous research conducted with plain images. Results from the study showed the grid had little effect on the password chosen however, in a survey of end-users, the grid proved to be more successful than an image without a grid in terms of usability when rated using a Likert scale.

Others have also utilised a visual approach. To demonstrate the strength of a chosen password, Ur et al. (2012) investigated how strength meters placed next to password fields improved the security and usability of passwords. Participants were asked to rate their password security perceptions on a Likert scale. Immediately after creating a password with the aid of a meter, they were surveyed regarding their opinion of the tool. The tool was deemed to be a useful aid in password creation with participants noting that use of words such as "weak" encouraged them into creating a stronger password. However, the study was repeated the following day and between 77% and 89% (depending on the different groups) were able to recall their passwords, which fails to sufficiently test the memorability of a password at a much later date. Additionally, 38% of participants admitted to writing down their password from the previous day, highlighting that despite the encouragement of the password meter, complex passwords are still difficult to remember. Therefore, users still participated in risky security behaviour, despite the fact a tool was developed to help them,

The concept of password meters has been explored by multiple researchers. Work was carried out by Egelman et al. (2013), exploring whether the use of password meters had an impact upon the password selected. Two different password metering systems were also implemented: one which looked like a traditional password meter (i.e. providing a meter with colours and text such as “weak”, “good”) and another, which compared password strengths to other users of the tool (e.g. “weaker than 40% of users”). An initial experiment was conducted where users were asked to change their real passwords. In this experiment, users were not told the purpose of the study, to avoid the introduction of bias. It was shown that the implementation of password meters caused users to create stronger passwords. Another experiment was run following the initial experiment. In this scenario, users were asked to create a password for an account they deemed to be unimportant. Results showed that password meters did not have an impact for these types of accounts. Again, this highlights that security tools such as password meters may not have an impact on end-user behaviour.

Vance et al. (2013) explored the use of fear appeals in relation to password security. Fear appeals are messages which seek to highlight or raise perception of a threat, and aid the user in dealing with the potential threat. In an experiment, users were asked to register for an account, and the password strength chosen by the end-users was observed. Users were free to choose any password they wanted e.g. there was no minimum length required. Participants were split into different groups: the control group were given no guidance on password creation, the static fear appeal treatment group received security information that did not change on user input, an interactive password meter group received an interactive password meter, and finally a group which received an interactive fear appeal treatment which provided security guidance which updated on user keypress. Results found that the interactive fear appeal treatment performed better in terms of choosing stronger passwords, and such an approach may aid in raising end-user security awareness. This approach utilised a text and colour to provide a visualisation of security advice.

Ciampa (2013) performed a study to explore the impact of different password strength meters, outwith the use of the traditionally used horizontal bar meters commonly seen online when registering for an account on a website. Specifically, he investigated whether or not password strength feedback prompted users to create stronger passwords. In the study, participants were asked to record 4 passwords they may use online for accounts. Subsequently, they had to visit websites which offered password strength checking services. Users also had to record if the password strength checks encouraged them to change their passwords. Results from this experiment showed that *"any feedback mechanism can influence users to create passwords with higher entropy".* Participants also noted that websites which indicated how long it would take to crack a particular password were useful, and had an impact.

Steinbart, Keith and Babb (2016) researched the use of models representing secure behaviour in a bid to discover what makes a user continue/discontinue to behave in a secure way. Experiments were conducted which sought to determine the way in which users logged into websites. To achieve this, a mobile app was created, named "findamine" which required participants to login on a regular basis. Participants were also able to log into a desktop-based website. Results found that the type of interface users logged into produced different results. When engaging in a security behaviour such as logging to a website, it was found that users desire a usable interface. In relation to mobile devices, if a password is too complex to enter on a small or limited keyboard, and the interface does not provide the option to store credentials, users will change their password to something which is weaker, and will thus engage in a risky security behaviour. This indicates that the design of a password area on a website has some impact in terms of whether the end-user engages in risky security behaviours.

De Carné De Carnavalet and Mannan (2015) investigated the use of password meters, performing a large-scale evaluation. An empirical analysis was conducted in this paper to determine how password meters function, ultimately highlighting how they can be improved. To achieve this, a number of factors were considered: meter characterisation (gauged characteristics of 22 meters analysed during the study), reverse engineering of password meters where possible, empirically evaluating password meters (by utilising millions of passwords against the meters, drawn from several password dictionaries) and meter weakness (taking into consideration the fact that some meters may mark trivial passwords as safe e.g. a password may be short but if it has lower and uppercase letters, numbers and symbols, it's still marked as secure).

Overall results from the study highlight a number of key issues. One such issue notes that password meters need to be improved, and potentially redesigned. To provide an example, checking if the entered password has previously been found on a leaked password list, and providing a notification to the user could be a potential change. Results also found that commonly used password managers such as LastPass and 1Password provide inaccurate measures of password strength, and should be redesigned, given how prominent they are. Despite the prevalence of password strength meters on the web, the flaws pointed out in this research indicate there needs to be another way of conveying security information to the end-user.

This section has provided an overview of recent research conducted into the use of security tools to help users choose stronger, more effective passwords. As the literature shows, password hygiene is still a problem for end-users, despite the number of approaches which have been taken to help them. Much of the research conducted into keeping users safe online, educating them about risky security behaviour has also revolved around phishing attacks. Recently, a number of solutions have been developed to gauge how best to inform users about the dangers of phishing attacks, with the hope that education will reduce participation in risky security behaviours.

2.4.1.2. Phishing tools

Unknowingly engaging with a phishing attempt, and potentially revealing personal information is another risky security behaviour. A number of tools have been developed in an attempt to educate users, teaching them how to spot a phishing attack. An overview of some of these tools has been provided in this section.

Dhamija and Tygar (2005) proposed the use of a method to enable users to distinguish between spoofed websites and genuine sites. A Firefox extension was developed which provided users with a trusted window in which to enter login details. A remote server generated a unique image which is used to customise the web page the user is visiting, whilst the browser detects the image and displays it in the trusted window e.g. as a background image on the page. Content from the server is authenticated via the use of the secure Remote Password Protocol. If the images match, the website is genuine and provides a simple way for a user to verify the authenticity of the website. At the time the paper was written, user evaluations had not been conducted, therefore the effectiveness of the tool could not be determined.

Sheng et al. (2007) tried a different approach to reducing risky behaviour, gamifying the subject of phishing with a tool named Anti-Phishing Phil. The game involves a fish named Phil who has to catch worms, avoiding the worms, on the end of fishermen's hooks (these are the phishing attempts). The study compared 3 approaches to teaching users about phishing: playing the Anti-Phishing Phil game, reading a tutorial developed or reading existing online information. After playing the game, 41% of participants viewed the URL of the web page, checking if it was genuine. The game produced some unwanted results in that participants became overly cautious, producing a number of false-positives during the experimental phase.

PhishGuru is another training tool designed by Kumaraguru et al. (2009) to discourage people from revealing information in phishing attacks. When a user clicks on a link in a suspicious email, they are presented with a cartoon message, warning them of the dangers of phishing, and how they can avoid becoming a victim. The cartoon proved to be effective: participants retained the information after 28 days. The tool did not cause participants to become overly cautious and they continued to click on links in genuine emails however, a longer study is required to fully gauge the success of the tool.

Similarly, an Android app called NoPhish (Canova et al. 2015) has been developed to educate users about phishing on mobile devices. The game features multiple levels where users are presented with a URL and are asked if it is a legitimate link or a phishing attempt. In a study conducted after playing the game, participants gave significantly more correct answers when asked about phishing. A further long-term study was conducted 5 months later. The long-term outcomes showed participants still performed well however, their overall performance decreased. This suggests there are issues with long-term retention.

Basnet and Doleck (2015) investigated the use of machine learning for the development of an anti-phishing URL tool. Work proposed the use of a heuristic approach, classifying a URL via the information available about it, utilising a training dataset from a website containing a repository of known phishing sites. The URL was checked against a number of features, including its positioning in other databases of known phishing sites, and its positioning in search engine results. Results found that these features are useful in the automatic classification of URLs as phishing attempts, producing an error rate of <0.3%. The authors state the approach discussed could be implemented into a tool to help end-users identify phishing attempts.

In 2016, Volkamer, Renaud and Reinheimer (2016) proposed the use of a just-in-time tool, TORPEDO, to provide tooltips in relation to potential phishing links in emails. This was implemented via a Thunderbird extension. URLs within emails are disabled for a short period of time, in the hope that users will consider checking the URL before clicking on what could be a potential phishing attempt, and, redirects are detected. This approach was compared against the end-user seeing the email URL within the status bar, without any tooltip feedback. When comparing the two approaches, TORPEDO performed better: 85.17% correct answers for identifying phishing emails, in comparison to the 43.31% who correctly identified phishing emails via the status bar.

An automatic phishing detection and incident response framework was created by Husák and Cegan (2014). This is based upon an automatic phishing incident processing tool named PhiGARo (Cregan et al. 2012). The aim of the framework was to utilise honeypots to capture email messages containing phishing attempts, rather than waiting for a user to report a phishing attempt, therefore eliminating the human factor. Use of the tool proved victims of phishing could be notified via email using this approach, and future phishing messages could be blocked to prevent end-users from further engaging in risky security behaviour.

The findings of research conducted on educating users about phishing attempts have had mixed results. Whilst they may potentially be useful in educating end-users, there are a number of problems with such tools. In some cases, users become overly cautious, and find it difficult to identify phishing attempts from genuine emails. Another issue highlighted is retention. Whilst some of these tools have an impact in the short-term, user performance diminishes over time. In developing a tool which utilises a monitoring solution and affective feedback, these issues should be taken into consideration whilst analysing the impact of such a tool.

2.4.1.3. Privacy issues

Information that allows phishing emails to be targeted towards specific users can come from revealing too much information online. A proposed series of nutrition labels for online privacy have been designed in an effort to reduce risky behaviour (Kelley 2009). While it has been shown users do not fully understand privacy policies online, the nutrition labels seek to present the information in a format which is easier for users to understand. Labels were designed using a simplified grid design with a series of symbols representing how a site utilises data: how it is collected and used, and whether data is required (opt-in or opt-out). Results from a small study found that visually, the labels were more interesting to read than a traditional security policy and presented an easier way for users to find information.

Besmer et al. (2009) acknowledged that various applications may place users at risk by revealing personal information. A tool was developed and tested on Facebook to present a simpler way of informing the user about who could view their information. A prototype user interface highlighted the information the site required, optional information, the profile data the user had provided and the percentage of the user's friends who could see the information entered. The study showed that those who were already interested in protecting their information found the interface useful in viewing how applications handled the data.

2.4.1.4. General warning tools

In addition to security tools which have been developed to target privacy issues on social networking sites, studies have also focussed on more general warning tools when the user is browsing the web. A Firefox extension developed by Maurer (2011) attempts to provide alert dialogs when users are entering sensitive data such as credit card information. The extension seeks to raise security awareness, providing large JavaScript dialogs to warn users, noting that the use of certain colours made the user feel more secure.

More recently, Volkamer et al. (2015) developed a Firefox Add-On, called PassSec in attempt to help users detect websites which provided insecure environments for entering a password. The extension successfully raised security awareness and significantly reduced the number of insecure logins.

2.4.2. Issues with traditional security tools and advice

Some of the tools discussed in the previous section provided unwanted results, in particular, studies found that, users became overly cautious when browsing the web and produced a number of false positive results when detecting phishing attacks (Sheng 2007). Another study highlighted that although the tool developed for submitting private information online performed well in experiments, it was difficult to encourage users to make use of it. Instead, several participants continued to use web forms which they were more familiar with (Wu, Miller and Little 2006).

There are a number of issues with traditional security advice, namely long term retention, long term behavioural change and security fatigue. Furnell and Thomson (2009) discussed the term "security fatigue" in relation to computer security in 2009. Even though companies try to educate employees about security, they may still fail to engage with the good practice they have been taught. There are a number of issues which can cause non-compliance in an employee. Such issues include a lack of awareness of security issues, and a lack of training in regards to computer security. Even if these issues are not at play, security fatigue may still set in. The work considers that there may be *a "threshold at which it simply gets too hard or burdensome for users to maintain security.".*

Potential security measures which can cause security fatigue include: firewall/antivirus (these can become intrusive), automatic software updates (these are becoming more frequent), and anti-phishing tools (which may cause browser latency). The reason why such measures cause fatigue must be explored. These factors include effort (how much does the user have to try to comply), difficulty (how easy is it to comply with the security measure), and importance (the priority given to secure an asset/account). Conclusions from the paper notes that a user will become less fatigued with security if they believe it is an important task.

Parkin et al. (2016) further investigated the concept of "security fatigue". Whilst Parkin et al. (2016) agrees with the work by Furnell and Thomson (2009) through the use of a model the paper identifies potential sources of this fatigue. These sources include an excessive cognitive load (e.g. trying to remember a password), excessive physical load and preparedness (e.g. having to remember to carry an authentication token), distraction from time-sensitive tasks (e.g. security policies can be seen as a burden due to work pressures), blocking of tasks and missed opportunities (e.g. waiting for IT to be set-up properly in a business), and potential embarrassment (e.g. being unable to access data when a client requests it).

Work by Stanton et al. (2016) builds upon the aforementioned research. Several hundred participants were interviewed with regard to perception of privacy and cybersecurity. The study was not initially designed to investigate security fatigue however, results began to show this as a recurring theme. In this study, security fatigue manifested as decision fatigue e.g. avoidance decisions which were unnecessary, and choosing the easiest option. This linked with a key finding from the paper by Furnell and Thomson (2009)- there is a cost-benefit issue in place, and users will choose to ignore security advice if it is too complex or requires a considerable amount of effort in comparison to the asset which they are trying to protect.

Many of the tools created focus on one specific area where users are vulnerable e.g. they educate people about privacy, passwords or phishing attempts. These tools come with additional problems such as security fatigue and issues with long term retention. Despite the number of tools created and designed to help protect users online, users continue to engage in risky security behaviour, placing their information and devices at risk. The tools developed span a number of years, indicating that the issue of risky security behaviour has yet to be resolved. Issues surrounding security fatigue must be considered when developing a suitable monitoring and affective feedback delivery system for this research project.

2.5. Monitoring Behaviour

To provide affective feedback to users in a timely manner, a monitoring solution must be constructed, to detect the moment a user has engaged in potentially risky security behaviour. Multiple approaches have been used in the past to monitor user behaviour. Fenstermacher and Ginsburg (2002) have experimented with the use of a system event-based approach (originally designed for gathering usability information) which linked applications running across the operating system. Each application invoked several method calls and functions, making use of Microsoft's Component Object Model and Python. An XML-based log file was then generated based-upon the actions of the user, containing information such as a timestamp, the application used and which event was triggered. This suggests a similar technique could be applied when monitoring risky security behaviour.

Additionally, a combination of video and task monitoring could be used to view user behaviour (Heishman, Z. and Wechsler 2007). In a study by Heishman, the eye movement of participants was monitored to interpret the affective state of the user. Results of the study found it was possible to detect the affective and cognitive states of users and that such a technique may be used when exploring further HCI concepts.

Doubleday et al. also successfully used both video and task monitoring to observe behaviour (Doubleday 1997). In this study, users were given a series of tasks to complete e.g. retrieving information from a database. Whilst completing the assigned tasks, users were asked to provide a running commentary of their thoughts. They were observed via a video camera during this process to gauge their level of interaction with the system. Additionally, they were provided with a questionnaire on completion, comprising of a 7-point Likert scale regarding usability aspects of the system e.g. the appeal of the system used. The research highlights that when monitoring risky behaviour, a multimodal approach is useful, allowing a comparison of results from each monitoring method.

2.6. Affective feedback

A possible method of educating end-users is through affective feedback, which belongs in the field of affective computing. Other methods of educating users in relation to security can include gamifying a specific threat such as phishing (Sheng et al. 2007), creating security policies (Kelley 2009), and the use of tooltips to present contextual text-based information (Volkamer, Renaud and Reinheimer 2016).

Affective computing can be defined as, "*computing that relates to, arises from, or deliberately influences emotions*" (Picard 2000). Affective feedback is an aspect that can influence the end-user and as such is defined as, "*the process of using technology to help people achieve and maintain specific internal states*" (McDarby et al. 2004). Thus, by influencing the end-user through affective feedback it may be possible to engage them into changing their behaviour.

Work by Iovane et al. (2012) proposes a methodology which attempts to identify and quantify the emotional state of the learner. The paper highlights the field of affective computing, stating that it has the potential to create systems which can adapt to the emotion state of the user. The authors note that emotion is *"assumed to play a major role for learning processes"*, and the work states that *"feedback is an important mechanism in learning."*. Arguedas et al. (2015) concur with this sentiment- *"emotion has emerged as a vital element in the learning process"*. Again, this suggests that affective feedback could be applied to a learning environment, and in the case of this PhD project, to the field of security education and awareness.

Selmi, Aïmeur and Hage (2013) explored the use of a theoretical framework in relation to an intelligent tutoring system, employing the use of peer affective feedback. Privacy issues were raised, to ensure learners were supported without bias. In connecting peers in an e-learning environment it was proposed that affective feedback, such as positive comments, and expressing concern for a peer in distress could be helpful in facilitating learning.

The use of affective feedback is not limited to educational systems. Novak, Nagle and Riener (2014) applied the concept to people playing a variant of the classic Nokia game, Snake. Users can self-report their current state, and the computer running the game has a probability of agreeing with the opinion of the user. Subsequently the level of difficulty in the game can be increased or decreased as a result of this outcome.

Ranieri and Romero (2016) discuss the use of affective feedback in relation to human-robot interaction. The authors applied an emotion-aware interaction strategy to a virtual agent within an Android application. The application inferred the emotional state of the end-user by mapping feature points on the face of the user, running it against a classification process. This means the on-screen avatar can respond appropriately to the end-user. Future work seeks to build and adapt the platform before additional studies are conducted.

In relation to security, several methods can be deployed to inform the user that they are exhibiting risky behaviour (summarised in Table 3). Ur et al. (2012) investigated ways in which feedback could be given to users, in the context of aiding a user in choosing a more secure password. Research conducted found that users could be influenced into increasing their password security if terms such as "weak" were used to describe their current attempt. In the research, colour was also used as a factor to provide feedback to users. When test subjects were entering passwords into the system, a bar meter was shown next to the input field. Depending upon the complexity of the password, the meter displayed a scale ranging from green/blue for a good/strong password to red, for a simplistic, easy to crack password. Data gathered from the experiments showed that the meters also had an effect on users, prompting them to increase system security by implementing stronger passwords, although long term retention was an issue.

Multimedia content such as the use of colour and sound can also be used to provide feedback to the user" (McDarby et al. 2004). In a game named "Brainchild" developed by McDarby et al., users must gain control over their bio-signals by relaxing. In an attempt to help users relax, an affective feedback mechanism has been implemented whereby the sounds, colours and dialogues used provides a calming mechanism e.g. blue can be seen as a calming colour (Adams and Osgood 1973).

Textual information provided via the GUI can be used to communicate feedback to the user (Dehn and Van Mulken 2012). Dehn and Van Mulken conducted an empirical review of ways in which animated agents could interact with users. In doing so, they provided a comparison between the role of avatars and textual information in human-computer interaction. It was hypothesised that textual information provided more direct feedback to users however, avatars could be used to provide more subtle pieces of information via gestures or eye contact. Ultimately it was noted multimodal interaction could provide users with a greater level of communication with the computer system.

Previous research has indicated that affective feedback can be utilised when aiding users in considering their security behaviour online, since it can detect and help users alter their internal states (McDarby et al. 2004). Work conducted by Robison et al. (2009) used avatars in an intelligent tutoring system to provide support to users, noting that such agents have to decide whether to intervene when a user is working, to provide affective feedback. However, there is the danger that agents may intervene at the wrong time and in doing so, may cause some negative affects when attempting to aid a student. In the context of learning environments, Iovane et al. (2012) also discussed this potential issue e.g. if the end-user appears to be bored, then a learning system should recognise and intervene to ensure they are appropriately challenged, keeping them engaged.

Hall et al. (2005) concurs with the notion of using avatars to provide affective feedback to users, indicating that they influence the emotional state of the end-user. Avatars were deployed in a personal social and health education environment, to educate children about the subject of bullying. Studies showed that the avatars produced an empathetic effect in children, indicating that the same type of feedback could be used to achieve the same result in adults.

Table 3 - comparison of feedback techniques

Technique	Description
Textual	Specific words were chosen to persuade participants to consider password security i.e. participants would not want a password to be described as "weak" (Ur 2012).
	Textual data can provide more direct feedback (Dehn and Van Mulken 2012).
Colour	Used colours in bar meters to indicate password strength (Ur 2012).
	Specific colours used to allow users to control their state (McDarby et al. 2004)
Sound	Specific music used to allow users to control their state i.e. calming music (McDarby et al. 2004)
Avatars	General overview of the role of animated agents in HCI (Dehn and Van Mulken 2012).
	Avatars were utilised in an intelligent tutoring system, to support users learning about microbiology and genetics (Robison et al. 2009)
	Avatars were deployed in a personal social and health environment to provide education on bullying (Hall et al. 2005)

2.7. Attitude vs. behaviour

Although it may be possible to utilise affective feedback to raise end-user security awareness, the relationship between attitude and behaviour must be considered. A number of studies have been carried out in this area, and some of the findings may relate to this research project.

In section 6 of Mostyn's "The attitude behaviour relationship" paper (1978), she examines the links between attitude and behaviour in relation to advertising. She notes that there is a wealth of literature on the subject, documenting instances where persuaders have successfully and unsuccessfully changed the attitudes of people. In order for an attitude to change, she refers to two key components which seem to cause an attitude shift. These are that firstly, a person must gain experience of the area the attitude is related to, and secondly, the person must come to terms with dissatisfaction which surround the old attitude they possessed.

Her work also discusses that it can be difficult to accurately measure change of attitude. This is typically done via the use of Likert scales and semantic differentials. However, results from these can vary differently when measuring attitude change, and attitudes should be measured on a number of occasions to build-up a true picture. Despite these points, she highlights that perhaps the act of measuring an attitude or behaviour will change the behaviour exhibited. These different views presented in the same paper show that this is a complex issue which researchers have been considering for years.

Others have also looked at this link between attitudes and behaviour. Hini, Gendall and Kearns (1995) examined this relationship in the context of attitudes in relation to the environment. 1449 participants took part in the experiment where there were asked a total of 188 questions in reference to behavioural measures or attitude measures in relation to the environment e.g. use of packaging materials. Results of the research showed there was a link between attitude and behaviour. Such a link has also been identified in other studies.

Olson and Zanna (1993) reviewed existing literature and found that there is a link between behaviour and attitude, stating "*behavior affects attitudes, not just the reverse*". However, the link found in Hini, Gendall and Kearns' study (1995) was weak. Specific to the context of this study, it was shown that environmental attitudes were not a consistent predictor of participant behaviour.

Myers (2004) provided a discourse regarding the relationship between attitude and behaviour. In discussing if attitudes will predict behaviour, they noted they may, given certain circumstances: if outside influences are minimised, if predicted behaviour corresponds to an actual attitude, and if the attitude held is strong. Despite these factors, he concurs with work by Hini, Gendall and Kearns (1995) noting that such a connection is often weak.

The issues of attitude and behaviour were explored by Avey, Wernsing and Luthans (2008), relative to organisational change. The level of positivity (psychological capital) exhibited by an employee was investigated in a bid to see if this had an impact on attitudes and behaviours. After surveying 132 employees from a number of different organisations, it was found that an employee's underlying level of psychological capital was directly linked to attitudes and behaviours within a company. Furthermore, these employees were more mindful. Overall, it was shown employees with a positive attitude exhibited less deviant behaviours, and were more committed to the company. In a separate study which sought to predict if people would purchase organic foods, conducted by Arvola et al. (2008) similar results were noted. Participants exhibiting positivity and the need to "do the right thing" predictively purchased organic food.

By understanding the relationship between attitude and behaviour, findings can be applied to the context of security awareness. Alkaldi and Renaud (2016) looked into reasons behind why people might decide to utilise or reject security tools on their smartphones. The work reviewed proposed models of security on mobile devices, before presenting the concept of a new model, termed the Integrated Model of Behaviour Prediction (IMBP). Such reasons, or background factors included the attitude the user had towards adopting the security behaviour and the intention to adopt the security behaviour. Future work by the researchers seeks to test the performance of such a model.

Despite being provided with security advice, it is possible this will change neither the attitude or the behaviour of the end-user. Herley (2009) investigated rational reasons as to why users may reject perfectly reasonable security advice in the context of mobile phones. Essentially, the paper posits that security advice can prevent users from falling victim to an attack, however, attacks are relatively rare, therefore users perceive adhering to security advice as a burden. This is a potential issue which could apply to this research project.

2.8. Summary of issues

Previous work has highlighted the multitude of flaws which users may encounter whilst browsing the web. Users may interact with poorly coded websites, exposing themselves to websites which are susceptible to XSS attacks. They may reveal too much information about themselves online, which may lead to them becoming targets in a spear phishing attempt. Additionally, end-users may be careless with their passwords, sharing them with colleagues, or selecting weaker passwords which are deemed to be more memorable or usable. This suggests that users need to be educated regarding such risky security behaviours.

As users are often unaware of the risky security behaviours they may exhibit, attempts have been make to quantify the perception of risk which users have. Various methods have been used, such as questionnaires used in conjunction with psychometric models, which allow users to take a reflective approach in measuring their perception of risk in a qualitative manner (Farahmand 2009). Several other studies have also used questionnaires, measuring different factors such as if risk perception was a psychological factor with the potential to influence problematic behaviours (Takemura 2011), or how anti-virus tools could lull users into a false sense of security regarding the security of their system (San-José and Rodriguez 2011).

Over the years, a number of tools have been developed to keep users safe online. The use of graphical passwords as a browser extension was explored by (Bicakci 2009), based on the notion that humans are better at memorising images than text. The extension sought to make passwords more usable and reduce the occurrence of risky security behaviour. Ur (2012) took a different approach, utilising password meters and words such as "weak" or "good" to denote strong/weak passwords, and to again make passwords more usable, reducing the need for risky behaviour. Others such as Sheng et al. (2007) have tried to educate users about phishing attacks gamifying the subject of phishing with a tool named Anti-Phishing Phil. In addition to this, approaches have also been taken to prevent users divulging too much information about themselves online in the first place. A series of food nutrition style labels were proposed to educate users about online privacy, providing a simple way of displaying the information users were making available about themselves (Kelley 2009). Another study in this area by Besmer et al. (2009) attempted to develop a simpler way of alerting users about the information they revealed about themselves.

Despite the various educational tools developed, there are several issues with some of the software created. Many of the tools seek to train the user about one specific area, such as phishing or poor password management. Users may be educated regarding one aspect of their security behaviour but may continue to engage in risky security behaviours in other ways. The tools developed span a number of years, indicating that the issue of risky security behaviour has yet to be resolved, and more education is needed. Integrating both a monitoring solution and an affective feedback system is a potential solution to this problem. Potentially, existing research could be applied to the problem of educating users about their risky security behaviours.

As more and more business is carried out online, it is important that average users are educated in how to behave safely online. In a study conducted by Ofsted in 2010 (cited by (Hoffman 2011)), it was reported that some children are now receiving security awareness education in schools, with a view to them maintaining such awareness when left unsupervised on machines. However, a large proportion of the population do not have access to this type of training. It is clear that education is required to help improve a user's understanding of security, a sentiment which has been echoed by the likes of Leah Hoffman who questioned: *"What if we had cybersecurity education programs, like we do for fire safety and AIDS?"* (Hoffman 2011).

Any system giving feedback on security behaviour must be able to a) monitor a users' behaviour and b) recognise it as insecure, and provide feedback. The first problem can be tackled using the event based approaches (typified by Hilbert and Redmiles (2000) and Fenstermacher and Ginsburg (2002) in which both the operating system and applications are instrumented so as to collect data on interface events and function calls (originally with the intention of extracting usability information). The analysis of such data into recognizable patterns of behaviour has been examined from a user perspective by Stanton et al. (2005), Ng et al. (2009) and more recently by Padayachee (2012).

The implementation of a monitoring framework is a necessary precursor to the work on affective feedback and is based upon known techniques as discussed in the preceding paragraph.

A possible method of educating end-users is through affective feedback, which belongs in the field of affective computing. Previous research utilising affective feedback considers a number of areas. As an example McDarby et al. (2004) considered the general benefits of affective feedback e.g. technology being used to help users alter their internal states. Robison et al. utilised avatars in an intelligent tutoring system and noted that *"throughout learning interactions, affect support systems continually encounter situations in which they must determine whether to intervene to provide affective support"* (Robison et al. 2009). Other research by Hall et al. (2005) indicates that affective feedback and interface characters are a suitable method for interacting with end-users and influencing their emotional state.

It has been highlighted that users may interact with machines for greater periods of time if a computer appears to respond to their emotions (Jameson and Riedl 2011), indicating that affective feedback would be an appropriate route to take when encouraging users to consider security mechanisms which are in place on machines. The relationship between attitude and behaviour must also be taken into account. Previous research has indicated that whilst there is a link between these factors (Myers 2004), the connection may be weak (Hini, Gendall and Kearns 1995).

Acknowledging that even intermediate/advanced users struggle with security and the obscure terms which surround it (Furnell et al. 2006), this identifies that there is a need to interact with users and aid them in enhancing security in this respect. Given the nature of affective computing, this is a possible solution to interacting with end-users.

Chapter 3. Research Goals

3.1. Project focus

The aim of this research project is to ascertain whether or not dynamically provided affective feedback enhances awareness of risky security behaviour in end-users. Furthermore, the project seeks to evaluate the possibility that by enhancing security risk awareness in end-users, the overall security of the computer system will also be enhanced as a result. Considering the research which has previously been conducted in the field of both affective computing and security risk awareness, the experiments conducted in this project will follow a similar approach.

The developmental process involves the creation of a monitoring solution in a vein similar to one proposed by Fenstermacher and Ginsburg (2009) which utilises an event-based approach whereby events triggered will be written to a log file for further analysis. An affective feedback mechanism will be constructed on top of the monitoring solution, delivering affective feedback at appropriate intervals.

During the experimental phase, users will be asked to complete a questionnaire, to quantify opinions regarding potential feedback received. Following the multi-modal approach taken by San-José and Rodriguez (2011), log data will be compared to questionnaire results, allowing both user behaviour and user security awareness to be measured. Conclusions will be drawn as to whether or not it is possible to utilise affective feedback in enhancing the security risk awareness in end-users.

3.2. Research Question

Factors discussed such as the need for security education in end-users, and the prospect of a monitoring solution, coupled with affective feedback being a suitable solution to the issue, this leads to the research question-

- *"Is it possible to enhance security risk awareness in end-users via dynamically provided affective feedback?"*

3.3. Addressing the issues

To address this question, several steps were completed in the development of a potential solution. Chapter 2 looked at the background of the risky behaviour of users in the context of a web browser, and possible methodologies which could be used to persuade users to change their behaviour online, including monitoring solutions and affective feedback. Since security awareness in the context of a web browser is being investigated, a solution to the problem in the form of a Firefox browser is a potential solution. Chapter 4 outlines small test extensions which were developed in order to prove an extension was able to monitor and capture risky security behaviours, and could deliver suitable methods of affective feedback when required.

To address the problems identified by this project, initially, a sub-domain of the security-risk problem was identified. The project addresses the issue of security and risks within the web browser, owing to the ubiquitous use of the internet in the 21st century.

Due to this a piece of software, a browser extension was developed which will act as a testing harness for alternative feedback agents. Again the project was restricted to a manageable size, investigating the sub-domain of risky security behaviour in terms of a web-browser environment. Specifically, the browser chosen for the project was Mozilla Firefox, as it had the necessary low-level hooks which would allow for rapid development of a system which could monitor user behaviour and trigger affective feedback at opportune moments. In monitoring user interaction, the software can compare this to models of known risky behaviour. It will then send a message to the agent under trial requesting feedback delivery. Mozilla Firefox is merely a method of delivering such a warning system.

Additionally, Mozilla Firefox was chosen as when the research project was proposed in 2012, Firefox retained the second largest browser share worldwide (behind Internet Explorer) (ARSTechnica 2012). The cross-platform nature of the browser also means that those who use Windows, OS X, and Linux operating systems may be aware of the browser.

A number of feedback agents were developed in order to assess the impact of affective feedback. These include a control extension (which monitors users' actions but provides no feedback), an extension which provides text-based affective feedback, an extension which provides text-based and colour-based affective feedback, an extension which provides text-based and avatar-based affective feedback and finally, an extension which provides text-based, colour-based and avatar-based affective feedback (Chapter 6 provides a full overview of the agents utilised). Previous research indicates that both avatars and textual feedback appear to be appropriate methods of educating users in regards to their behaviour when interacting with a device, prompting users to change their behaviour (Hall et al. 2005) (McDarby et al. 2004) (Dehn and Van Mulken 2012). This suggests that such an approach would be applicable for this project also. Their performance was evaluated against each other via user evaluations.

Each of the extensions were tested with users. Initially the evaluation was qualitative, utilising questionnaires. Several studies conducted in the field of affective feedback advocate the use of questionnaires and Likert scales to evaluate the effectiveness of an agent (Pfleeger and Caputo 2012) (Robison et al. 2009) (Wixon 2011) (Lottridge, Chignell and Jovicic 2011). Therefore, a comparable approach has been undertaken within this project.

Specifically, the questionnaires used with the Likert scales attempt to address components of the research question, covering areas such as: how a user perceived their initial behaviour when interacting with a web browser, whether users found affective feedback provided to be helpful and whether the feedback given highlighted issues, and allowed them to reconsider their security behaviour. The difference between what the users said they did was compared against the actual logs for each of the experiments and the difference in awareness in risky actions between groups of users was quantified. The user tests involved a number of groups. Each group was assigned a different feedback agent to use (including a non-affective agent to serve as a control group), and the results were then compared.

Users' actions were logged via the monitoring system during the experimental phase, and users were subsequently provided with a questionnaire to determine their level of security awareness. Based on the data, it was possible to determine if a monitoring agent with affective feedback can be used to enhance security awareness. The final aims of the research project are to a) assess if security risk awareness improves in end-users and b) if overall system security improves through the use of affective feedback. A full description of the methodology used is described in Chapter 5, Chapter 6, and Chapter 7. The results gained as a result of the methodology will be presented in Chapter 8, prior to them being discussed, analysed and broken down in Chapter 9. Finally, Chapter 10 will provide overall conclusions, as to the answer to research questions, along with some careful consideration of future work which could be conducted.

3.4. Summary

To investigate the research goal and provide an answer to the research question, the section below provides an overview of the methodology which will be followed.

- **Research aim:**
    - Develop and apply knowledge of monitoring techniques and affective feedback, establishing if this changes users' awareness of risky security behaviour in the context of a browser-based environment.
- **Research question:**
    - *"Is it possible to enhance security risk awareness in end-users via dynamically provided affective feedback?"*
- **Issues which highlight the need for research:**
    - there's a multitude of flaws which users may fall victim to whilst browsing the web
    - users are often unaware of the risky security behaviors they may exhibit
    - a range of tools, created over a number of years have been developed to keep users safe online- this highlights there still a problem with online security
    - more and more business is carried out online: there is a need to educate users regarding online safety
    - affective feedback has previously been used in educational environments

- **How will the issues be addressed?**

    - consider the current awareness of risky security behaviours in end-users and examine differing affective feedback techniques

    - develop a user monitoring system for use within a browser-based environment

    - develop prototype software containing affective feedback agents

    - construct an experimental design to address the research question

    - quantify the difference in awareness in end-users using statistical analysis and draw conclusions

- **Features of tool developed:**

    - ability to monitor end-user behaviour via the use of a browser extension

    - in relation to existing research (Bubaš, Orehova and & Konecki 2008) (Milne, Labrecque and Cromer 2009), the following behaviours will be monitored, owing to the fact these behaviours can occur within the context of a browser-based environment

        - if there are commonly used words in a password

        - if a password contains personal information

        - password length

        - if there are malicious links found on a page

        - if the current page visited is malicious

- if a site is served via HTTP
- if the current page is a top 20 social media site

- on detection of an occurrence of the aforementioned behaviours, an affective feedback mechanism will be triggered

- types of affective feedback which will be delivered to end-users on-screen (outlined in diagram 1)
  - colour
  - text
  - human avatars

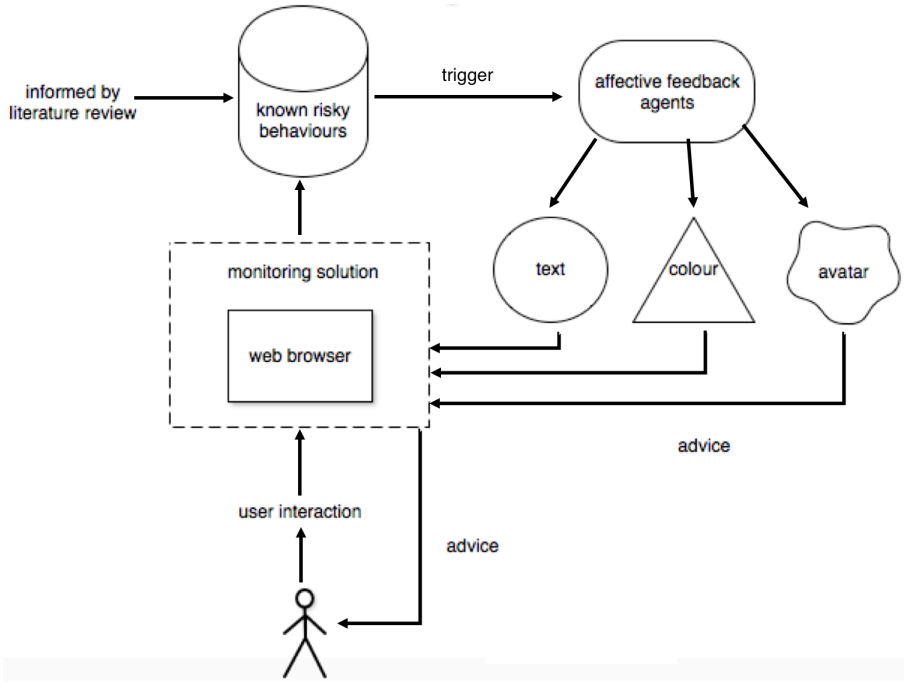


Diagram 1- overview of the tool developed

- **Outcomes of the research:**

    - an understanding of users' awareness of risky security behaviours

    - determine if affective feedback provided had an impact on the data recorded regarding the actions and behaviour of users

    - determine if affective feedback had an impact on the end-users and subsequent behaviour

    - provide an overall conclusion as to whether affective feedback enhances security risk awareness in end-users and improves security behaviour

Chapter 4. Mozilla Firefox and Prototype Browser Extensions

The research project sought to develop a software prototype which was composed of a monitoring solution, and eventually an affective feedback delivery system within the confine of a browser-based environment. If the user partakes in potentially risky security behaviour whilst browsing the web, e.g. revealing login credentials on an untrusted website, then an affective feedback mechanism is triggered, alerting the user regarding their behaviour. Owing to the open-source nature of Mozilla Firefox and the ease of creating extensions with hooks to the necessary low-level components, the browser was an ideal development platform to allow for the implementation of a user behaviour monitoring system and an affective feedback delivery system.

4.1. Mozilla Firefox- a brief history

The Mozilla Firefox browser was originally a branch project, created from the release of the Mozilla Application Suite browser code. Prototype versions of the browser were released under the name of Phoenix in 2002. After a period of development, the first official version of Firefox was released in 2004: Firefox 1.0 (Mozilla a) 2015). As of April 2016, the browser holds an approximate market share of 15.6% (ARS Technica UK 2016), coming in second place to Google's Chrome, and narrowly rising above Microsoft's Internet Explorer and Edge browsers. Table 4 contains an overview of different web browsers, and the add-on technologies they utilise.

Table 4 – Summary of browsers and add-on features

Browser	Cross Platform Support	Add-on Technology	Market Share (ARS Technica UK 2016)
Mozilla Firefox	Yes	XUL-based	15.6%
Google Chrome	Yes	WebExtensions (HTML, JavaScript, CSS).	60.5%
Microsoft Internet Explorer	No	.NET Framework	15.5%
Opera	Yes	WebExtensions (HTML, JavaScript, CSS).	8.4% (listed as “others”)
Safari	No	Safari Extensions (HTML, JavaScript, CSS).	8.4% (listed as “others”)

The browser offers cross-platform support, with the ability to run on a number of different operating systems e.g. Microsoft Windows 98 and onwards, Apple's OS X and a variety of Linux distributions. In addition to this, Firefox provides users with the opportunity to customise the browsing experience, allowing extensions to be readily installed. Mozilla describe extensions as add-ons which "*add new features to Firefox or modify existing functionality*" (Mozilla b) 2015). New features that extensions may add to the browser can include additional search tools, increased security (blocking adverts and scanning sites for malicious links), download management and, integration with social media websites. XUL-based extensions allow access to low-level components, and allow the developer increased flexibility in customising the extension.

4.1.1. Mozilla Extensions: how are these constructed?

There are a number of ways of developing a Firefox extension: utilising XUL (XML User Interface Language), or developing in Mozilla's Add-on SDK (software development kit), which was previously called Mozilla JetPack (Mozilla Developer Network 2015).

Extensions developed using the Add-on SDK are more limited in their functionality in comparison to XUL-based extensions, restricting how users can interact with the user interface (i.e. they must strictly follow usability guidelines for Firefox). The Add-on SDK environment makes development easier, providing the developer with access to JavaScript APIs, allowing them to make use of commonly used functions. Additionally, it provides access to UI components recommended by the usability guidelines, with the aim of ensuring that the extension developed integrates with the existing browser interface. Mozilla also claim that whilst it is still possible to develop an insecure extension under the SDK, it is harder to write a malicious extension which could do serious damage (Mozilla Developer Network 2015).

Most traditional extensions, now known as legacy extensions, are written using XUL. XUL-based extensions allow the developer to extensively customise the user interface, owing to the fact that this type of extension is not restricted to the APIs supported by the Add-on SDK. Additionally, the developer also has access to the XPCOM (cross platform component object model) (Mozilla Developer Network 2015). When developing Firefox extensions, there are a number of key files which are required and can be modified, allowing the extension to potentially monitor behaviour, provide the user with feedback, or modify the user interface. All XUL-based extensions follow a similar structure, where a number of necessary files must be included in order for the extension to run (outlined in Figure 1).

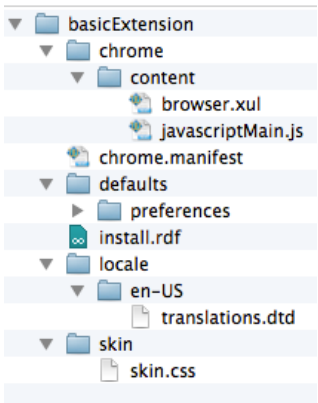


Figure 1 - overview of file structure

Before an extension can be installed to the browser, the various files and folders it consists of must be packaged into a Firefox browser extension archive file. This file takes the form of a .xpi file, which stands for a XPInstall (or cross-platform) install file.

The Browser.xul file within the content folder contains hooks which are required to link to other files. This file has the ability to link to multiple JavaScript files, such as the Bootstrap and jQuery libraries. The file also allows additional XUL constructs to be added, allowing the menus and toolbars within Firefox to be modified e.g. adding a new menu item which, when clicked, allows a user to run an extension. These factors make Mozilla Firefox extensions a suitable method of monitoring user behaviour and delivering affective feedback at appropriate moments.

In order to begin investigating how best to assemble a XUL-based extension, a basic template created by Robert Nyman (Nyman 2009) was investigated and reconstructed.

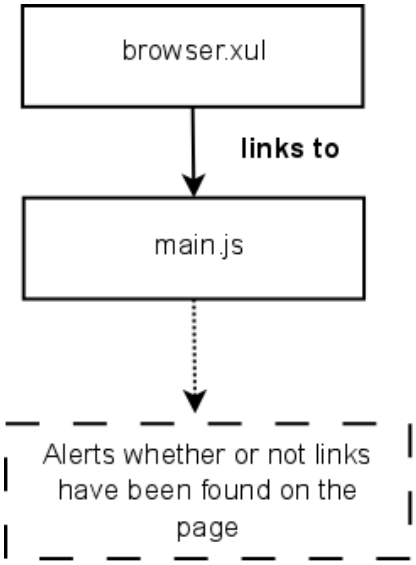


Figure 2 - architecture of the linkTargetFinder extension

This extension was named the linkTargetFinder and its main purpose was rather basic. When run, it simply searched the page for the target URL of any links which may be on the page. If links were found, the JavaScript file embedded within the extension produced an alert box noting that links had been found on the page. If there were no links to be found on the page, similarly, the JavaScript file embedded within the extension produced an alert box saying that no links had been found. Figure 2 provides an overview of the key files involved with checking the content of the webpage, and subsequently producing the alert both on-screen, highlighting whether there are/are not any links on a particular web page.

After successfully compiling this extension, this template was used as the basis for the rest of the prototype extensions, and both the final monitoring solution and delivery of the affective feedback mechanism.

4.2. Prototype extensions

A number of small prototype extensions were created during the research to test the functionality of the Firefox extension platform to ascertain if it was suitable for the scope of the project. The end goal of the project was to create a final prototype with the ability to a) monitor the actions of the user and b) provide affective feedback at appropriate intervals in a bid to encourage the end-user to think about their online security awareness and, considering the overall level of security of their system. It should be noted that whilst Firefox was used to create prototype extensions, the concept of the research project was to create a monitoring solution and an affective feedback mechanism; to this end, Firefox was merely the vehicle for delivering the overarching idea.

This section will discuss each of the small prototypes developed and will explain the rationale and the purpose behind each of the tests. Table 5 provides an overview of each of the prototype extensions, and their purpose.

Table 5- overview of prototype extensions

Extension Name	Purpose
multiplejs	Check multiple JavaScript files could be used in an extension.
hideAllTheThings	Check it was possible to manipulate the DOM by hiding elements.
injectGifs	Check it was possible to inject GIFs into a webpage, with a view to adding animated agents at a later date.
highlightTags	Manipulate the DOM to highlight specific tags on the page. Could be used t.o highlight malicious links in the final extension developed
secureLink	Checks if a page is HTTP/HTTPS. Could be used to warn users if they are submitting information over an unencrypted connection.
captureStoreLinks	Grabs all links on a page. Compared them against a blacklist and determines of they are malicious. Could be used to warn users about malicious links in the final extension developed,
mouseNearLink	Adds an extra border to all links on a page. When the cursor approaches a link, it is checked to determine if it's malicious. If the link is malicious, it is highlighted, warning the user.
autoRunExtension	Checks a Firefox extension can automatically run when a web page is loaded. Will be used to automatically run the final extension developed.
Logging Keystrokes	Logs keypresses, and writes them to a file. Shows a log file can be utilised, and the actions of the user can be recorded. Acts as a precursor to the aspect of the monitoring solution in the final extension developed.

4.2.1. Prototype- multiplejs

The multiplejs extension was created to test that an extension could link to and utilise multiple JavaScript files within a Firefox extension. Within the structure of the extension, the browser.xul file links to a number of different JavaScript files: both file1.js and file2.js contain a single function which produces an on-screen alert, the jQuery library, and main.js (Figure 3). The extension does not run automatically when a webpage is loaded however, when a button on the toolbar is pressed, browser.xul calls main.js and an alert box is produced. The main.js file then calls a function from file1.js, producing a second alert box. Finally, main.js calls a function from file2.js which again produces a final alert box.

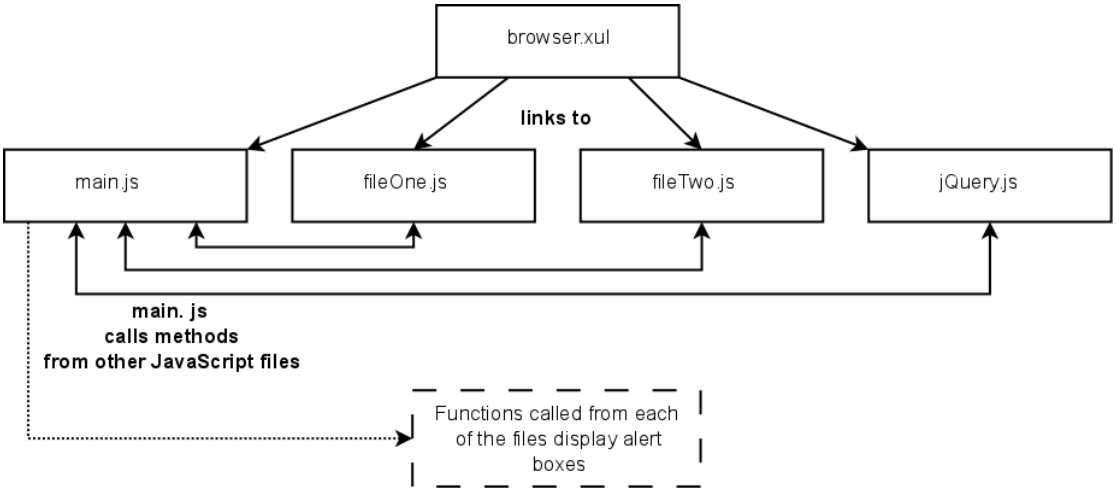


Figure 3 - overview of the extension testing multiple JavaScript files

This extension shows that it is possible to link to multiple JavaScript files from within a Firefox extension and utilise functions from each of these files. In addition to this, it also highlights that JavaScript libraries such as jQuery can be embedded within a Firefox extension, increasing the functionality of the software developed.

4.2.2. Prototype- hideAllTheThings

In order to deliver affective feedback to users via the browser based on their actions, it was identified there was a need to manipulate the DOM (document object model) of the webpage. To test whether or not this was possible from a Firefox extension, a small prototype extension was developed called hideAllTheThings.

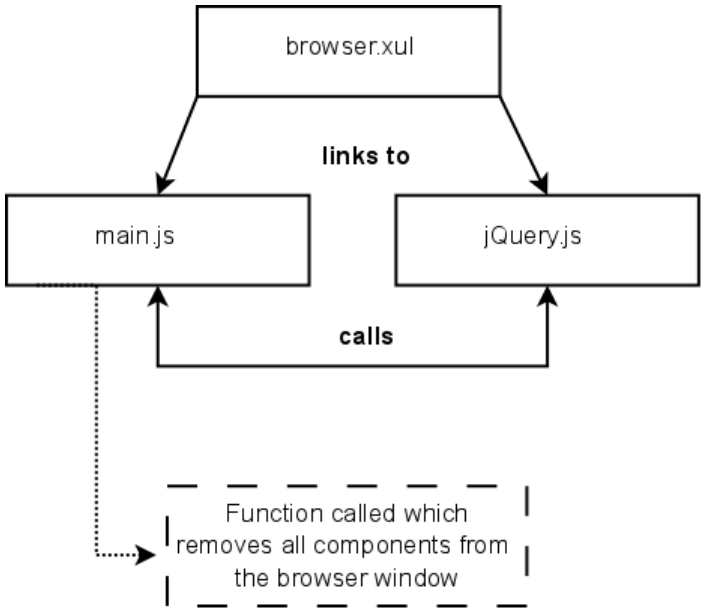


Figure 4 - overview of the extension which hides all Firefox components

The browser.xul files contains links to both the main.js file and the jQuery library. When the extension is manually run on a webpage, a function in the main.js file removes all elements from the screen (Figure 4).

hideAllTheThings was an important extension developed during the prototyping process as it demonstrated how an extension handles working with the jQuery library and how it manipulates part of the DOM. A small test was conducted whereby jQuery was added into the extension, denoted by $ff (standing for Firefox in Figure 5). The no conflict function ensured the jQuery library running within the extension does not interfere with a webpage which might be running a version of jQuery itself.

If jQuery was used to hide an element on a webpage, the line of code $ff("*").remove(); would be used. This would hide all elements included in the DOM of a web page. As this prototype runs jQuery within a browser extension, entering this line of code produces a different effect. Instead, every element within the Firefox window is hidden. This includes the actual browser window, along with every single component which creates the chrome (user interface of the browser). When run manually on a webpage, the user is left with nothing but a blank white screen, with no access to even the menu buttons to close the window.

```
//variable for new instance of jQuery- $ff
$ff = jQuery.noConflict();

//test-  HIDE ALL THE THINGS (within the webpage)!
$ff("*", window.content.document).remove();

//test-  HIDE ALL THE THINGS- even stuff which sits in the chrome of the browser
$ff("*").remove();
```

Figure 5 - code to remove elements on page

To enable affective feedback to be implemented at a later stage, JavaScript must skip outside the chrome of the browser and target the DOM directly. This was achieved by modifying the original line of code to read $ff("*", window.content.document).remove(); which targets the webpage loaded in the window. This removes every element from the web page, and leaves the chrome of the browser and menu systems intact, allowing affective feedback to be integrated later e.g. highlighting a link in red to denote that it is malicious. It is possible to remove any HTML element from the webpage, e.g. a paragraph tag, or an anchor tag. If the ID or the class of the element is known, then it can be targeted, and subsequently removed.

4.2.3. Prototype- injectGifs

This extension, when run, manipulates the DOM of a web page and appends a selected GIF to every paragraph element. Whilst this may seem like a meaningless extension to develop in the context of this PhD project, the original intent behind it was to discover if the DOM could be manipulated with a view to adding animated affective agents to a web page, depending on user behaviour.

The browser.xul files contains links to both the main.js file and the jQuery library. When the extension is manually run on a web page, a function in the main.js file pulls in a GIF from an external URL, finds all paragraphs on the web page, and then finally appends the GIF onto the page (Figure 6).

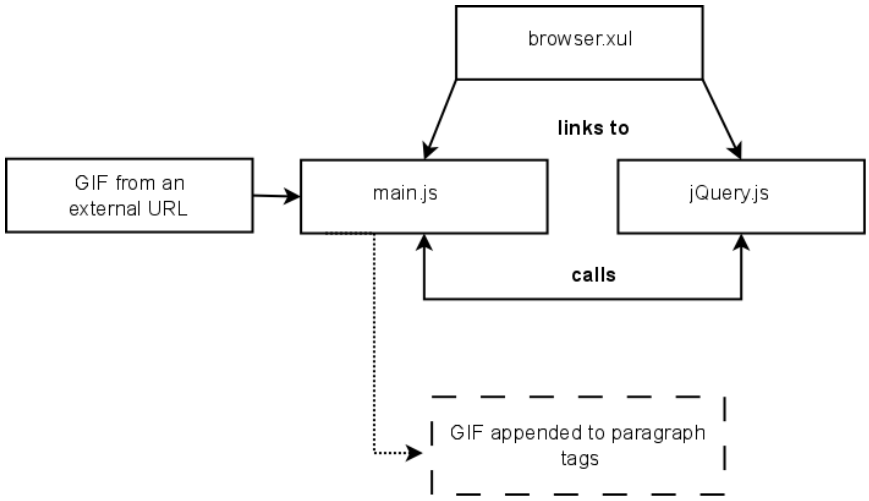


Figure 6 - overview of the injectGIFs extension

Figure 7 shows the injectGIFs extension running on a web page. In this instance, every paragraph tag on the Google home page has had a GIF of a cartoon banana attached to it. Although this may not seem like the most serious of examples, it provides a small proof of concept, showing that animated avatars can be appended to a web page when a Firefox extension is run.

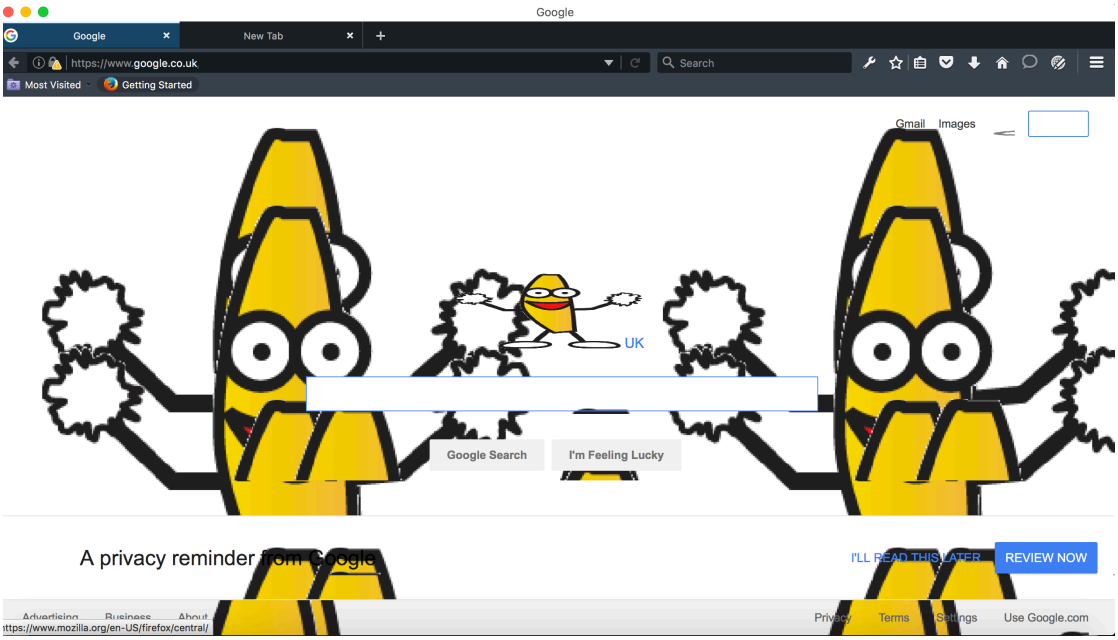


Figure 7 - screenshot of injected GIFs

4.2.4. Prototype- highlightTags

When run, this extension highlights tags on a website which may have the potential to be malicious, and cause problems for the end-user. A number of HTML tags are highlighted by the extension and these include the <a>, <form>, <input>, <textarea> tags. Highlighting a form clearly displays to the user that there is one on the page and that they should be wary of entering information into the page. If the code behind a particular website is insecure or is poorly developed, then any of these tags can be manipulated by those with malicious intent, for example, the anchor tags could be used as part of an XSS (cross-site scripting) attack.

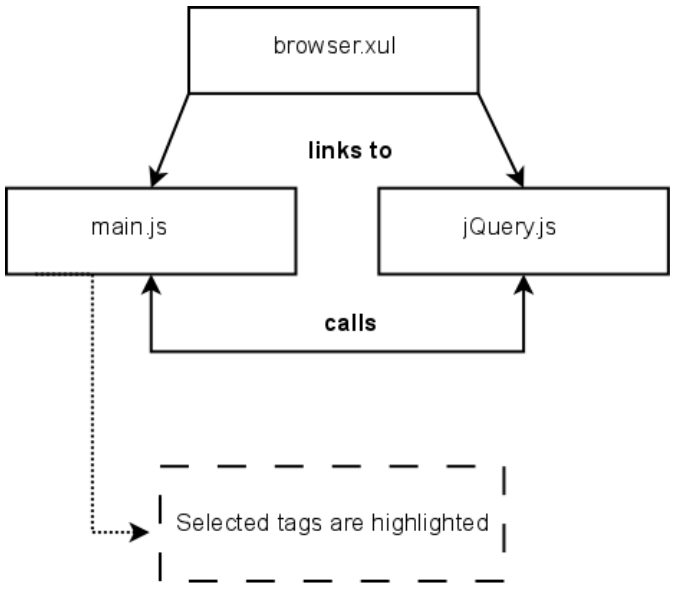


Figure 8 - overview of the highlightTags extension

The extension does not run automatically on every website the user visits, as it is a prototype extension, however, when its manually run by pressing a button on the main toolbar, Figure 9 provides an example of the way in which tags are highlighted on a page. It should be noted at this stage that the colours chosen to highlight each of the tags were chosen randomly and have no affective motive behind them.

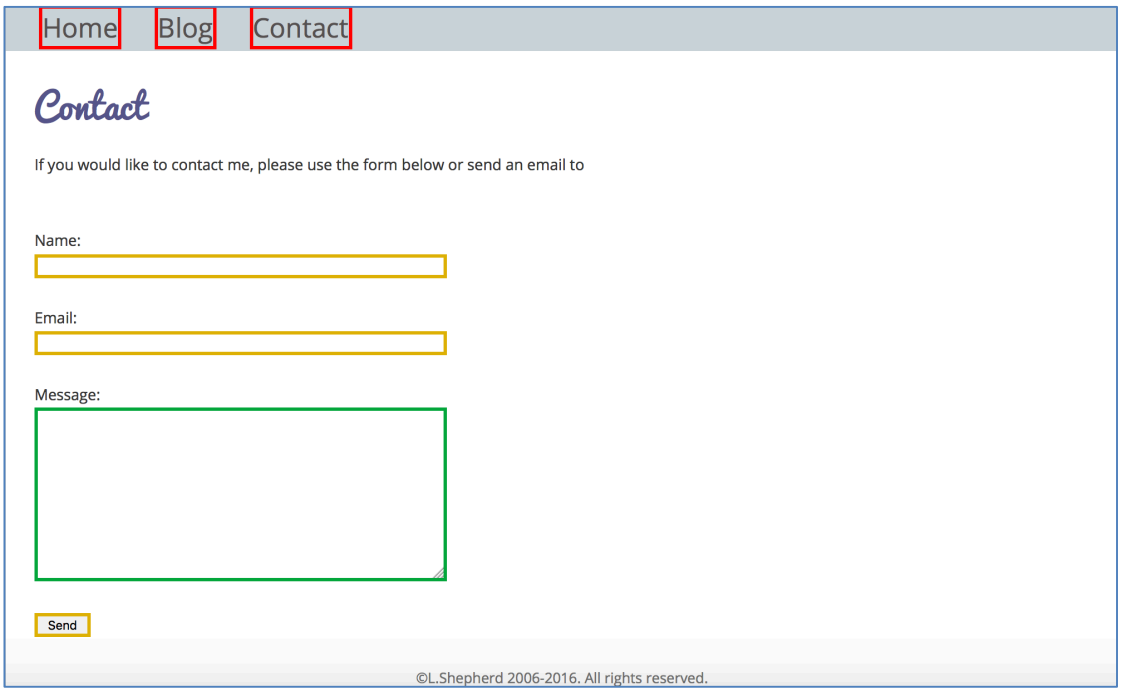


Figure 9 - select tags highlighted

4.2.5. Prototype- secureLink

The basic secureLink extension was designed 1) to check whether a website was encrypted or not by performing a simple check to determine if the URL protocol used was HTTP or HTTPS (whereby HTTPS denotes an encrypted page, unless there are some issues with the server) and 2) to check and see if the current URL is malicious.

The browser.xul file links to the main JavaScript file within the extension and when the extension is manually triggered on a website, it parses the DOM of the site and creates an array consisting of the URL of the current page, along with all the other links which are on that particular webpage. JavaScript loops through the array, and determines if each of the links have either the HTTP or a HTTPS protocol. Following this, an AJAX request sends the array of links to a web server, where a PHP file processes each of the links.

The PHP file stores all links in the url_capture.sql database, which could potentially be used to develop a personalised profile for a user in the future, depending upon links they have visited previously. Additionally, the PHP file checks all links on the page against a large text file of known malicious links. The malicious sites in the text file were gathered from the hpHosts database which is a "*community managed and maintained hosts file that allows an additional layer of protection against access to ad, tracking and malicious websites*" (hpHosts 2016). Utilising this information, this allows the links stored in the url_capture.sql database to be marked as safe/or unsafe.

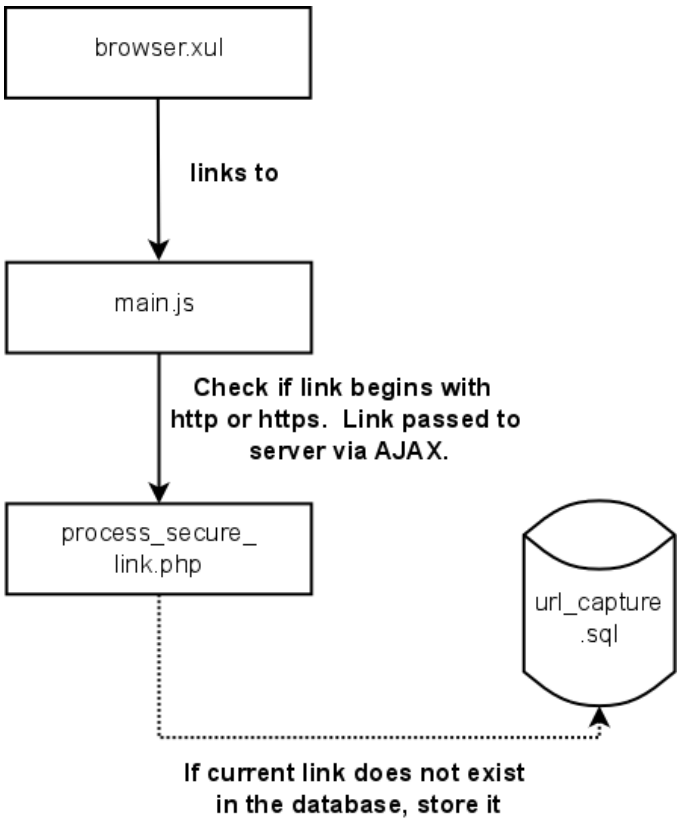


Figure 10 - overview of the secureLink extension

There is the potential for an unsafe link to be marked as safe in the database. Such an issue may occur if the hpHosts database is unaware of a new malicious link and has not yet updated. It should be noted that the hpHosts database is also used by the anti-malware tool, MalwareBytes, therefore the database itself has been deemed to be reasonably robust.

4.2.6. Prototype- captureStoreLinks

The captureStoreLinks prototype extension provides similar functionality to the aforementioned secureLink extension. Again, when the extension is run manually via a button on the toolbar, the main JavaScript file is triggered, as it parses the DOM of the site and creates an array consisting of the URL of the current page, along with all the other links which are on that particular webpage. When run, the extension grabs the URLs of all the links on the page. These links are passed to a PHP processing script on a server which inserts them into the url_capture.sql database and, checks if the links are potentially malicious (against hpHosts file). Again, the purpose of the prototype extension was to create a small proof of concept showing it was possible to determine if links were malicious via a Firefox extension.

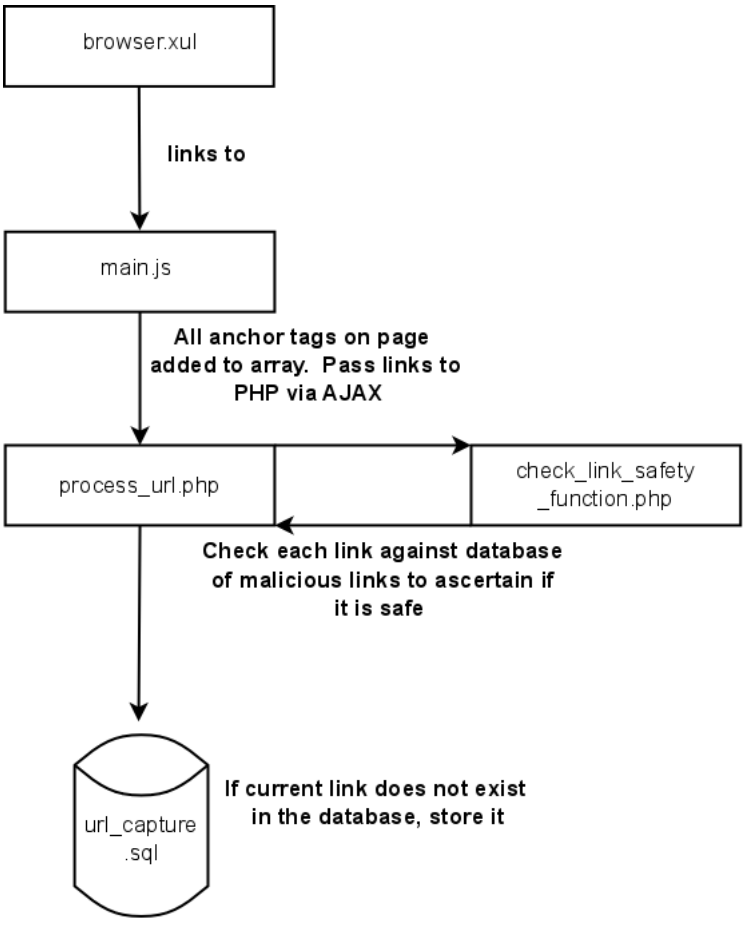


Figure 11 - overview of captureStoreLinks extension

4.2.7. Prototype- mouseNearLink

When run via a button on the toolbar, the mouseNearLink extension retrieves the URL of the link the user's cursor is closest to. On detecting a URL, the extension passes it to the server; if the link is found to be malicious in some way, the DOM of the current website the user is visiting is manipulated, highlighting the dangerous link in red.

To delve into the technical details (Figure 12), when run, browser.xul within the extension is linked to both a main JavaScript file and the jQuery library. When the user loads a web page, a JavaScript function parses the DOM of the browser and adds a unique event listener to every anchor tag on the page, and pads the margin of each link slightly. When the cursor encroaches the space around the link, the event listener is triggered, prompting the JavaScript to pass the link via AJAX to the process_url.php page residing on a server.

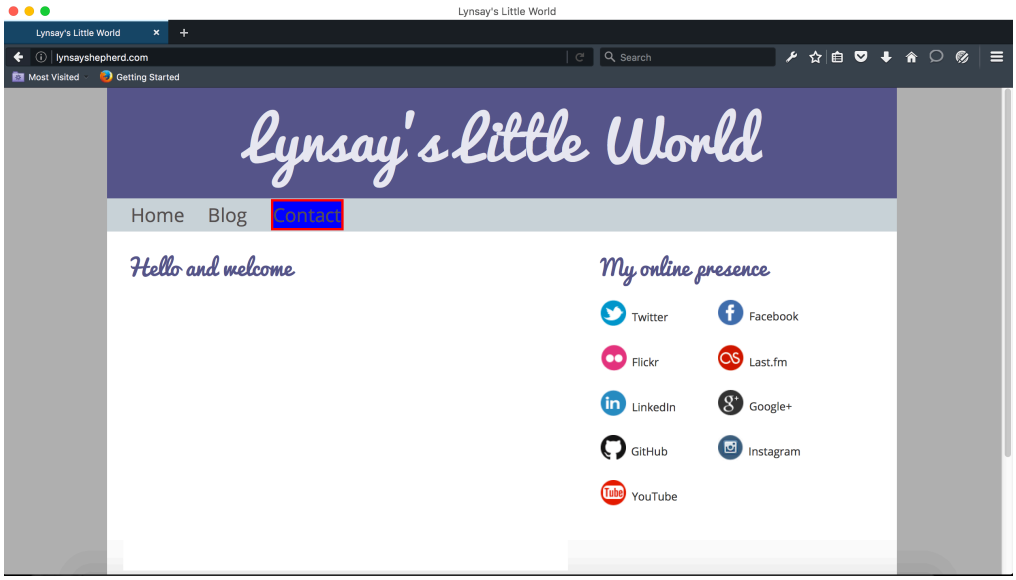


Figure 12- overview of mouseNearLink extension

On reaching the server, the link is stored in the url_capture.sql database. The link is also passed to another PHP function, in the check_link_safety_function.php file, where it is run against the dodgy_links.txt file (this file is a blacklist of malicious links and has been sourced from the hpHosts database). If the link is found to be malicious, a notification is passed back to the main JavaScript file which then utilises jQuery's CSS() function, manipulating the DOM of the browser, clearly highlighting the malicious link on the web page (Figure 13).

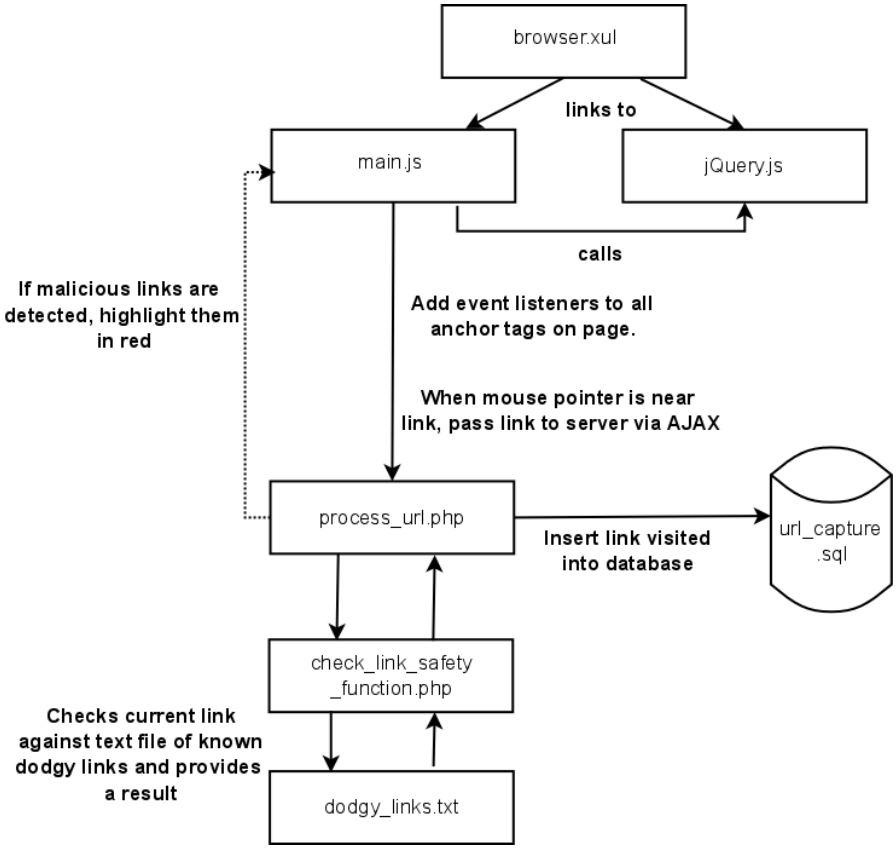


Figure 13 - effects of the extension

The mouseNearLink prototype extension proves that it's possible to detect malicious links on a page a user is visiting, highlighting them in a bid to warn users that they should not click on them. The basis of this concept was used to deliver some affective feedback in the final version of the tool developed to ascertain if such feedback had an impact on the users. This also presents a full example of how a Firefox extension may be developed to monitor user behaviour and provide basic feedback.

4.2.8. Prototype- autoRunExtension

Until this point during the development of the small prototype extensions, each of them had to be run manually by the user i.e. the extensions did not run automatically on page load. Instead, users had to either click on a toolbar button, or select a menu item from within the chrome of the browser every time they visited or reloaded a new web page. This is cumbersome and would defeat the purpose of a monitoring solution if the user had to enable it every time.

A solution was found in the form of a code snippet on the Mozilla website (Mozilla c) 2015) which suggested the extension could be triggered to run automatically on page load. In order to do this, the extension adds an event listener to the page, and waits for the DOM content to load before proceeding with the function of the extension.

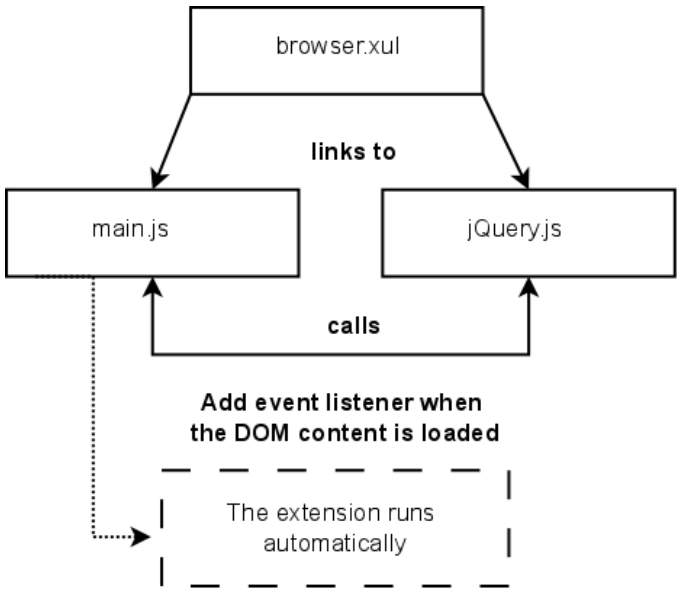


Figure 14 - overview of the autoRun extension

In the case of the autoRunExtension prototype, browser.xul within the extension is linked to a main JavaScript file and a copy of the jQuery library. When the user visits a new page and the DOM content has finished loading, a function from the main.js file is called automatically and in this case, the function produces an alert box on-screen every time a user visits a new page.

Without the aid of the event listener which tells the extension to wait for the DOM, it would have been impossible to develop a tool to deliver automatic affective feedback. Instead, the project would have had to rely on the end user clicking a button on the toolbar every time they visited a new page. Ultimately, this would have become irritating, and the users would have failed to trigger the feedback. Though this is a simple extension, this was a huge development in terms of the research project.

4.2.9. Prototype- Logging Keystrokes

A keystroke logging prototype extension was developed in an attempt to provide a very basic monitoring solution to ascertain what a user is typing on a web page, with a view to determining whether or not they are revealing information in a password/login field and to illustrate that a log file can be utilized on the server. This extension was developed with the concept of delivering affective feedback to the end-user in mind.

If a form field is requesting sensitive information such as a password, an affective agent will be triggered to warn users about the potential dangers of risky security behaviour. In this extension, jQuery is included as one of the JavaScript files which the browser.xul overlay file imports. The keypress() function within the jQuery library has been used and each time the event is triggered, it generates a host of information, including the key pressed, the character code of the key pressed, the time stamp of when a user pressed the key and the type and ID of the HTML element in which the keypress was triggered e.g. (Figure 15 shows the keypress event).

```
$aa(window.content.document.body).keypress(function( event ) {
    if ( event.which == 13 ) {
        event.preventDefault();
    }
    showKeyDetails(event);
});
```

Figure 15 - code snippet showing that the keypress function is called when the user types anywhere within the body of a webpage

In the case of the keypress extension, keystrokes are written to a log file on a server, along with a timestamp (Figure 16). The extension passes keypress information to a PHP file via AJAX. The PHP script separates the contents of the keypress array, and attaches a timestamp, before appending it to a log file, illustrating how simple it is to develop a simple keystroke logger within a Firefox extension. In the prototype extension, this process is repeated for each individual key pressed.

```
                //post the arrays to appropriate PHP page
                requester.open("POST",
"http://localhost/phd_work/process_ff_extension_data/process_logBehaviour/process_key_info.php", true);
                requester.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
                requester.send(keyDetailsArray);
```

Figure 16 - the AJAX call to the PHP file which handles the keypress array

```
[05-04-2015 18:04:17] - User entered the site
[05-04-2015 18:04:17] - https://www.google.co.uk/search?q=google
[05-04-2015 18:04:22] User typed:
[05-04-2015 18:04:26] User typed: g
[05-04-2015 18:04:28] User typed: o
[05-04-2015 18:04:29] User typed: o
[05-04-2015 18:04:31] User typed: g
[05-04-2015 18:04:32] User typed: l
[05-04-2015 18:04:34] User typed: e
[05-04-2015 18:04:48] - User exited the webpage
```

Figure 17 - sample data from the log file

Again, this was a very important prototype extension in terms of the development of the project as a whole. By demonstrating that users' actions could be written to a specifically chosen file on a server, it proved that this could be an important part of a monitoring solution. Furthermore, the extension also displays that it's possible to investigate and determine what the user is typing in particular fields. This extension has the potential to be used as a malicious keystroke logger, since it has the ability to store the contents of a password textbox in plaintext on a server. However, with modification, the basis of the extension could be extended, checking the password a user has entered against a list of commonly used passwords, without storing the actual password. Therefore, this could be used as part of a larger extension which with monitors user behaviour and delivers affective feedback for example if a user has a short, a weak, or a common password.

4.3. Summary of Mozilla Firefox and prototype extensions

The testing of these small prototype extensions confirmed the model of Mozilla Firefox extensions were suitable for the scope of the PhD project. During the development phase of the prototype extensions, knowledge was gained by the creation of small proof of concepts. Several of these concepts were then deemed suitable to utilise in the main body of the final version of the developed prototype extension, such as the auto run functionality, which any developed monitoring solution will need to do.

Browser extensions which provide feedback regarding certain risky security behaviours already exist. These include TORPEDO (Volkamer, Renaud and Reinheimer 2016), PhiGARo (Cregan et al. 2012), GPEX (Bicakci et al. 2009), and PassSec (Volkamer et al. 2015). However, the browser extension developed as part of this research project makes use of feedback which is considered to be affective, which makes it different.

Affective feedback mechanisms which will be utilised in the final prototype extension include colour-based feedback (e.g. green indicating good behaviour), text-based feedback using specific terms and avatars using subtle cues within the browser window. Chapter 6 will discuss why these types of feedback have been chosen for inclusion in the prototype, and will detail the specific colours, text, and avatars chosen.

Experiments using these agents will investigate a) if security risk awareness improves in end-users and b) if overall system security improves through the use of affective feedback (Shepherd, Archibald and Ferguson 2014).

Chapter 5. Monitoring Solution

The work developed as part of the research project proposes the use of a browser extension to automatically detect risky security behaviour. Previous research has indicated affective feedback may serve as a suitable method to educate users regarding risky security behaviours (Hall et al. 2005) (McDarby et al. 2004) (Robison et al. 2009). Within the scope of the browser environment, it is proposed that on detection of risky security behaviour, the browser will be used as a delivery mechanism for affective feedback, warning users about the risk of taking action.

This section will discuss the technological aspects of the system in detail, providing a full explanation of how the monitoring solution was implemented.

5.1. System overview

The research project proposed the creation of a software prototype in the form of a browser, including the ability to monitor user behaviour and provide suitable affective feedback. The prototype extension developed will utilise several feedback agents. Should the monitoring system detect a users' engagement in known potentially risky security behaviour whilst browsing the internet e.g. entering a commonly used password into a website, an affective feedback mechanism will trigger, warning users regarding the dangers of their actions (Figure 18).

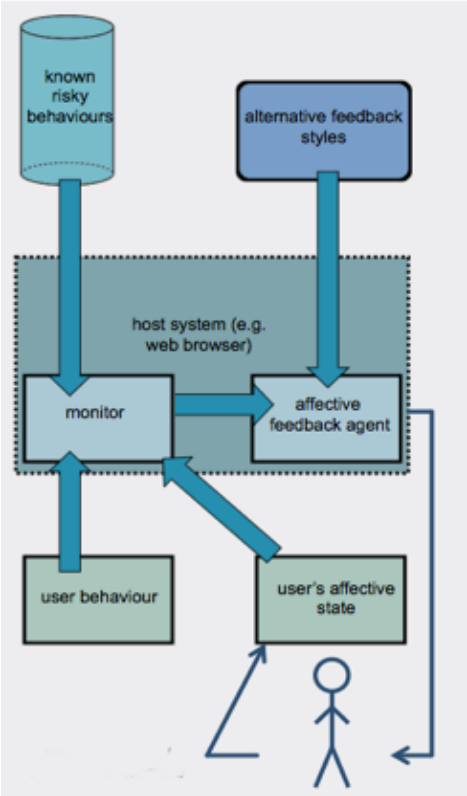


Figure 18 - overview of system architecture

The aforementioned feedback mechanisms have been explored in previous pieces of research (Shepherd, Archibald and Ferguson 2014). Feedback will include the use of text-based feedback using specifically chosen words with a positive/negative weighting and, avatars, with subtle facial cues, expressing to users that they have engaged in safe/unsafe behaviour.

Additionally, colour-based feedback will be used, with green indicating a positive action. Red will be used to highlight a dangerous action, owing to its use as a warning colour in Western society, and its history as a warning colour in evolutionary psychology Kralik, J.D. et al. (2011). At this stage, colours used in the research will not take colour-blind users into account.

Risky behaviours which the monitoring solution seeks to detect include using common passwords or a password containing personal details, or visiting a malicious site. Full details of the behaviours the monitoring solution detects can be found in section 5.2.2.

Experiments conducted using these affective feedback agents investigate if security risk awareness improves in end-users (see Figure 18). The success of the software will be gauged via a series of end-user experiments followed by a questionnaire utilising a Likert scale. Logs created by the monitoring solution will be compared against answers given in the questionnaires. This allows a comparison between how users thought they performed vs. how they actually performed, giving an overall representation of the impact of the software.

5.2. Monitoring Solution

5.2.1. Overview of the monitoring system

In order to detect potentially risky security behaviours and trigger affective feedback at opportune moments, a monitoring system had to be created within the confines of a browser-based environment. Owing to the functionality and necessary low level hooks which the Mozilla extension framework possesses, outlined in section 4.1.1. of this document, a Firefox extension was deemed to be a suitable environment, and would ultimately allow the impact of affective feedback on end-user security awareness to be measured.

Despite the suitability of the environment, creating the software presented challenges when integrating such a tool into the confines of a browser-based environment.

5.2.2. Actions the monitoring solution oversees

The literature review identified papers (Bubaš, Orehova and & Konecki 2008) (Milne, Labrecque and Cromer 2009) which define specific risky security behaviours. A smaller subset of these behaviours were chosen for implementation, owing to their suitability for monitoring in the content of a web browser. Checks for the following behaviours were built into a monitoring solution and each of the behaviours chosen has been backed-up with a rationale. The technical details will be explained in section 5.2.5.

5.2.2.1. Commonly used words in a password

One of the risky behaviours listed in a paper by Milne Labrecque and Cromer (2009) asks users if they have "*Used a password that is a word that can be found in a dictionary*". By simply checking the encrypted contents of a password field on a web page, a test to check if a user has engaged in this behaviour has been built into the monitoring solution.

5.2.2.2. Password contains personal information

Again from the paper by Milne, Labrecque and Cromer (2009), users were asked if they have ever *"Used a password or login that contains personal information"*. Again, functionality to check if this is the case has been built into the prototype monitoring solution.

5.2.2.3. Password length

The OWASP (Open Web Application Security Project) (OWASP 2016) guidelines state that the minimum recommended length for a password is 8 characters. A simple length check has been built into the monitoring solution.

5.2.2.4. Malicious links found on page

Milne, Labrecque and Cromer (2009), asked users if they had ever "*Clicked on links in an email without knowing the sender*". Although the prototype extension Firefox extension can handle malicious links within a webmail-based page, the concept has been extended to check all links found on the web page a user is visiting, and to check them against the hpHosts database of known malicious links (hpHosts 2016).

5.2.2.5. Current page is a malicious link

Again, similar to the aforementioned paragraph, the concept of malicious links in emails noted in Milne, Labrecque and Cromer (2009), has been extended to checking the current page the user is visiting against the database of known malicious links.

5.2.2.6. Site is served via HTTP

A check to verify if a page is served via HTTP has been implemented into the extension. This has been added because most modern web browsers have some warning notification between HTTP and HTTPS on the address bar however it can be difficult for users to find an explanation of what that actually means. The HTTP check will be there to warn users they should not reveal private/important information because a HTTP connection is unencrypted.

5.2.2.7. Current page is a top 20 social media site

Many users reveal too much information about themselves online which can be used to build up a profile about them via OSINT (open source intelligence), with the potential to target users via specifically crafted malicious links in email addresses. Milne, Labrecque and Cromer (2009), also ask in their paper if users have "*Used social networking sites*", linking to the fact people reveal a lot of information about themselves online (Kaspersky Lab 2013). The extension has built-in functionality which will check to see if users have visited a top 20 social media website (as of the first-quarter of 2016).

5.2.3. Utilities used

To effectively monitor end-users and provide the necessary trigger warnings, some external utilities were required to the delivery this information. Each utility required is discussed in this section.

5.2.3.1. Top passwords

To perform a check to ascertain if a user's password contained a commonly used dictionary word, it was necessary to obtain a list of commonly used passwords. Such a list was obtained from Daniel Miessler's GitHub repository (Miessler 2014). This list is maintained by Daniel Miessler and Jason Haddix (both information security specialists) as part of the SecLists project and both of the aforementioned authors are part of the OWASP (Open Web Application Security Project) community.

The list used from the repository was the 10k_most_common.txt file, which provided a suitable number of commonly used passwords to check user passwords against. To make querying the list more efficient in terms of the research project (owing to the fact PHP was used), the list was converted into a MySQL database residing on a server. The database was named top_passwords.sql.

5.2.3.2. Personal information

One of the password criteria for checking passwords in this extension was to see if the password contained personal information. There was some consideration given to using OSINT to build up a profile on each of the participants during the experimental phase however, this proved to be difficult, as participants may not have had a Twitter, Facebook account etc. Instead, a form was created asking users to provide information about themselves on a voluntary basis (for more information about the experimental process, see (Chapter 7).

Any information the users provided was stored in a MySQL database table named initial_form. The database stores multiple pieces of information- users' first name, middle name, surname, mother's maiden name, names of pets, phone number, any hobbies they may have. Of course, if the user chooses, all of these fields can remain blank. Having such a database allows the monitoring solution to check if any part of a password entered during the experiments contains any of this personal information they have revealed.

5.2.3.3. Known malicious links

Another of the features built into the extension is the ability to check if a) the current website the user is on is malicious and b) if any of the subsequent links on the page are malicious. To enable this feature, a database of known malicious links was required. The database which was used as part of this research project was the hpHosts (2016) database, maintained by the anti-malware company MalwareBytes.

The database is constantly updated with the latest sites which are deemed to be malicious in some way. The site classifies the ways in which links it stores are potentially malicious (hpHosts 2016). The types of links included are-

- Ad or tracking servers
- Sites which distribute Malware
- Sites which distribute or develop exploits
- Sites which provide fraudulent services
- Spamming servers
- Servers which spam the hpHosts forums
- Browser, DNS, operating system hijacking sites

- Sites which use misleading marketing tactics
- Illegal pharmacy sites
- Phishing sites
- Sites distributing copyrighted material illegally

The browser extension developed during this research project does not filter by individual classifications and instead takes the database as a whole. During the development process the decision was made to utilise a static version of the database for prototyping purposes. The hosts.txt from the hpHosts website was downloaded in January 2016. Again, to make the list of hosts integrate into the project, the list of malicious links was copied into a MySQL database residing on the server. All 350,898 links were stored in a database named malicious_urls.

5.2.3.4. Top 20 social media websites

To determine if a user had interacted with social networking sites, a method was required to identify these sites during the monitoring process. To facilitate this, a list of top social networking sites was gathered, with a view that this subset of social networking sites would be the ones users were most likely to visit during the experimental process; it would be impossible to gather a list of every social networking site available on the internet at this current time.

A list of the top 20 social media sites as of March 2016 was gathered from the Alexa website (Alexa 2016). Alexa is a company owned by Amazon and the list is created from traffic estimated based on a sample of millions of internet users. Businesses can use the website to benchmark and optimize the browsing experience for users, and as such, the Alexa website is deemed to be a useful tool in determining the number of site visitors.

The current top 20 list includes social networking sites such as Facebook and Twitter. To integrate the list into a format usable with the monitoring solution, the list was converted into a MySQL database on a server named social_media_urls.

5.2.4. The logging process

The development of a monitoring solution required a method of logging what the users had been doing. Previous research conducted (Fenstermacher and Ginsburg 2002) noted the use of an XML log file generated by the users' actions within a particular application. Drawing inspiration from this approach, a logging system was developed for the Firefox monitoring solution whereby a unique log is generated on a server for each user and their actions are recorded there.

Difficulties were encountered whilst developing a log for each user. In an early version of the extension, a path was coded to an activity.log file stored on the server, with the activity.log file created manually, and having content appended to it via information passed from the JavaScript of the extension to the PHP files on the server via AJAX. This however posed problems when multiple users need to engage with the extension: all behavioural information was redirected to the activity.log file and it became impossible to differentiate one user from the other. Entry and exit timestamps also became mixed and a better solution was needed; one log per user.

Mozilla suggested the use of Local Storage for logging, as the Firefox browser is equipped with a directory service and the nsIFile interface allowing the creation of a log file (Mozilla d) 2015). Utilising this method would have had disadvantages. It is recommended that log files are stored in the local profile of Firefox. During the experiments, this would make the retrieval of data rather difficult, with each machine the users had used being physically checked. Log files would then be saved to a USB stick manually, and stored in one central location. It would also have been impossible for PHP and AJAX to write to the log file owing to security concerns. Due to these reasons, a better solution was needed.

With the advent of HTML 5, web applications now have the ability to store data locally within a browser. Previously, some information could be stored via cookies, and had to be included with every single request to a server however, local storage allows data of up to 5MB to be saved. In terms of security, it does not *have* to be sent to the server. The concept of local storage was utilised in the research project as a method of generating a new log for each end user. Due to the nature of the system, the design was more complex.

The monitoring solution must automatically run every time the user loads a new page. Initially, there was an attempt to invoke local storage within the main JavaScript file running the Firefox extension, as opposed to in the code of a specific website. Normally, a developer would use local storage on a website they had created, for example to store a name or some other details. Since the Firefox extension can target any website, and the developers of this research project cannot modify the code of just any website, this method did not work as local storage is tied to a specific page e.g. www.abertay.ac.uk. Additionally, the Gecko web browser engine which powers Firefox (and branches of the browser such as SeaMonkey) does not support saving information from locally-based extensions.

A workaround was required to allow the JavaScript within the extension to label all websites as http://example.com. Essentially, all sites loaded during the experimental process were treated as http://example.com within the JavaScript code, and all sites referred to this for local storage. One method of achieving this was discussed by the Fartersoft website in great detail (Farter 2011), and the implementation used in the research project is outlined in the paragraphs below.

```
var url = "http://example.com";
var ios = Components.classes["@mozilla.org/network/io-service;1"]
          .getService(Components.interfaces.nsIIOService);
var ssm = Components.classes["@mozilla.org/scriptsecuritymanager;1"]
          .getService(Components.interfaces.nsIScriptSecurityManager);
var dsm = Components.classes["@mozilla.org/dom/storagemanager;1"]
          .getService(Components.interfaces.nsIDOMStorageManager);

var uri = ios.newURI(url, "", null);
var principal = ssm.getCodebasePrincipal(uri);
var storage = dsm.getLocalStorageForPrincipal(principal, "");

//attempt to generate a unique(ish) ID for the log file name
var uIDOne=(new Date().getTime()+'').substr(3,7);
var uIDTwo = (new Date().getTime()).toString(36);
var logName=uIDOne+uIDTwo+".log";

storage.setItem("logName", logName);
```

Figure 19 - the workaround code to allow Firefox extensions to access local storage

In the code snippet displayed in Figure 19, a URL is defined which will act as the URL for the extension. In this case, every page visited by the user will be called http://example.com in the view of the browser and local storage. It is important not to choose a URL which the user may end up visiting- if for example the URL google.com was chosen, this could potentially cause conflicts with local storage as it is a real website. In addition to this, if a second extension is running within the browser concurrently and it used the same workaround, it would also need to have a unique, non-real-world, dummy URL. Issues could be caused owing to the same origin rule. It would be beneficial to generate a random string based upon the current UNIX timestamp to create a non-real-life URL.

Various interfaces are then imported for use within the extension-

- nsIIOService- provides access to URL parsing utility functions

- nsIScriptSecurityManager- enforces security within the extension, including same-origin

- nsIDOMStorageManager- manages storage, including local storage

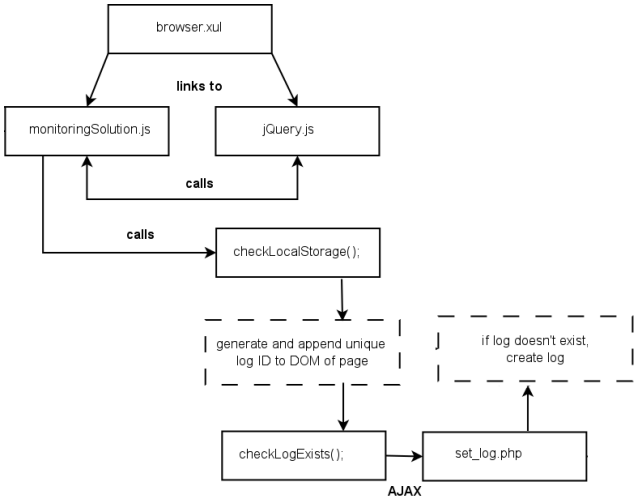
The code then assigns the URL variable, in this case is example.com as the site to be used for localstorage within the extension. Following this, a unique ID is generated for use in the experimental process of testing the extension, creating a value which ends in .log. The logname variable then stores the generated unique log id within localstorage.

Utilising the jQuery library within the extension, the DOM of the web page is also manipulated. A small grey box is appended to the top-right-hand corner of the screen, along with the log ID, as illustrated in Figure 20. This has been placed here as part of the experimental design and aids users in finding out their unique log number.

Figure 20 - screenshot of the appended log ID

Furthermore, the logging process then creates a log file with the same unique ID for the user on a server. Once local storage has been checked, another function is triggered to verify if a log file of the same name appears on the server which the extension is linked to. The checklog function utilises an AJAX request and passes the name of the log in localstorage to a set_log.php file residing on a server, which contains processing scripts for the monitoring solution. The PHP file_exists function is called: if a file with the same log name resides on the server, the script does nothing, else, a new log file is created with the same name as logNme in localstorage, and it also has the necessary write permissions for the user and the extension. When this has been completed, the extension can begin writing user behavioural information to the log file. An overview of this is given in Figure 21.

Figure 21 - generating a unique ID for localStorage and creating a log on the server



Each time a user loads a page, and before they engage in any further behavioural activity, there is some basic information which is recorded. This includes a timestamp of when the user entered the given website, the actual URL of the website visited, a notification if the site is served via HTTP and the user agent behind the browser (in this example, Mozilla, Gecko engine and the version of Firefox which was used). It should be noted that the user agent can be faked although in this scenario, the user agent is just recorded, and nothing is done with the information gathered. The other piece of basic information which is recorded is the timestamp of when a user leaves the page, so if necessary the time the user spent on a page can be calculated. This might be applicable in future work which is why the functionality was built-in. One of these records is generated for each website the user visits.

```
[24-04-2016 15:42:48] - User entered the site
[24-04-2016 15:42:48] - http://driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/
[24-04-2016 15:42:48] - HTTP: this site is served via http
[24-04-2016 15:42:48] - Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
[24-04-2016 15:45:20] - User exited the webpage
```

Figure 22 - the basic information which is recorded when a user visits a website

When the extension automatically detects any of the risky behaviours outlined in section 5.2.2. , further log entries are triggered. During the experimental phase, these will help reflect what the user has actually done in the web browser, vs. what they say they have actually done in the questionnaire. The subsequent information recorded is outlined in Table 6. The triggers which have been outlined in Table 6 have been drawn from existing literature reviewed during the research project. Papers by Bubaš, Orehova and & Konecki (2008) and Milne, Labrecque and Cromer (2009) specifically identified risky security behaviours which could be implemented into an extension, and detected in the context of a browser-based environment.

Table 6 - risky security behaviour triggers and the subsequent information recorded in the log

Trigger	Sample information recorded in log
Password contains a commonly used password	[22-04-2016 15:29:13] - Common password entered
Password contains personal information	[24-04-2016 15:48:12] - Personal details in password entered
Password is too short	[24-04-2016 15:48:12] - Password is short
Malicious links found on page	[22-04-2016 15:38:48] - Potentially malicious link detected on page: driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages /end_experiment/end1.php
Site is served via HTTP	[22-04-2016 15:25:13] - HTTP: this site is served via http
Current site is a top 20 social media site	[22-04-2016 15:38:52] - User visited a top 20 social media site.
Current site is malicious	[22-04-2016 15:38:49] - User visited potentially malicious link: driesh.abertay.ac.uk/~l514921/final_phd_work/ user_pages/end_experiment/end1.php

5.2.5. Identifying behaviour in the context of the browser- technical details

This section will explain the technical details behind the detection of risky security behaviour within the web browser. Each section contains a diagram, discussing how detection of that particular threat has been constructed. A diagram showing the inner workings of the monitoring solution as a whole can be found in Appendix (i) .

5.2.5.1. User enters page trigger

When a user enters a page, the monitoringSolution.js file firstly triggers a check to ensure local storage has been set-up correctly, and that a log file exists on the server (see section 5.2.4. for full details of the logging process).

When a unique log file has been generated, the pageDetails function is called, which gets the details of the current page the user is visiting. This appends the timestamp, the current URL, whether the site was served via HTTP, and the user agent, and passes it to a PHP logger_script on a server via AJAX. This also triggers the HTTP warning. The PHP script appends the information to the correct log file and awaits further behavioural information to be logged via triggers. The process is outlined in Figure 23.

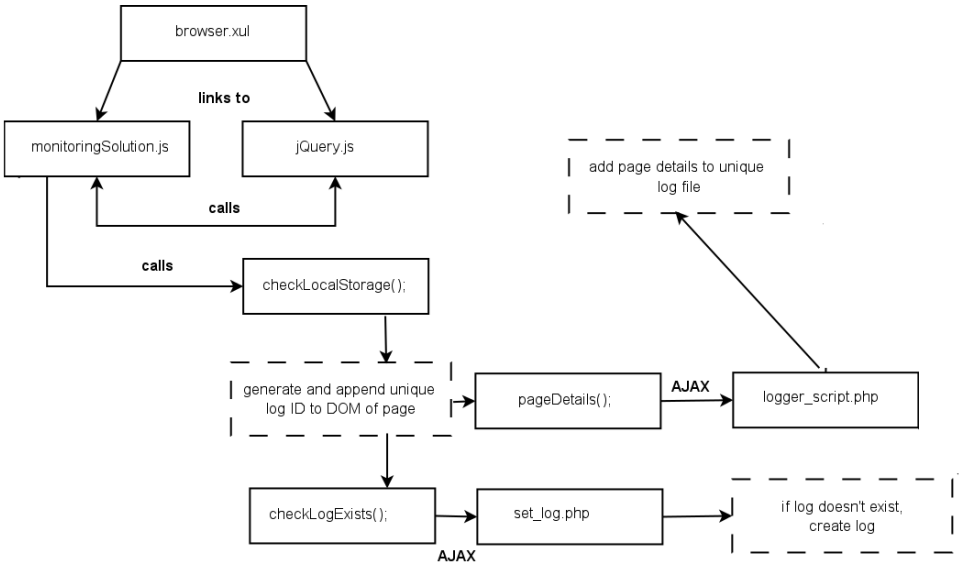


Figure 23 - process triggered when user enters a page

5.2.5.2. User exits page trigger

Similar to when a user enters a page, the exit timestamp is also recorded. The monitoringSolution.js file triggers the pageExit function when the window event handler onbeforeunload is called. pageExit grabs the current timestamp, and passes it to the PHP logger_script via an AJAX request. The PHP script appends the information to the correct log file. The process is outlined in Figure 24.

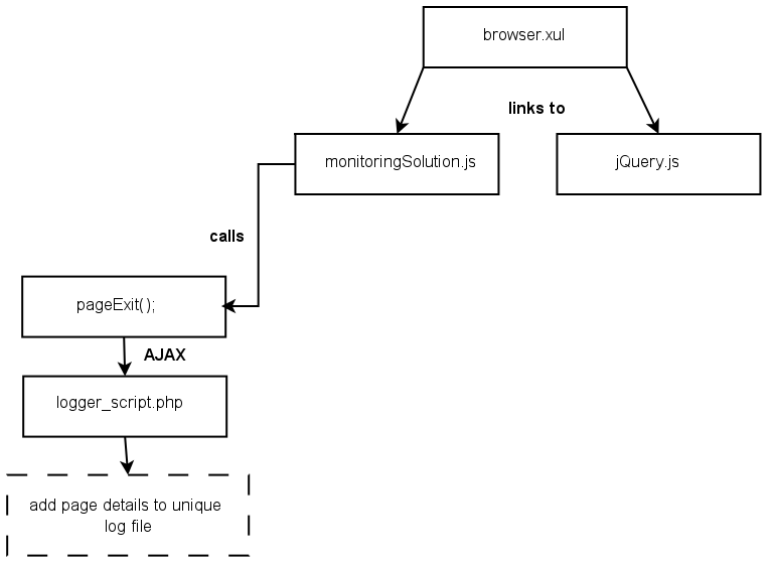


Figure 24 - process triggered when user exits page

5.2.5.3. Password triggers

There are a number of ways in which a password can trigger text to be written into the log file for the user, as shown in Figure 25. The monitoringSolution.js firstly has to ascertain if there is a password field on the page a user is viewing by utilising the jQuery library and the input:password selector. When the id of the password field has been gained, the passwordCount function is triggered, which will aid in alerting if a user password is too short. In turn, the updateCount function is called to keep an accurate count of the password length, making use of the keyup functionality in jQuery. When a password is less than 8 characters in length it will trigger a message stating the password is too short.

Additionally, each time the user types another character into the password field the password is encrypted and checked to see if it is a commonly used password as the checkCommonPassword function is also called. The passwordChecker.php script checks the current password against the database of top 10000 used passwords (Daniel Miessler, 2014). If the encrypted password is found in here, another alert is triggered and information is written to the log file.

Finally, the password is compared against a database of personal information the users may have revealed during the experimental process. If the user's password matches any of the information in the database, a further alert is triggered and information reflecting this is written to the log.

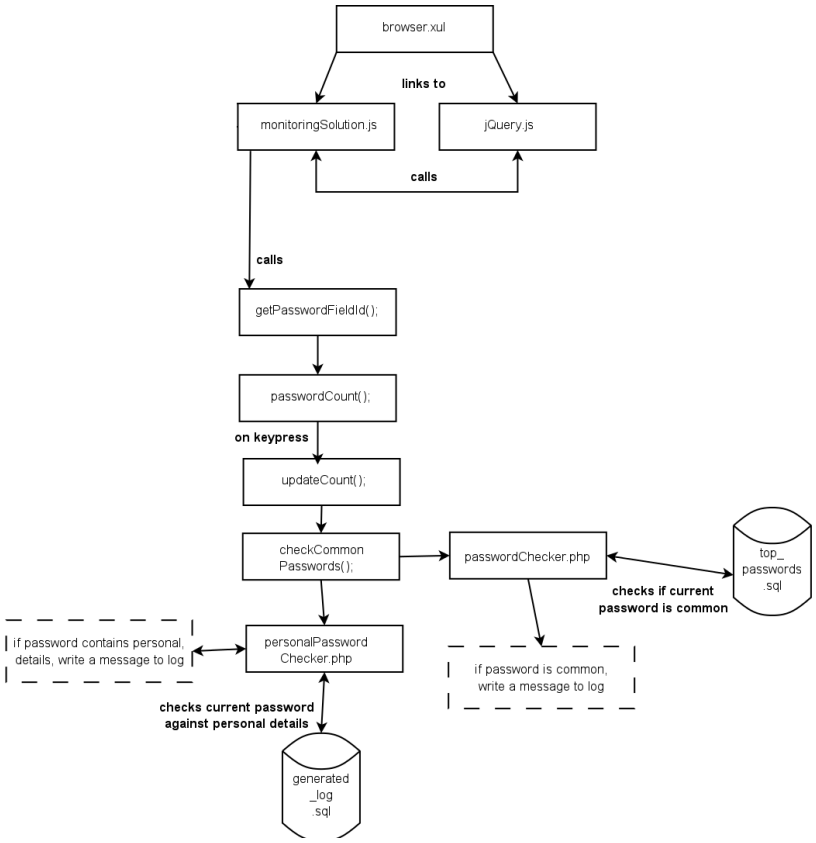


Figure 25 - password processes which trigger information to be written to the log file

5.2.5.4. Malicious site triggers

The first way in which the extension can check for malicious links is when a user loads a page in the browser. When a user has loaded a new page, and the pageDetails function has passed information to the PHP logger script via AJAX, the logger script then calls a function in another PHP file on the server: the checkMalCurrent.php file. This file takes the current URL of the page the user is on, and checks it against a database of known malicious links (hpHosts, 2016). If the current website the user is on is malicious, a trigger writes information to the log stating that this is the case, as outlined in Figure 26.

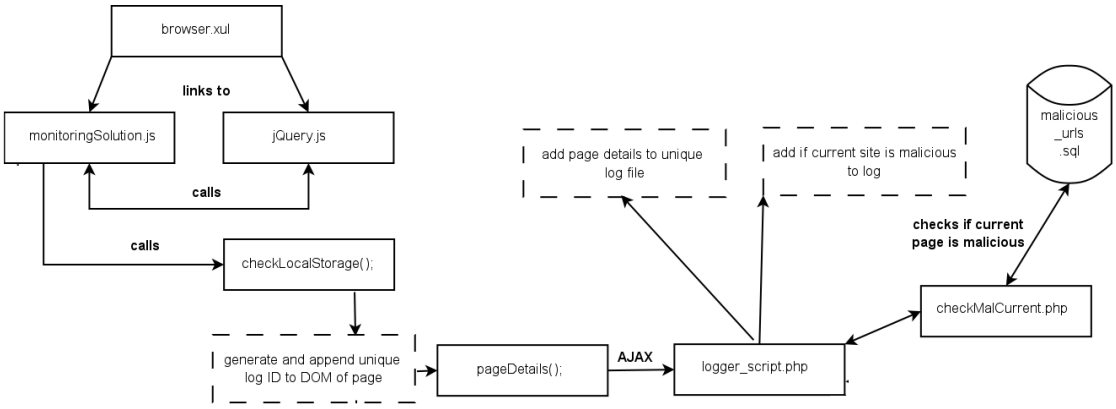


Figure 26 - malicious site trigger

5.2.5.5. Malicious links trigger

A second way of checking for malicious content on a page involves checking for malicious links which a page may contain. When a new page is loaded, the monitoringSolution.js file calls the maliciousLinkChecker function grabs all hyperlinks on a page and combines them into one JavaScript array. This array is then passed to a PHP file called maliciousLinkChecker.php via an AJAX request. The PHP file takes each of these links and checks them against a database of known malicious links (hpHosts 2016). Each time a malicious link is detected on the page, a note is made of it in the users log file. The process is outlined in Figure 27.

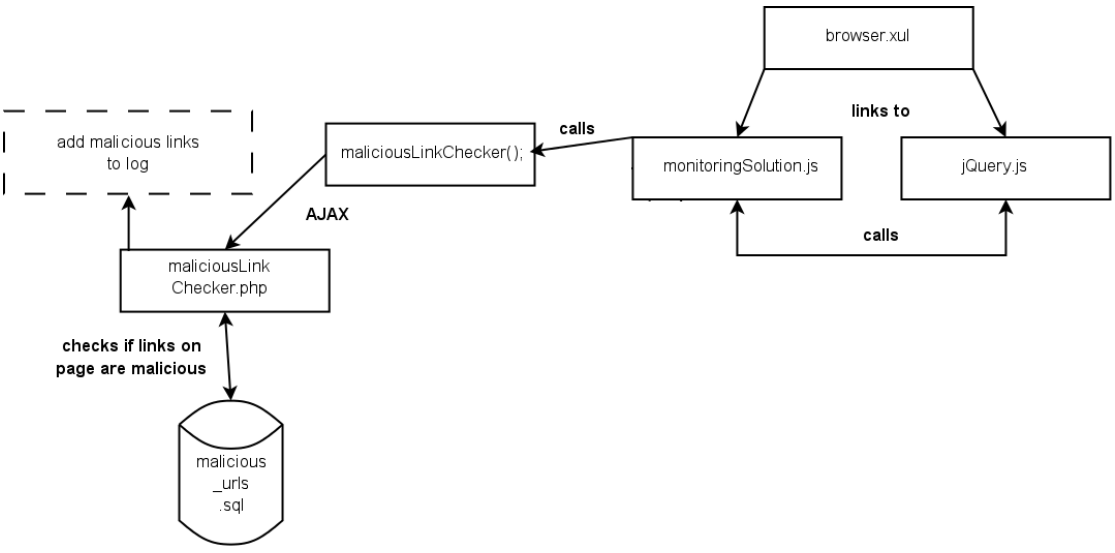


Figure 27 - malicious link trigger

5.2.5.6. Social media trigger

The extension can also detect if the current page a user is on is a top 20 social media website. When the user loads a page in the browser and the monitoringSolution.js file has established local storage has been set-up correctly and that a unique log has been generated, pageDetails function is called. pageDetails passes general page information to the PHP logger script via AJAX,and the logger script then calls a function in another PHP file on the server: the socialMediaCheck.php PHP file. This takes the current URL of the webpage and runs it against a database of the top 20 social media websites (as of the first-quarter of 2016) (Alexa 2016). If the current site is found to be in this database, this information is written to the log file. The process is outlined in Figure 28.

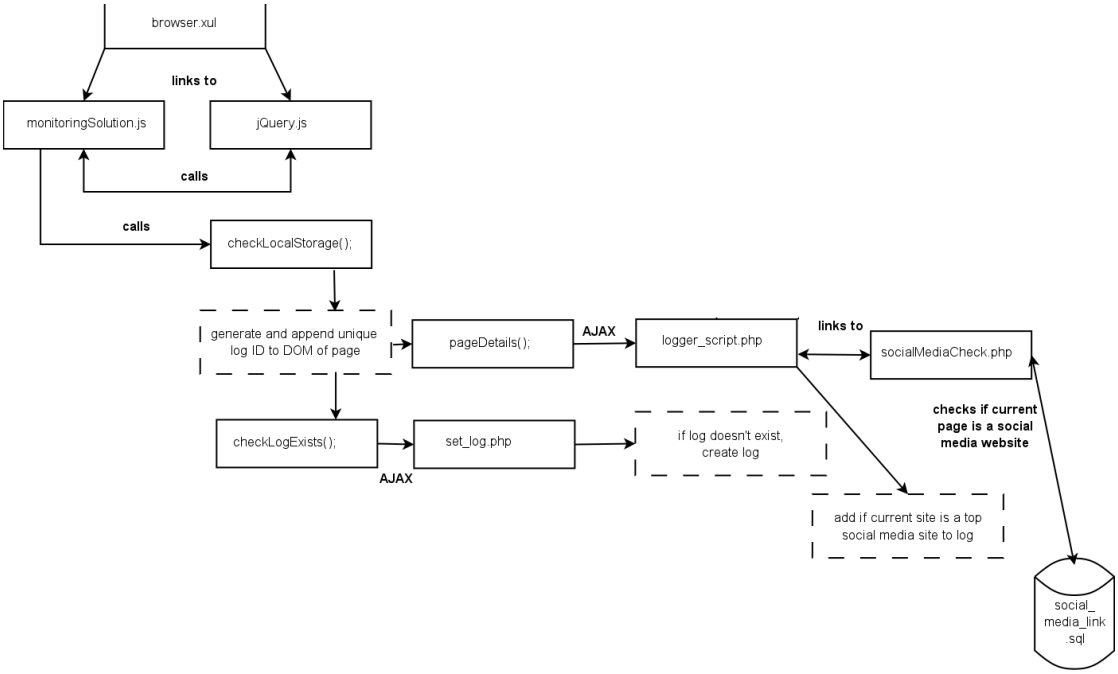


Figure 28 - social media trigger

5.3. Summary of the monitoring solution

To validate the plausibility of monitoring user behaviour, and subsequently detecting risky security behaviour within the realms of a browser-based environment, a platform for creating an appropriate browser-based extension was required. In this instance, a Mozilla Firefox browser was deemed an appropriate testing harness for verifying known risky security behaviours which could be identified in the context of a browser.

The monitoring solution testing-harness within the browser is successfully able to detect a number of previously identified risky security behaviours, including if a user has visited a malicious link, if they have a commonly used password, if they have personal information in their password, or if they have visited social media websites where they have the potential to reveal information about themselves.

In addition to this, the monitoring solution has the ability to generate a unique log file for each user, providing a timestamp of each website visited and including information such as whether or not the site visited was malicious, or if any link on the web page was deemed to be malicious.

The crux of the research project is to test whether or not affective feedback has an impact on the security behaviour of the end-user. To this end, the monitoring solution is ultimately a vehicle for the delivery of a system which provides dynamic affective feedback on detection of risky security behaviour. Chapter 6 will explain how an affective feedback mechanism was integrated with the existing browser-based monitoring solution, discussing the types of affective feedback delivered.

Chapter 6. Delivering Affective Feedback

6.1. Overview of the affective feedback system

During the research project, the initially developed monitoring solution was built upon, delivering dynamic affective feedback on detection of known risky security behaviours. This section seeks to provide an overview of this system, discussing the types of affective feedback which are delivered. It will go on to discuss the utilities and resources used in delivering affective feedback, before explaining how the feedback was delivered in the context of a browser-based environment.

6.2. Types of affective feedback utilised

Rosalind Picard is one of the pioneers in the field of affective computing. In her ground-breaking text Affective Computing, she defines affective feedback as "*computing that relates to, arises from, or deliberately influences emotions*" (Picard 2000). A further definition by McDarby et al. (2004) notes that affective feedback is also *"the process of using technology to help people achieve and maintain specific internal states".*

Previous research has indicated there are a number of types of affective feedback which could be utilised within the web browser window, to help guide users into making more appropriate decisions, based-on the situation they encounter. Depending on the actions of the user, they may be offered positive reinforcement because of their behaviour, negative reinforcement, or a mixture of both positive and negative. Specifically, the 3 different methods which were chosen were colours, avatars and text. The feedback provided is visual. Excluding the use of screen readers for those who are visually impaired, users will generally use the PC/laptop monitor. Consideration was also given to the use of auditory feedback, such as a warning sounds to alert users to their actions. Since the PC/laptop sounds does not have to be switched on for the user to browse the internet, this was ruled out as a possible feedback method. The following section will discuss each type of feedback in more detail.

6.2.1. Colour choice

As discussed in the literature review, there are multiple methods of providing affective feedback to the end-user. One such method involves the use of certain colours in a bid to influence users. In Western culture, the colour red has long been associated with danger. Research carried out by Kralik, J.D. et al. (Association for Psychological Science 2011) has even proposed that the link between red and dangerous situations may be rooted in evolutionary psychology.

Adams and Osgood (1973) performed a cross-cultural study, focussing on the affective meanings of colours. The work attempted to gauge feelings about the use of specific colours, by performing a comparison of results from 89 previous studies. Results were mixed for some colours, highlighting multiple meanings. They found that green is seen as a good colour (blue and white also fall into this category), yellow is weak (as is grey and white), and red is seen as active and strong.

A more recent research paper by Kumi et al. (2013) examines how colour and affect can influence learning outcomes. The study acknowledged that affective reactions to colour must be taken into account when designing/delivering visual presentations, noting that the use of colours can have an impact on behaviour/attitude. In this study, 79 participants were asked to observe a lecture with a yellow, or a blue background, prior to completing a questionnaire on their attitude and affective reaction. In this instance, it was found that blue helped participants remember information that was delivered during the presentation.

In terms of security, a number of studies have been conducted, into the use of colour-based feedback. A paper by Ur (2012) explored the effectiveness of coloured bar-meters to indicate password strength. Results showed colour had an impact on the users where green/blue indicated a strong password and red indicated a weak password. Colour-based feedback, in combination with sound, was also one method of affective feedback successfully implemented in a game called “Brainchild” developed by McDarby et al. (2004) which attempts to help users relax.

6.2.2. Avatar

Several papers in the literature review also indicate human avatar-based feedback may be an appropriate form of affective feedback when attempting to educate users. Again the Brainchild tool by McDarby et al. (2004) indicated affective feedback can help users alter their internal states. Avatars have been used to good effect in intelligent tutoring systems (Robison et al. 2009), with Hall et al. (2005) agreeing that the use of avatars may prove effective in influencing the emotional state of the end-user, thus forming part of this research.

6.2.3. Text

Past research in the literature review has also indicated text-based feedback as an appropriate form of affective feedback for disseminating information to the end-user. Again in Ur et al. (2012) paper when investigating password strength meters, text-based feedback was also applied to describe user passwords e.g. "weak". Again, the results highlighted this had an impact on the end-users as they did not like their passwords being described as “weak”. Other research, like the work conducted by Dehn and Van Mulken (2012) concluded that textual information provided more direct feedback to end-users.

6.3. Utilities used

6.3.1. Colour Lovers

On integrating colour into the Firefox extensions, the standard CSS values for red, yellow and green (as outlined in Table 7, column 2), proved to be high contrast and distracting. The Colour Lovers website (Colour Lovers 2016) was used to find slightly toned down version of these colours and ultimately the hex values found in column 3 of the table were used.

Table 7 - colours used in extension

Colour	Basic RGB hue	Softer Hue (used in feedback)
Red	#FF0000	#CF4250
Yellow	#FFFF00	#EBA560
Green	#00FF00	#78BF60

6.3.2. Avatar research

The avatars chosen for use in this research project come from a paper by Sacharin et al. (2012). The paper was produced by members of the Swiss Center for Affective Sciences which explored the perception of how people reacted to changing emotional expressions. In the paper a number of avatars were generated by FACSGen 2.0 at the Swiss Center for Affective Science: derived from Ekman's theory of basic emotions (Ekman 1999). These emotions were happiness, surprise, sadness, anger, disgust and fear. Since the paper was also studying transitionary emotions, it included avatars which were 50% anger-happiness, (61%/39%) happiness-disgust, 50% happiness-fear.

Ultimately, the paper revealed that participants were uncertain about each of the emotions that were included in the mixed-expression avatars, and that this was more prevalent in expression sequences in comparison to simple static images. Due to this conclusion, static images of avatars were chosen from this paper to be delivered as a form of affective feedback on detection of risky security behaviour.

6.3.2.1. Avatars used in the extension

To allow for delivery of avatar-based affective feedback within the browser-based environment, 2 avatars displaying subtle facial cues were selected from the paper by Sacharin et al. (2012). The paper makes reference to the previously identified 6 basic emotions: happiness, anger, sadness, fear, disgust, and surprise, and also includes a neutral avatar, devoid of any such emotion. The avatars selected for inclusion in this research project are happiness (Figure 29) and sadness (Figure 30), to denote positive and negative feedback accordingly. The avatar representing sadness (as opposed to anger or disgust) was chosen as sadness is generally seen to be the opposite of happiness.

Figure 29 - image of happiness from Sacharin et al. (The perception of changing emotion expressions, 2012) used to denote positive affect

Figure 30 - image of sadness from Sacharin et al. (The perception of changing emotion expressions, 2012) used to denote negative affect

6.3.3. AFINN sentiment analysis

To provide the appropriate level of text-based feedback to end-users, a suitable source of affective text was needed. During the development phase of the project, two main wordlists were viewed with the aim of utilising them to produce affective text.

The first of these wordlists is known as ANEW (Affective Norms for English Words) which was developed by Margaret M. Bradley, and Peter J. Lang in 1999 at the University of Florida. The words in this list have been weighted by a number of participants, and compiled into a paper with a list of weightings (Bradley and Lang 1999). Despite being a widely used source of affective text, the terms of use stated that the wordlist is to be used only in "*basic and health research projects*" (ANEW 2015). Therefore, it was decided to use a different wordlist which may be more applicable to a cyber security/browser-based project.

Instead, a wordlist initially developed in 2011 was chosen, called AFINN, which is a play on the ANEW project, although it is not affiliated with it in any way. The AFINN database was developed by Finn Å rup Nielsen at DTU Informatics, Technical University of Denmark (Nielsen 2011). A 2011 paper describes the construction of the wordlist, scoring of the words, and the overall impact. Specifically, it was the AFINN-111.txt wordlist which was used in during the experimental design process. This is the newest version of the wordlist, succeeding the AFINN-96.txt. The AFINN-111.txt wordlist has 2477 words in it, providing more of a selection.

The wordlist was specifically developed for microblogs e.g. services such as Twitter where users post short messages. This concept fits in nicely with this research project as the affective feedback solution aims to regularly updates end-users with short messages depending upon their actions.

The wordlist was compiled from a number of sources, including Urban Dictionary in a bid to incorporate some internet slang terms. Again, internet terms have the potential to be useful in delivering affective text in the context of a browser-based environment. In addition to Urban Dictionary (Urban Dictionary 2016), the wordlist all made use of the Original Balanced Affective Word List (Siegle 1994), Twitter feeds and, the Compass DeRose Guide to Emotion Words (DeRose 2005) to provide a mix of words.

The author of the AFINN wordlist notes that words on the list were scored via the SentiStrength system, ranging from −5 (very negative) to +5 (very positive). Each of the words were rated on valence only i.e. on their intrinsic attractiveness (positive weighting) or their aversiveness (negative weighting). In evaluating the wordlist against ANEW, the author thought that whilst AFINN performed better across the entire lexicon (potentially due to the fact internet slang/obscene words were included) however it was deemed that ANEW scoring was better overall (Nielsen 2011). Since the publication of the paper by the wordlist author, AFINN has been used in a number of other papers, to good effect.

Since publication of the wordlist, several papers have investigated its use, and implemented it in studies. One such study by (Ozdemir and Bergler 2015), compared the wordlist against a variety of lexica available to researchers. Despite AFINN being one of the smallest wordlists available to researchers, it was the best solo performer when analysing tweets and figurative language.

The wordlist was also used as part of an attempt to analyse sentiment in Shakespeare's plays (Nalisnick and Baird 2013). The wordlist was used to try and define the sentiment of characters towards others and although the paper noted that "*AFINN is designed for modern English*", it proved it was still plausible to determine affect.

In addition to this, the AFINN wordlist was also used in an approach to classify Ekman’s emotional categories in user text (Gievska, Koroveshovski and Chavdarova 2014). Multiple wordlists were utilised, with AFINN being one of them, as part of a hybrid approach to make the results as accurate as possible.

6.3.3.1. Text used in the extensions

During the development of the affective feedback software, a number of placeholder phrases were used until the final version of the affective text was constructed. These phrases were used to show a piece of trigger text could be displayed on-screen. Only the developer could view the placeholder phrase. Each placeholder phrase was linked to one of the aforementioned triggers, outlined in 5.2.2. When a specific behaviour was triggered, the appropriate version of these phrases appeared.

The placeholder phrases were initially used in the extension and are shown in Table 8. These are non-affective phrases.

Table 8 - triggers and placeholder text

Risky security behaviour trigger	Placeholder text
Password commonality	Password is common
	Password is uncommon
Password with personal details	Password contains personal details
	Password does not contain personal details
Password length	Password is too short
	Password is equal to or longer than the minimum length
Malicious links	No malicious links on the page
	Malicious links found on page
HTTP site	Site served via HTTP
Social media site	Site is top 20 social media site
Malicious website	Current site is malicious

6.3.3.2. Splitting the wordlist

The AFINN wordlist comes as one large text file, and the words within the file are ordered in an alphabetical fashion, meaning that it can be difficult to pick out positive and negative words whilst scrolling through the file because they are all mixed in together. A suitable script was needed in order to first of all split these words into 2 separate text files: one for positively weighted words, and one for negatively weighted words. A small python script was created to achieve this goal.

The python script developed initially reads in the AFINN wordlist. Following this, it assesses the score given to each of the words, and converts this score to an integer value. If the integer value of the score is less than 0, the word must have a negative weight, and so it is appended to a file named afinn_neg.txt which stores a complete list of negative words derived from the initial word list. In all other cases, the score given to a word must be a positive value, thus these lines are appended to a file named afinn_pos.txt, which stores a list of positively weighted words derived from the original text file. Finally, both afinn_pos.txt and afinn_neg.txt files were compared to ensure the number of words included added up to the number of words found in the original AFINN-111.txt wordlist.

6.3.3.3. Identifying words to construct phrases

After splitting the lists into both positively and negatively weighted words, the words on the lists then had to be used in the construction of appropriate affective sentences. Not all of the words included in the separate text files were suitable for inclusion in affective text, therefore basic criterion had to be developed in order to choose appropriate words.

Owing to these factors, the following criteria were decided upon:

- Words chosen had to make sense in terms of the warnings the affective text
- Words chosen had to be syntactically correct when disseminating information to users
- No offensive words (e.g. swear words)

The researcher conducting the project, read the negative word list line-by-line, and words outlined in Table 9 were chosen for potential inclusion in the affective feedback tests. The words were chosen as there was an assumption that these words would make syntactic sense in the context of a browser-based feedback system. In the table, each of the words are sorted by negativity, from least negative to most negative (with -1 being least negative). Variations of the same word have been grouped together for conciseness.

Table 9 - list of negative words

Negative word(s)	Weighting
attack, attacked, attacking, attacks	-1
avoid	-1
expose, exposed, exposes, exposing	-1
hacked	-1
hide	-1
accident, accidental, accidentally	-2
complacent	-2
discouraged	-2
dodgy	-2
danger	-2
exploit, exploited, exploiting	-2
harm, harmed, harmful, harming, harms	-2
stolen	-2
threat	-2
insecure	-2
vulnerability	-2
warn	-2
weak, weakness	-2
bad	-3
criminal	-3
illegal	-3
warning, warnings	-3
fraud, fraudster	-4

Similarly, the positive words chosen have been outlined in Table 10. Again, variations of the same word have been grouped together, and words are ranked from least positive to most positive.

Table 10 - list of positive words

Positive word(s)	Weighting
increase, increased	1
safe, safely	1
trust	1
adequate	1
validated	1
careful	2
positive	2
recommend, recommended	2
secure	2
strong	2
trusted	2
excellent	3
good	3
brilliant	4

6.3.3.4. Construction of final affective phrases

The final pieces of affective text which were integrated into the extension had to be designed in such a way that when weighted words were placed into the phrases, the phrases themselves still made sense. In addition to this, positive and negative versions of phrases were required for password commonality, password with personal details, password length, if malicious links were present on a page, or if a user was visiting a malicious website.

In the case of unencrypted sites (HTTP) and social media sites, users were provided only with negative feedback. The theory behind this is that these two warnings are more of a grey area. A user can visit a social media site and be perfectly safe, provided you are mindful regarding the information you are sharing with others. Similarly, a user can visit an unencrypted website and behave in a completely safe way. This is the rationale for providing warnings for these categories only.

When writing an affective phrase for one of the triggers, care was taken to provide balanced phrases. To give an example, the positive malicious links message telling users they are safe has a positive rating of 2. Conversely, the negative message for the same trigger has a negative rating of -2, meaning the warnings carry the same severity. In some cases, multiple weighted words were added to affective phrases to provide the same level of weighting. An assumption was made by the researcher that the impact of using multiple weighted words was summative. Again, with the positive malicious links message, the weighted words "validated" and "safe" have been included. These each carry a weighting of 1, giving an overall score of 2. In terms of the opposing, negative message, the only weighted word which has been used is "harmful", which has a negative weighing of -2.

The difference in weighting between triggers does not represent the severity of the risk associated with engaging with a particular trigger. An example of this can be seen with the password commonality rating. This has a rating of positive or negative 1. A different trigger, password length, has a rating of positive or negative 4. In terms of this research project, this does not indicate that a short password is much worse than having a common word in your password. The severity of triggers has not been evaluated in this research project.

The final affective sentences implemented into the research project are listed in Table 11. The words listed in bold in the table are ones which have been drawn from the affective wordlist.

Table 11 - final affective phrases and overall weighting

Risky security behaviour trigger	**Final affective text chosen**	**Overall sentence score**
Password commonality	Your password is a commonly used word. In an **attack**, it may be easier for hackers to guess.	-1
	Adequate- your password is not a common word.	1
Password with personal details	Your password contains personal details. In an **attack**, it may be easier for hackers to guess.	-1
	Adequate- your password does not contain personal details. It will be harder for attackers to guess.	1
Password length	Your password is too short. A **weak** password is **insecure**	-4
	Your password is equal to or longer than the minimum length. A **strong** password is more **secure**	4
Malicious links	Links found on the page have been **validated** and deemed **safe**.	2
	Harmful links have been found on the page.	-2
HTTP site	**Warning:** this website is not encrypted. Other users can potentially see information you are sending to the site.	-3
Social media site	**Warning:** this website is a popular social media site. Consider how much information you are divulging about yourself- attackers can potentially use this against you to gain access to your accounts.	-3
Malicious website	The current website you are visiting is malicious and is potentially **harmful**	-2
	The current website you are visiting is not malicious and is **trusted**	2

Password info: Length- your password is too short. A weak password is insecure.

Figure 31 - example of the affective text in use during experiments

6.4. The logging process

During the end user experiments (see Chapter 7), on beginning the questionnaire as part of the experiment, users must take note of the number of the USB they have been given. USB sticks have been labelled with numbers 1-5 and correspond to a version of the final research tool developed. This determines the specific type of feedback the user will receive during the experiment e.g. USB no. 2 refers to text-based affective feedback only. Please see 7.2. for the full list of USB stick numbers and the corresponding feedback type.

As an additional method of associating log files with the user questionnaire responses, the type of feedback the user receives is also written into the unique log file generated for each user (as shown in Figure 32).

```
Affective feedback: text and avatar.------------------------------------------------------------
[24-04-2016 15:42:48] - User entered the site
[24-04-2016 15:42:48] - http://driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/
[24-04-2016 15:42:48] - HTTP: this site is served via http
[24-04-2016 15:42:48] - Mozilla/5.0 (Windows NT 10.0; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
[24-04-2016 15:45:20] - User exited the webpage
```

Figure 32 - sample log file with affective feedback type written to it

The affective feedback type was added to the log via the checkLogExists function in the original MonitoringSolution.js file which is one of the building blocks of the extension (see section 5.2.4. for details of the full logging process). When a user starts a new experiment/or loads a new web page, the extension must run a check to ensure local storage has been set-up correctly, and that an appropriate log file already exists on the server. For each of the final extensions developed, an extra variable named extensionFeedback has been added which simply contains the value "Affective Feedback: <feedback type here>". This value is passed to the set_log.php file on the server via AJAX, and the appropriate line of text is added to the correct log file. It is added for every new site the user loads.

6.5. Delivery of affective feedback in the context of the browser

In order to implement an affective feedback delivery methodology in the context of a browser-based environment, the initial monitoring solution outlined in Chapter 5 had to be created. This monitoring system provides the basic framework on top of which the affective solution is built. The monitoring system allows for detection of risky behaviours, and embeds specific triggers which are fired on detection of a known risky security behaviour on the user's part.

This section will detail how the affective solution was integrated into the original monitoring solution which was created. It will go on to detail how affective feedback such as specific text, colours, and avatars are delivered on detection of risky security behaviour: what triggers it, the types of feedback delivered and how it is displayed on-screen to the user.

6.5.1. Integrating the monitoring solution and the affective feedback solution

The main browser.xul file which is one of the key components of the extension links to the original MonitoringSolution.js file and the jQuery library embedded within the extension, as well as the new file, AffectiveFeedback.js. As the name suggests, the AffectiveFeedback.js provides an affective feedback solution which is built on top of the existing Monitoring Solution framework.

As in section 5.2.2. , the Monitoring Solution already logs user behaviours when the user hits particular triggers. These triggers are outlined in Table 12.

Table 12 - triggers incorporated in the monitoring solution

User action	**Triggers**
When a user enters a page	• website encryption • if the site is a top 20 social media website • if the site is malicious • if malicious links are present on the page
When a user enters a password	• password length • password commonality • password personal details

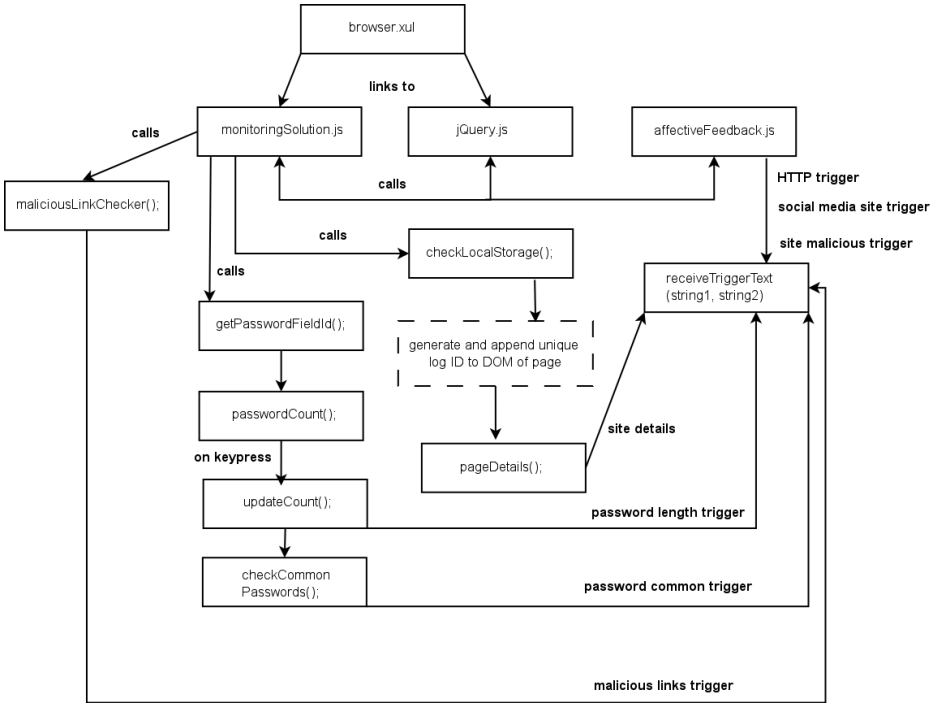


Figure 33 - how methods in the original monitoring solution integrate with the affective feedback solution

When integrating the AffectiveFeedback.js file into the MonitoringSolution.js file, a few changes had to be made to the MonitoringSolution.js file, so it could pass the relevant information to subsequently display affective feedback on-screen for the user.

The key change that was made was that on each of the triggers, reference to a function called receiveTriggerText was made. The receiveTriggerText function takes 2 parameters. The first of these parameters passes specific pieces of trigger text over to the AffectiveFeedback.js file, so it knows which piece of feedback to display to the user (Figure 33). The second parameter is also there to pass across any other information that might be relevant to the first parameter: more often than not, this parameter is given the value of null because there is no additional information available. The AffectiveFeedback.js file handles all decisions relating to the display of the affective information the user sees on-screen.

6.5.2. Clearing the affective content

When a new page is loaded in the browser, the first function which is called from the AffectiveFeedback.js file is the clearAffectiveContent function. This is called every single time to ensure the user does not see affective information which pertains to a previous website they have visited, reducing possible confusion.

6.5.3. Displaying affective feedback

Once old affective feedback has been removed from the browser window, the affective text and image areas need to be replaced. This is achieved when the addAffectiveBar function is called. The affective toolbar itself is made up of separate areas. Firstly, there's the main affective area at the bottom of the screen, which is split into 2 components: affective text, and the affective avatar. The text box is then split into 3 distinct sections, to make it easier to provide information to users. There's a password area, a malicious links area, and a general warning area. Not all feedback will be in use at all times e.g. some extensions only provide text as a form of feedback. In this case, the avatar box is blacked out, and the separate bars do not change colour. Figure 34 shows the structure of the affective feedback bar in the browser.

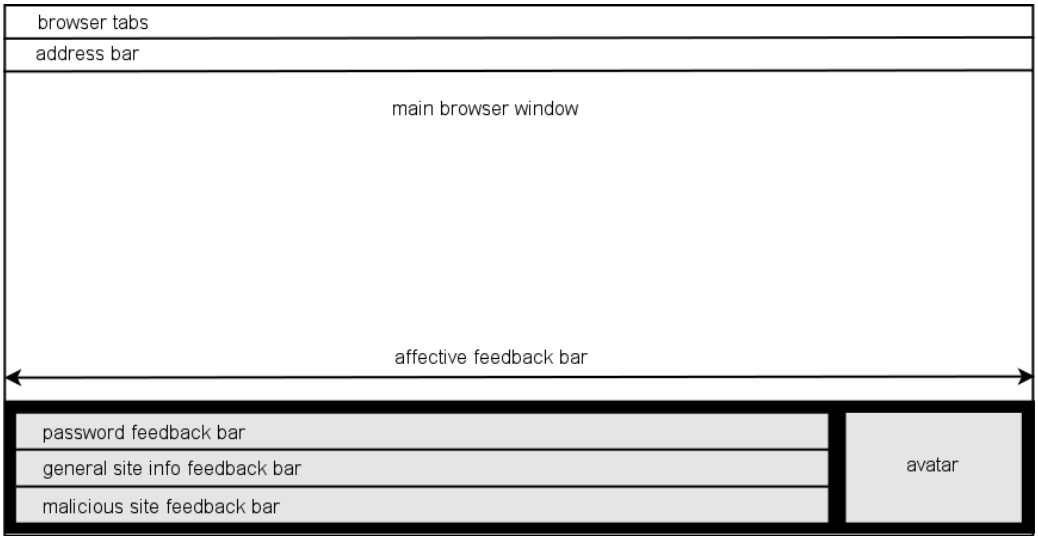


Figure 34 - positioning of affective feedback within the browser window

The affective feedback toolbar has been placed at the bottom of the browser. The reasoning behind this is that in previous versions of the Firefox browser (and various other browsers on the market), there was a status bar available, indicating if a website had fully loaded, where resources were being loaded from, and the location of hyperlinks users may have hovered over. The aim of placing the bar at the bottom of the screen was to make it as unobtrusive as possible.

Figure 35 shows the final version of the affective toolbar in the browser window.

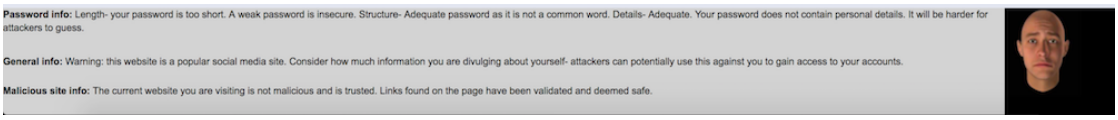


Figure 35 - final affective bar structure

6.5.4. Triggering affective feedback

When one of the triggers is activated in the MonitoringSolution.js file, information is then passed into the AffectiveFeedback.js file via the receiveTriggerText function. The diagram displayed in Figure 36 shows how the skeleton of the affective bar is added to the screen, and how trigger keywords are passed across from the Monitoring Solution, eventually triggering the affective feedback mechanism.

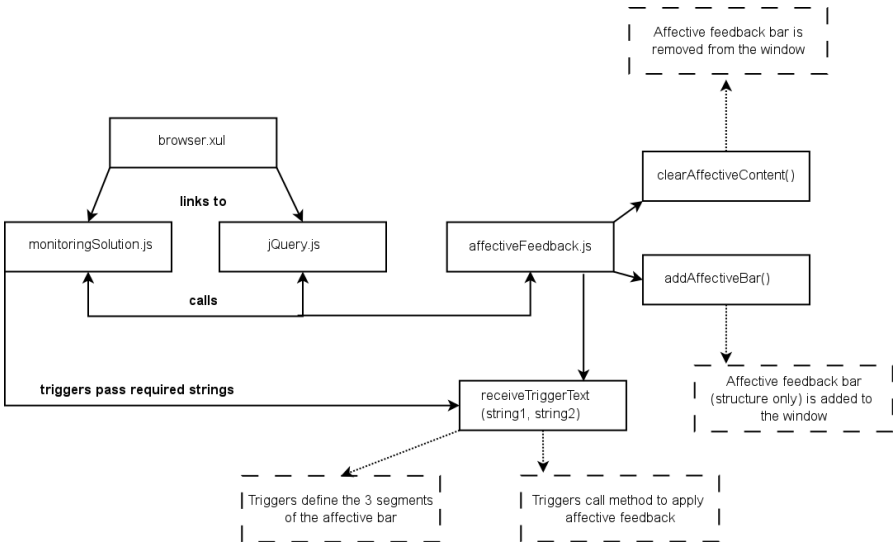


Figure 36 - how triggers generate affective feedback

There are a number of triggers in place in the system, which are linked to known risky security behaviours. Table 13 provides an overview of the types of risky security behaviours the monitoring system is looking for, along with the keyword information which triggers delivery of affective feedback.

Table 13 - table of the trigger keywords

Trigger	Description	Parameter 1 (trigger text)	Parameter 2
Password commonality	Commonly used password	“passwordcommon”	null
	Not a commonly used password	“passworduncommon”	null
Password with personal details	Password contains personal details	“passpersonal”	null
	Password does not contain personal details	“passnotpersonal	null
Password length	Password is too short	“passshort”	null
	Password is longer than the minimum length	“passlong”	null
Malicious links	No malicious links found	“nomallinks”	null
	Malicious links found on page.	“mallinks”	Array of malicious links found
HTTP site	Site is served via HTTP	“siteDetailsFound”	Array of site details
Social media site	Site is a top 20 social media site	“siteDetailsFound”	Array of site details
Malicious site	Site is a known malicious site	“siteDetailsFound”	Array of site details

As part of the experimental design, a number of extensions were developed, containing multiple versions of affective feedback delivery. A function was written for each of these methods. In total, 5 versions of the extension were developed, however the system was designed so that an affective delivery function could be added for each delivery system. The function calls to the inactive delivery system were simply commented out, leaving only one delivery system per extension. Table 14 shows the function names and the types of feedback they were to deliver.

Table 14 - affective functions and feedback delivered

Affective function name	Affective feedback delivered	Notes
<none>	No feedback, monitoring only	All affective functions commented out in code
textAffectiveBar()	text	-
textColourAffectiveBar()	text, colour	-
textAvatarAffectiveBar()	text, avatar	-
textColourAvatarAffectiveBar()	text, colour, avatar	-

In terms of an explanation of how the affective feedback system works, the extension which delivers all available types of affective feedback will be explained in this section- text, colour and avatars. Specifically, the function which will be discussed is named textColourAvatarAffectiveBar(). All other extensions developed make used of a smaller combination of these types of feedback.

6.5.4.1. Trigger- Commonly used password

If a password is entered whilst the tool is running and the monitoring solution deems it to be a commonly used password, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the sad avatar.

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value is “Structure- your password is a commonly used word and in an attack, it may be easier for hackers to guess”.

3. get the hex value for a red colour, indicating a poor security choice.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.2. Trigger- Not a commonly used password

If a password is entered whilst the tool is running and the monitoring solution cannot find a match against a list of commonly used passwords, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the happy avatar.

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value "Structure- Adequate password as it is not a common word”.

3. get the hex value for a green colour, indicating a good security choice.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.3. Trigger- Password contains personal details

If a password is entered whilst the tool is running and the monitoring solution matches personal information in the password against the database of information the user may have provided, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the sad avatar.

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value is "Details- your password contains personal details. In an attack, it may be easier for hackers to guess".

3. get the hex value for a red colour, indicating a poor security choice.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.4. Trigger- Password does not contain personal details

If a password is entered whilst the tool is running and the monitoring solution does not match any personal information in the password against the database of information the user may have provided, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the happy avatar.

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value is "Details- Adequate. Your password does not contain personal details. It will be harder for attackers to guess".

3. get the hex value for a green colour, indicating a good security choice.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.5. Trigger- Password is too short

If a password is entered whilst the tool is running and the monitoring solution deems it to be too short, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the sad avatar.

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value is “Length- your password is too short. A weak password is insecure”.

3. get the hex value for a red colour, indicating a poor security choice.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.6. Trigger- Password is longer than the minimum length

If a password is entered whilst the tool is running and the monitoring solution deems it to be longer than the minimum length, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the happy avatar.

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value is “Length- your password is equal to or longer than the minimum length. A strong password is more secure”.

3. get the hex value for a green colour, indicating a good security choice.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.7. Trigger- No malicious links found

The monitoring solution checks all links on the web page the user is visiting to determine if any of the links are potentially malicious. If no malicious links are found on the page, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the happy avatar.

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value is "Links found on the page have been validated and deemed safe.".

3. get the hex value for a green colour, indicating a good security choice.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.8. Trigger- Malicious links found on page

The monitoring solution checks all links on the web page the user is visiting to determine if any of the links are potentially malicious. If malicious links are found on the page, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the sad avatar.

2. call to the affectiveTextValue function. The case statement gets the value of thecorrect affective text which matches the trigger. The text value is " "Harmful links have been found on the page".

3. call to find all links on the page.

4. checks links against the array of malicious links provided by the monitoring solution.

5. get the hex value for a red colour, indicating a poor security choice.

6. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

7. highlights malicious links in red warning colour.

6.5.4.9. Trigger- Site is served via HTTP

If a site is served via HTTP, this is not inherently bad, unless the user is providing information which should be encrypted. If they are browsing a web page without entering any information, this is not a problem. Due to this, HTTP sites are considered to be general information by the feedback system. When a HTTP page is detected, the following steps are carried out by the affective solution:

1. no additional affective avatar is called

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value is “Warning: this website is not encrypted. Other users can potentially see information you are sending to the site”.

3. get the hex value for a orange colour, indicating a security choice which could be good or bad, depending on the site visited.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.10. Trigger- Site is a top 20 social media site

Visiting social media websites is not necessarily a poor security choice. Provided users do not reveal too much personal information about themselves, they do not pose much of a security risk. Due to this, social media sites are considered to be general information by the feedback system. When a top 20 social media site is loaded, the following steps are carried out by the affective solution:

1. no additional affective avatar is called

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value is "Warning: this website is a popular social media site. Consider how much information you are divulging about yourself- attackers can potentially use this against you to gain access to your accounts".

3. get the hex value for an orange colour, indicating a security choice which could be good or bad, depending on the information divulged by the user.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.11. Trigger- Site is a known malicious site

If the user visits a known malicious site whilst the tool is running, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the sad avatar.

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value is "The current website you are visiting is malicious and is potentially harmful".

3. get the hex value for a red colour, indicating a poor security choice.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.12. Trigger- Site is not a malicious site

If the user does not visit a known malicious site whilst the tool is running, the following steps are carried out by the affective solution:

1. call to affectiveAvatarImage function which gets URL of the happy avatar.

2. call to the affectiveTextValue function. The case statement gets the value of the correct affective text which matches the trigger. The text value "The current website you are visiting is not malicious and is trusted".

3. get the hex value for a green colour, indicating a good security choice.

4. call to textColourAvatarAffectiveBar() which displays the appropriate pieces of information on-screen.

6.5.4.13. Traffic light system

Within the affective feedback solution, there is also a system of flags in place, which is designed to provide an overall level of feedback, depending on the users' actions.

One example of this would involve the password feedback. There are multiple areas of password feedback which can be shown to the user involving length, commonality, or if it includes personal details. A password may be long (good), uncommon (good) but may contain personal details (potentially bad). To prevent the system from providing users with positive feedback when they have failed any 1 of the 3 password security checks, the password flags are checked and provide an override. So whilst users may have an uncommon, long password, they are still shown negative affective text, colours and avatars. They will only be shown positive feedback when they meet all 3 levels of the password security criteria. Each bar has its own set of flags which determine the overall colours of the password, general info and malicious links bar.

The avatar displayed on-screen also has its own set of flags. Due to the fact there is only one avatar on display on-screen at any given time, security criteria have to be met for each of the password, general info and malicious links bars. If all security criteria are met, the avatar will look happy. If any security area fails, the flags built into the system will trigger an override and the avatar will remain with a sad expression until the risky security behaviours are avoided.

6.6. Final tool developed

A number of versions of the final tool were developed, as the project required the impact of affective feedback to be tested against a control environment. In the end, 5 versions of the tool were created, and Table 15 provides an overview of each feedback type.

- **Spengler-Zuul (none)-** monitors users but showed no on-screen feedback.

- **Spengler-Zuul (text)-** monitors users and displays text-based affective feedback.

- **Spengler-Zuul (text and avatar)-** monitors users and displays text-based affective feedback, alongside an avatar situated in the bottom right of the screen.

- **Spengler-Zuul (text and colour)-** monitors users and displays text-based affective feedback, with a colour coded traffic light system background.

- **Spengler-Zuul (text and colour and avatar)-** monitors users and displays text-based affective feedback, with a colour coded traffic light system background. Additionally, an avatar is situated in the bottom right of the screen.

Table 15 - overview of types of feedback included in each extension

Extension name	Text-based feedback	Colour-based feedback	Avatar-based feedback
Spengler-Zuul (none)			
Spengler-Zuul (text)	X		
Spengler-Zuul (text and avatar)	X		X
Spengler-Zuul (text and colour)	X	X	
Spengler-Zuul (text, colour, and avatar)	X	X	X

Further information will be provided in this section, including screenshots for each of these tools, highlighting how they work and detailing the user experience.

6.6.1. Tool etymology

The system consisting of the monitoring solution and the affective feedback mechanism has been termed the Spengler-Zuul tool. XUL was developed by Mozilla and the name is a play on Zuul, a character from the Ghostbusters 1984 movie (imdb.com 2016). Further references to the film can be found within the XUL documentation, with both the Keymaster and the Gatekeeper mentioned. In addition to this, until October 2014, Mozilla Firefox contained a JavaScript debugger named Venkman, named after Dr. Peter Venkman from the film.

In this tradition, since the extension developed for this project was constructed using XUL, the tool has been named Spengler-Zuul, referencing both Zuul and Dr Egon Spengler.

6.6.2. Spengler-Zuul (none)

The Spengler-Zuul (none) tool provides no affective feedback to the user, and instead acts as a control extension. During the experimental process, users were required to visit the same websites, though they were given no cues as to the malicious links which may have appeared on the pages.

The only different thing the user sees in comparison to a normal Firefox browsing environment is the addition of the small grey bar in the top-right of the screen which displays a unique log ID, which was utilised during the experimental process (Figure 37).

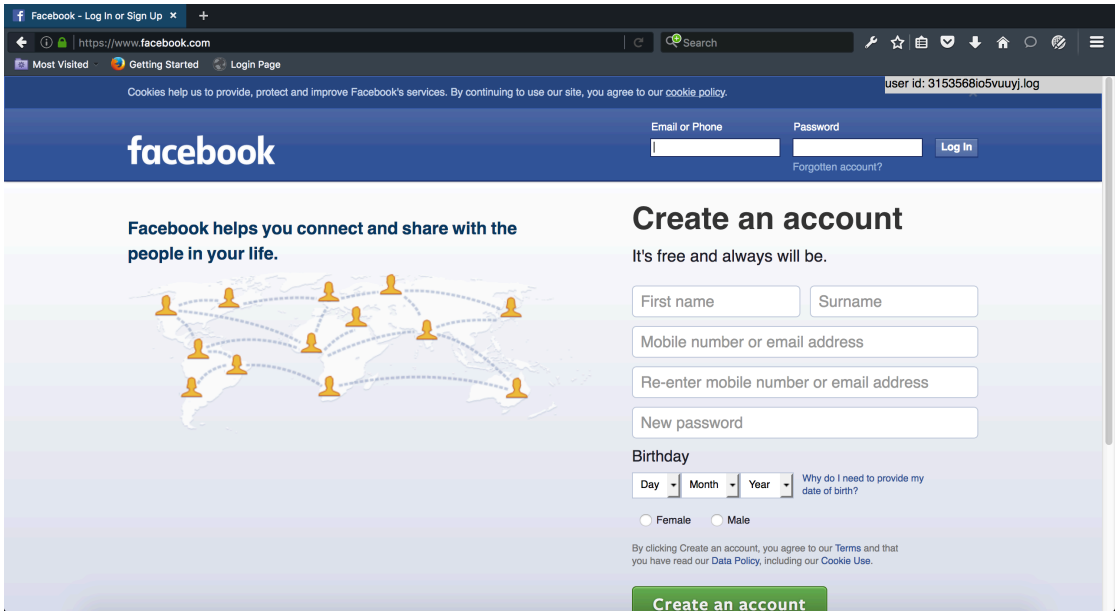


Figure 37 - screenshot of the Spengler-Zuul (None) tool running on the Facebook home page

6.6.3. Spengler-Zuul (Text)

The Spengler-Zuul (text) tool provides a single, text-based method of affective feedback to the end-user when security behaviours have been triggered. Users are presented with a small grey toolbar which spans the bottom portion of the screen, alongside 3 segments of affective text (see section 6.3.3.4. for details on affective text). It is separated into a password section, general information section and malicious sites information section. The user will also see the addition of the small grey bar in the top-right of the screen which displays a unique log ID. The toolbar at the bottom of the screen will deliver affective text based upon their actions in the browser e.g. that their password is too short (Figure 38).

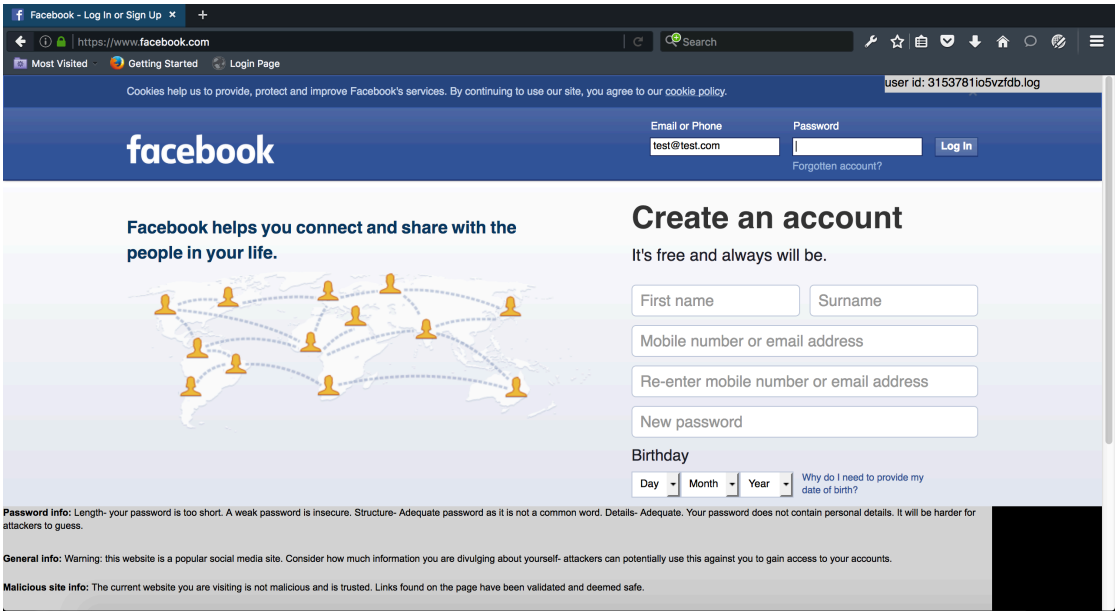


Figure 38 - screenshot of the Spengler-Zuul (text) tool running on the Facebook home page

6.6.4. Spengler-Zuul (Text, Colour)

The Spengler-Zuul (text and color) tool provides multiple methods of affective feedback. Text-based affective feedback is delivered, alongside colour-based feedback. Users are presented with a toolbar at the bottom of the screen which is split into 3 segments: password information, general site information, and malicious site information. The toolbar remains grey however, when a user exhibits positive or negative security behaviour e.g. has a lengthy password, the appropriate section of the bar will change colour, in this case indicating green for good. Additionally, the text will also aid in confirming the behaviour the user has just exhibited.

The password bar handles multiple triggers- length, if the password is common, or if the password contains personal details. If the user fails any of these checks, the bar will remain red, for danger. To give an example, a user may have a lengthy password that is not common, however it may contain personal information they have provided online. By exhibiting risky security behaviour in the personal details section, an overall negative response is triggered.

In the case of the screenshot shown in Figure 39, the user has a short password which is insecure. This has both been highlighted on the toolbar at the bottom of the screen, and the background colour of the password box where the user enters their password has also changed colour to reflect a negative result.

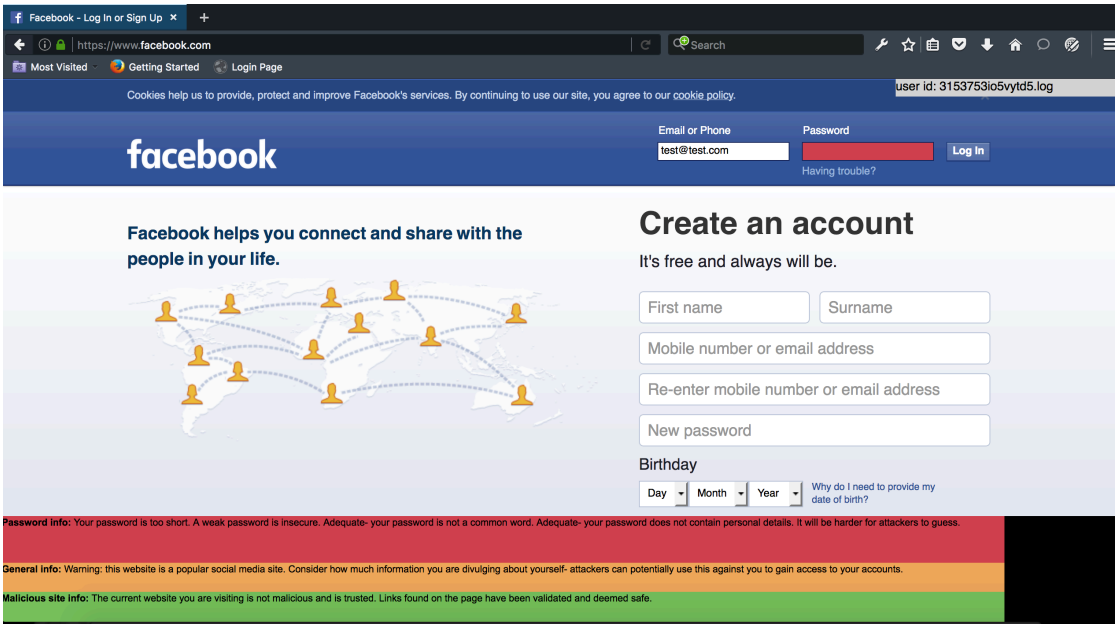


Figure 39 - screenshot of the Spengler-Zuul (text and colour) tool running on the Facebook home page

6.6.5. Spengler-Zuul (Text, Avatar)

Spengler-Zuul (text and avatar) tool provides multiple methods of affective feedback. Text-based affective feedback is delivered, alongside an avatar of an adult male, containing subtle facial cues, at the bottom-right of the screen. Again the toolbar at the bottom of the screen is split into 3 segments: password information, general site information, and malicious site information.

Each segment of the toolbar remains grey, delivering textual feedback on triggers. Should the user engage in risky security behaviour relating to one of the triggers, the avatar will also exhibit facial cues which appear to make him look sad. Oppositely, if the user exhibits safe behaviour in each of the segment triggers, the avatar will change, with facial cues making him look happy.

In the example shown in Figure 40, the user has not yet typed a password in the password box. Therefore, the extension detects the password as being too short, causing the appropriate textual feedback and sad avatar.

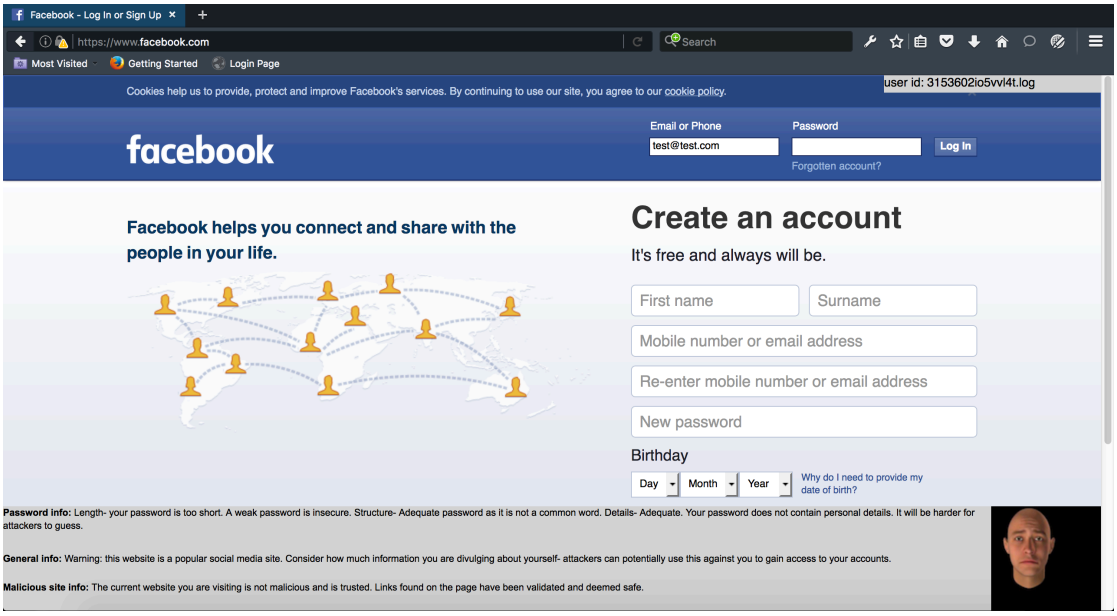


Figure 40 - screenshot of the Spengler-Zuul (text and avatar) tool running on the Facebook home page

6.6.6. Spengler-Zuul (Text, Colour, Avatar)

The Spengler-Zuul (text and avatar and colour) tool provides 3 different methods of affective feedback. Text-based affective feedback is delivered, alongside an avatar of an adult male, containing subtle facial cues. Furthermore, the toolbar at the bottom of the screen is split into 3 segments: password information, general site information, and malicious site information. and each of these is colour-coded like a traffic light system, as outlined in section 6.6.4. .

Each segment of the toolbar starts off grey however it changes colour depending of the positive or negative security behaviour exhibited by the end user. Additionally, the avatar included in the bottom-right of the screen, will also reflect the users' choices, appearing sad or happy based up on the users' decisions. Finally, the affective text will provide an explanation in relation to what the user has done.

In the example shown in Figure 41, the user has moved focus to the password field but has not yet started typing a password. The extension flags this as a short password, causing the appropriate text to be delivered to the end user, and the password segment of the toolbar and the password field turn red, indicating negative behaviour. Also, the avatar in the corner appears sad.

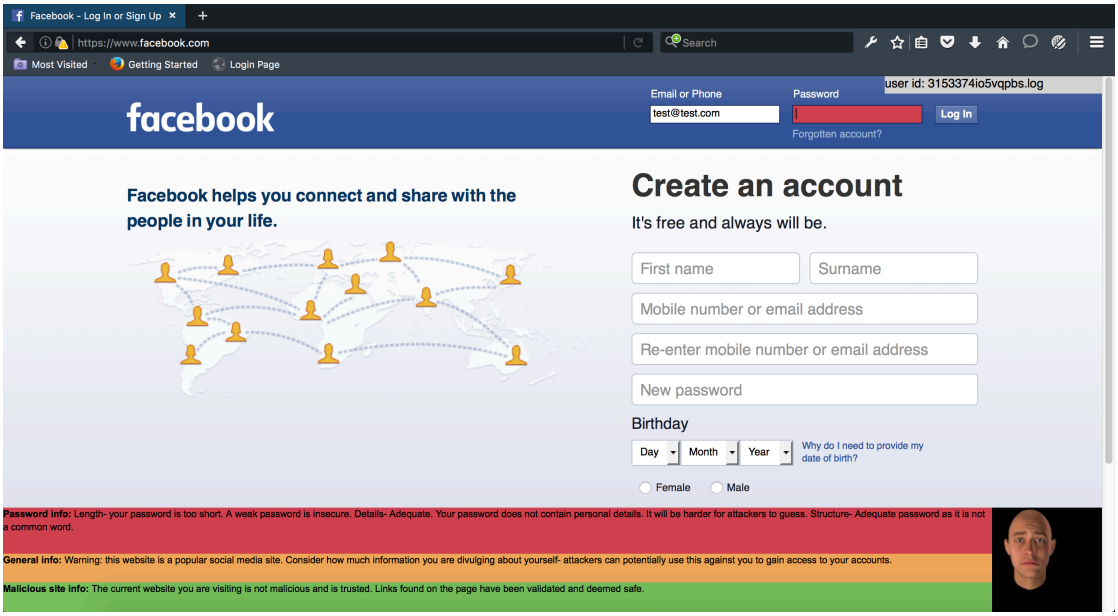


Figure 41 - screenshot of the Spengler-Zuul (text and colour and avatar) tool running on the Facebook home page

6.7. Summary of the affective feedback solution

The core of the project is to assess whether the use of affective feedback enhances users' awareness of risky behaviour. In order to evaluate the impact of affective feedback, a method of delivering such feedback to users was required, in the context of a browser-based application.

By building upon the existing monitoring solution framework outlined in Chapter 5, an affective feedback solution was also delivered within the confines of the browser environment. Depending on the specific extension the user is engaged with, users can be subjected to multiple different types of affective feedback, including text, colour and avatars, when previously identified behaviours trigger such feedback.

The development of such an environment means each of the extensions with different combinations of affective feedback can be tested in an attempt to see which kind of feedback (if any) has the largest effect on users' consideration of their risky behaviour, and whether or not affective feedback as a whole has any impact on risky security behaviour. To this end, Chapter 7 will outline the methodology followed for this evaluation process before the results of using such a tool are outlined in Chapter 8.

Chapter 7. Methodology and Evaluation

To determine if affective feedback presented to users had any impact on their security awareness, and behaviours online, an evaluation regime was developed in an attempt to gather data in this respect. The methodology will cover each stage of the evaluation process, and provide a rationale for the way in which the tests were carried out.

The overarching strategy will be discussed, with further in-depth discussion of the sites used in the evaluation process, the participant selection process, and the development of the user questionnaire.

7.1. Basic evaluation strategy

To give a brief overview of the evaluation process, participants were initially given the "Information For Participants" handout (see Appendix (iii) . Following this they were then given a random USB stick, labelled with a number from 1-5. Each of the USB sticks contained a portable version of the Firefox browser, with a version of the monitoring solution/affective feedback mechanism add-on pre-installed. After signing the consent form, users were asked to work their way through the instruction sheet (see Appendix (v) . On completion of the computer-based part of the experiment, participants were asked to complete a paper-based questionnaire regarding how well they thought they responded to the feedback they may or may not have been shown on-screen. In the background, the users' actions on the computer-based part of the experiment are also logged, meaning the information they provide in the questionnaire can be corroborated against the information found in each of the unique log files.

7.2. Use of USB sticks

Owing to the restrictive, though appropriately security-conscious nature of Abertay University's IT policy, the browser extensions could not be installed on individual machines, hence the reason why the experiments were carried out via the use of USB sticks. Although plugging in an unknown USB stick can be deemed to be a risky security behaviour in itself (United States Computer Emergency Readiness Team 2011), it was deemed necessary in this scenario to allow research to be conducted. The USB sticks were plugged into university machines only and were not allowed to be used on participant's personal machines.

Running the experiments from the USB sticks also had an additional benefit. Coupled with that fact that the logging mechanism created a unique log for each test participant on a central server, it meant the log files were easily gathered by the researcher conducting the project. Rather than having to collect log files from every single machine the participants used, they were simply gathered from one folder located on a university web server.

As part of the experimental design process, 5 different extensions were created in a bid to determine of affective feedback had any impact on the end user. For full details of each of these extensions, see section 6.6. During the experiments, participants were given a USB stick at random, which had numbers from 1-5 on them. Each of these numbers corresponded to the type of feedback they would receive during the experiment (participants were never explicitly told what type of feedback they would receive, only that they may or may not receive on-screen feedback). Below is a list of the USB stick numbers and corresponding types of feedback participants received (Table 16).

Table 16 - USB stick number and corresponding feedback received

USB stick number	Affective feedback delivered
1	No feedback, monitoring only
2	text
3	text, avatar
4	text, colour
5	text, colour, avatar

7.3. Participants

Initially, the study wished to investigate the impact of affective feedback on average computer users i.e. those who used computers regularly to perhaps browse the web, but did not have an advanced degree in the subject. The study was eventually expanded to include those that were studying for degrees in subjects such as ethical hacking and computing, in an effort to see how participants in these fields reacted to affective feedback, and to see if their increased knowledge of computer security had any impact on the results of the study.

Participants were mostly gathered from classes within the of School of Arts, Media and Games, the School of Science Engineering and Technology, and the Graduate School within Abertay University.

All experiments took place within a quiet, desktop environment in an attempt to remove any external stimuli which could have distracted participants during the study.

7.4. Form design

This section will discuss the forms used in the experiment and the thought process behind using them.

7.4.1. Information for participants

Participants were initially told, that the purpose of the 15-minute study was to assess whether or not specially developed Firefox extensions assist you whilst browsing the web. To keep the explanation as simple as possible, participants were told the experiment would involve visiting certain websites and that during this time, a Firefox extension may provide you with on-screen feedback and it will record the sites you have visited. Care was taken to avoid mentioning what kind of feedback would be provided or where it would appear on-screen. The fact that risky security behaviours were also being measured was omitted from the information for participants, in order to avoid influencing them in any way.

Participants were free to withdraw from the study at any time, with no questions asked. Any information gathered during the project was held in accordance with the Data Protection Act (1998). In addition to this, the information held within the system was not used to identify individuals taking part in the experiments. On completion of the experimental process, the information provided by the test participants was removed from the server. A complete version of this form can be found in Appendix (iii) .

7.4.2. Consent form

As part of the experimental process, each test participant had to sign a consent form to verify they understood the instructions and volunteered to take part in the experiments. A complete version of this form can be found in Appendix (iv) .

7.4.3. Instructions for participants

Initially, participants were warned Firefox might be slow to respond as it's running on a USB drive, rather than a HDD. Participants are also guided to write down the number which can be found on their USB stick, along with the unique log ID for the user which appears in the top-right of the screen when the Firefox browser loads.

The next sub-section of the instruction sheet involves the web-browsing aspect of the experimental process. Participants are asked to visit a number of websites (see section 7.5. for information on the websites visited), whereby they may be presented with additional information on-screen (depending on the test in which they are participating, they may see 1 or more forms of affective feedback appearing on-screen, depending on their actions). Participants were asked to look at each website and read any information given carefully. Again, at no point do the instructions make reference to the fact the experiment is actually monitoring behaviour and is ultimately looking at security behaviour- such information would result in bias.

On completion of the computer-based portion of the experiment, participants are guided to request a paper questionnaire from the researcher running the experiment. A complete version of the form can be found in Appendix (v) .

7.5. Sites to visit

During the computer-based portion of the experiments, users are asked to visit a number of websites. This section will give an overview of each of the sites users were asked to visit, and will provided a rationale as to why each of these sites have been included in the evaluation.

7.5.1. Experiment details page

URL: http://driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/

This website is the start page for the experiment process, and is simply a repeat of the information for participants. In order to continue with the study, participants must check a box at the bottom of the page, again agreeing to the terms and conditions.

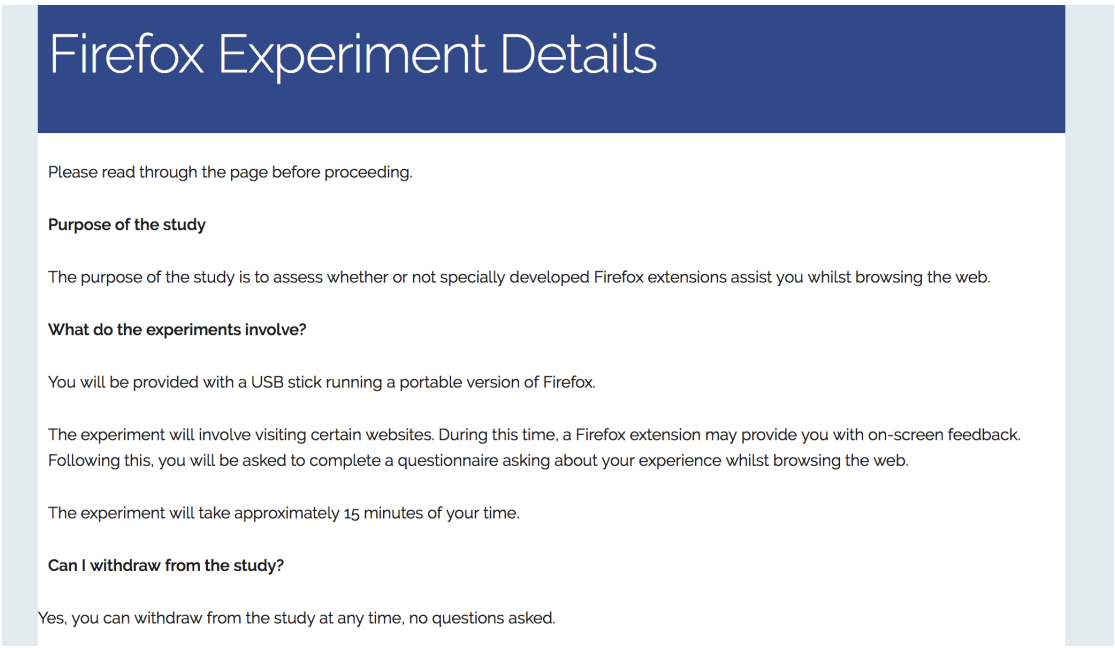


Figure 42 - partial screenshot of the experiment details page

7.5.2. Initial user form page

URL:
http://driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/initial_form/index.php?agree=on

The initial user page was engineered and used in the evaluation methodology in an attempt to gain information about test participants, and create a profile of information. Users were asked to divulge the following pieces of information on the form: first name, middle name(s), surname, mother's maiden name, names of pets (if applicable), phone number, and hobbies.

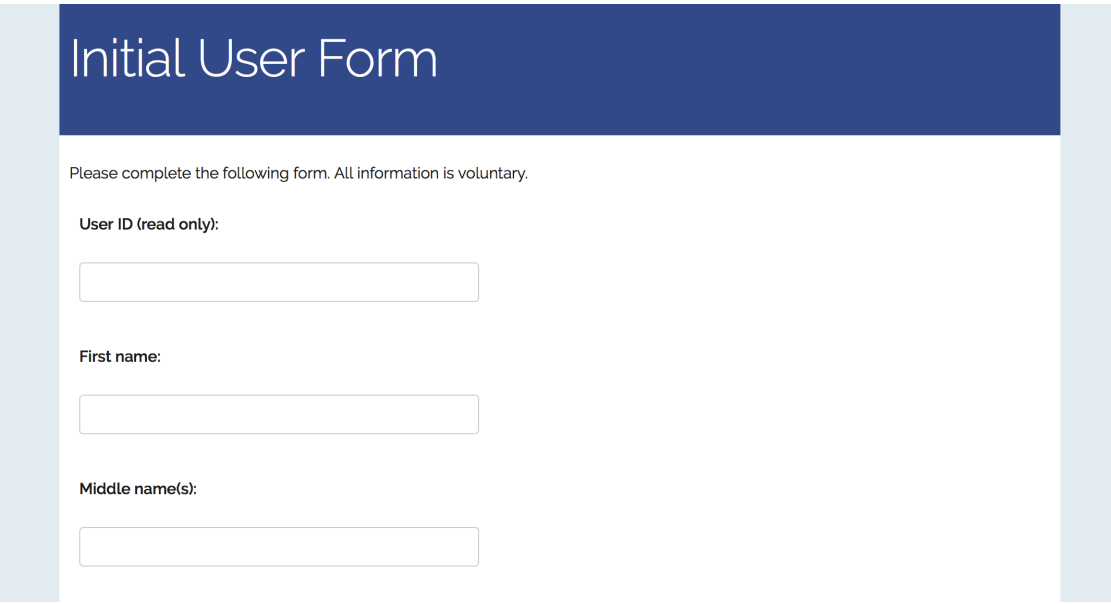


Figure 43 - partial screenshot of the initial user form

A paper by Milne, Labrecque and Cromer (2009) previously defined a list of risky security behaviours which included using a dictionary word as a password, and using a password which contains some personal information such as a mother's maiden name or the name of a pet. Additional research has noted that users divulge too much information about themselves on social networking sites (Kaspersky Lab 2013) and owing to these pieces of research, this particular web form was designed in a way to elicit personal information from the test participant.

At the very top of the web page, it states "*Please complete the following form. All information is voluntary.*" so this also provides a test as to whether the participant has read all instructions carefully. This means users do not have to complete the form or provide any personal details. It is possible to submit the form without completing any of the fields/revealing any personal information.

The information gained from this page is written to a database. Later in the experiment, if participants choose to enter a password during the tests, the password entered is checked against the information they may or may not have revealed during the experiments. Ultimately, this web page helps in identifying if a user has engaged in risky security behaviour.

7.5.3. Other site form page

URL: http://driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/other_site/index.php

The "other site" web page only asks users for their full name and their email address. The paper by Milne, Labrecque and Cromer (2009) deems using a private email address to register for a contest on a website as a risky security behaviour. Whilst deceiving test participants about a fake competition may have been deemed unethical, as part of the experiments, the researchers chose to ask for an email address anyway.

The web page does not provide any information about what the address will be used for therefore they are providing an email address without being informed what it could potentially be used for. The website states *"Please enter your email address. Providing information is voluntary."* at the very top of the page, meaning the form can be submitted without users revealing any information about themselves.

Any information can be entered into these fields, and a simple test performs a check to investigate if the user left these fields blank.

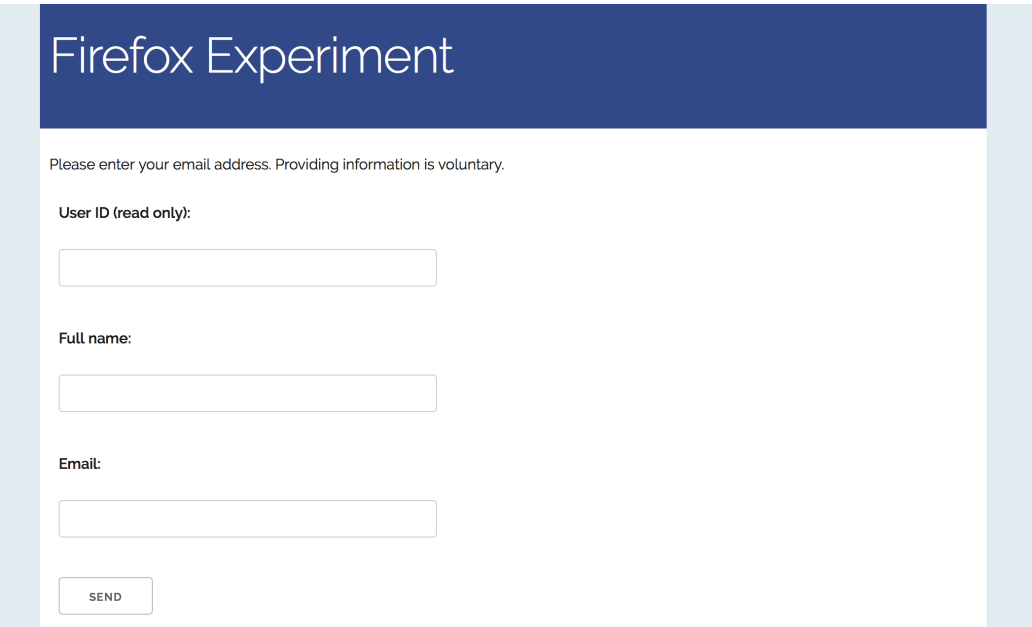


Figure 44 - screenshot of the "other site" page

7.5.4. Continue page

URL:
http://driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/other_site/continue.php

The continue page is just a transition page which directs how the participant should progress throughout the experiment. If the user has a Facebook account which they wish to use in the experiment, they are taken to the Facebook website. Otherwise, they are directed to a sample Bad SSL web site.

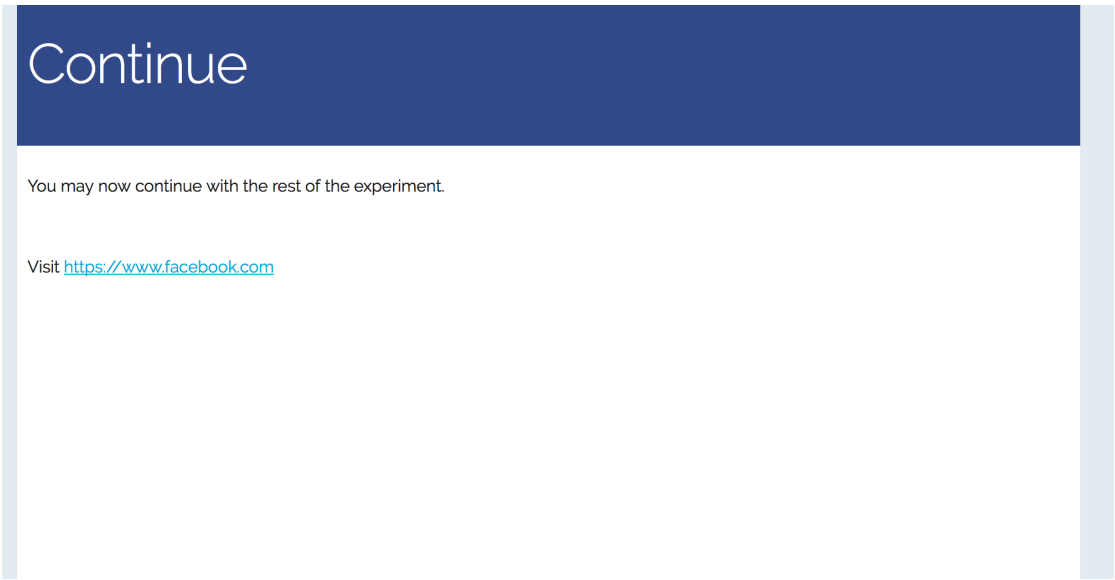


Figure 45 - screenshot of the continue page

7.5.5. Facebook page

URL: https://www.facebook.com

If test participants had a Facebook account and were willing to use it as part of the experiment, they were asked to enter their password, and read any information they may be provided with. Following this, users were asked to post a status update, and to then log out.

This part of the test was not mandatory. Users did not have to use their Facebook accounts if they did not wish to. They could even log in and then log out without entering a status update. If participants did not have a Facebook page or do not want to log into their Facebook account, they could skip to the Bad SSL portion of the experiment.

Research by Milne, Labrecque and Cromer (2009) notes using a social networking website can be classed as a risky security behaviour. Such a comment can be attributed to the fact people often reveal too much information about themselves online (Kaspersky Lab 2013), which has even prompted the FBI to warn the general public about the rise of spear phishing attacks (FBI 2013).

The rationale behind this part of the experiment is to firstly guide participants to purposely visit a social media website. By asking users to post a status update, it became an opportunity for them to potentially reveal personal information about themselves. Finally, it provides an encrypted password to check against any of the personal information they might have revealed about themselves at the beginning of the experiment.

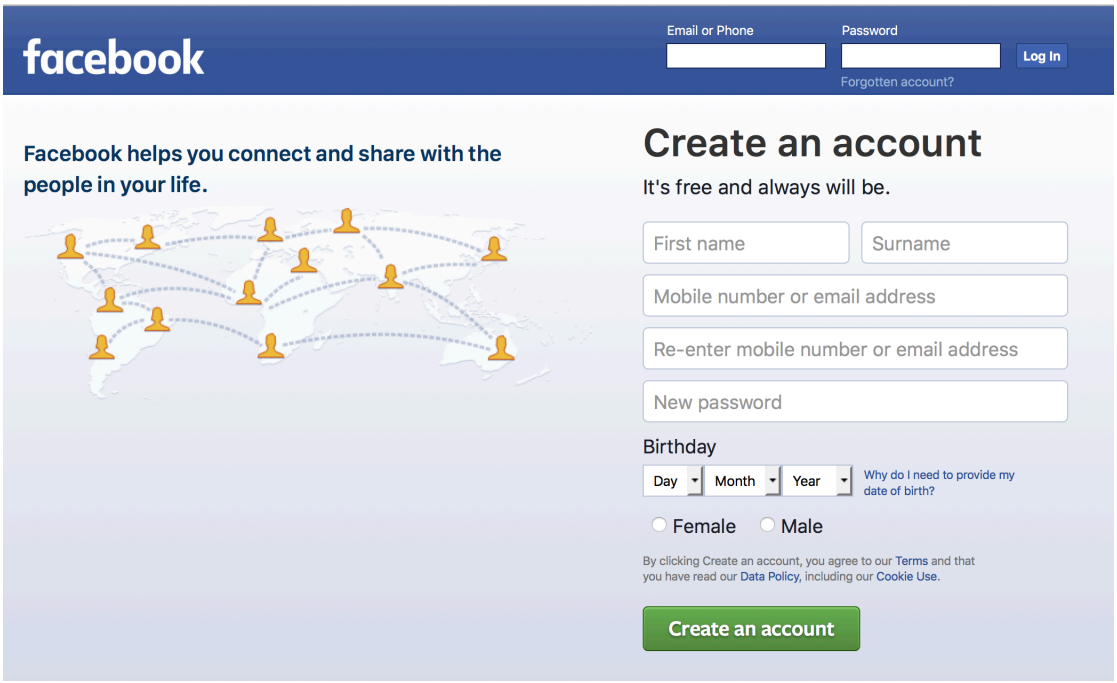


Figure 46 - screenshot of Facebook

7.5.6. Bad SSL page

URL: http://http-password.badssl.com/

Test participants do not have to do anything on this page, other than read all the information provided on the page. The page is a HTTP (unencrypted page) which asks for a password, highlighting that the information could be viewed and used for malicious purposes. The page triggers the HTTP warning in a bid to determine if users notice the information they are provided with, which is the rationale.

Figure 47 - screenshot of the Bad SSL page

7.5.7. End experiment page

URL: http://driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/end_experiment/

Participants are presented with a page containing 3 links: end link 1, end link 2, and end link 3. They are asked to click on one of these links to end the experiment. On clicking any one of these links, participants are shown a page which asks them to complete a short questionnaire, and that they should ask the researcher running the experiment for a copy of the questionnaire.

One of the links presented on the page is classed is a malicious link. This was spoofed by placing one of the links into the database of malicious links which the monitoring solution references. This triggers the malicious link warnings within the affective feedback mechanism, meaning that participants get a text-based, colour-based, or avatar-based warning about the malicious link. If the user is part of the control group, which delivers no feedback, users have no idea which of the links they are presented with is malicious. Similarly, if the user is evaluating one of the extensions which do not deliver colour-based feedback, they are warned one of the links is malicious, but the link is not highlighted in a warning colour, again showing they might click on a malicious link without knowledge of what they've done.

The spoofed malicious link on the page is end link 1, with the address of http://driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/end_experiment/end1.php

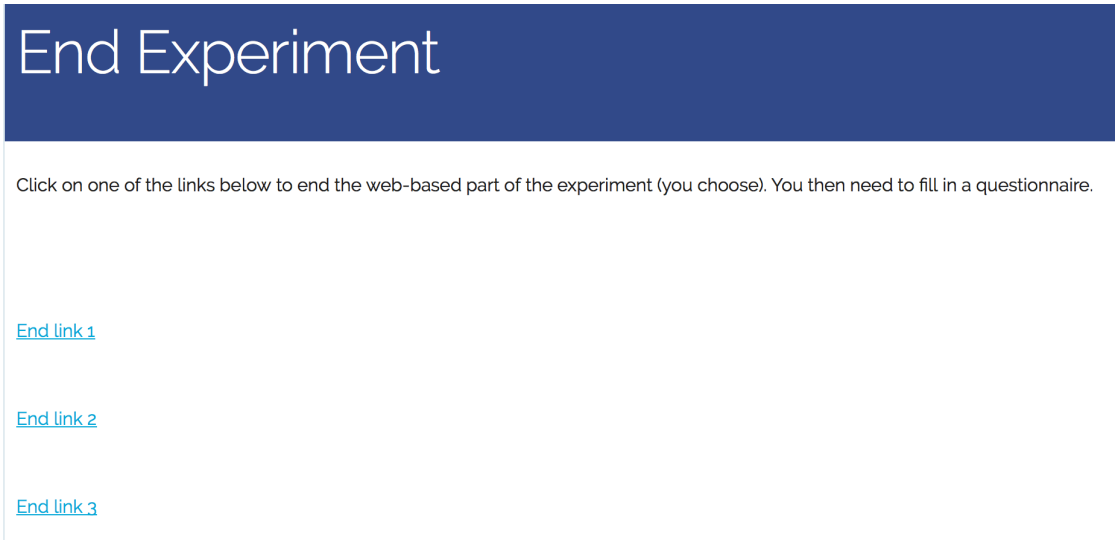


Figure 48 - screenshot of the end experiments page

7.5.8. Summary of the sites used

Table 17 includes a summary of all the sites utilised during the experiments carried out with participants.

Table 17 - Summary of websites used

Name	Website	Purpose
Experiment details	driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/	A repeat of the experiment information for participants.
Initial user form	driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/initial_form/index.php?agree=on	Gain information about test participants.
Other site form	driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/other_site/index.php	Gain further information about test participants.
Continue	driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/other_site/continue.php	Explains how the participant should progress through the experiment.
Facebook	www.facebook.com	Explore awareness of social media websites.
Bad SSL	http-password.badssl.com/	Sample HTTP which asks for a password-feedback trigger.
End experiment	driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/end_experiment/	One links presented is spoofed malicious link.
Experiment end	driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/end_experiment/end1.php	Spoofed malicious link. Ends the experiment.
Experiment end	driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/end_experiment/end2.php	Ends the experiment.
Experiment end	driesh.abertay.ac.uk/~l514921/final_phd_work/user_pages/end_experiment/end3.php	Ends the experiment.

7.5.9. Website flowchart summary

Below is a flowchart to summarize how participants can progress through the websites involved in the evaluation process.

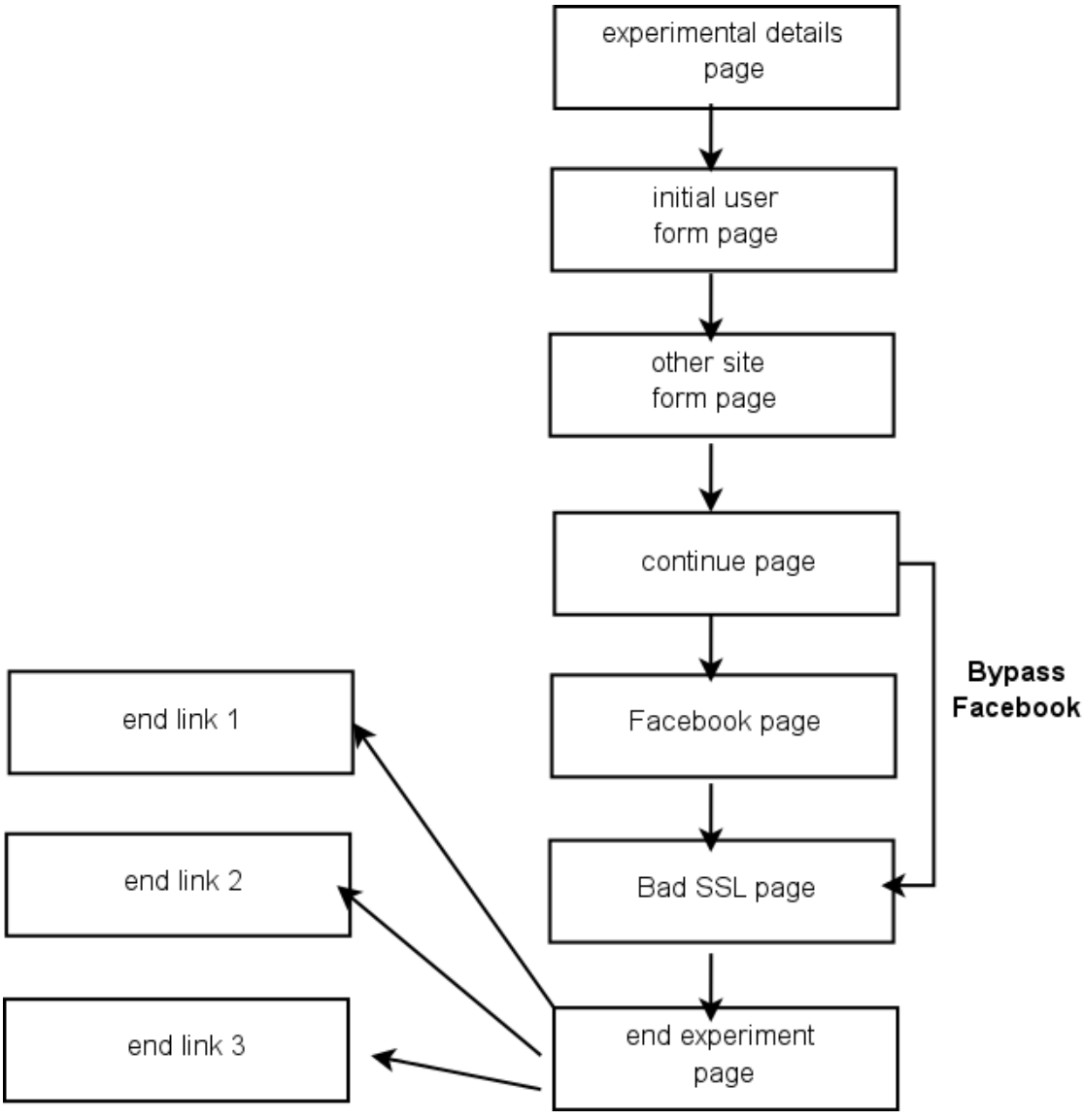


Figure 49 - flowchart of website progression

7.6. Extensions vs. participants

There are 5 possible experiments regarding the monitoring solution and affective feedback system (outlined in 7.2.). Participants were only allowed to take part in the experiment once, in order to prevent habitualization, and to reduce the bias of knowing what to expect from the experiments.

7.7. Questionnaire design

In this section, each of the questions asked in the questionnaire will be discussed, highlighting why the question was asked, and what information was gained from asking the question. The Likert-based scoring system for questions will also be discussed, providing a quantitative approach. Finally, the questions will also be comparable to the information captured in the log files.

7.7.1. Questions asked and rationale- general information

A series of questions were asked in order to gain background information about the participant, and determine if they knew much about security or risky behaviours. Table 18 shows the questions asked, and the rationale behind asking the question. In this research project, questionnaires were chosen as opposed to interviews, as they granted the collection of quantitative data from the evaluation process, and allowed for objective analysis. Additionally, they allowed data to be collected from a larger range of participants in a shorter timescale.

Table 18 - general information questions and rationale

Question asked	Reason
What number of USB stick did you receive?	Verify the type of experiment took part in- which type of affective feedback, or if they were in the control group.
What was your user ID?	Link questionnaire to log.
What course of study are you on?	For general information.
What year of study are you in?	For general information.
What age category are you in?	With age, yellow pigments accumulate in the lens of the eye, causing it to absorb more blue light (Salvi, Akhtar and Currie 2006). Age has been asked in the questionnaire to determine if this yellowing has an impact on security warnings.
How would you rate your knowledge of computer security?	Gain a general idea of how the knowledgeable the user thinks they are regarding security.
Were you connected to a public wi-fi network when you participated in the experiments?	Milne, Labreque and Cromer (2009) determines using public wi-fi can be a risky security behaviour. As such this question was included to make users consider the type of connection used.
Did you reveal any personal information about yourself online during the experiment?	Again, Milne, Labreque and Cromer (2009) notes this is a risky security behaviour. This answer can be compared against user logs.
Are you colourblind?	Similar to issues with aging (Salvi, Akhtar and Currie 2006), colourblindness has an impact on the delivery of colour. This was asked to assess if it impacted colour-based affective feedback.
Did you enter a private email address into Firefox during the study?	Milne, Labreque and Cromer (2009) deems entering a private email address a risky security behaviour. Users answers can be compared against the logs.
If you logged into Facebook, did you use a password which can be found in a dictionary?	Milne, Labreque and Cromer (2009) deems using a common password a risky security behaviour. User answers can be compared against log files.

If you logged into Facebook, did you use a password containing personal details such as mother's maiden name or the name of a pet?	Milne, Labreque and Cromer (2009) deems a password containing personal details as a risky security behaviour. User answers can be compared against log files.
Did you visit any malicious websites?	User answers can be compared against the log files.
Did you click on any malicious links?	User answers can be compared against the log files. Similar question to above.
Did you notice any of the built-in browser warnings?	Assess if the user noticed any of the warnings in Firefox, opposed to those included with the affective feedback delivery system.

7.7.2. Questions asked and rationale- feedback

The second part of the questionnaire, asked participants questions specifically relating to the additional affective feedback they may or may not have been shown during the course of the experimental process. Table 19 shows each of the questions and a rationale behind asking the question.

Table 19 - feedback questions and rationale

Question asked	Reason
Did you receive any on-screen feedback during the experiments?	Observe if user noticed affective feedback delivered. Not evaluated- used to jog participant's memory.
If you received feedback, what type of feedback did you receive?	Observe if user noticed the type of affective feedback delivered.
If you received multiple types of feedback, which type had the biggest impact?	Observe which type of feedback had the biggest impact on the user, if they received multiple modes of affective feedback.
Did you receive any password-related feedback?	Observe if user received feedback related to passwords. Not evaluated- used to jog participant's memory.
If you received negative password-related feedback, did it make you consider changing your Facebook password?	If user received password feedback, did it have an impact on their reasoning, or security behaviour?
Did you receive any social media-related feedback?	Observe if user received any feedback relating to social media sites visited. Not evaluated- used to jog participant's memory.
If you received social media-related feedback, did it make you consider the information you share online?	If user feedback about social media sites, did it have an impact on their reasoning, or security behaviour?

Did you receive any feedback about potentially malicious links on a page?	Observe if user received any feedback relating to malicious links on a page. Not evaluated- used to jog participant's memory.
Did you receive any feedback about visiting a malicious page?	Observe if user received any feedback relating to a malicious page visited. Not evaluated- used to jog participant's memory.
If you received feedback about malicious links on a page, did it make you consider which links you were clicking on?	If user feedback about malicious links, did it have an impact on their reasoning, or security behaviour?
Did the feedback make you hesitate to provide information online?	Did feedback provided have an impact on their state or what they were thinking about their security behaviour?
Did the feedback clearly highlight any issues with the page?	Did feedback provided clearly highlight potential issues on the pages on which it was triggered.
Do you think the feedback provided helped to increase your security awareness?	Did feedback increase the security awareness of the end user?
Did you find the feedback useful?	Was the affective feedback provided useful and informative?
Did the feedback encourage you to learn more about online security?	Did the affective feedback encourage the user to think about learning about security in the future?
Any other comments about the extension?	Free-form question to gauge general opinions about the affective feedback system.

7.7.3. Questionnaire vs. the log files

A vast quantity of data was recorded for each of the participants who agree to take part in the experimental process. The monitoring solution stores user input to assess risky security behaviour, and also generates a log file for each of the users, based on a unique ID. This unique ID was also copied over to the questionnaire which each participant complete. The use of a logging process similar to (Fenstermacher and Ginsburg 2002) along with the use of a questionnaire means it is possible to check the answers participants gave in the questionnaire against the actual actions undertaken during the browser-based portion of the experiment by comparing log files, database entries and questionnaires.

7.7.4. Use of Likert scales

The questionnaire made use of questions with possible answers which translate to the requisite points on a Likert scale. The purpose behind the utilising Likert scale data was to produce quantitative, measurable results.

The research study opted to employ use of Likert scales due to similar approaches found in multiple studies pertaining to affective research. Such studies which have used a similar approach include those by Abeyratna et al. (2010), who utilised affective feedback and Likert scales in order to understand feedback received from customers. Hernandez et al. (2014) have also used Likert scales when investigating how computer users felt. In particular, this study specifically used them to detect and recognise when computer users were stressed. Finally, Lottridge, Chignell and Jovicic (2011) highlight the use of Likert scales when designing for affective interaction, and understanding human emotions. Owing to the multiple papers which use Likert scales to measure users' perception in affective interaction, a similar approach was taken for this research project.

7.8. Analysis of information gathered

7.8.1. Assimilating information

The data from the questionnaires and logs were gathered into one location to make the analysis straightforward. To this effect, all questionnaire data was entered into a MySQL database. Logs were also parsed and information pertaining to the triggers were stored in another MySQL database. This allows questionnaire data to be compared against the log files e.g. check what participants said they did vs. what they actually did. By utilising the PHPMyAdmin interface, MySQL queries were run to extract the appropriate data.

7.8.2. Statistical analysis

Statistical analysis was carried out on the results. The analysis methods chosen are largely dependent on the normality of the data gathered during experiments. Methods used are outlined throughout Chapter 8.

7.9. Methodology summary

This chapter has discussed the methodology and strategy behind the evaluation process, detailing the types of participants involved, how participants interact with the affective feedback system, and the delivery of the evaluation system. Additionally, the design of the questionnaire has been discussed, providing a detailed justification as to why each of the questions were chosen for inclusion in the experiment. The design has attempted to follow the precedents set by other studies which have looked into the role of affective feedback, with the use of quantitative data produced from Likert scales. In combination with the log files from each of the experiments, comprehensive results will be shown, comparing how users thought they performed vs. how they actually performed.

The following chapter will present the results gained from the experimental process, and these will be analysed in the discussion chapter.

Chapter 8. Results

This section will detail the results of the experimental process. Initially, bar charts are used to visualise data, looking at the basic figures obtained as a result of the questionnaire. The results are then analysed via descriptive statistical in 3 key ways, before conclusions are drawn:

- log files from the monitoring solution are compared with data from the questionnaire
- log files from the control group are compared with log files from each of the groups from the experiments which delivered affective feedback
- questionnaire results from the control group are compared with questionnaire results from each of the groups from the experiments which delivered affective feedback

By analysing data in multiple ways, the results seek to determine:

- users' awareness of risky security behaviours i.e. do the log files reflect what users said they did in the questionnaires
- if affective feedback provided had an impact on the data recorded in the log files
- if affective feedback had an impact on the end-users, and their subsequent behaviour

8.1. Pilot study

Initially, a pilot study was conducted, to ensure the experimental process ran smoothly, and that the logging processes captured data appropriately, owing to the complexity of the system, and the reliance on the back-end servers. In addition to this, there was a need to ensure multiple users could run the system at the same time, identifying any preliminary problems.

10 participants were recruited for the small pilot study. Since no issues were reported with the system, and no changes needed to be made to the experimental design, the results of the pilot study were simply included as part of the larger result set, which included 72 participants.

8.2. General information section of the questionnaire

This section presents the raw data gained from the general information section of the questionnaire. The result of each question is displayed as a bar chart to reflect answers.

8.2.1. Experiments and participants

Data shown in Figure 50**Error! Reference source not found.** reflects how many people took part in each of the 5 available experiments. Care was taken to ensure each of the experimental groups were approximately the same size. Experiment groups were independent i.e. no single participant took part in multiple different experiments.

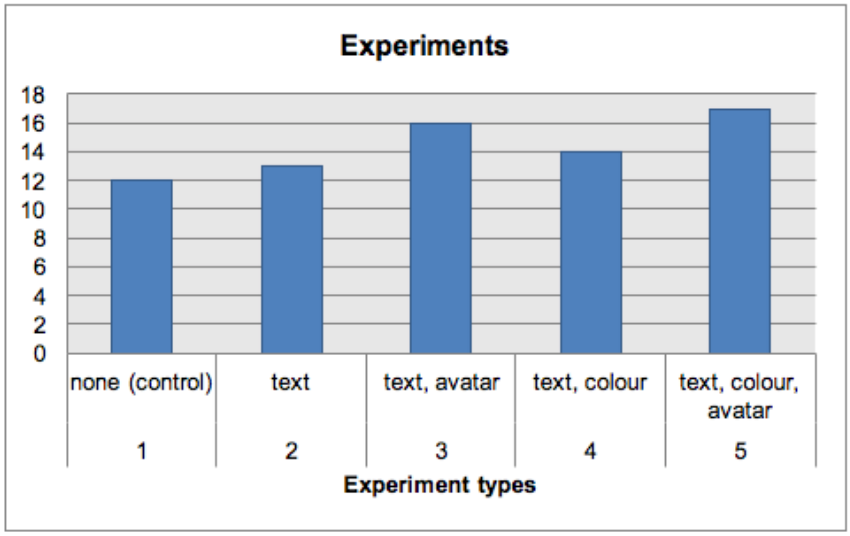


Figure 50 - participants in each experiment

8.2.2. Course of study are you on/year

During the experiments, participants were asked which course they were studying at university, if this was applicable. Asking this question provided a general indication of the level of computing knowledge a participant may possess. Figure 51 highlights many participants have some level of computing knowledge.

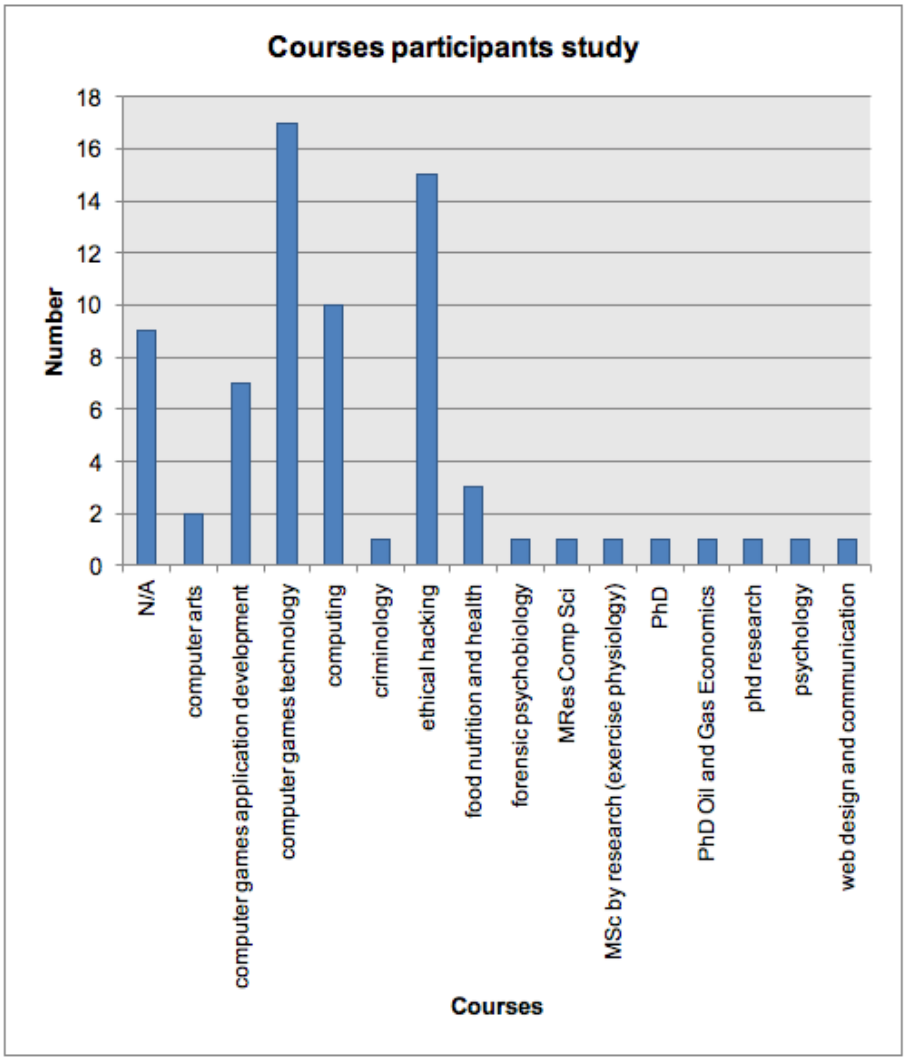


Figure 51 - courses participants are enrolled on

8.2.3. Age categories

The age range of the participant was asked in order to determine if colour-based affective feedback had a differing impact on older users owing to the yellowing of the eye lens with age. Figure 52 shows that the majority of participants were in the 18-34 years old ranges, meaning there was insufficient data to assess the relationship between age and the impact of colour-based affective feedback.

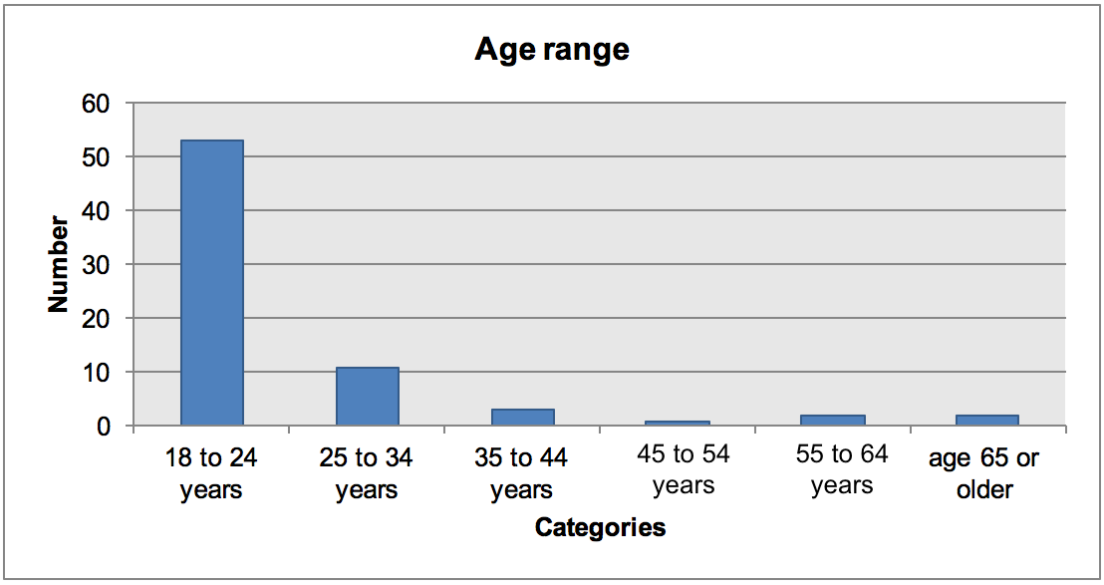


Figure 52 - age range of participants

8.2.4. Knowledge of computer security

Participants were asked to rate their own knowledge of computer security to gather an overall opinion. Figure 53 reflects that most participants thought they had an average or very good knowledge of security.

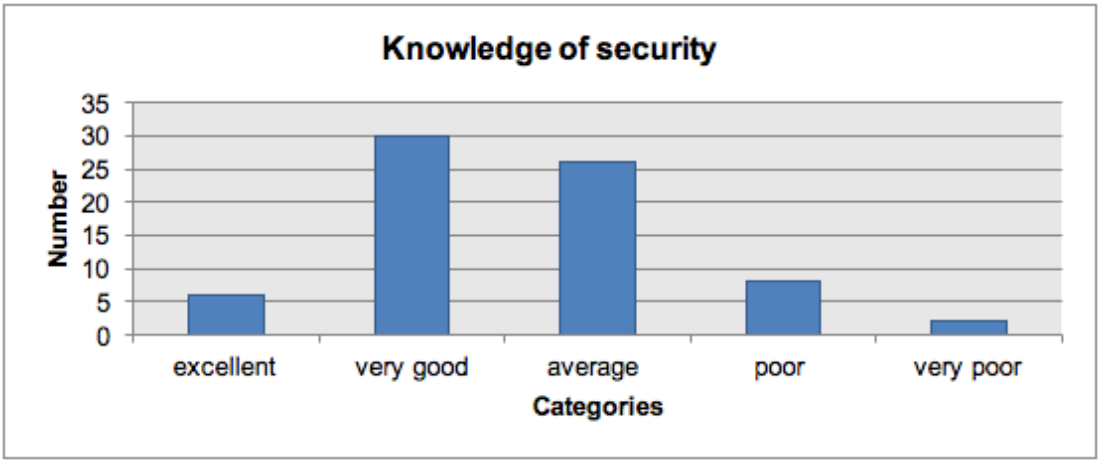


Figure 53 - participants knowledge of security

8.2.5. Public wi-fi network

Participants were asked if they used a public Wi-Fi network during the experimental process (in reality only Eduroam or a home network was used for each experiment). Figure 54 reflects that most participants answered correctly however many were unsure or erroneously said “yes”, perhaps highlighting a gap in security knowledge.

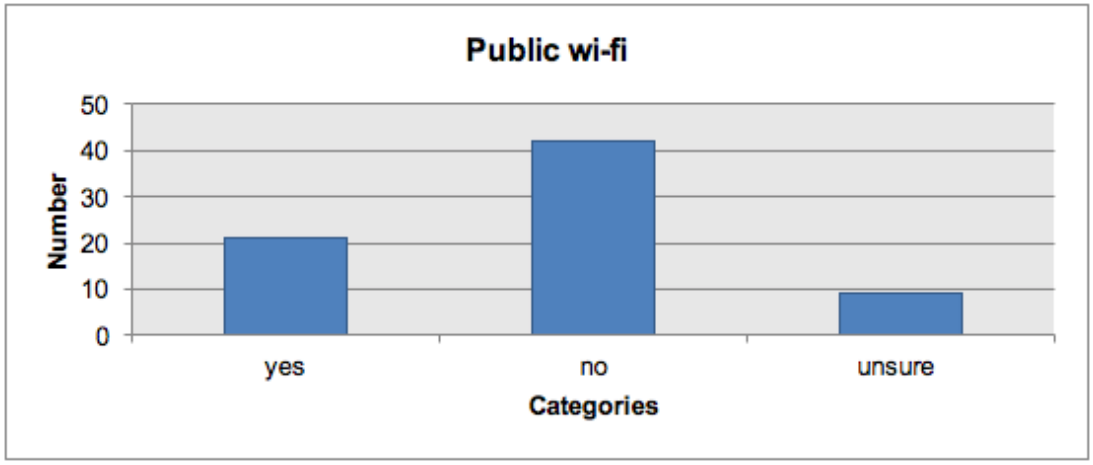


Figure 54 - wi-fi used

8.2.6. Revealing personal information

Figure 55 displays the answers participants gave when asked if they provided any personal information during the experimental process. In this scenario, the majority of participants openly admitted to revealing information about themselves online, even though it was voluntary part of the experiment.

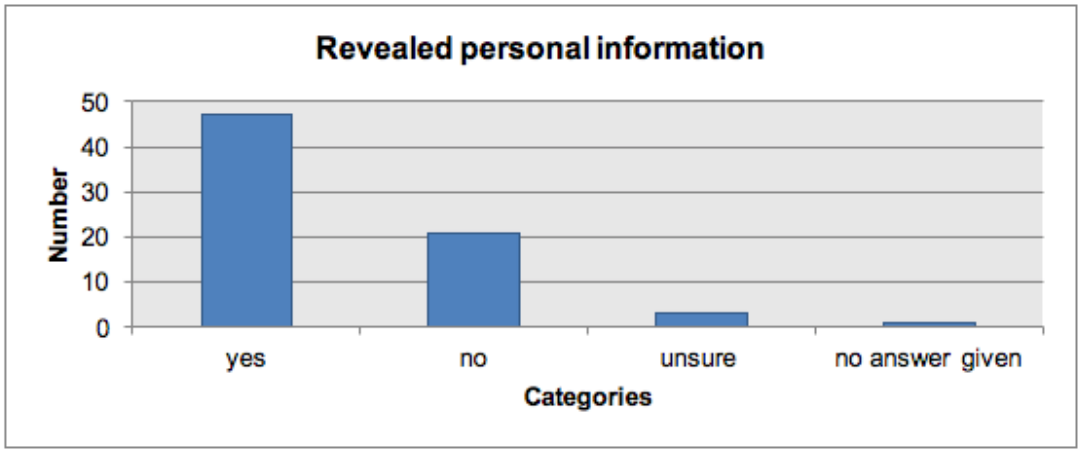


Figure 55 - participants who revealed personal information

8.2.7. Colour-blind participants

The impact of certain pieces of affective feedback such as colour-based feedback may have had a differing effect on participants who were colour-blind. Figure 56 highlights overwhelmingly that the majority of experiment participants were not colour-blind, therefore the numbers are too low to assess the relationship between colour-blindness and colour-based affective feedback. It should be acknowledged that some people may be unaware that they are colour-blind, and simply asking participants may not reflect an accurate result.

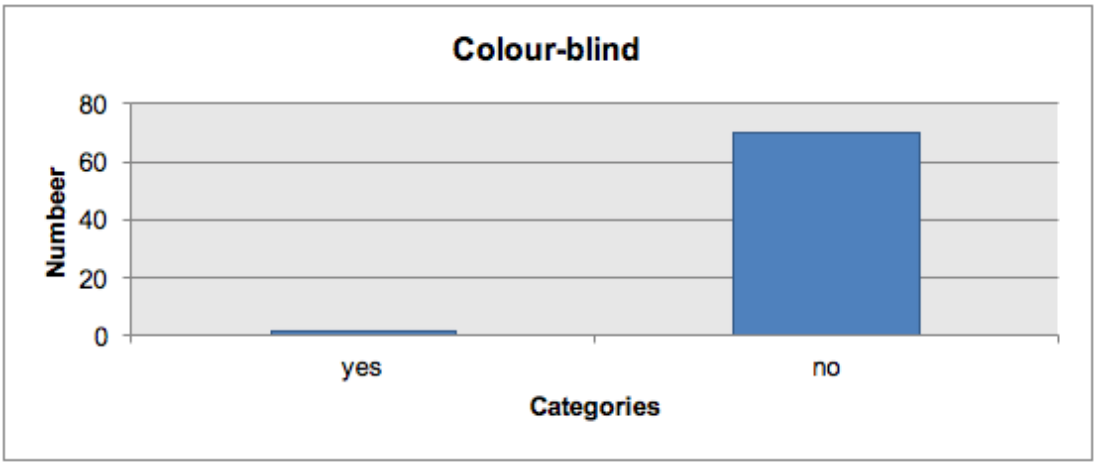


Figure 56 - colour-blind participants

8.2.8. Used a private email address

Participants were asked if they had entered a private email address during the experimental process. What is classed as a private email address is highly subjective (e.g. some people may consider their work email address to be public, whereas they may consider a Gmail address which they use for online shopping to be private) however, the majority of participants admitted to entering an email address, as displayed in Figure 57.

Figure 57 - participants who entered a private email address

8.2.9. Entered a dictionary password

When asked if participants entered a dictionary password during the experiments, the majority said “no”, as reflected by Figure 58.

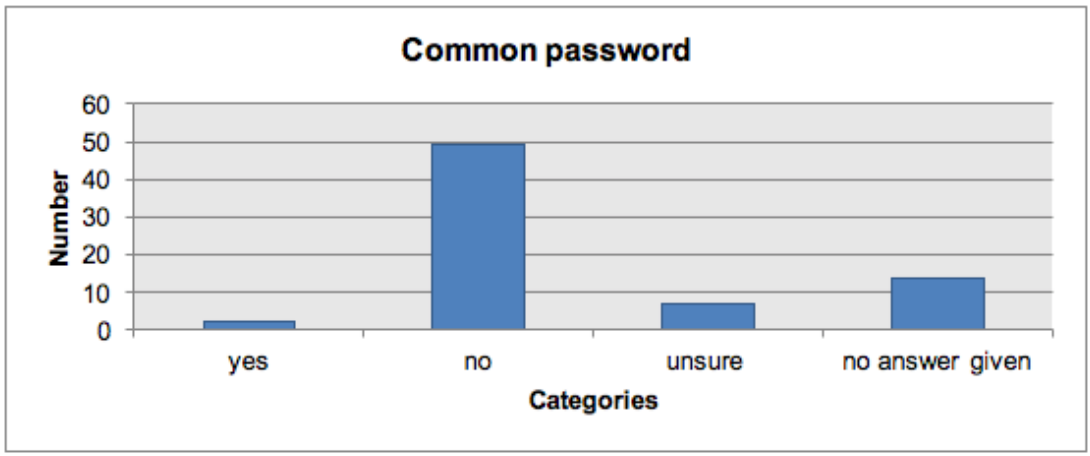


Figure 58 - participants who entered a dictionary password

8.2.10. Entered password containing personal details

When asked if participants included personal details in their passwords during the experiments, the majority said “no”, as reflected by Figure 59.

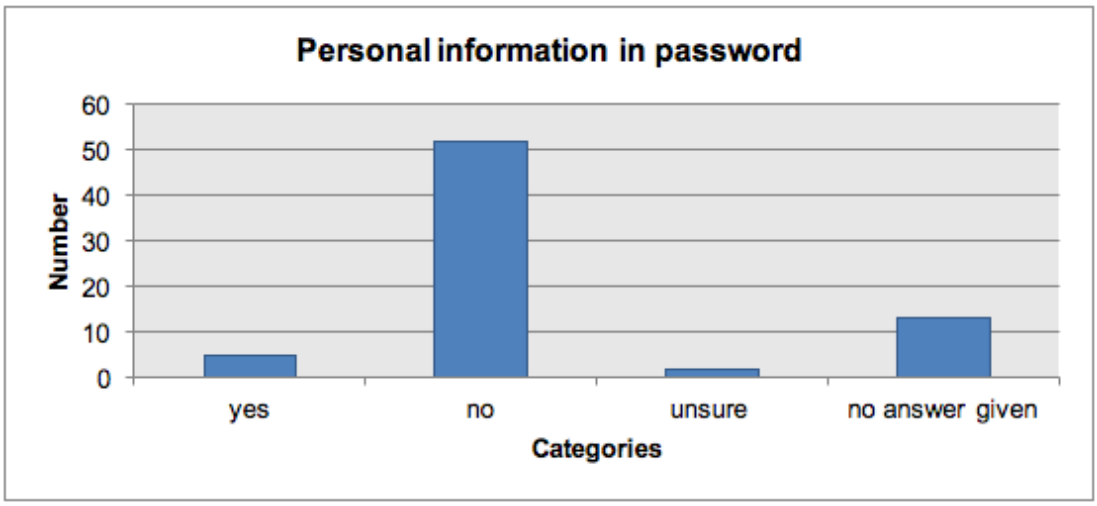


Figure 59 - participants and personal details in passwords

8.2.11. Visiting malicious websites

When asked if participants had visited malicious sites during the experiments, the majority said “no”, as reflected by Figure 60.

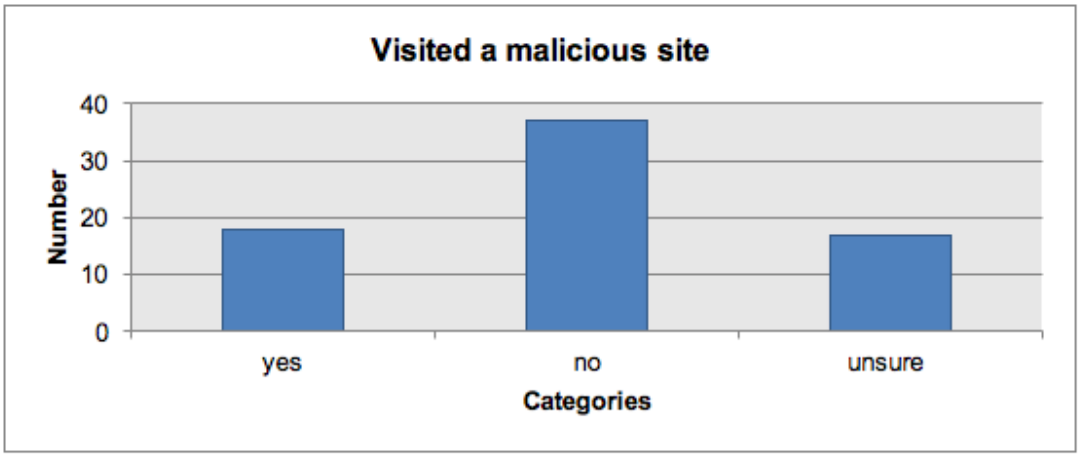


Figure 60 - participants who visited malicious sites

8.2.12. Click on any malicious links

When asked if participants had clicked on a malicious link during the experiments, the majority said “no”, as reflected by Figure 61.

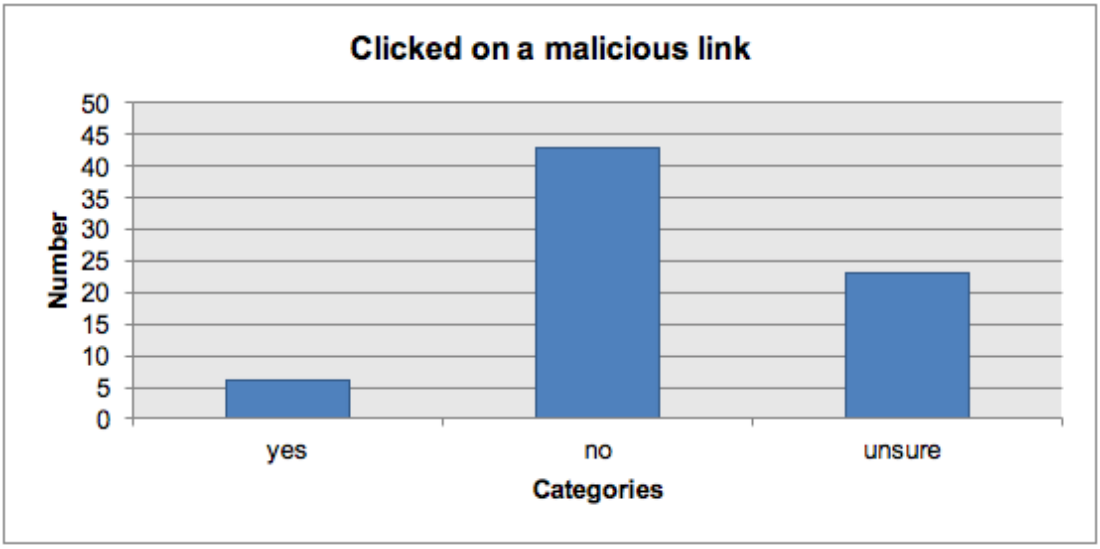


Figure 61 - participants who clicked on a malicious link

8.2.13. Built-in browser warnings

When asked if participants noticed standard built-in browser warnings during the experiments, the majority said “yes”, as reflected by Figure 62.

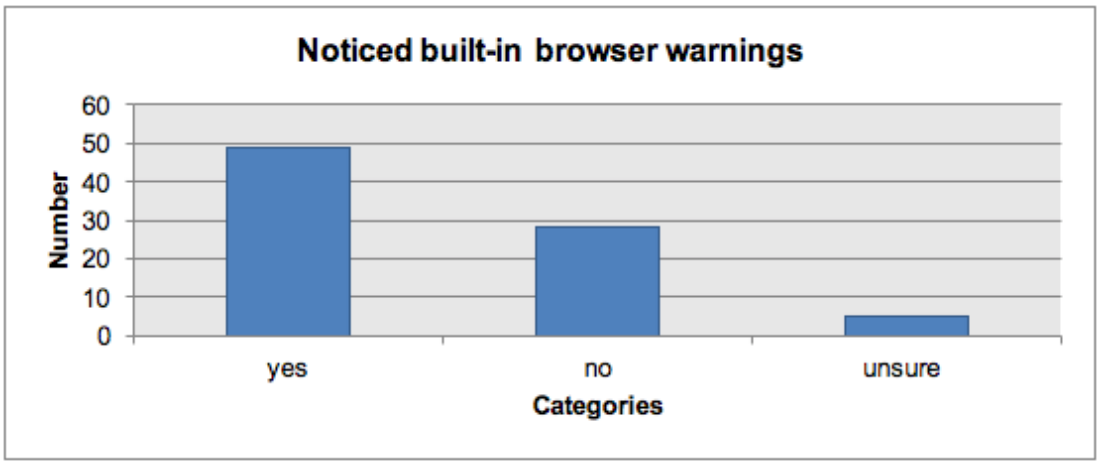


Figure 62 - participants who noticed browser warnings

8.3. Feedback section of the questionnaire

This section presents the raw data gained from the feedback section of the questionnaire. The result of each question is displayed as a bar chart to reflect answers.

8.3.1. Received on-screen feedback

When participants were asked if they had received on-screen feedback during the experiments, the majority of responses stated "yes", as shown in Figure 63.

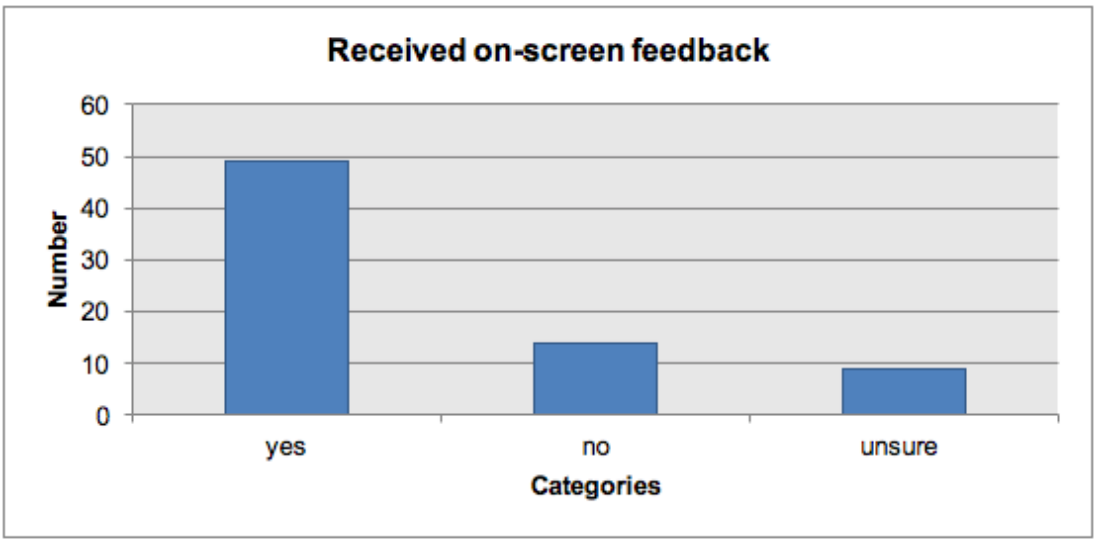


Figure 63 - participants who received on-screen feedback

8.3.2. Feedback type received

When participants were asked about the type of feedback they received during the experiments, the majority of responses said colour and text, with text alone coming in second place (Figure 64). In comparison, Figure 65 shows the actual feedback participants received. In this case, text is shown to have the highest level, as 4 out of the 5 extensions created utilised some form of text-based feedback i.e. 60 of the 72 participants received text-based feedback. The figure also illustrates occurrences of participants receiving text-based feedback when it was grouped with another feedback agent e.g. colours or an avatar.

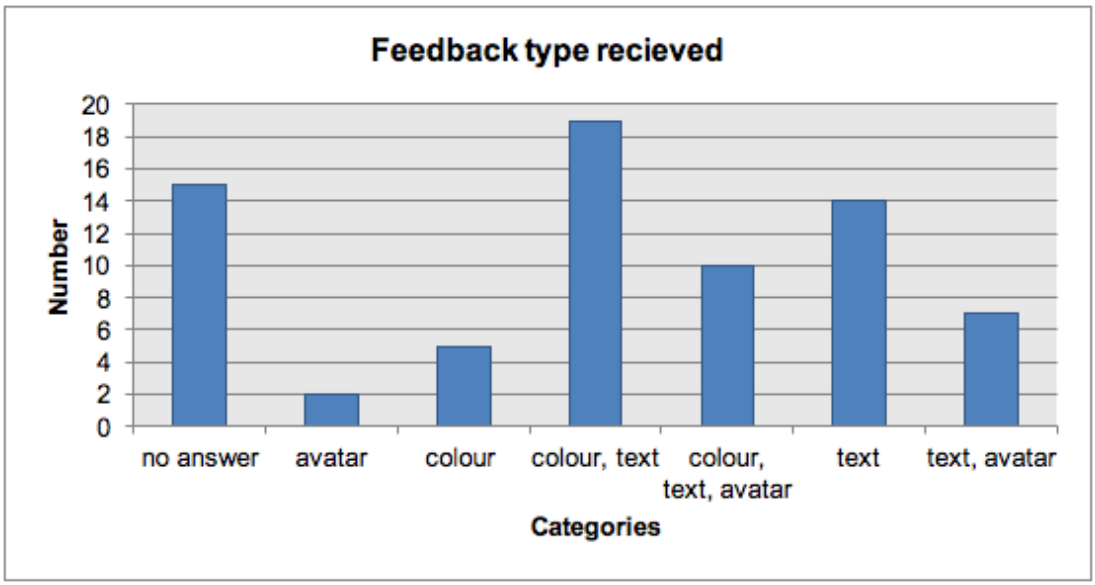


Figure 64 - feedback type received

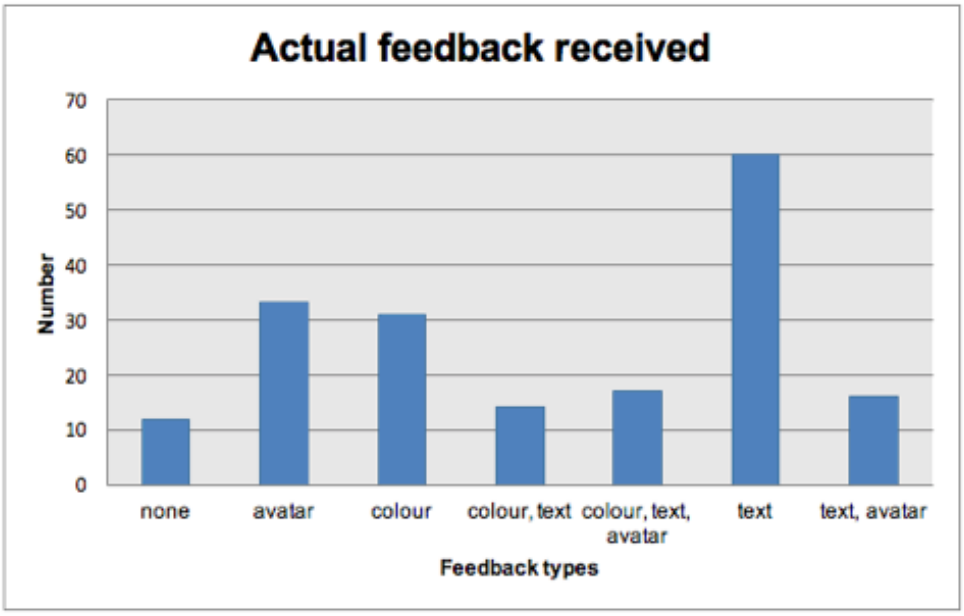


Figure 65 - actual feedback type received by participants

8.3.3. Feedback with biggest impact

When asked what type of feedback had the biggest impact on participants, those who answered the question stated colour had the largest impact, followed by text (Figure 66).

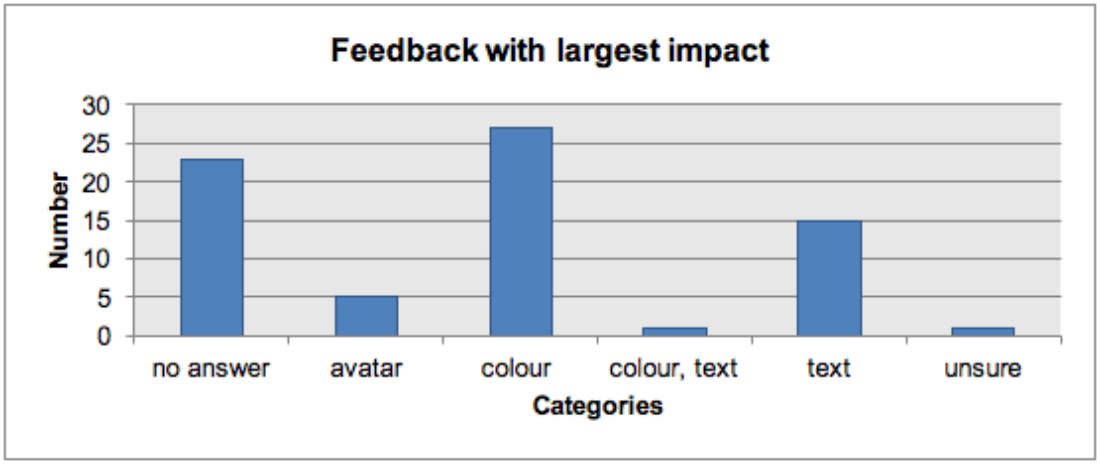


Figure 66 - feedback with the largest impact on participants

8.3.4. Password-related feedback

Participants were asked if they received password feedback during the experimental process: the majority of respondents said "yes" (Figure 67).

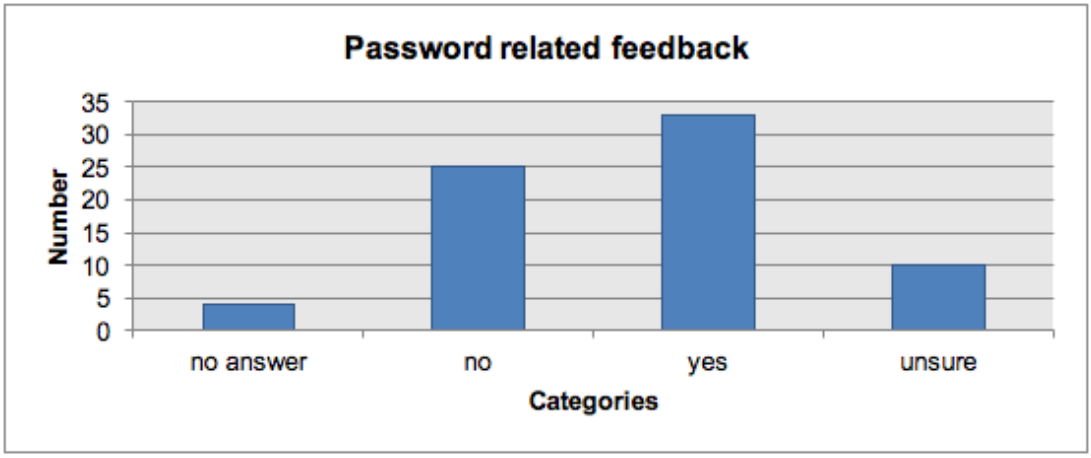


Figure 67 - participants who received password feedback

8.3.5. Changing Facebook password

Participants were asked if password feedback received made them consider changing their Facebook password. Those that answered the question largely agreed that it made that consider changing their password (Figure 68).

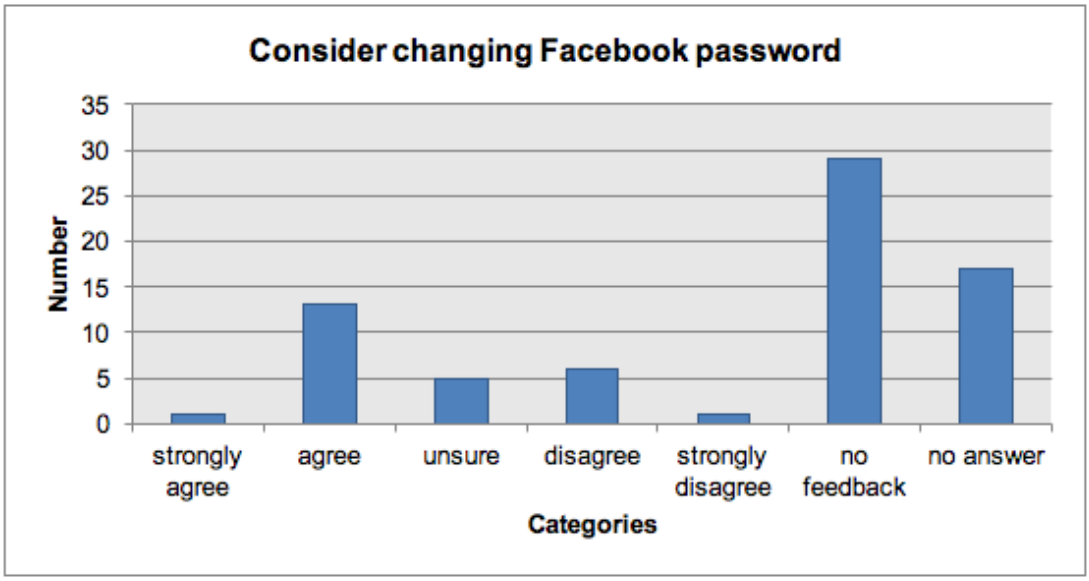


Figure 68 - participants who considered changing their password

8.3.6. Social media-related feedback

Participants were asked if they received social-media feedback during the experimental process: the majority of respondents said "no" (Figure 69).

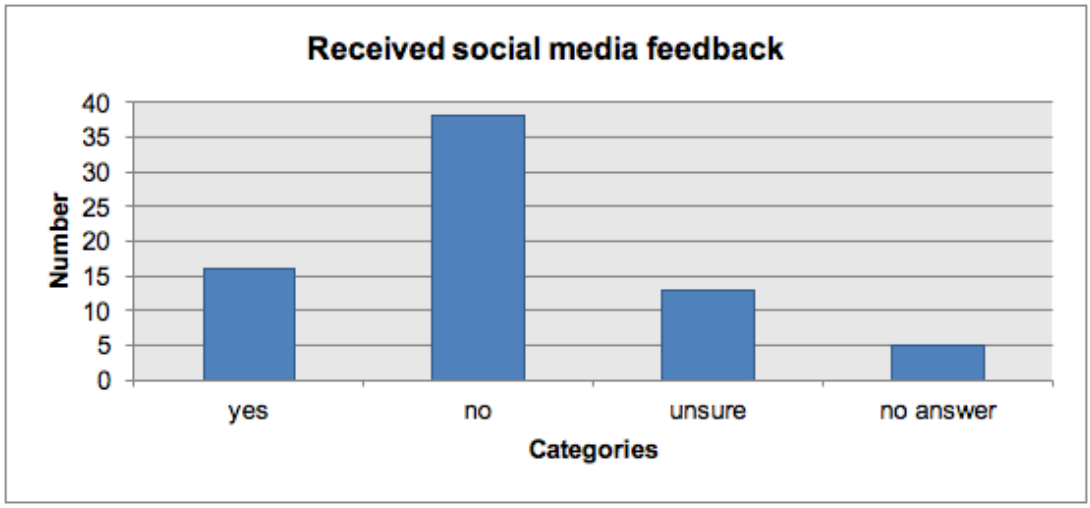


Figure 69 - participants who received social-media feedback

8.3.7. Consider information shared

Participants were asked if the social-media feedback received made them consider the information which they shared online. Those that answered the question were unsure in this scenario (Figure 70).

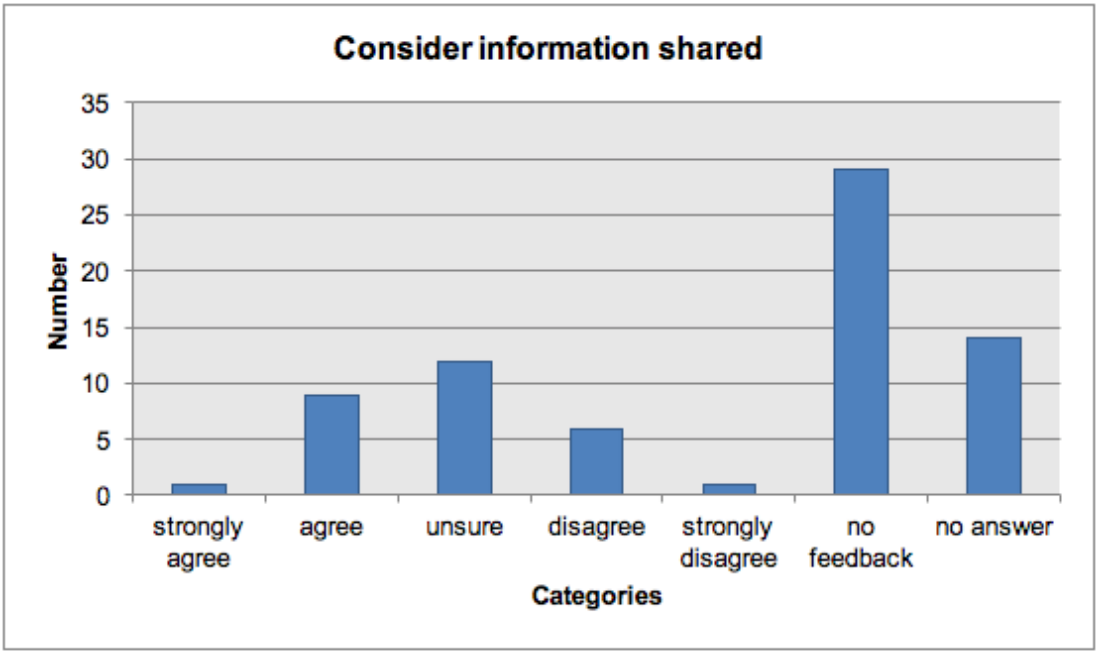


Figure 70 - participants and consideration of information shared

8.3.8. Malicious link feedback

Participants were asked if they received feedback about malicious links during the experimental process: the majority of respondents said "yes" (Figure 71).

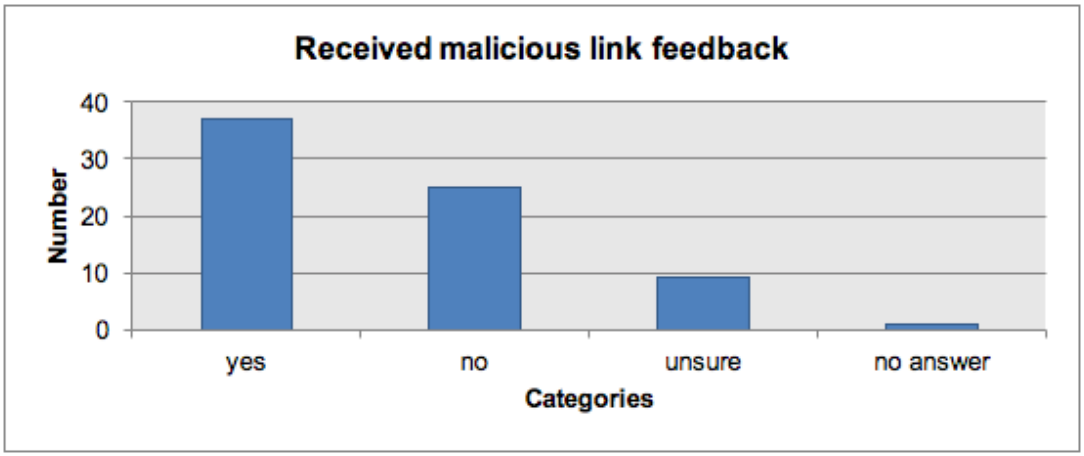


Figure 71 - participants who received malicious link feedback

8.3.9. Malicious page feedback

Participants were asked if they received feedback about malicious sites during the experimental process: the majority of respondents said "no" (Figure 72).

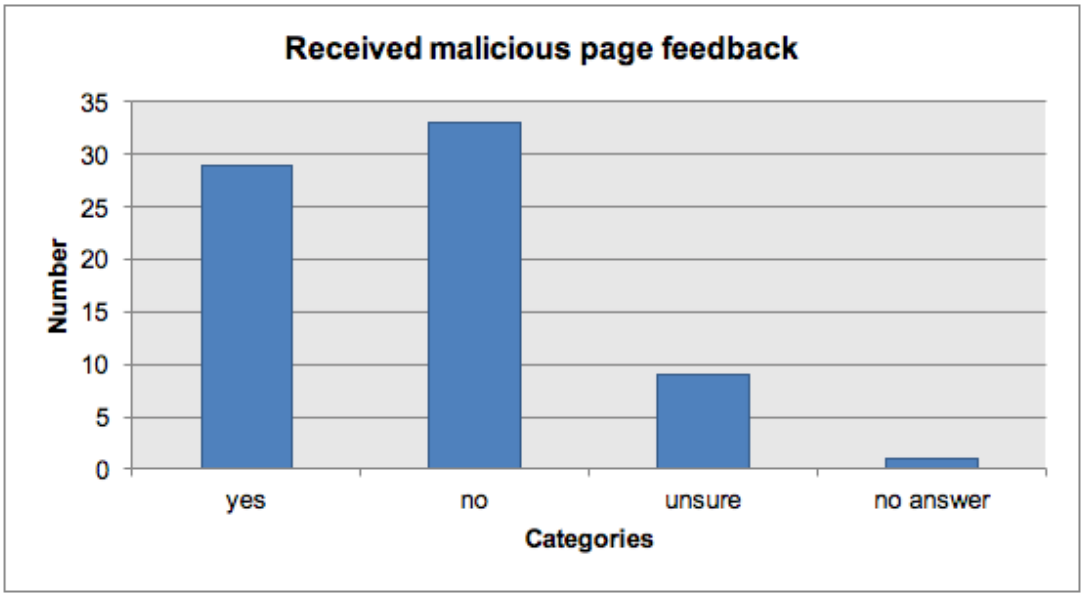


Figure 72 - participants who received feedback about malicious sites

8.3.10. Clicking on links

When asked if feedback provided made participants consider links they were clicking on, the majority answered "agree" (Figure 73).

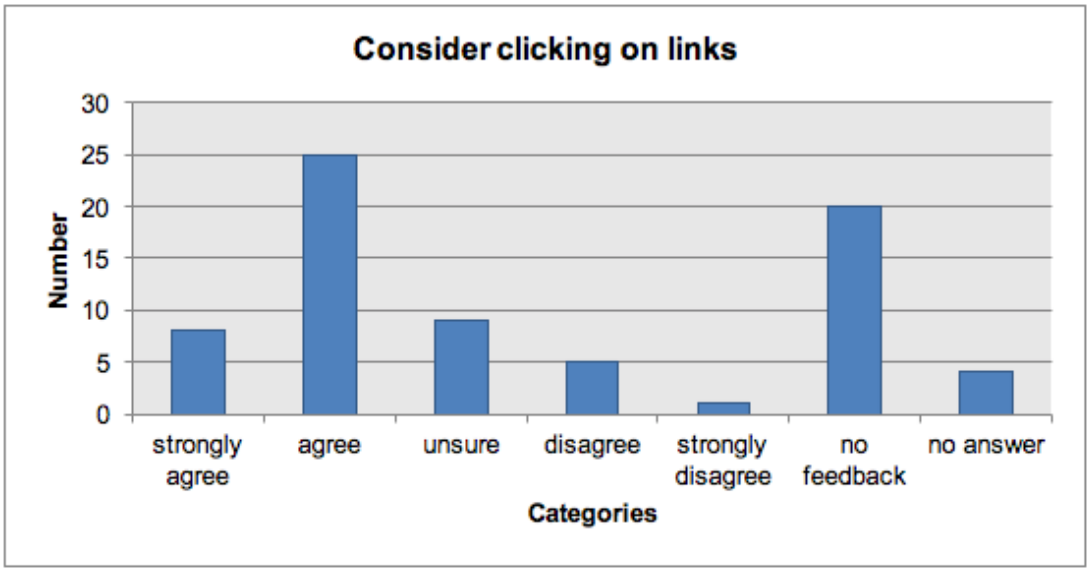


Figure 73 - participants who said feedback made them consider clicking on links

8.3.11. Hesitation to provide information

When asked if feedback provided made participants hesitate to provide information online, the majority agreed the feedback made them hesitate (Figure 74).

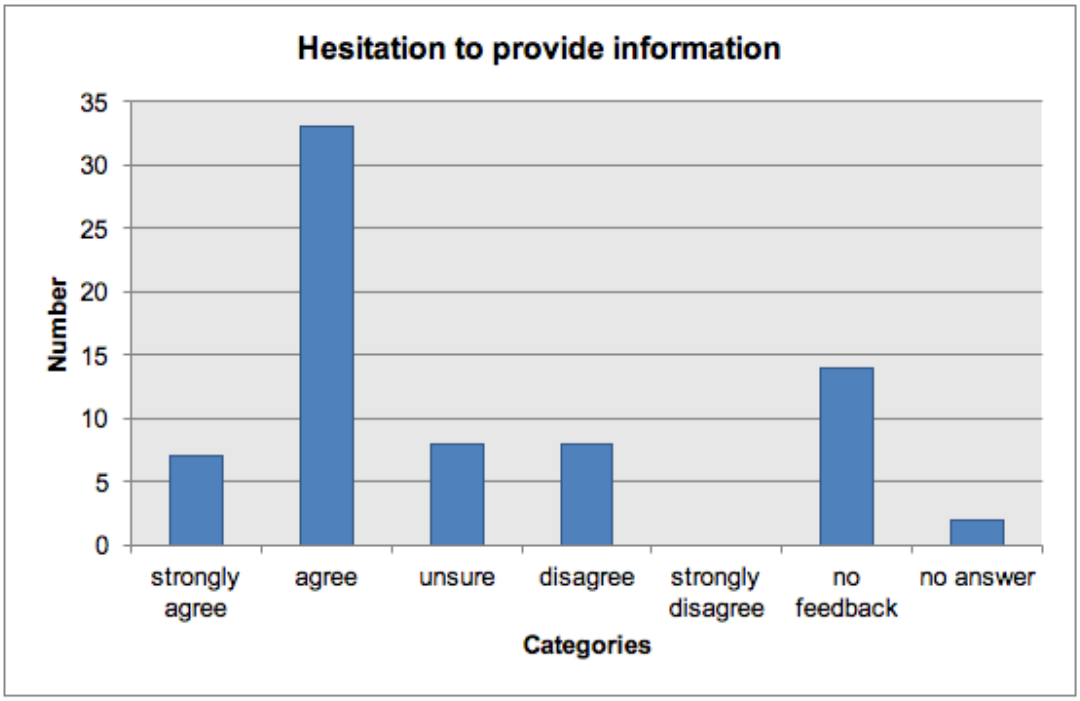


Figure 74 - did feedback make participants hesitate to provide information?

8.3.12. Highlighting issues on page

When asked if feedback provided clearly highlighted issues on a particular web page, the majority of participants agreed (Figure 75).

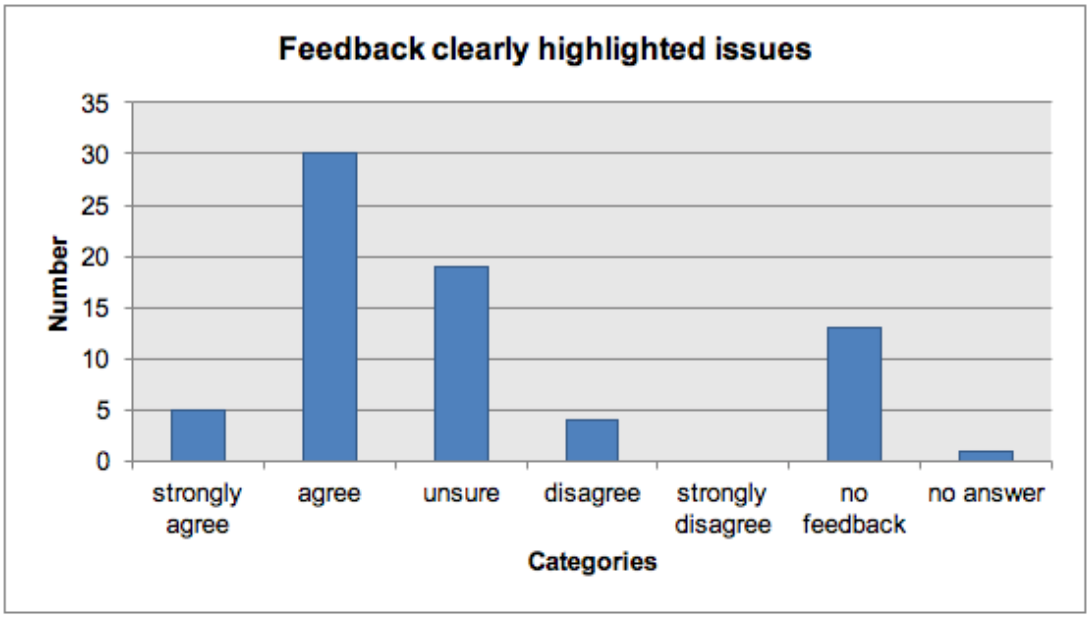


Figure 75 - did feedback clearly highlight page issues?

8.3.13. Security awareness

When asked if feedback provided increased the security awareness of participants, the majority of them agreed it did (Figure 76).

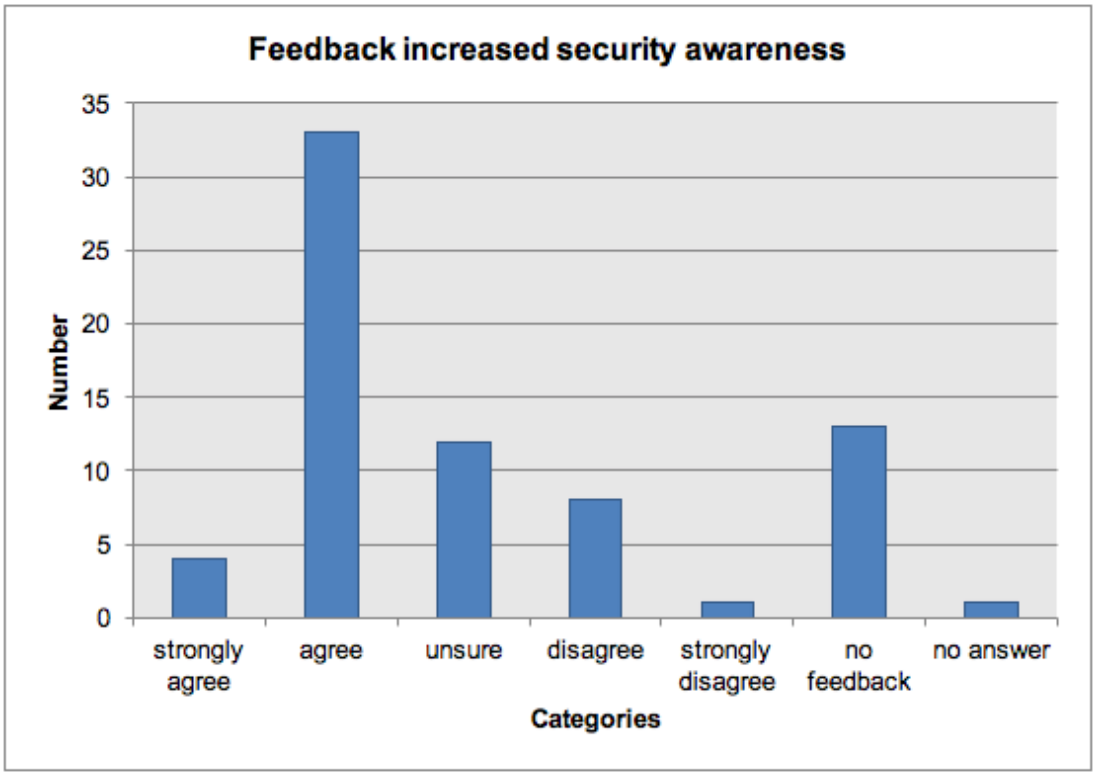


Figure 76 - did feedback increase security awareness?

8.3.14. Useful feedback

When asked if feedback provided was useful, the majority of participants agreed it was useful (Figure 77).

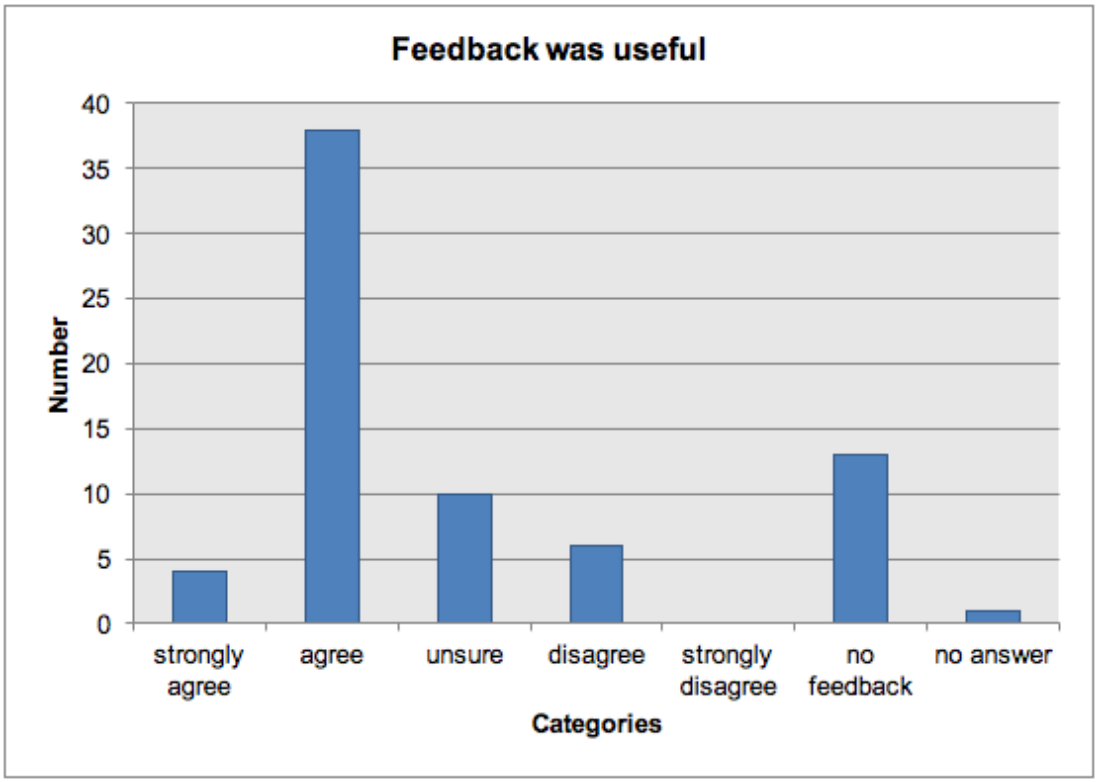


Figure 77 - was feedback useful?

8.3.15. Learning more about security

When asked if feedback provided encouraged participants to learn more about security, the majority of them agreed that it encouraged them to learn more (Figure 78).

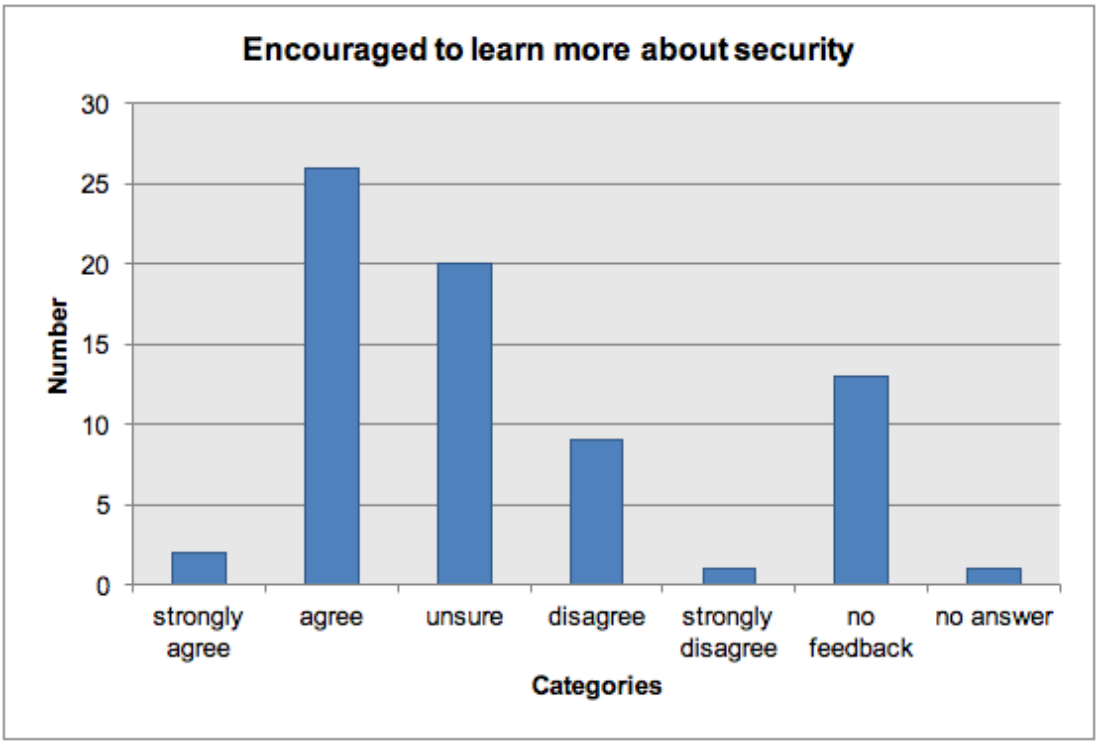


Figure 78 - did feedback encourage participants to learn more about security?

8.4. Diverging bar charts for feedback questions

Diverging bar charts have been created to show the spread of answers over the Likert scale more accurately for the following questions:

- If you received negative password-related feedback, did it make you consider changing your Facebook password?
- If you received social media-related feedback, did it make you consider the information you share online?
- If you received feedback about malicious links on a page, did it make you consider which links you were clicking on?
- Did the feedback make you hesitate to provide information online?
- Did the feedback clearly highlight any issues with the page?
- Do you think the feedback provided helped to increase your security awareness?
- Did you find the feedback useful?
- Did the feedback encourage you to learn more about online security?

Each of these bar charts can be found in Appendix (viii) - diverging bar charts based on Likert data.

8.5. Assessment of log data vs. questionnaire data

Information recorded by the monitoring solution in log files and database records made it possible to compare what users did during experiments against the answers they provided in the questionnaires. To this effect, 5 questions were analysed in detail. This section details the questions analysed, and the assumptions made with the data provided. Section 8.6. then goes on to discuss the statistical analysis methods used, before section **Error! Reference source not found.**states the results of the statistical analysis in comparing log files against questionnaire data.

8.5.1. Questions analysed in further detail

8.5.1.1. Did user reveal personal information?

In determining if the participant revealed personal information, at least one of the fields in the intial_form MySQL database had to contain a value

8.5.1.2. Did user enter email address?

In determining if the participant revealed a private email address, at least one of the fields in the other_site MySQL database had to contain a value.

8.5.1.3. Did user enter a common password?

This information was pulled from the unique log files generated by the monitoring solution.

8.5.1.4. Did user have personal details in password?

This information was pulled from the unique log files generated by the monitoring solution.

8.5.1.5. Did user visit a malicious site?

This information was pulled from the unique log files generated by the monitoring solution.

8.5.2. Comparison figures

Figure 79 provides an overview of what participants did in the log files and databases, generated by the monitoring solution in comparison with the answers participants gave in the questionnaire. The statistical significance of these figures will be discussed in **Error! Reference source not found.**

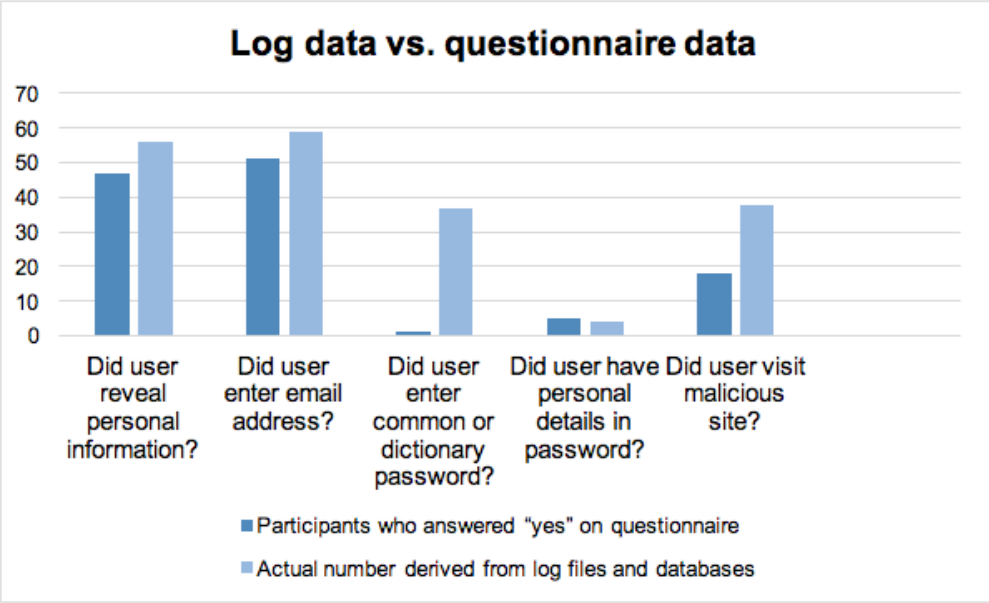


Figure 79 - log file and database results vs. questionnaire data

8.5.3. Breakdown of log comparison figures by feedback method

Graphs in this section provide an overview of what participants did in the log files and databases, generated by the monitoring solution, in comparison with the answers participants gave in the questionnaire. These figures are broken down by what was asked in the questionnaire. The statistical significance of these figures will be discussed in **Error! Reference source not found.**

Figure 80 shows the difference between participants who said they revealed personal information and the number who actually revealed personal information.

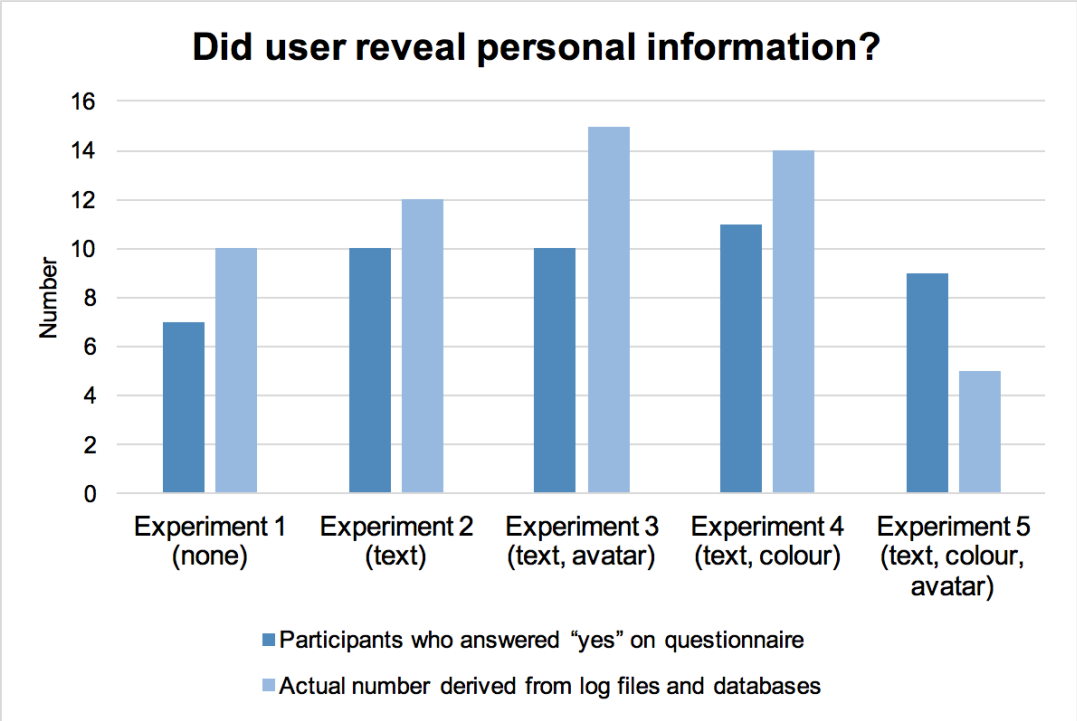


Figure 80 - difference between participants who said they revealed personal information and the number who actually revealed personal information

Figure 81 shows the difference between participants who said they entered an email address and the number who actually entered an email address.

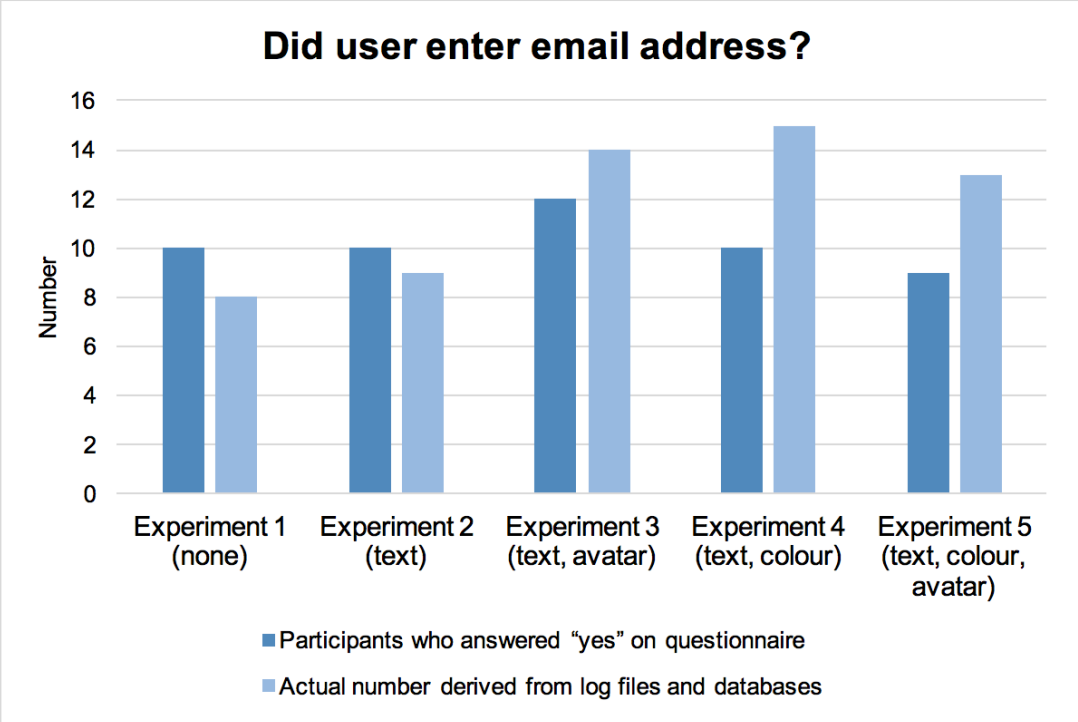


Figure 81 - difference between participants who said they entered an email address and the number who actually entered an email address

Figure 82 shows the difference between participants who said they entered a common/dictionary password and the number who actually entered a common/dictionary password.

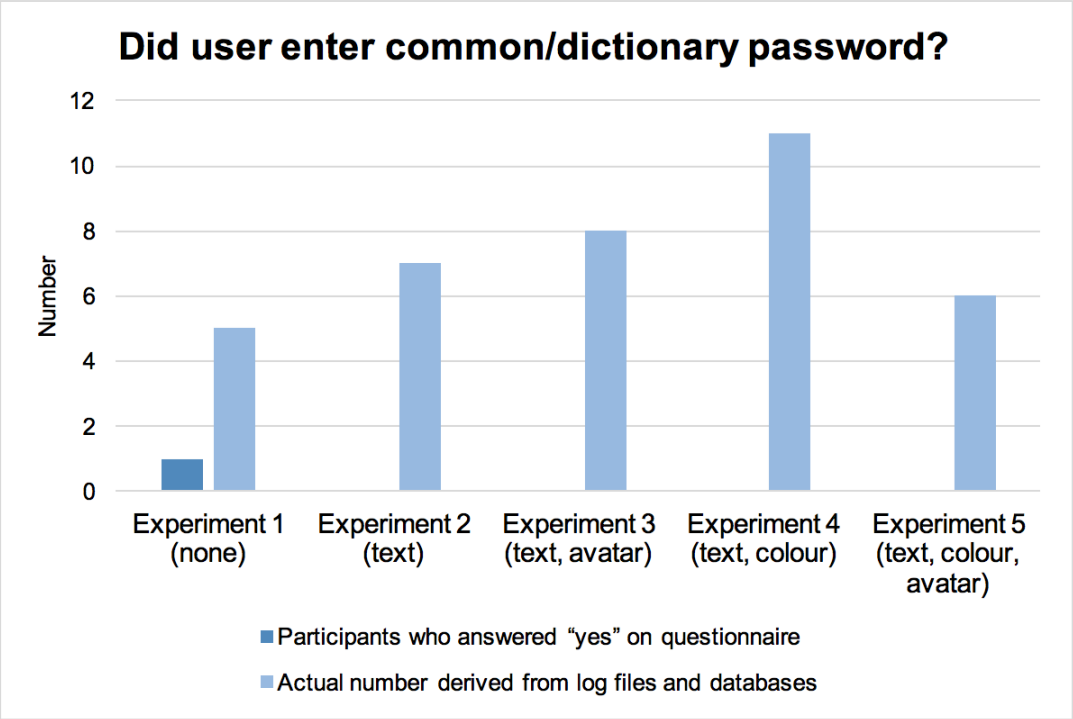


Figure 82 - difference between participants who said they entered a common/dictionary password and the number who actually entered a common/dictionary password

Figure 83 shows the difference between participants who said they revealed personal details in their password and the number who actually revealed personal details in their password.

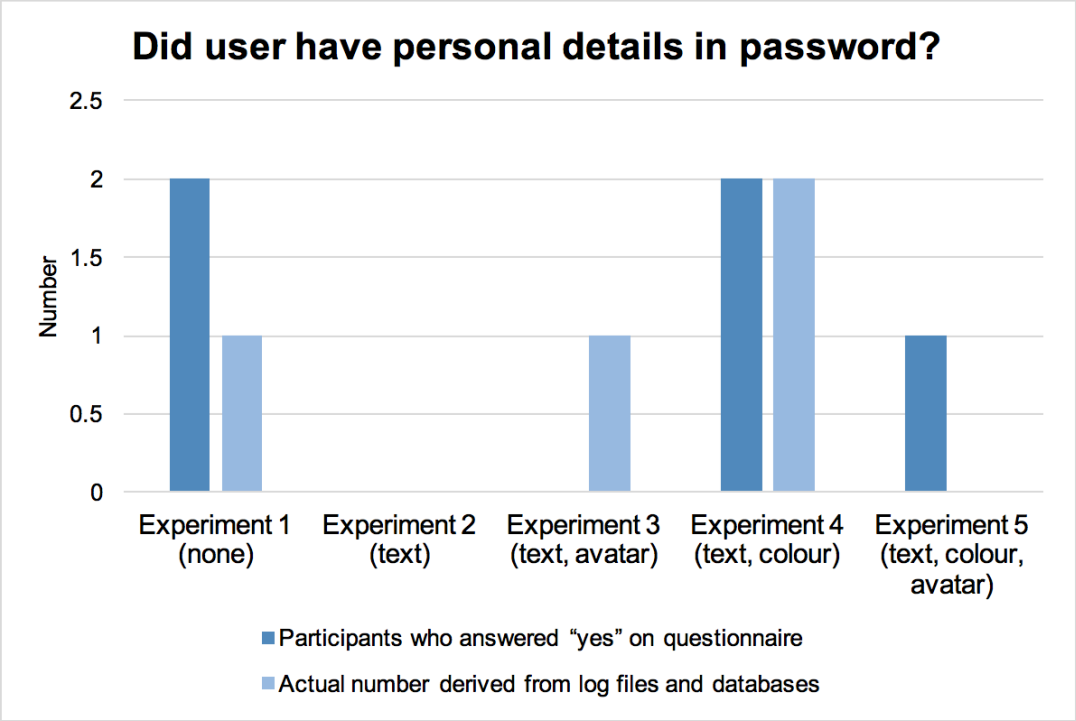


Figure 83 - difference between participants who said they revealed personal details in their password and the number who actually revealed personal details in their password

Figure 84 shows the difference between participants who said visited a malicious site and the number who actually visited a malicious site.

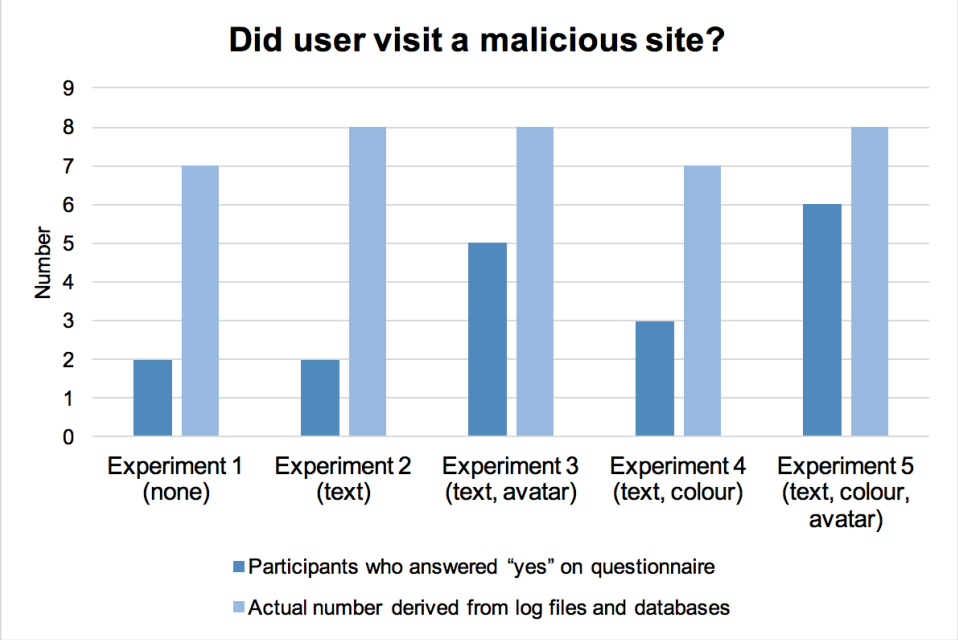


Figure 84 - difference between participants who said they visited a malicious site and the number who actually visited a malicious site

8.6. Assessment of log vs. questionnaire data- statistical tests

A number of statistical methods were used to analyse the data gained from the log files, databases and questionnaires.

In this instance, a binary comparison method was required i.e. in the questionnaires, participants who answered “yes” in comparison to participants who did not. Similarly, when parsing the log files and databases, a positive/yes result was searched for e.g. looking for users who revealed personal information about themselves in comparison to those who did not.

Due to the need for a binary comparison, the N-1 Two Proportion Test based upon the N-1 Chi-Square was utilised (Measuring Usability LLC 2016). In deriving statistical significance, the alpha p-value was set at 0.05 and a two-tailed test was used in a bid to detect an effect in either direction. Regarding the p-value, it is *“the probability of finding the observed, or more extreme, results when the null hypothesis (H 0) of a study question is true”* (Stats Direct 2016).

In the rare occasion where one of the counts falls below the value of 1, the Fisher Test is used, whilst still carrying out a binary comparison.

8.7. Comparing the log vs. questionnaire

This section details the statistical significance values between the log files and databases vs. the questionnaires. To achieve statistical significance, the p value needs to register as p≤ 0.05. Table 20 provides an overview of the results, showing which of the questions and experiment numbers raised a statistically significant result (difference between the log and the questionnaire). Section 8.7.1. onwards states the full results.

Table 20 - summary table of log data vs. questionnaire data results

Statistical significance: log and databases vs. questionnaire					
Question	**Experiment 1 (none)**	**Experiment 2 (text)**	**Experiment 3 (text, avatar)**	**Experiment 4 (text, colour)**	**Experiment 5 (text, colour, avatar)**
Did user reveal personal information?	Yes	No	Yes	No	No
Did user enter email address?	No	No	No	Yes	Yes
Did user enter a common password?	No	Yes	Yes	Yes	Yes
Did user have personal details in password?	No	No	No	No	No
Did user visit a malicious site?	Yes	Yes	No	No	No

The main difference highlighted is that when asked if they used a common password, participants largely said “no”. However, there is a significant statistical difference when the log files are viewed, indicating that many users did in fact have common elements in their passwords. The same difference is seen across all experiments containing affective feedback, suggesting it did not have an impact on the actions of users in this instance.

In terms of revealing personal information, there was a significantly higher number of participants who revealed personal information about themselves as per the databases vs. those who stated they revealed personal information in the questionnaire in experiments 1 and 3. This potentially highlights a lack of security awareness in end users who have not realised the information divulged. This could also explain the similar results for “Did user enter an email address?” in groups 4 and 5, and “Did user visit a malicious site?” in groups 1 and 2.

8.7.1. USB 1 Experiment- Control group

8.7.1.1. Did user reveal personal information?

When participants were asked if they revealed personal information during the course of the experiments, 58.3% of users said “yes” in the questionnaire. When the log files were examined, it was revealed all participants in the control group revealed some form of data.

The two-tailed p-value: was 0.0232859. This is $p \leq 0.05$ and therefore indicates a significant result.

Results of the chi-squared test also indicate there’s a 97.671% chance the proportions are different between the questionnaire data and the log file data, with a 98.836% chance the log data file contains a higher proportion.

8.7.1.2. Did user enter email address?

When participants were asked if they revealed a private email address during the course of the experiments, 83.3% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 80% of participants in the control group revealed an email address.

The two-tailed p-value: was 0.843669. $p > 0.05$ therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 15.633% chance the proportions are different between the questionnaire data and the log file data, with a 57.817% chance the questionnaire data contains a higher proportion.

8.7.1.3. Did user enter common/dictionary password?

When participants were asked if they entered a dictionary password during the course of the experiments, 8.3% of users said yes in the questionnaire. When the log files were examined, it was revealed 41.7% participants in the control group entered a commonly used password.

The two-tailed p-value: was 0.0649045. $p > 0.05$ and therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 93.51% chance the proportions are different between the questionnaire data and the log file data, with a 96.755% chance the log data file contains a higher proportion.

8.7.1.4. Did user have personal details in password?

When participants were asked if they included personal details in their passwords during the course of the experiments, 16.7% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 8.3% participants in the control group has personal details in their password.

The two-tailed p-value: was 0.5456987. $p > 0.05$ and therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 45.43% chance the proportions are different between the questionnaire data and the log file data, with a 72.715% chance the questionnaire data contains a higher proportion.

8.7.1.5. Did user visit malicious site?

When participants were asked if they visited a malicious site during the course of the experiments, 16.7% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 58.3% participants in the control group had visited a malicious site.

The two-tailed p-value: was 0.0390372. This is $p \leq 0.05$ and therefore indicates a significant result.

Results of the chi-squared test also indicate there’s a 96.096% chance the proportions are different between the questionnaire data and the log file data, with a 98.048% chance the log data file contains a higher proportion.

8.7.2. USB 2 Experiment- text-based feedback

8.7.2.1. Did user reveal personal information?

When participants were asked if they revealed personal information during the course of the experiments, 76.92% of users said “yes” in the questionnaire. When the log files were examined, it was revealed all participants in the text-based feedback group revealed data.

The two-tailed p-value: was 0.0821939. $p>0.05$ therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 91.781% chance the proportions are different between the questionnaire data and the log file data, with a 95.89% chance the log data file contains a higher proportion.

8.7.2.2. Did user enter email address?

When participants were asked if they revealed a private email address during the course of the experiments, 76.92% of users said yes in the questionnaire. When the log files were examined, it was revealed 69.23% of participants in the text-based feedback group revealed an email address.

The two-tailed p-value: was 0.6646114. $p>0.05$ therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 33.539% chance the proportions are different between the questionnaire data and the log file data, with a 66.769% chance the questionnaire data contains a higher proportion.

8.7.2.3. Did user enter common/dictionary password?

When participants were asked if they entered a dictionary password during the course of the experiments, 0% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 53.85% participants in the text-based feedback group entered a commonly used password.

The two-tailed p-value: was 0.0024061. $p \leq 0.05$ and therefore this indicates a significant result.

Results of the chi-squared test also indicate there’s a 99.7591% chance the proportions are different between the questionnaire data and the log file data, with a 99.88% chance the log data file contains a higher proportion.

8.7.2.4. Did user have personal details in password?

When participants were asked if they included personal details in their passwords during the course of the experiments, 0% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 0% participants in the text-based feedback group has personal details in their password. Owing to values equalling zero, Fisher Exact Test was utilised.

The two-tailed p-value: was 1. $p \geq 1$ and therefore this is not a significant result.

Results of test indicate there’s a 0% chance the proportions are different between the questionnaire data and the log file data, with a 0% chance the log data contains a higher proportion.

8.7.2.5. Did user visit malicious site?

When participants were asked if they visited a malicious site during the course of the experiments, 15.38% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 61.54% participants in the text-based feedback group had visited a malicious site.

The two-tailed p-value: was 0.0177061. This is $p \leq 0.05$ and therefore indicates a significant result.

Results of the chi-squared test also indicate there’s a 98.229% chance the proportions are different between the questionnaire data and the log file data, with a 99.115% chance the log data file contains a higher proportion.

8.7.3. USB 3 experiment- text, avatar-based feedback

8.7.3.1. Did user reveal personal information?

When participants were asked if they revealed personal information during the course of the experiments, 62.5% of users said “yes” in the questionnaire. When the log files were examined, it was revealed all participants in the text and avatar-based feedback group revealed some form of data.

The two-tailed p-value: was 0.0093746. $p \leq 0.05$ therefore this is a significant result.

Results of the chi-squared test also indicate there’s a 99.063% chance the proportions are different between the questionnaire data and the log file data, with a 99.531% chance the log data file contains a higher proportion.

8.7.3.2. Did user enter email address?

When participants were asked if they revealed a private email address during the course of the experiments, 75% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 93.33% of participants in the text and avatar-based feedback group revealed an email address.

The two-tailed p-value: was 0.1724471. $p > 0.05$ therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 82.755% chance the proportions are different between the questionnaire data and the log file data, with a 91.378% chance the log data contains a higher proportion.

8.7.3.3. Did user enter common/dictionary password?

When participants were asked if they entered a dictionary password during the course of the experiments, 0% of users said “yes” in the questionnaire. When the log files generated were examined, it was revealed 53.85% participants in the text and avatar-based feedback group entered a commonly used password.

The two-tailed p-value: was 0.0013065. $p \leq 0.05$ and therefore this indicates a significant result.

Results of the chi-squared test also indicate there’s a 99.869% chance the proportions are different between the questionnaire data and the log file data, with a 99.935% chance the log data file contains a higher proportion.

8.7.3.4. Did user have personal details in password?

When participants were asked if they included personal details in their passwords during the course of the experiments, 0% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 6.25% participants in the text and avatar-based feedback group has personal details in their password.

Owing to values equalling zero, Fisher Exact Test was utilised. The two-tailed p-value: was 1. $p \geq 1$ and therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 0% chance the proportions are different between the questionnaire data and the log file data, with a 50% chance the log data contains a higher proportion.

8.7.3.5. Did user visit malicious site?

When participants were asked if they visited a malicious site during the course of the experiments, 31.25% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 50% participants in the text and avatar-based feedback group had visited a malicious site.

The two-tailed p-value: was 0.2878704. $p \geq 0.05$ and therefore is not a significant result.

Results of the chi-squared test also indicate there’s a 71.213% chance the proportions are different between the questionnaire data and the log file data, with a 85.606% chance the log data file contains a higher proportion.

8.7.4. USB 4 Experiment- text, colour-based feedback group

8.7.4.1. Did user reveal personal information?

When participants were asked if they revealed personal information during the course of the experiments, 78.57% of users said “yes” in the questionnaire. When the log files were examined, it was revealed all participants in the text, colour-based feedback group revealed some form of data.

The two-tailed p-value: was 0.0718608. $p \geq 0.05$ therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 92.814% chance the proportions are different between the questionnaire data and the log file data, with a 96.407% chance the log data file contains a higher proportion.

8.7.4.2. Did user enter email address?

When participants were asked if they revealed a private email address during the course of the experiments, 71.43% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 100% of participants in the text, colour-based feedback group revealed an email address.

The two-tailed p-value: was 0.0284599. $p \leq 0.05$ therefore this is a significant result.

Results of the chi-squared test also indicate there’s a 97.154% chance the proportions are different between the questionnaire data and the log file data, with a 98.577% chance the log data contains a higher proportion.

8.7.4.3. Did user enter common/dictionary password?

When participants were asked if they entered a dictionary password during the course of the experiments, 0% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 78.57% participants in the text, colour-based feedback group entered a commonly used password.

The two-tailed p-value: was 2.94E-5. $p \leq 0.05$ and therefore this indicates a significant result.

Results of the chi-squared test also indicate there’s a 99.997% chance the proportions are different between the questionnaire data and the log file data, with a 99.999% chance the log data file contains a higher proportion.

8.7.4.4. Did user have personal details in password?

When participants were asked if they included personal details in their passwords during the course of the experiments, 14.29% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 14.29% participants in the text, colour-based feedback group has personal details in their password.

The two-tailed p-value: was 1. $p \geq 1$ and therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 0% chance the proportions are different between the questionnaire data and the log file data, with a 50% chance the log data contains a higher proportion.

8.7.4.5. Did user visit malicious site?

When participants were asked if they visited a malicious site during the course of the experiments, 21.43% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 50% participants in the text, colour-based feedback group had visited a malicious site.

The two-tailed p-value: was 0.1213351. $p \geq 0.05$ and therefore is not a significant result.

Results of the chi-squared test also indicate there’s a 87.866% chance the proportions are different between the questionnaire data and the log file data, with a 93.933% chance the log data file contains a higher proportion.

8.7.5. USB 5 Experiment- text, colour, avatar-based feedback group

8.7.5.1. Did user reveal personal information?

When participants were asked if they revealed personal information during the course of the experiments, 52.94% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 35.71% participants in the text, colour, avatar-based feedback group revealed some form of data.

The two-tailed p-value: was 0.345397. $p \geq 0.05$ therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 65.46% chance the proportions are different between the questionnaire data and the log file data, with a 82.73% chance the questionnaire file contains a higher proportion.

8.7.5.2. Did user enter email address?

When participants were asked if they revealed a private email address during the course of the experiments, 52.94% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 86.67% of participants in the text, colour, avatar-based feedback group revealed an email address.

The two-tailed p-value: was 0.0432167. $p \leq 0.05$ therefore this is a significant result.

Results of the chi-squared test also indicate there’s a 95.678% chance the proportions are different between the questionnaire data and the log file data, with a 97.839% chance the log data contains a higher proportion.

8.7.5.3. Did user enter common/dictionary password?

When participants were asked if they entered a dictionary password during the course of the experiments, 0% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 35.29% participants in the text, colour, avatar-based feedback group entered a commonly used password.

The two-tailed p-value: was 0.007832. $p \leq 0.05$ and therefore this indicates a significant result.

Results of the chi-squared test also indicate there’s a 99.217% chance the proportions are different between the questionnaire data and the log file data, with a 99.608% chance the log data file contains a higher proportion.

8.7.5.4. Did user have personal details in password?

When participants were asked if they included personal details in their passwords during the course of the experiments, 5.88% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 0% participants in the text, colour, avatar-based feedback group has personal details in their password. Owing to values equalling zero, Fisher Exact Test was utilised.

The two-tailed p-value: was 1. $p \geq 1$ and therefore this is not a significant result.

Results of the chi-squared test also indicate there’s a 0% chance the proportions are different between the questionnaire data and the log file data, with a 50% chance the log data contains a higher proportion.

8.7.5.5. Did user visit malicious site?

When participants were asked if they visited a malicious site during the course of the experiments, 35.29% of users said “yes” in the questionnaire. When the log files were examined, it was revealed 47.06% participants in the text, colour, avatar-based feedback group had visited a malicious site.

The two-tailed p-value: was 0.4923308. $p \geq 0.05$ and therefore is not a significant result.

Results of the chi-squared test also indicate there’s a 50.767% chance the proportions are different between the questionnaire data and the log file data, with a 75.383% chance the log data file contains a higher proportion.

8.8. Comparing experiment groups- control group log data vs. affective feedback log data

This section details the statistical significance values between the control experiment log files and databases, vs. the affective feedback log files and databases. This will highlight differences between the actions of participants in the control group vs. participants who received some form of affective feedback. To achieve statistical significance, the p value needs to register as $p \leq 0.05$. Again the N-1 Two Proportion Test is used.

Table 21**Error! Reference source not found.** provides an overview of the results, showing which of the questions and experiment numbers raised a statistically significant result (difference between the control log and the experiment log). Section 8.8.1. explores the results in more detail.

Table 21 - summary table of control log vs. affective log results

Statistical significance: log files				
Question	**Control vs. Experiment 2 (text)**	**Control vs. Experiment 3 (text, avatar)**	**Control vs. Experiment 4 (text, colour)**	**Control vs. Experiment 5 (text, colour, avatar)**
Did user reveal personal information?	No	No	No	Yes
Did user enter email address?	No	No	No	No
Did user enter a common password?	No	No	No	No
Did user have personal details in password?	No	No	No	No
Did user visit a malicious site?	No	No	No	No

In comparing data from the control experiment log files and database records, against experiments containing affective feedback, the majority of results gained were insignificant. The only significant result gained was when the control experiment was compared against experiment 5, which contained text, colour and avatar-based affective feedback. In experiment 5, fewer participants revealed information about themselves when compared to the control group.

8.8.1. Control log vs. text-based feedback log

8.8.1.1. Did user reveal personal information?

When logs from the control experiment were viewed, 100% of users in the group were found to have revealed personal information. In comparison, when the text-based group logs were reviewed, 100% participants revealed personal information.

In comparing the two log files, there was a value equalling zero, therefore the Fisher Exact Test was utilised. The two-tailed p-value: was 1. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 0% chance the proportions are different between the control log data and the comparison text-based group log data, with a 0% chance the comparison text-based group log contains a higher proportion.

8.8.1.2. Did user enter email address?

When logs from the control experiment were viewed, 80% of users in the group were found to have revealed a private email address. In comparison, when the text group logs were reviewed, 69.23% participants revealed a private email address.

The two-tailed p-value: was 0.568506. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 43.149% chance the proportions are different between the control log data and the comparison text-based group log data, with a 71.575% chance the control log contains a higher proportion.

8.8.1.3. Did user enter common/dictionary password?

When logs from the control experiment were viewed, 41.67% of users in the group were found to have used a common/dictionary password. In comparison, when the text group logs were reviewed, 53.85% participants revealed the use of a common/dictionary password.

The two-tailed p-value: was 0.5507273. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 44.927% chance the proportions are different between the control log data and the comparison text-based group log data, with a 72.464% chance the text-based log contains a higher proportion.

8.8.1.4. Did user have personal details in password?

When logs from the control experiment were viewed, 8.33% of users in the group were found to have personal details in their password. In comparison, when the text-based group logs were reviewed, 0% participants had personal details in their password.

Owing to values equalling zero, Fisher Exact Test was utilised. The two-tailed p-value: was 0.48. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 52% chance the proportions are different between the control log data and the comparison text -based group log data, with a 52% chance the control log contains a higher proportion.

8.8.1.5. Did user visit malicious site?

When logs from the control experiment were viewed, 58.33% of users in the group were found to have visited a malicious site. In comparison, when the text-based group logs were reviewed, 61.54% participants had visited a malicious site.

The two-tailed p-value: was 0.8727803. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 12.722% chance the proportions are different between the control log data and the comparison text-based group log data, with a 56.361% chance the text-based group log contains a higher proportion.

8.8.2. Control log vs. text, and avatar-based feedback log

8.8.2.1. Did user reveal personal information?

When logs from the control experiment were viewed, 100% of users in the group were found to have revealed personal information. In comparison, when the text and avatar-based group logs were reviewed, 100% participants revealed personal information.

In comparing the two log files, there was a zero value, therefore the Fisher Exact Test was utilised. The two-tailed p-value: was 1. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 0% chance the proportions are different between the control log data and the comparison text and avatar-based group log data, with a 0% chance the comparison text and avatar-based log contains a higher proportion.

8.8.2.2. Did user enter email address?

When logs from the control experiment were viewed, 80% of users in the group were found to have revealed a private email address. In comparison, when the text and avatar-based group logs were reviewed, 93.33% participants revealed a private email address.

The two-tailed p-value: was 0.3247559. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 67.524% chance the proportions are different between the control log data and the comparison text and avatar-based group log data, with a 83.762% chance the text and avatar-based log contains a higher proportion.

8.8.2.3. Did user enter common/dictionary password?

When logs from the control experiment were viewed, 41.67% of users in the group were found to have used a common/dictionary password. In comparison, when the text and avatar-based group logs were reviewed, 50% participants revealed the use of a common/dictionary password.

The two-tailed p-value: was 0.6674362. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 33.256% chance the proportions are different between the control log data and the comparison text and avatar-based-based group log data, with a 66.628% chance the text and avatar-based-based log contains a higher proportion.

8.8.2.4. Did user have personal details in password?

When logs from the control experiment were viewed, 8.33% of users in the group were found to have personal details in their password. In comparison, when the text and avatar-based group logs were reviewed, 6.25% participants had personal details in their password.

Owing to a zero value, Fisher Exact Test was utilised. The two-tailed p-value: was 1. p≥ 0.05 therefore this is not a significant result.

Results of the test also indicate there's a 0% chance the proportions are different between the control log data and the comparison text avatar-based group log data, with a 31.746% chance the control log contains a higher proportion.

8.8.2.5. Did user visit malicious site?

When logs from the control experiment were viewed, 58.33% of users in the group were found to have visited a malicious site. In comparison, when the text and avatar-based group logs were reviewed, 50% participants had visited a malicious site.

The two-tailed p-value: was 0.6674362. p≥ 0.05 therefore this is not a significant result.

Results of the test also indicate there's a 33.256% chance the proportions are different between the control log data and the comparison text and avatar-based group log data, with a 66.628% chance the control group log contains a higher proportion.

8.8.3. Control log vs. text and colour-based feedback log

8.8.3.1. Did user reveal personal information?

When logs from the control experiment were viewed, 100% of users in the group were found to have revealed personal information. In comparison, when the text and colour-based group logs were reviewed, 100% participants revealed personal information.

In comparing the two log files, there was a value equalling zero, therefore the Fisher Exact Test was utilised. The two-tailed p-value: was 1. p≥0.05 therefore this is not a significant result.

Results of the test also indicate there's a 0% chance the proportions are different between the control log data and the comparison text and colour-based group log data, with a 0% chance the comparison text and colour-based log contains a higher proportion.

8.8.3.2. Did user enter email address?

When logs from the control experiment were viewed, 80% of users in the group were found to have revealed a private email address. In comparison, when the text and colour-based group logs were reviewed, 100% participants revealed a private email address.

In comparing the two log files, there was a value equalling zero, therefore the Fisher Exact Test was utilised. The two-tailed p-value: was 0.15. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 85% chance the proportions are different between the control log data and the comparison text and colour-based group log data, with a 85% chance the text and colour-based log contains a higher proportion.

8.8.3.3. Did user enter common/dictionary password?

When logs from the control experiment were viewed, 41.67% of users in the group were found to have used a common/dictionary password. In comparison, when the text and colour-based group logs were reviewed, 78.57% participants revealed the use of a common/dictionary password.

The two-tailed p-value: was 0.0586504. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 94.135% chance the proportions are different between the control log data and the comparison text and colour-based-based group log data, with a 97.067% chance the text and colour-based log contains a higher proportion.

8.8.3.4. Did user have personal details in password?

When logs from the control experiment were viewed, 8.33% of users in the group were found to have personal details in their password. In comparison, when the text and colour-based group logs were reviewed, 14.29% participants had personal details in their password.

The two-tailed p-value: was 0.642362. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 35.764% chance the proportions are different between the control log data and the comparison text and colour-based group log data, with a 67.882% chance the text and colour-based group log contains a higher proportion.

8.8.3.5. Did user visit malicious site?

When logs from the control experiment were viewed, 58.33% of users in the group were found to have visited a malicious site. In comparison, when the text and colour-based group logs were reviewed, 50% participants had visited a malicious site.

The two-tailed p-value: was 0.676922. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 32.308% chance the proportions are different between the control log data and the comparison text and colour-based group log data, with a 66.154% chance the control group log contains a higher proportion.

8.8.4. Control log vs. text, colour and avatar-based feedback log

8.8.4.1. Did user reveal personal information?

When logs from the control experiment were viewed, 100% of users in the group were found to have revealed personal information. In comparison, when the text, colour and avatar-based group logs were reviewed, 35.71% participants revealed personal information.

The two-tailed p-value: was 0.0016917. p≤0.05 therefore this is a significant result.

Results of the test also indicate there's a 99.831% chance the proportions are different between the control log data and the comparison text, colour and avatar-based group log data, with a 99.915% chance the control log contains a higher proportion.

8.8.4.2. Did user enter email address?

When logs from the control experiment were viewed, 80% of users in the group were found to have revealed a private email address. In comparison, when the text, colour and avatar-based group logs were reviewed, 86.67% participants revealed a private email address.

The two-tailed p-value: was 0.6625203. p≥ 0.05 therefore this is not a significant result.

Results of the test also indicate there's a 33.748% chance the proportions are different between the control log data and the comparison text, colour and avatar-based group log data, with a 66.874% chance the text, colour and avatar-based log contains a higher proportion.

8.8.4.3. Did user enter common/dictionary password?

When logs from the control experiment were viewed, 41.67% of users in the group were found to have used a common/dictionary password. In comparison, when the text, colour and avatar-based group logs were reviewed, 35.29% participants revealed the use of a common/dictionary password.

The two-tailed p-value: was 0.732144. p≥ 0.05 therefore this is not a significant result.

Results of the test also indicate there's a 26.786% chance the proportions are different between the control log data and the comparison text, colour and avatar-based group log data, with a 63.393% chance the control log contains a higher proportion.

8.8.4.4. Did user have personal details in password?

When logs from the control experiment were viewed, 8.33% of users in the group were found to have personal details in their password. In comparison, when the text, colour and avatar-based group logs were reviewed, 0% participants had personal details in their password.

In comparing the two log files, there was a cell value equalling zero, therefore the Fisher Exact Test was utilised. The two-tailed p-value: was 0.4137931. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 58.621% chance the proportions are different between the control log data and the comparison text, colour and avatar-based group log data, with a 58.621% chance the control group log contains a higher proportion.

8.8.4.5. Did user visit malicious site?

When logs from the control experiment were viewed, 58.33% of users in the group were found to have visited a malicious site. In comparison, when the text, colour and avatar-based group logs were reviewed, 47.06% participants had visited a malicious site.

The two-tailed p-value: was 0.5565279. $p \geq 0.05$ therefore this is not a significant result.

Results of the test also indicate there's a 44.347% chance the proportions are different between the control log data and the comparison text, colour and avatar-based group log data, with a 72.174% chance the control group log contains a higher proportion.

8.9. Assessment of affective feedback attitudes- statistical tests

A number of statistical methods were used to analyse the data gained from the experiments.

8.9.1. Shapiro-Wilk Normality Test

To analyse the impact of affective feedback on the end-users, it was necessary to have a control group who visited all the same websites, but received no feedback. This control group were given USB number 1, and the extension carried a monitoring solution only.

Since the control group was to be compared against all the other groups, Likert data from the control group needed to be tested to assess of the data distribution was normal, and to obtain the p-value. If the data did not include a normal distribution, a non-parametric test was needed to discern statistical significance. As Table 22 indicates none of the Likert scale based questions featured a normal distribution in accordance with the Shapiro-Wilk Normality Test, therefore further analysis would require the use of a non-parametric method. The p-values in the table were obtained via the use of the shapiro.test method in the R statistical computing program (The R Foundation 2015).

In terms of the Shapiro-Wilk Normality Test, if the p-value gained is less than or equal to the chosen alpha level (typically 0.01 or 0.05), the null hypothesis indicating the distribution is normal is rejected i.e. the data is not normal.

Table 22 - Shapiro-Wilk Normality Test control group results

Question	p-value	Normally distributed?
If you received negative password-related feedback, did it make you consider changing your Facebook password?	0.003397	no
If you received social media-related feedback, did it make you consider the information you share online?	0.004484	no
If you received feedback about malicious links on a page, did it make you consider which links you were clicking on?	0.009813	no
Did the feedback make you hesitate to provide information online?	0.001431	no
Did the feedback clearly highlight any issues with the page?	0.003397	no
Do you think the feedback provided helped to increase your security awareness?	0.004484	no
Did you find the feedback useful?	0.009813	no
Did the feedback encourage you to learn more about online security?	0.003715	no

8.9.2. Mann-Whitney U Test

Since the Shapiro-Wilk test indicated the data from the control/USB 1 group was not normally distributed, a non-parametric type of test was required to analyse the statistical significance of results gained.

Laerd Statistics notes that "*The Mann-Whitney U test is used to compare differences between two independent groups when the dependent variable is either ordinal or continuous, but not normally distributed.*" (Lund Research Ltd 2013). This indicates the Mann Whitney U test (sometimes called the Wilcoxon–Mann–Whitney test) is suitably applicable, in that the data from the Likert scale is ordinal. Also, each group who took part in the experiments was independent i.e. participants were only allowed to take part once, regardless of the experiment they took part in. Each group who received affective feedback was to be tested against the control group.

To calculate the statistical significance, the online Social Science Statistics calculator (Stangroom 2016) was used, after performing a few calculations manually to ensure its integrity. Tests were run using a 0.05 alpha level, and were two-tailed, in a bid to detect an effect in either direction. To this effect, if a test achieved a $p \leq 0.05$, there was deemed to be a statistically significant result between the two samples.

In the following section where the control group is compared against each of the affective extensions, the following terms are used:

- Median- midpoint of a frequency distribution

- U value- difference between two rank totals calculated by the Mann-Whitney U test

- p-value- *"the probability of finding the observed, or more extreme, results when the null hypothesis (H 0) of a study question is true"* (Stats Direct 2016)

8.10. Comparing experiment groups- affective feedback attitudes

This section details the statistical significance values between the opinions of participants who took part in the control experiment (no affective feedback) vs. those who took part in experiments containing affective feedback. To achieve statistical significance, the p value needs to register as $p \leq 0.05$.

Table 23 provides an overview of the results, showing which of the questions and experiment numbers raised a statistically significant result (difference between control responses and the affective feedback responses). Section 8.10.1. onwards describes the results in more detail.

Table 23 - summary table of control log vs. affective feedback attitude results

Statistical significance by question and experiment				
Question	**Control vs Experiment 2 (text)**	**Control vs Experiment 3 (text, avatar)**	**Control vs Experiment 4 (text, colour)**	**Control vs Experiment 5 (text, colour, avatar)**
If you received negative password-related feedback, did it make you consider changing your Facebook password?	No	No	No	No
If you received social media-related feedback, did it make you consider the information you share online?	No	No	No	No
If you received feedback about malicious links on a page, did it make you consider which links you were clicking on?	No	Yes	No	No
Did the feedback make you hesitate to provide information online?	No	Yes	No	Yes
Did the feedback clearly highlight any issues with the page?	No	No	No	No
Do you think the feedback provided helped to increase your security awareness?	Yes	Yes	Yes	Yes
Did you find the feedback useful?	Yes	No	Yes	Yes
Did the feedback encourage you to learn more about online security?	Yes	Yes	Yes	Yes

In comparing data from the control experiment when participants were asked *"Do you think the feedback provided helped to increase your security awareness?",* all affective experiments produced a positive, statistically significant result. This indicates that in the opinion of the participants, the affective feedback has had an impact on security awareness.

Similarly, when asked *"Did the feedback encourage you to learn more about online security?",* again, all affective experiments produced a statistically significant result in comparison to the control responses. This indicates that in the opinion of the participants, the affective feedback has had some form of impact on them, encouraging them to improve their behaviour in the future.

In terms of finding the feedback useful, the only group which failed to produce a statistically significant result in this instance was experiment 3 (text and avatar-based feedback) in comparison to the control. Other results were mixed, with text and avatar-based feedback proving successful in coercing users into hesitating to provide information online and making them consider the links they were clicking on. Experiment 5 (text, colour, and avatar-based feedback) also appeared to make participants hesitate to provide information.

8.10.1. Control vs. text-based affective feedback

8.10.1.1. If you received negative password-related feedback, did it make you consider changing your Facebook password?

This question assessed if negative password related feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 2 were shown text-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1.5) and sample 2 (median=0). The p-value is 0.53526 meaning the result is not significant at $p \leq 0.05$. The U-value is 55.5. The critical value of U at $p \leq 0.05$ is 33. Again the result is not significant at $p \leq 0.05$.

8.10.1.2. If you received social media-related feedback, did it make you consider the information you share online?

This question assessed whether or not social media-related feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 2 were shown text-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1) and sample 2 (median=1). The p-value is 0.8181 meaning the result is not significant at $p \leq 0.05$. The U-value is 56. The critical value of U at $p \leq 0.05$ is 29. Again, the result is not significant at $p \leq 0.05$.

8.10.1.3. If you received feedback about malicious links on a page, did it make you consider which links you were clicking on?

This question assessed whether or not malicious link feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 2 were shown text-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1) and sample 2 (median=2). The p-value is 0.71138 meaning the result is not significant at $p \leq 0.05$. The U-value is 59.5. The critical value of U at $p \leq 0.05$ is 33. Again, the result is not significant at $p \leq 0.05$.

8.10.1.4. Did the feedback make you hesitate to provide information online?

Participants were asked if any of the feedback shown during the experimental process made them hesitate to provide information online. Participants in sample 1 were shown no feedback (control). Participants in sample 2 were shown text-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=0) and sample 2 (median=4). The p-value is 0.11184 meaning the result is not significant at $p \leq 0.05$. The U-value is 44. The critical value of U at $p \leq 0.05$ is 37. Again, the result is not significant at $p \leq 0.05$.

8.10.1.5. Did the feedback clearly highlight any issues with the page?

Participants were asked if feedback provided clearly highlighted any issues with the web pages visited. Participants in sample 1 were shown no feedback (control). Participants in sample 2 were shown text-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1.5) and sample 2 (median=3). The p-value is 0.4354 meaning the result is not significant at p≤ 0.05. The U-value is 58. The critical value of U at p≤ 0.05 is 37. Again, the result is not significant at p≤ 0.05.

8.10.1.6. Do you think the feedback provided helped to increase your security awareness?

Participants were asked if feedback provided increased their security awareness. Participants in sample 1 were shown no feedback (control). Participants in sample 2 were shown text-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 2 (median=4). The p-value is 0.04036 meaning the result is significant at p≤ 0.05. The U-value is 36. The critical value of U at p≤ 0.05 is 37. Again, the result is significant at p≤ 0.05.

This result indicates there is a difference between samples. On further inspection of the median values, sample 2 (text-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.1.7. Did you find the feedback useful?

Participants were asked if the feedback they were provided with was useful. Participants in sample 1 were shown no feedback (control). Participants in sample 2 were shown text-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 2 (median=4). The p-value is 0.04338 meaning the result is significant at p≤ 0.05. The U-value is 36.5. The critical value of U at p≤ 0.05 is 37. Again, the result is significant at p≤ 0.05.

This result indicates there is a difference between samples. On further inspection of the median values, sample 2 (text-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.1.8. Did the feedback encourage you to learn more about online security?

Participants were asked if the feedback encouraged them to learn more about online security. Participants in sample 1 were shown no feedback (control). Participants in sample 2 were shown text-based affective feedback.

The Mann-Whitney U test indicated there was a marginal statistical significance between sample 1 (median=1) and sample 2 (median=3). The p-value is 0.0466 meaning the result is significant at $p \leq 0.05$. The U-value is 37. The critical value of U at $p \leq 0.05$ is 37. Again, the result is significant at $p \leq 0.05$.

This result indicates there is a difference between samples. On further inspection of the median values, sample 2 (text-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.2. Control vs. text, and avatar-based feedback

8.10.2.1. If you received negative password-related feedback, did it make you consider changing your Facebook password?

This question assessed whether or not negative password related feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 3 were shown text, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1.5) and sample 3 (median=3). The p-value is 0.8493 meaning the result is not significant at $p \leq 0.05$. The U-value is 74. The critical value of U at $p \leq 0.05$ is 41. Again, the result is not significant at $p \leq 0.05$.

8.10.2.2. If you received social media-related feedback, did it make you consider the information you share online?

This question assessed whether or not social media-related feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 3 were shown text, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1) and sample 3 (median=3). The p-value is 0.4965 meaning the result is not significant at $p \leq 0.05$. The U-value is 65. The critical value of U at $p \leq 0.05$ is 41 so again, the result is not significant at $p \leq 0.05$.

8.10.2.3. If you received feedback about malicious links on a page, did it make you consider which links you were clicking on?

This question assessed whether or not malicious links feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 3 were shown text, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 3 (median=4). The p-value is 0.01928 meaning the result is significant at $p \leq 0.05$. The U-value is 41.5. The critical value of U at $p \leq 0.05$ is 49. Again, the result is significant at $p \leq 0.05$.

This result indicates there is a difference between samples. On further inspection of the median values, sample 3 (text, and avatar-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.2.4. Did the feedback make you hesitate to provide information online?

Participants were asked if any of the feedback shown during the experimental process made them hesitate to provide information online. Participants in sample 1 were shown no feedback (control). Participants in sample 3 were shown text, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=0) and sample 3 (median=4). The p-value is 0.0455 meaning the result is significant at $p \leq 0.05$. The U-value is 52.5. The critical value of U at $p \leq 0.05$ is 53. Again, the result is significant at $p \leq 0.05$.

This result indicates there is a difference between samples. On further inspection of the median values, sample 3 (text, and avatar-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.2.5. Did the feedback clearly highlight any issues with the page?

Participants were asked if feedback provided clearly highlighted any issues with the web pages visited. Participants in sample 1 were shown no feedback (control). Participants in sample 3 were shown text, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1.5) and sample 3 (median=4). The p-value is 0.33204 meaning the result is not significant at $p \leq 0.05$. The U-value is 74.5. The critical value of U at $p \leq 0.05$ is 53. Again, the result is not significant at $p \leq 0.05$.

8.10.2.6. Do you think the feedback provided helped to increase your security awareness?

Participants were asked if feedback provided increased their security awareness. Participants in sample 1 were shown no feedback (control). Participants in sample 3 were shown text, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 3 (median=4). The p-value is 0.01314 meaning the result is significant at p≤ 0.05. The U-value is 42. The critical value of U at p≤ 0.05 is 53. Again, the result is significant at p≤ 0.05.

This result indicates there is a difference between samples. On further inspection of the median values, sample 3 (text, and avatar-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.2.7. Did you find the feedback useful?

Participants were asked if the feedback they were provided with was useful. Participants in sample 1 were shown no feedback (control). Participants in sample 3 were shown text, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1) and sample 3 (median=4). The p-value is 0.05744 meaning the result is not significant at p≤ 0.05. The U-value is 54.5. The critical value of U at p≤ 0.05 is 53. Again, the result is not significant at p≤ 0.05.

8.10.2.8. Did the feedback encourage you to learn more about online security?

Participants were asked if the feedback encouraged them to learn more about online security. Participants in sample 1 were shown no feedback (control). Participants in sample 3 were shown text, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 3 (median=4). The p-value is 0.01314 meaning the result is significant at p≤ 0.05. The U-value is 42. The critical value of U at p≤ 0.05 is 53. Again, the result is significant at p≤ 0.05.

This result indicates there is a difference between samples. On further inspection of the median values, sample 3 (text, and avatar-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.3. Control vs. text and colour

8.10.3.1. If you received negative password-related feedback, did it make you consider changing your Facebook password?

This question assessed whether or not negative password related feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 4 were shown text, and colour-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1.5) and sample 4 (median=1). The p-value is 0.50926 meaning the result is not significant at $p \leq 0.05$.The U-value is 49.5. The critical value of U at $p \leq 0.05$ is 29 so again, the result is not significant at $p \leq 0.05$.

8.10.3.2. If you received social media-related feedback, did it make you consider the information you share online?

This question assessed whether or not social media-related feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 4 were shown text, and colour-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1) and sample 4 (median=0). The p-value is 0.80258 meaning the result is not significant at $p \leq 0.05$. The U-value is 61.5. The critical value of U at $p \leq 0.05$ is 33 so again, the result is not significant at $p \leq 0.05$.

8.10.3.3. If you received feedback about malicious links on a page, did it make you consider which links you were clicking on?

This question assessed whether or not malicious links feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 4 were shown text, and colour-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1) and sample 4 (median=3.5). The p-value is 0.238 meaning the result is not significant at $p \leq 0.05$. The U-value is 60.5. The critical value of U at $p \leq 0.05$ is 45. Again, the result is not significant at $p \leq 0.05$.

8.10.3.4. Did the feedback make you hesitate to provide information online?

Participants were asked if any of the feedback shown during the experimental process made them hesitate to provide information online. Participants in sample 1 were shown no feedback (control). Participants in sample 4 were shown text, and colour-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=0) and sample 4 (median=3). The p-value is 0.18352 meaning the result is not significant at $p \leq 0.05$. The U-value is 53. The critical value of U at $p \leq 0.05$ is 41. Again, the result is not significant at $p \leq 0.05$.

8.10.3.5. Did the feedback clearly highlight any issues with the page?

Participants were asked if feedback provided clearly highlighted any issues with the web pages visited. Participants in sample 1 were shown no feedback (control). Participants in sample 4 were shown text, and colour-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1.5) and sample 4 (median=4). The p-value is 0.29372 meaning the result is not significant at p≤ 0.05. The U-value is 63. The critical value of U at p≤ 0.05 is 45. Again, the result is not significant at p≤ 0.05.

8.10.3.6. Do you think the feedback provided helped to increase your security awareness?

Participants were asked if feedback provided increased their security awareness. Participants in sample 1 were shown no feedback (control). Participants in sample 4 were shown text, and colour-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 4 (median=4). The p-value is 0.01278 meaning the result is significant at p≤ 0.05. The U-value is 35. The critical value of U at p≤ 0.05 is 45. Again, the result is significant at p≤ 0.05.

This result indicates there is a difference between samples. On further inspection of the median values, sample 4 (text, and colour-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.3.7. Did you find the feedback useful?

Participants were asked if the feedback they were provided with was useful. Participants in sample 1 were shown no feedback (control). Participants in sample 4 were shown text, and colour-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 4 (median=4). The p-value is 0.04236 meaning the result is significant at p≤ 0.05. The U-value is 44. The critical value of U at p≤ 0.05 is 45. Again, the result is significant at p≤ 0.05.

This result indicates there is a difference between samples. On further inspection of the median values, sample 4 (text, and colour-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.3.8. Did the feedback encourage you learn more about online security?

Participants were asked if the feedback encouraged them to learn more about online security. Participants in sample 1 were shown no feedback (control). Participants in sample 4 were shown text, and colour-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 4 (median=3.5). The p-value is 0.02202 meaning the result is significant at $p \leq 0.05$. The U-value is 39. The critical value of U at $p \leq 0.05$ is 45. Again, the result is significant at $p \leq 0.05$.

This result indicates there is a difference between samples. On further inspection of the median values, sample 4 (text, and colour-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.4. Control vs. text, colour and avatar

8.10.4.1. If you received negative password-related feedback, did it make you consider changing your Facebook password?

This question assessed whether or not negative password related feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 5 were shown text, colour, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1.5) and sample 5 (median=1). The p-value is 0.71138 meaning the result is not significant at p≤ 0.05. The U-value is 59.5. The critical value of U at p≤ 0.05 is 33. Again, the result is not significant at p≤ 0.05.

8.10.4.2. If you received social media-related feedback, did it make you consider the information you share online?

This question assessed whether or not social media-related feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 5 were shown text, colour, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1) and sample 5 (median=3). The p-value is 0.5287 meaning the result is not significant at p≤ 0.05. The U-value is 66. The critical value of U at p≤ 0.05 is 41 so again, the result is not significant at p≤ 0.05.

8.10.4.3. If you received feedback about malicious links on a page, did it make you consider which links you were clicking on?

This question assessed whether or not malicious links feedback shown during the experiment had an impact on the end user. Participants in sample 1 were shown no feedback (control). Participants in sample 5 were shown text, colour, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1) and sample 5 (median=3). The p-value is 0.1141 meaning the result is not significant at p≤ 0.05.The U-value is 61.5. The critical value of U at p≤ 0.05 is 53. Again, the result is not significant at p≤ 0.05.

8.10.4.4. Did the feedback make you hesitate to provide information online?

Participants were asked if any of the feedback shown during the experimental process made them hesitate to provide information online. Participants in sample 1 were shown no feedback (control). Participants in sample 5 were shown text, colour, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was statistical significance between sample 1 (median=0) and sample 5 (median=4). The p-value is 0.0271 meaning the result is significant at $p \leq 0.05$.The U-value is 51.5. The critical value of U at $p \leq 0.05$ is 57. Again, the result is significant at $p \leq 0.05$.

This result indicates there is a difference between samples. On further inspection of the median values, sample 5 (text, colour and avatar-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.4.5. Did the feedback clearly highlight any issues with the page?

Participants were asked if feedback provided clearly highlighted any issues with the web pages visited. Participants in sample 1 were shown no feedback (control). Participants in sample 5 were shown text, colour, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1.5) and sample 5 (median=3). The p-value is 0.36282 meaning the result is not significant at $p \leq 0.05$. The U-value is 81. The critical value of U at $p \leq 0.05$ is 57. Again, the result is not significant at $p \leq 0.05$.

8.10.4.6. Do you think the feedback provided helped to increase your security awareness?

Participants were asked if feedback provided increased their security awareness. Participants in sample 1 were shown no feedback (control). Participants in sample 5 were shown text, colour, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 5 (median=3). The p-value is 0.04884 meaning the result is significant at $p \leq 0.05$. The U-value is 57. The critical value of U at $p \leq 0.05$ is 57. Again, the result is significant at $p \leq 0.05$.

This result indicates there is a difference between samples. On further inspection of the median values, sample 5 (text, colour and avatar-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.10.4.7. Did you find the feedback useful?

Participants were asked if the feedback they were provided with was useful. Participants in sample 1 were shown no feedback (control). Participants in sample 5 were shown text, colour, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was no statistical significance between sample 1 (median=1) and sample 5 (median=4). The p-value is 0.07346 meaning the result is not significant at $p \leq 0.05$. The U-value is 61. The critical value of U at $p \leq 0.05$ is 57. Again, the result is not significant at $p \leq 0.05$.

8.10.4.8. Did the feedback encourage you to learn more about online security?

Participants were asked if the feedback encouraged them to learn more about online security. Participants in sample 1 were shown no feedback (control). Participants in sample 5 were shown text, colour, and avatar-based affective feedback.

The Mann-Whitney U test indicated there was a statistical significance between sample 1 (median=1) and sample 5 (median=3). The p-value is 0.04136 meaning the result is significant at p≤ 0.05. The U-value is 55.5. The critical value of U at p≤ 0.05 is 57. Again, the result is significant at p≤ 0.05.

This result indicates there is a difference between samples. On further inspection of the median values, sample 5 (text, colour and avatar-based affective feedback) has a higher rating, which suggests users felt it had more of an impact in comparison to the control.

8.11. Comments about the extension

At the end of the questionnaire, participants were asked *"Any other comments about the extension?"* as a free-form question, with a view to obtaining information which could be used to improve the monitoring solution and affective feedback delivery system in future research.

Comments received provided mixed answers; a full list can be found in Appendix (vii) - response to "Any other comments about the extension?".

8.12. Limitations of the study

The research goals for this project have been met, although consideration has been given to the limitations of the research.

Owing to the number of participants who engaged with the study, and the division of participants into 5 experimental groups (experiment 1: n=12, experiment 2: n=13 , experiment 3: n=16 , experiment 4: n=14 , experiment 5: n=17), the sample sizes were relatively low. In addition to this, the demographics were not representative of the general population, with the majority of participants being younger, university students, with knowledge of a computing-based subject.

There may also have been potential issues with the experimental design. In some instances, participants reported receiving on-screen feedback, despite the fact they were part of a control group who did not receive feedback. It is conceivable they thought some of the websites they were asked to visit provided feedback e.g. the red background of the Bad SSL site. In relation to feedback questions users received, if they answered "*no*" to the first question of *"Did you receive any on-screen feedback during the experiments?"*, they still had to answer the rest of the questions on the sheet of paper. This may have led some of them into believing they also received on-screen feedback.

Another limitation relates to the phrasing of some of the questions. In order to ensure the questions were clear for the participants, it might have been useful to explain some concepts to them during the experimental process. One such example of this is the definition of commonly used passwords (passwords which have been cracked, and appear on multiple wordlists e.g. “Trustno1”), and dictionary passwords (a word which can be found in the dictionary, or a password which has been cracked before e.g. “password”).

Potential issues may also have arisen with the extension. It cannot reliably know that personal information is contained within a password. Instead, it can only check if personal information provided within the context of the experiment has been included within the password.

The affective feedback delivery bar was placed at the bottom of the screen in an attempt to emulate the positioning of the status bars which previously appeared in browsers. Conceivably, the bar could have been made to appear more prominent on-screen, by modifying the colours presented, or by conducting a study to find the optimal position for imparting information to the end-user.

The extension also suffers from scalability issues. When running on pages containing a large number of links, the affective feedback mechanism can lag. This is due to the fact each link is checked against the database to ascertain if it is malicious. This issue was mitigated during the experimental phase- websites with a limited number of links were chosen, to ensure accurate results were gained, and that the monitoring solution and affective feedback mechanism did not encounter any errors.

8.13. Overall results summary

The results section has highlighted there were some significant differences between what users stated they did during experiments, versus what they actually did during the experimental process, in terms of security behaviour such as the information they revealed about themselves. One issue is that there is a significant statistical difference between the log files when compared against the questionnaires when users were asked if they used a common password. More users utilised a common password, than admitted to this fact across all affective experiments. This means affective feedback did not have an impact on the end-user, and no affective feedback mechanism out-performed the other.

A significantly higher number of users revealed personal information, than reported doing so in the questionnaire when comparing experiments 1 and 3. Similar results were noted for the question of *"Did user enter an email address?"* in experiments 4 and 5, and *"Did user visit a malicious site?"* in experiments 1 and 2. The mixed results in regards to different affective feedback mechanisms show that no affective feedback mechanism out-performed the other.

Few significant differences were seen in the log files of the control experiment when compared to the log files of the experiments of participants who received affective feedback. A significant result was gained with experiment 5 (text, colour, avatar) in comparison to the control experiment. Fewer participants in experiment 5 revealed information about themselves in comparison to the control experiment. In this instance, affective feedback may have helped users consider their security behaviour, or participants in that group may have possessed an increased knowledge of security. The demographics of the group show although there were some participants who studied a computing-based subject and may therefore know about security, there was an overall mix of people in the group.

When asked about the impact the affective feedback had on the end users, some found that it made them hesitate to provide information online, or made them think about the links they were clicking on. Also, a majority of participants indicated that providing affective feedback was useful, increased security awareness and encouraged them to learn more about online security. Overall, results between groups generally highlighted that any affective feedback mechanism was viewed as potentially useful by the end-user.

Chapter 9 will discuss the results fully, before conclusions are drawn about the overall success of the research project in Chapter 10.

Chapter 9. Discussion

This chapter will discuss the results which were obtained and analysed in Chapter 8, scrutinising them in greater detail. The discussion of the results will examine how they relate to the research question *"Is it possible to enhance security risk awareness in end-users via dynamically provided affective feedback?".*

The discussion section will critique the what the participants said they did in the questionnaire provided compared to how the participants actually fared in terms of the log data. In this particular part of the questionnaire, participants were asked simple yes/no questions which allow for a binary comparison of those who said “yes” against those who triggered a positive result in the appropriate log file. This will aid in determining a general overview of participants’ security awareness level

To link back to the research question, the results of the control group log data versus the affective feedback log data will also be discussed i.e. highlight if there's a difference between the log files of those who received affective feedback. This will provide another aspect of an answer to the research question and will assess if the affective feedback had an impact on what the users actually did during the experiments.

The Likert-based questionnaire feedback will also be inspected in an attempt to answer the research question. In this instance, the Likert scale data from the control group was compared to the experiment groups which delivered affective feedback, in a bid to determine if participants thought the affective feedback provided had an impact on their security awareness levels.

Potential issues related to the tool developed will also be discussed, using the general feedback gained from participants as a basis for the discussions. Finally, future work will be explored, covering possible ways in which issues could be mitigated in future experiments, and how the developed solution could be used in future research.

9.1. Discussion of results

9.1.1. Questionnaire results vs. the log and databases

When the questionnaire results were compared to the log files and the MySQL database records, there was one key question regarding risky security behaviour which produced a statistically significant result (as shown in Table 20, section 8.7.).

During the experimental process, when participants were asked if they had used a dictionary password, the majority of those asked stated “no”. However, after analysing the requisite log files, there was a noted statistical significance which indicated that the majority of the participants had a common element in their password. The same statistical difference is noted across all of the experiments which delivered varying combinations of affective feedback.

Since the same difference is seen across all experiments containing affective feedback, it suggests the delivery of the feedback did not have an overall impact on the actions of the participants in this instance, however, there is another potential explanation for such a result.

This result highlights there is still a need to raise security awareness in end-users and educate people regarding security behaviours which are perceived to be risky (Hoffman 2011). One interpretation of the result is that participants may not have been aware of the term “dictionary word” in relation to password. Additionally, they may not have been aware that dictionary words in passwords contribute to poor password hygiene (Milne, Labrecque and Cromer 2009). These findings also link in with the research conducted by Ur et al. (2016). This paper found that end-users had a number of misconceptions about common passwords and dictionary passwords.

When participants were asked if they had revealed personal information about themselves during the course of the experiments, there was a significant difference between those who admitted to revealing information about themselves (as per the questionnaire data), in comparison to the number of participants who actually revealed personal information about themselves, as revealed by the appropriate database records.

In experiment 1 (control) and experiment 3 (text and avatar-based affective feedback), there was a significantly higher proportion of participants who revealed personal information about themselves in the database, in comparison to those who stated they revealed information about themselves when answering the questionnaire. Again, this result could be explained by the fact participants had a poor understanding of risky security behaviour, and perhaps did not understand the consequences which could arise from sharing such information. Such findings link to work by Stanton et al. (2005) where a taxonomy of security behaviours was presented. One behaviour identified was "naïve mistakes" where the user does not realise that their behaviour is flawed.

A poor understanding of risky security behaviours could also explain the similarly statistically significant results gained when participants were asked if they entered a private email address during the course of the study. Whilst the concept of a private email address is purely subjective (what constitutes a private email address may differ depending on the user and purpose of the address), the database files were parsed in an effort to determine if the user had provided some form of information in the private email address field. Experiment 4 (text and colour-based feedback) and experiment 5 (text, colour and avatar-based feedback) produced statistically significant results, with more users revealing email addresses in the log files. Milne, Labrecque and Cromer (2009) questioned users regarding information they revealed online and found similar results. When participants in the study were asked if they had revealed information such as private email addresses, a large number of participants said they had. Again, this also ties into work by Stanton et al. (2005) where users do not realise such behaviour could be problematic.

When asking users if they had visited a malicious website during the course of the experiment, a statistically significant result was gained in experiment 1 (control) and experiment 2 (text-based feedback). Essentially, more users visited malicious sites (according to the log files) than admitted to visiting malicious sites in the questionnaire. Since experiment 1 does not contain any form of affective feedback whereas experiment 2 does, such a result could again be attributed to the participant's lack of security awareness when browsing sites online. The proportion of those visiting malicious sites in experiment 1 also highlights the requirement for a tool to help users- if users are not provided with any feedback (like in experiment 1), they will have no way of knowing a link they are clicking on is malicious.

All information provided during the experimental process was voluntary, and this statement was clearly displayed at the top of the web pages which asked for information such as mother's maiden name, hobbies, email address, etc., which shows participants either chose to divulge sensitive information, or that they actively engaged in risky security behaviour by failing to read the page properly. It is known that often, users will reject rational security advice they are provided with, as they perceive the steps required to engage in secure behaviour to be burdensome (Herley 2009).

9.1.2. Control group log data vs. affective feedback log data

When the log files and database records from the control experiment were compared to the log files and the database records from affective feedback-based experiments, the majority of results gained were insignificant (as shown in Table 21, section 8.8.).

When users were asked if they revealed information about themselves during the course of the experimental process, there was a statistical difference noted in the actual number of people who revealed information in the log files of experiment 5 (text, colour and avatar-based feedback). In experiment 5, fewer participants revealed information about themselves when compared to the control group log files.

Such a result potentially indicates the affective feedback delivered in experiment 5 may have encouraged and assisted participants in considering their security behaviour online, and increased their awareness. On the other-hand, it is possible the particular group of participants already possessed a good knowledge of risky security behaviours. Exploring the courses participants in experiment 5 were studying, there is a variety of subjects. Of those who answered the question, there were 4 computing students, and 2 ethical hacking students. The rest were a mix of food nutrition and health, PhD Oil and Gas Economics, computer games application development, computer games technology, and forensic psychobiology students. In this group, the ethical hacking students will have covered security extensively on their course, and the computing students should have some awareness of security. The other subjects mentioned do not cover security in-depth, meaning affective feedback may have been useful in this instance.

9.1.3. Questionnaire feedback and attitudes towards affective feedback

When comparing the questionnaire results regarding the impact of the affective feedback, there were statistically significant differences when experiment 1 (control) participants were compared to those who engaged with the affective feedback-based experiments (shown in Table 23, section 8.10.).

When participants were asked *"Do you think the feedback provided helped to increase your security awareness?"*, all affective questionnaire data produced a positive, statistically significant result when compared to the control group questionnaire data. This indicates that in the opinion of the participants, the affective feedback was successful in creating a positive impact on the security awareness of the end-user.

A similar statistically significant result was generated when participants were asked "*Did the feedback encourage you to learn more about online security?*". All affective questionnaire data produced a positive, statistically significant result when compared to the control group questionnaire data. This result highlights again that the affective feedback appears to have influenced the participants into thinking about their security behaviours online, with the possibility of prompting them to engage in better security choices in future web-browsing. The result also links back to the need for education: in this instance it appears the participants are eager to learn. Affective feedback can trigger emotions and this is consistent with work presented by Iovane et al. (2012) and Arguedas et al. (2015) whereby they argue that emotion is a key part of the learning process.

The results of the two questions "*Do you think the feedback provided helped to increase your security awareness?*" and "*Did the feedback encourage you to learn more about online security?"* produced statistically significant results for all affective experiments. When interpreting the data, this indicates that no form of affective feedback delivered outperformed the other- essentially any form of affective feedback made an impact. This is an interesting result as the raw results shown in 8.3.3. indicated users felt colour had the largest impact, though it was only used in 2 of the experiments.

When asked if the feedback provided was useful, only one comparison group failed to produce a statistically significant result. The group in question was experiment 3 (text and avatar-based feedback). This result correlates with the graph in 8.3.3. where participants indicated that colour had the largest impact during the experimental process, though it should be noted that experiment 2 (text-based feedback) produced a statistically significant result, despite the lack of colour-based feedback.

The other results gained from the experiments were mixed. When asked if the feedback made them hesitate to provide information online, both experiment 3 (text and avatar-based feedback) and experiment 5 (text, colour and avatar-based feedback) were successful to this end, again showing an impact on end-user security behaviour. Experiment 3 also appeared to have an impact on the way they browsed online, making them consider the links they were clicking on, guiding them to avoid engagement in risky security behaviours. On the other hand, work by Myers (2004) and Hini, Gendall and Kearns (1995) have noted there is a weak link between behaviour and attitude, and therefore is suggestive that the feedback provided may not necessarily cause users to change their behaviour. The concept of "security fatigue" must also be taken into consideration. Even if users are provided with affective feedback to raise security awareness, they may not comply with it. Furnell and Thomson (2009) made a similar observation that employees within companies may fail to adhere to good practice, when they have been taught about security issues.

In terms of the affective feedback delivered, some comments from the free-form section of the questionnaire state participants think the affective solution is a useful application, with comments such as "*I find the extension useful for people who do not know much about online security*", *"Very helpful, especially for strong passwords",* and *"I think this is a good idea to raise awareness on online security especially people that are new to technology".*

9.2. Potential issues

9.2.1. Avoiding bias

Several steps were taken to avoid introducing any type of bias into the experiments**.**

When partaking in the experiments, participants were initially told the purpose of the research was to assess whether or not specially developed Firefox extensions provided assistance when browsing the web. They were also told that the Firefox extension might provide them with on-screen feedback.

Participants were not told about the type of feedback they would receive, or the location it might appear in. The term "risky security behaviour" was not mentioned on any part of the participant information sheet, to avoid introducing participants to a conscious bias.

The measures taken to reduce the level of bias involved in the experiments may have confused some participants, judging by some of the comments left in response to the free form question (see Appendix (vii)) e.g. *"I couldn't understand fully the experiment and what and why Facebook was involved in it."*.

9.2.2. Control group experiments

The control group experiments may have been construed as confusing, owing to the lack of feedback and the fact that participants still had to go through the same websites as a participant who received affective feedback. This information was reflected in response to the free-form question included in the questionnaire e.g. *"Personally I didn't notice anything out of the ordinary"*, *"I did not see any noticeable effects of the extension"* and *"I couldn't understand fully the experiment and what and why Facebook was involved in it.".*

If users had been informed that they were in the control group, or an affective feedback group, this could have introduced bias into the experiment (see 9.2.1.), and may have skewed the final results. Whilst control group users had to simply visit sites and received no feedback, this process ensured the integrity of the research. Several of the participants in the control group stated they received some form of feedback which could not have been the case. In this scenario, users may have misinterpreted part of a web page or part of the standard Firefox web browser window as some form of affective feedback delivery system.

Potentially participants in the control group may have thought the BadSSL page (7.5.6.) was providing feedback, in that it was a bright red page. In future experiments, this page could be replaced with a simple, plain web page delivered via HTTP with a password field on it. This would trigger the same feedback warnings however it may reduce the perception of the web page itself providing feedback.

Participants may also have considered that built-in browser security warnings were part of a feedback delivery system. The potential built-in browser warnings are discussed in the following section, 9.2.3.

9.2.3. Impact of feedback vs. built in browser warnings

Relating to participants in the control group, a few submitted questionnaire answers indicating they had received some form of feedback, which is not possible. The types of built-in warnings and feedback which Firefox provides have been investigated in order to identify a source of the alleged feedback. Table 24 outlines the trigger embedded within the monitoring solution, and as of Mozilla Firefox version 43, provides potential warnings and information delivered by the browser.

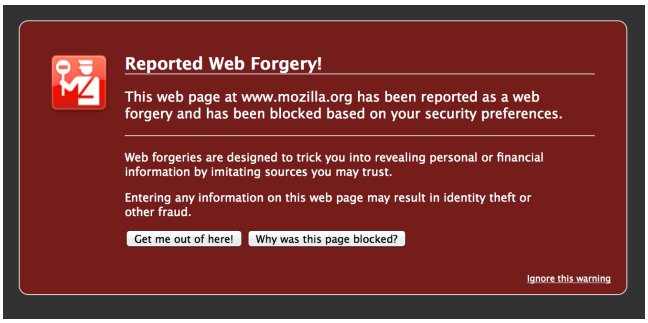
In this instance, Firefox provides no such feedback or warnings for common passwords, malicious links on pages, social media sites, or the use of public Wi-Fi. It does provide feedback if a user visits a malicious website but since the malicious website used during the experimental process was spoofed, the Firefox malicious website warning did not appear on-screen.

Regarding HTTP and HTTPS websites, Firefox provides some colour and text-based warnings (and Table 24 reveals how to view such information). The feedback here is not necessarily obvious and users may have failed to notice this.

There is scope for future work in this respect, in comparing the affective feedback delivery system in comparison to the Firefox browser. To access some of the security information in Firefox, several clicks are needed (outlined in Table 24). The affective feedback delivery system has a fixed bar at the bottom of each page, and potentially provides a more direct feedback mechanism.

Table 24 - monitoring solution triggers compared to built-in Firefox feedback

	Current Firefox Warning	
Trigger	**Action**	**Result**
HTTP Site	lynsayshepherd.com as an example	Site loads
	Click globe icon on address bar	Red text- *"connection is not secure"*
	Click arrow	Text: *"Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.)".*
	Click more information	Text: *"The web site lynsayshepherd.com does not support encryption for the page you are viewing. Information sent over the internet without encryption can be seen by other people while it is in transit."*
HTTPS Site	Google.com as an example	Site loads
	Click green padlock on address bar.	Green text- *"secure connection".*
	Click arrow. *"Verified by Google"*	Text: Connection Encrypted (encryption details)- *"The page you are viewing was encrypted before being transmitted over the Internet".*
	Click more information	Text: *"Encryption makes it difficult for unauthorized people to view information travelling between computers. It is therefore unlikely that anyone read this page as it*

		traveled across the network."
Common password	No standard warning.	No standard warning.
Malicious link visited		
Malicious link on page	No standard warning.	No standard warning.
Social media site	No standard warning.	No standard warning.
Public wi-fi	No standard warning.	No standard warning.

9.2.4. Sample sizes

Despite recruiting 72 participants, when these were divided into experimental groups (experiment 1: n=12 , experiment 2: n=13 , experiment 3: n=16 , experiment 4: n=14 , experiment 5: n=17), the sample sizes were low. This may have had an impact of the granularity of the results.

9.2.5. Efficiency of the tool developed

The affective feedback mechanism can be inefficient when running on pages containing a large number of link, as each link is checked against a database to detect if it is malicious. To mitigate any issues during the experimental phase, websites with a limited number of links were chosen, to ensure accurate results were gained, and that the monitoring solution and affective feedback mechanism did not encounter any errors. Timeliness of feedback provided in a learning environment is paramount (McDarby et al. 2004)(Iovane et al. 2012). By minimising the risk of the extension failing, this helped to ensure feedback appeared at the correct time.

9.2.6. USB security issues

During the free-form question, one of the participants noted that they *"Shouldn't have plugged the USB in to begin with. Highly reduces threat."*, referring to the fact the experimental process was run from a USB stick. This participant is correct in noting that plugging in an untrusted USB stick into a computer is deemed to be a risky security behaviour (United States Computer Emergency Readiness Team 2011).

However, the research was conducted within the confines of Abertay University, and there are restrictions placed upon the software which can be installed on lab machines. Since the software developed was purely a prototype, it was not appropriate to install it on lab machines. Steps were taken to mitigate the risks posed from using the USB sticks. The USB sticks were plugged into university machines only and were not allowed to be used on participant's personal machines.

9.2.7. XUL-based extensions

The monitoring solution and the affective feedback delivery systems were developed as XUL-based extensions. Towards the end of the research project, Mozilla Firefox announced a signing strategy, whereby extensions cannot be installed into the browser unless they have been signed and verified by Mozilla themselves, in an attempt to ensure extension are secure, and are not malicious. Since the software developed as part of this research project is purely experimental, it would be unwise to release it publically, and submit it to Mozilla for signing.

To mitigate any issues, the experiments were conducted via the Mozilla Firefox Developer Edition which has no such issues with requiring signed Firefox extensions.

Some of the security issues which surround XUL arise from the way in which it allows developers to customise their extensions. They allow the developer to extensively customise the user interface, create their own modified JavaScript files, utilise APIs which may not be supported by the Add-on SDK and access the XPCOM (cross platform component object model). Figure 85 provides an overview of the Mozilla platform (Suggi, Liverani and Freeman 2009). At this point it would be prudent for developers to consult the security model used in the creation of Firefox extensions but research presented in 2009 confirmed that worryingly, the "*Mozilla extension security model is nonexistent*" (Suggi, Liverani and Freeman 2009).

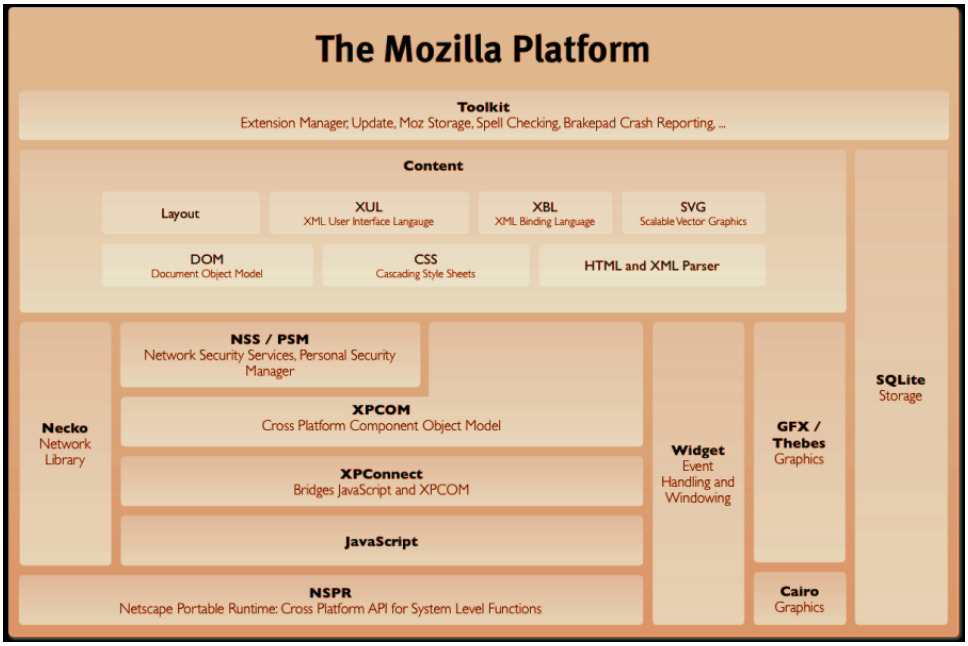


Figure 85 - an overview of the Mozilla platform

The same piece of research notes that there are no boundaries between extensions, meaning that it's possible for one extension to modify another. Additionally, the XPCOM C++ components are subject to memory corruption, and the vulnerabilities are platform independent. Other applications which employ the use of the same extension system are also vulnerable to compromise e.g. the Thunderbird email client (Suggi, Liverani and Freeman 2009).

Similar sentiments have been echoed in a piece of research conducted in 2013, which highlights that little has been done to address the potential security flaws in extensions. The research notes that "*once an extension has been installed, it can enjoy the same privilege level as an administrator of a local machine*", meaning that extensions, malicious or not can read/write/modify local file systems (Shahriar 2013).

Add-ons available from the Mozilla gallery website are deemed to be safe. Extensions submitted to this gallery are checked over, and approved by Mozilla, in a bid to prevent users from installing malicious tools (Mozilla b) 2015). However, in the past, this approach has failed to detect all malicious extensions. It was reported in 2010 that Mozilla failed to detect malware in 2 extensions available from the Add-on gallery. These were experimental extensions which were yet to undergo a public review process however, the extensions contained Trojan horses designed to hijack Windows PCs, and up to 4600 users may have been infected by the issue (Computerworld 2010).

As of August 2015, Mozilla announced the company was effectively deprecating XUL-based extensions, and moving to a new API named WebExtensions, which will be compatible with Chrome and Opera (hence making it easier for developers to create cross-platform extensions) (Mozilla e) 2015). This has been announced in an attempt to improve the security of the web-browsing experience for end-users.

9.2.8. Colour-blind participants

Some people are unaware they are colour-blind, therefore this issue may have applied to some of the participants who took part in the evaluation process: simply asking if participants are colour-blind may not reflect an accurate result.

9.3. Future work

Comments yielded from the free-form section of the questionnaire, and issues encountered during the developmental and experimental processes have identified a number of areas which could be explored in future work.

9.3.1. Adaptation of the extension format

As section 9.2.7. discusses, Mozilla Firefox is moving away from the XUL-based extension format. Whilst Mozilla Firefox is merely the vehicle which is used to investigate the use of a monitoring solution and an affective feedback mechanism, if the underlying concepts are to be explored in the future, the system will need to be moved to the WebExtensions format. One such benefit of this is that the system will be compatible with Chrome and Opera, meaning it can be tested across various devices, providing scope for further research.

9.3.2. Affective feedback delivered

Further research could involve changing some of the affective feedback which was delivered to the participants during the experiment.

The avatars used for this body of research were chosen from a paper by Sacharin et al. (2012), written at the Swiss Center for Affective Sciences and which explored the perception of how people reacted to changing emotional expressions. As part of the experimental process during this body of research, comments were received from participants stating *"The avatar is creepy."*. The avatar utilised was a bald male. One possible avenue for further research is the impact the gender of the avatar has in terms of affect. Such studies have been explored by Gulz et al. (2007) and have the potential to be applied to the realm of cyber security.

Consideration could also be given to the specific phrasing and wordlist used in the affective feedback mechanism. During the experimental process, one participant noted *"I would like to understand the details of why the sites are decided as safe/unsafe"*, indicating they felt there may have been a potential issue with the way in which text-based feedback was delivered to them.

The wordlist which helped in the construction of the affective phrases was called AFINN (AFINN-111.txt) (Nielsen 2011). Potentially, further work could be carried out by applying another wordlist such as ANEW (Affective Norms for English Words) (Bradley and Lang 1999) to the affective phrases included in the affective feedback mechanism. There are also a number of other wordlists available- running a comparison in terms of risky security behaviour could aid in establishing which is the most efficient and appropriate list to use when interacting with average end-users of the internet.

9.3.3. Positioning of the affective feedback on-screen

When reviewing comments made by participants during the experimental process, there were conflicting opinions regarding the positioning of the affective feedback on-screen:

- *"It is fairly large across the bottom of the page, could potentially be made a little smaller"*

- *"When concentrating on the questions and the login details, the feedback didn't draw my attention immediately. It was when I looked away that I noticed the colour then the face."*

The rationale behind placing the affective feedback delivery bar at the bottom of the screen was an attempt to emulate the positioning of the status bars which used to appear in browsers, stating that a site was loading, where it was loading content from, hyperlinks, etc. The affective feedback bar was made large in order to incorporate the various types of information it needed to deliver: password information, general information and information about malicious sites and links. There was too much information to condense into a small sized bar however, the existing bar could be adapted. In making it more transparent, it may seem like it is taking up less of the screen.

Further work carried out in this respect would involve delivering affective feedback on different parts of the screen, in an attempt to ascertain the optimal position for imparting information to the end-user.

9.3.4. Long-term study

The results indicate that when the questionnaire data was compared to the log files and the MySQL database records, there were several areas where there was a statistical significance where users chose to divulge information about themselves across the experiments. The main area in which this occurred was when participants were asked if they had used a dictionary password. The majority of users said "no" in the questionnaire, however this was not reflected in the log files and database records.

The same statistical difference is seen across all of the experiments which delivered varying combinations of affective feedback. This suggests the affective feedback did not make an impact on the actions of the participants. When control logs were compared to affective feedback log files, the majority of results which were returned were insignificant, again suggesting little difference was made by the affective feedback.

However, in gauging the opinions of the participants in relation to affective feedback, positive results were gathered. In asking the participants *"Do you think the feedback provided helped to increase your security awareness?"*, all affective experiment questionnaire data produced a positive, statistically significant result when compared to the control group questionnaire data. The same result was obtained by *asking "Did the feedback encourage you to learn more about online security?"* suggesting participants thought affective feedback had an impact. The weak link between attitude and behaviour (Hini, Gendall and Kearns 1995) should be taken into consideration. Although users felt affective feedback had an impact, this might not translate into a change of behaviour.

When combining these 3 analyses, in the majority of cases, the affective feedback did not change the behaviour of the users during the experimental process however, when polling the opinions of the participants, they indicated they felt like affective feedback could make an impact, and encouraged them to learn. This result may be due to a social desirability response. Participants may have answered the questions in a way that allows them to be perceived favourably by others. Potentially, this suggests that a study over a longer period, utilising affective feedback could slowly raise awareness of risky security behaviour in end-users, and the change would eventually be reflected in log files. Research relating to security fatigue means this may not necessarily be the case however (Furnell and Thomson 2009), as generally speaking, users have issues with long-term retention of security information. Additionally, even if users are provided with security advice, they may reject the information they have been given (Herley 2009).

9.3.5. Specific groups

A piece of feedback received during the experiments stated *"I think this is a good idea to raise awareness on online security especially people that are new to technology."*.

Further research could be explored, in a way to modify the delivery and application of the affective feedback to make it appeal to specific groups. The Office of National Statistics in the UK has noted the rise of Internet users who are aged 75 and over (Office for National Statistics 2016). In 2011, the number of over 75s who recently used the internet was 19.9%. In 2016, this figure has risen to 38.7%. Regardless of the age of the user, they still need to be educated about the dangers of risky security behaviour. Modifying the extension to deliver more appropriate feedback e.g. have less of a focus on colour as the lens of older people tend to yellow, distorting colours (Salvi, Akhtar and Currie 2006) could provide another avenue for investigation.

Similarly, the affective feedback could be modified to appeal to children, helping to educate them about staying safe online from a young age. Some research has stated that fire safety awareness is important, and is taught in schools from a young age; the same should apply to staying safe online (Hoffman 2011).

9.4. Discussion summary

The results display there appears to be value to delivering affective feedback in the context of a browser-based environment, in an effort to enhance the security awareness of end-users, and to encourage them to learn more about online security. Results reflect that according to participants the affective feedback delivery mechanism encouraged them to learn more about online security, and that it helped to increase their online security awareness. Participants largely found the feedback useful, and it made some participants contemplate links they were clicking on, along with consideration of the information shared online. Whilst the results of affective feedback were not directly reflected in the log files, the affective feedback solution could potentially be rolled out as a longer-term solution. Using such a delivery system over the course of a year or more may yield further results, and changes may be reflected in the log files.

Chapter 10. Conclusion

10.1. Research outcomes

The research question driving this body of research was *"Is it possible to enhance security risk awareness in end-users via dynamically provided affective feedback?".* To fully investigate the issue, there were several facets which had to be explored:

- users' awareness of risky security behaviours i.e. do the log files reflect what users said they did in the questionnaires;
- whether affective feedback provided had an impact on the data recorded in the log files;
- whether affective feedback had an impact on the end-users and their subsequent behaviour

10.1.1. User awareness: log files and questionnaires

In addressing the first of these sub-issues, it was found that depending on the question asked, there was a statistical significance between the answer the participants gave in the questionnaire in comparison to the actions they carried out, as recorded in the log files and the database records. Across several of the experiment groups, it was revealed via the database records that 100% of participants in some of the groups revealed personal information about themselves. However, the values gained from questionnaires indicated participants had not realised they had provided such information. This highlights that participants have engaged in risky security behaviour, and points to a poor level of security awareness in the end user.

Significant results were also gained among participants who answered the question asking if they had a dictionary word as a password. Again, more participants had some common element in their password as determined by the log files than admitted to via the questionnaire. The same difference is seen across all experiments containing affective feedback, and reveals a general level of poor password hygiene.

A statistically significant number of users revealed an email address during the course of the experiments, specifically in experiment 4 (text and colour-based feedback) and experiment 5 (text, colour and avatar-based feedback), whilst the other affective feedback-based experiments did not produce a significant result.

In asking participants if they had visited a malicious website during the course of the experiment, a statistically significant result was gained in experiment 1 (control) and experiment 2 (text-based feedback) whereby users visited more malicious links than they admitted to. The result for experiment 1 also highlights the requirement for a tool to help users- if users are not provided with any feedback, they will have no way of knowing a link they are clicking on is malicious.

Generally speaking, what the participants said they did in the questionnaires fail to match with the information gathered in the log files. In many cases, participants were found to have engaged in many more instances of risky security behaviours and it appears they were not aware that they were doing so. The results gained here indicate a generally low level of awareness of risky security behaviour, highlighting a need to raise security awareness in end-users and educate people about security behaviours which are perceived to be risky. The results were uniform across some of the questions asked of the users, particularly surrounding the issue of the information they revealed about themselves. Overall, it appears the delivery of affective feedback did not change the actual behaviour of the end users in this particular body of research.

10.1.2. Impact of affective feedback on log files

Affective feedback did not appear to have an impact on the behaviour of users as recorded by the log files and database records. The majority of results gained were insignificant. One anomaly was generated by experiment 5 (text, colour and avatar-based feedback) when participants were asked about the information they revealed about themselves, in comparison to the control log file. This produced a significant result, where fewer participants in experiment 5 (text, colour, avatar-based feedback) divulged information and this suggests affective feedback may have made a difference. Overall, it has been concluded affective feedback did not have an impact on participant behaviour, as per the log files and database records.

10.1.3. Impact of affective feedback on end-users

Several questions indicated affective feedback successfully impacted on end-users' awareness of risky security behaviours. When compared to the control group, statistically significant results were recorded by those who received some form of affective feedback. Those who received affective feedback felt it helped to increase their security awareness, and that the feedback encouraged them to learn more about online security, a factor which could potentially improve their security awareness in the future, and modify their behaviour. Overall this suggests that affective feedback had an impact on end-users' awareness and will allow them to consider whether their online behaviours could be perceived as risky.

10.1.4. Overall conclusions

In the case of the log files and questionnaires, participants were found to have engaged in instances of risky security behaviours which they were unaware of, and this indicates a generally low level of awareness of risky security behaviour. Whilst the results indicate the affective feedback did not make a difference to behaviour during the course of the experiments, participants felt that the affective feedback delivered had an impact and allowed them to consider whether their online behaviours could be perceived as risky. To conclude, the affective feedback did not have an impact on behaviour, however it enhanced the users' awareness of security risks online. If affective feedback was delivered over a longer period of time, on a daily basis, the log files could potentially reflect positive behavioural changes as end-users become more knowledgeable regarding the subject matter.

10.2. Summary of work conducted

The research goal of the project was to develop and apply knowledge of monitoring techniques and affective feedback, establishing if users' awareness of risky security behaviour is changed, in the context of a browser-based environment. The research question behind the project asked *"Is it possible to enhance security risk awareness in end-users via dynamically provided affective feedback?".*

To answer this question, consideration was given to the current level of awareness in end-users in relation to risky security behaviour. Differing affective feedback techniques were also examined, allowing for the development of a combined monitoring solution and affective feedback system. This system was composed of several Mozilla Firefox extensions, which had the ability to monitor end-user behaviour, and delivered feedback via a combination of affective agents. An experimental design was constructed, to address the research question. Participants took part in a user evaluation of the software tool developed, answering a questionnaire on completion.

Outcomes of the research provided an understanding of users' awareness of risky security behaviours, and determined if affective feedback provided had an impact on the data recorded regarding the behaviour of users. This provided an overall conclusion as to whether affective feedback enhanced security risk awareness in end-users, improving security behaviour.

10.3. Significance of the research

Despite the widespread availability and deployment of anti-malware tools such as virus scanners and firewalls, end-user devices are still open to compromise via the risky security behaviour of the end-users themselves (Li and Siponen 2011). What constitutes risky behaviour is not necessarily obvious to all end-users and as such it is difficult to recognise.

Computer users often perceive the security measures in place within a system to be obtrusive, restricting their ability to perform tasks effectively. Owing to this issue, they often attempt to circumvent these measures, at the risk of breaching system security (Pfleeger and Caputo 2012). In addition to this, computer users are bombarded with data, to the point of information overload, making it difficult for them to discern what is actually happening on their machines (Xu 2011). This lack of awareness can cause a number of problems- average users can easily click on malicious links which are purportedly secure; a fact highlighted by the number of users who have computers infected with viruses and malware. To complicate matters further, if system security has been compromised, an average user is generally unaware.

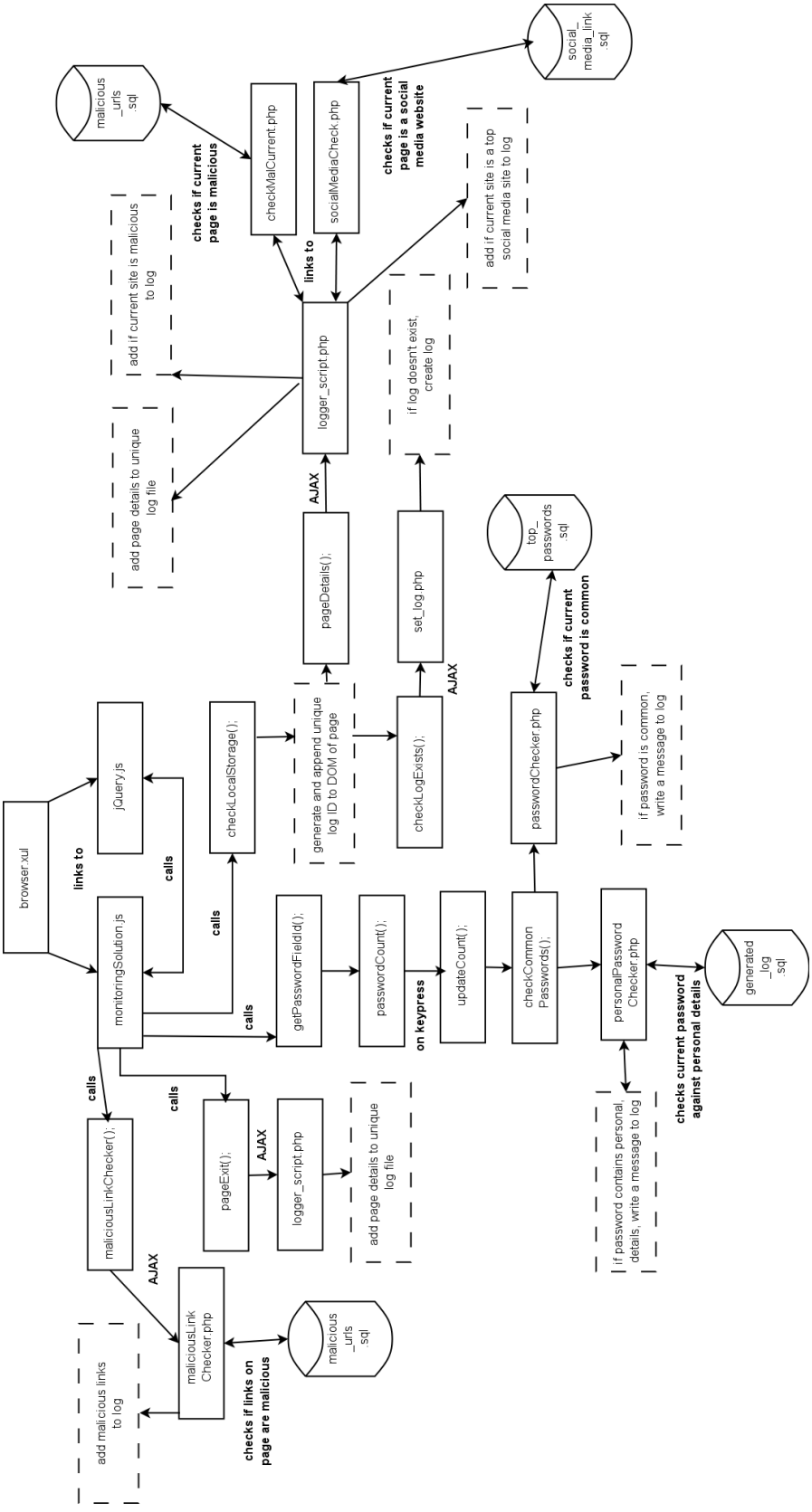
In a study conducted by Ofsted in 2010 (cited by Hoffman 2011), it was reported that some children are now receiving security awareness education in schools, with a view to them maintaining such awareness when left unsupervised on machines. However, a large proportion of the population do not have access to this type of training. It is clear that education is required to help improve a user's understanding of security, a sentiment which has been echoed by the likes of Leah Hoffman who questioned: *"What if we had cybersecurity education programs, like we do for fire safety and AIDS?"* (Hoffman 2011).

The novel aspect of this body of research was to apply a combined monitoring solution and affective feedback delivery approach to a browser-based environment in an effort to ascertain if it could enhance the awareness of risky security behaviours in end-users. Affective feedback was thought to be an appropriate method for improving security awareness in end users as it has parallels with techniques used in some types of online education based systems (Hall et al. 2005) (McDarby et al. 2004) (Robison et al. 2009).

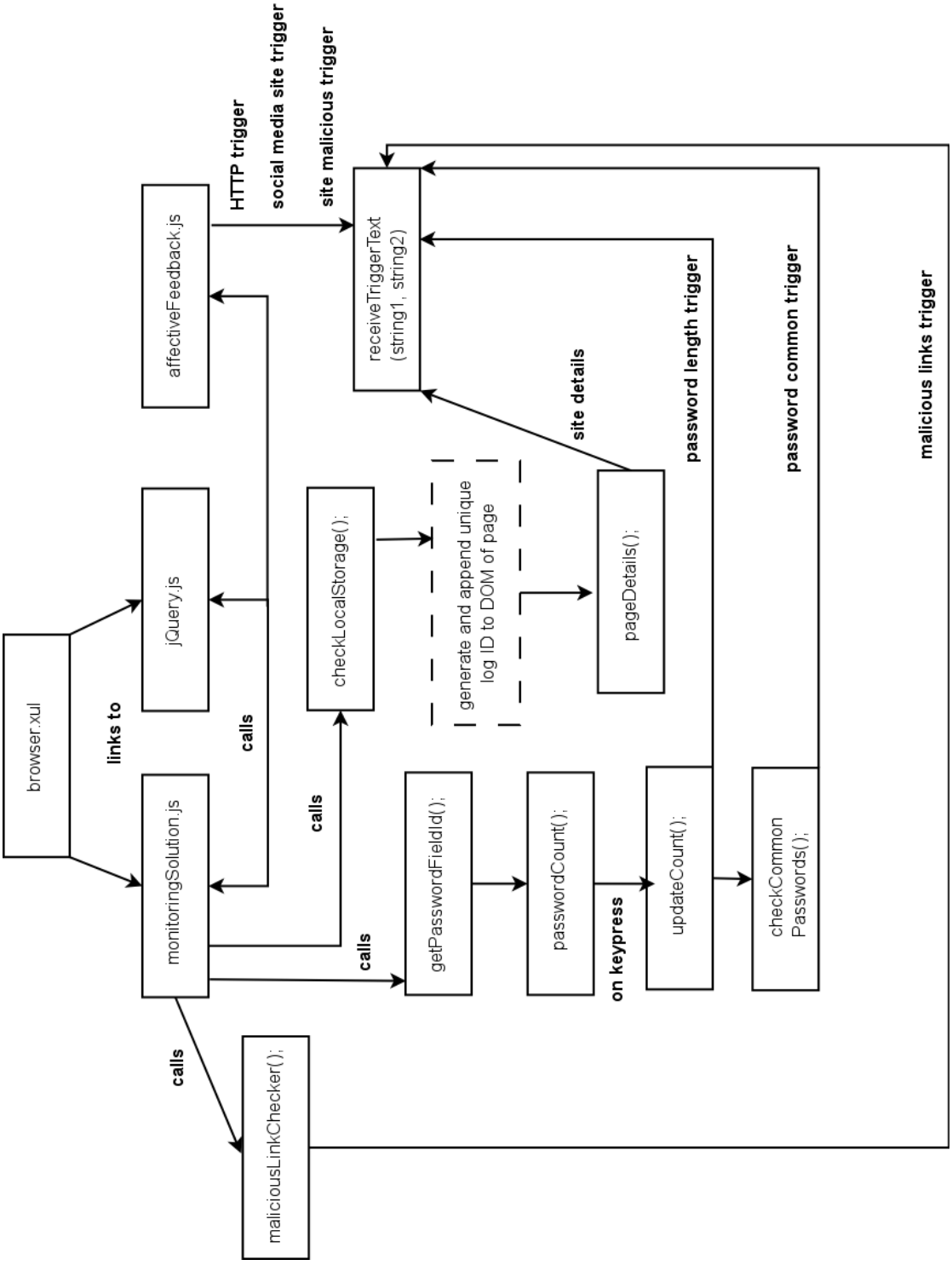
This body of research has made a contribution to the field of affective computing and usable security. Whilst the results indicate the affective feedback made no difference to behaviour, users said it had an impact on them, persuading them to say they would consider their security behaviours online, and encouraging them to pursue online security education. This may be due to a social desirability response, whereby participants answered the questionnaires in a way which allows them to be perceived favourably by others. Since the affective feedback has shown the potential to raise security awareness in end-users, the work satisfies the research question *"Is it possible to enhance security risk awareness in end-users via dynamically provided affective feedback?".*

Appendices

Appendix (i) - overview of the monitoring solution



Appendix (ii) - overview of the affective feedback solution



.

Appendix (iii) - information for test subjects

Purpose of the study

The purpose of the study is to assess whether or not specially developed Firefox extensions assist you whilst browsing the web.

What do the experiments involve?

You will be provided with a USB stick running a portable version of Firefox.

The experiment will involve visiting certain websites. During this time, a Firefox extension may provide you with on-screen feedback and it will record the sites you have visited. Following this, you will be asked to complete a questionnaire asking about your experience whilst browsing the web.

The experiment will take approximately 15 minutes of your time.

Can I withdraw from the study?

Yes, you can withdraw from the study at any time, no questions asked.

Confidentiality

Data used within the system will be held in accordance with the Data Protection Act (1998). Information held within the system will not be used to identify individual test subjects. Information provided by test participants will be removed from the server following the experiments. Passwords are not stored on the server and cannot be viewed.

Risks involved

There are no known risks of being involved with this study.

Further information

If you have any questions or queries regarding this study, contact Lynsay Shepherd – lynsay.shepherd@abertay.ac.uk

Outcome

The results of the study will be published in September 2016 when the dissertation is submitted.

Ethical approval

This study has been approved by the Ethics Committee.

Appendix (iv) - consent form

Consent Form

I agree to take part in the Firefox Extension experiment.

Print name: _____

Sign name: _____

Date: _____

Appendix (v) - instructions for test subjects

Initial steps

- Note: Firefox might be a little slow to respond/load because it's running off a USB stick.

- Insert USB stick

- Click on Firefox developer edition on the USB (if you are unsure about this, please ask for help)

- What number is on your USB stick? Write it here: _____

- There should be a random ID in the top-right of your screen. If the number isn't there, ask for help.

- Write down the ID from the top-right of the screen: _____

Web browsing

- You will be required to visit a number of websites and you may be presented with additional information on-screen. Read the website and information carefully.

- When Firefox loads, you will be presented with a repeat of the information about the experiments. Read the page and tick the box to continue. A proceed button should appear on-screen.

- You will be taken to the "Initial User Form" site which asks for some details. Work your way through this page. Click the button at the end of the form.

- After this page, “Other Site” will ask for more details. Work your way through this page. Click the button at the end of the form.

- If you have a Facebook account, follow the instructions below. If you don’t have a Facebook account, turn the page for further instructions

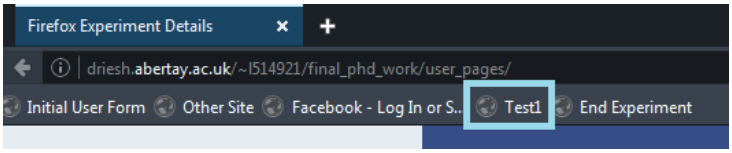
If you have a Facebook account

- There will be a link to Facebook on-screen. Click on the link.

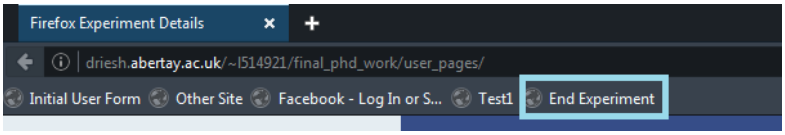
- Enter your password but don’t log in just yet. Read any information you’re provided with.

- Login, post a status update and log out.

- On the toolbar at the top of the screen, click on the Test1 link (see image.) Read any information you’re provided with.



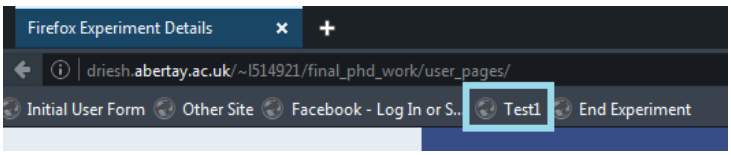
- On the toolbar at the top of the screen, click on the “End Experiment” link (see image.) Read any information you’re provided with.



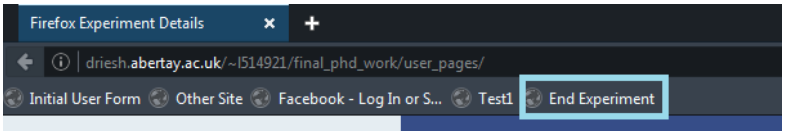
- Click any of the links to end the web-based portion of the experiment.

If you do not have a Facebook account

- On the toolbar at the top of the screen, click on the Test1 link (see image below) Read any information you're provided with.



- On the toolbar at the top of the screen, click on the "End Experiment" link (see image below) Read any information you're provided with.



- Click any of the links to end the web-based portion of the experiment.

Next: complete the questionnaire

Appendix (vi) - experiment questions

General Questions

What number of USB stick did you receive?

_____

What was your user ID (see your "instructions for test subjects") form?

_____

What course of study are you on (if applicable)?

_____

What year of study are you in (if applicable)?

_____

What age category are you in (circle one)?

Under 18 years 18 to 24 years 25 to 34 years 35 to 44 years 45 to 54 years 55 to 64 years Age 65 or older

How would you rate your knowledge of computer security (circle one)?

Excellent Very good Average Poor Very Poor

Were you connected to a public wi-fi network when you participated in the experiments (circle one)?

Yes No Unsure

Did you reveal any personal information about yourself online during the experiment (circle one)?

Yes No Unsure

Are you colourblind (circle one)?

Yes No Unsure

Did you enter a private email address into Firefox during the study (circle one)?

Yes No Unsure

If you logged into Facebook, did you use a password which can be found in a dictionary (circle one)?

Yes No Unsure

If you logged into Facebook, did you use a password containing personal details such as mother's maiden name or the name of a pet (circle one)?

Yes No Unsure

Did you visit any malicious websites (circle one)?

Yes No Unsure

Did you click on any malicious links (circle one)?

Yes No Unsure

Did you notice any of the built-in browser warnings (circle one)?

Yes No Unsure

Feedback Questions

Did you receive any on-screen feedback during the experiments (circle one)?

Yes No Unsure

If you received feedback, what type of feedback did you receive (circle all that apply)?

Colour Text Avatar

If you received multiple types of feedback, which type had the biggest impact (circle one)?

Colour Text Avatar

Did you receive any password-related feedback (circle one)?

Yes No Unsure

If you received negative password-related feedback, did it make you consider changing your Facebook password (circle one)?

Strongly Agree Agree Unsure Disagree Strongly Disagree I didn't receive feedback

Did you receive any social media-related feedback (circle one)?

Yes No Unsure

If you received social media-related feedback, did it make you consider the information you share online (circle one)?

Strongly Agree Agree Unsure Disagree Strongly Disagree I didn't receive feedback

Did you receive any feedback about potentially malicious links on a page (circle one)?

Yes No Unsure

Did you receive any feedback about visiting a malicious page (circle one)?

Yes No Unsure

If you received feedback about malicious links on a page, did it make you consider which links you were clicking on (circle one)?

Strongly Agree Agree Unsure Disagree Strongly Disagree I didn't receive feedback

Did the feedback make you hesitate to provide information online (circle one)?

Strongly Agree Agree Unsure Disagree Strongly Disagree I didn't receive feedback

Did the feedback clearly highlight any issues with the page (circle one)?

Strongly Agree Agree Unsure Disagree Strongly Disagree I didn't receive feedback

Do you think the feedback provided helped to increase your security awareness (circle one)?

Strongly Agree Agree Unsure Disagree Strongly Disagree I didn't receive feedback

Did you find the feedback useful (circle one)?

Strongly Agree Agree Unsure Disagree Strongly Disagree I didn't receive feedback

Did the feedback encourage you to learn more about online security (circle one)?

Strongly Agree Agree Unsure Disagree Strongly Disagree I didn't receive feedback

Any other comments about the extension?

Appendix (vii) - response to “Any other comments about the extension?”

- *"I couldn't understand fully the experiment and what and why Facebook was involved in it."*
- *"No."*
- *"I did not see any noticeable effects of the extension."*
- *"Didn't highlight which links were malicious on the page or I didn’t notice it."*
- *"It wasn’t clear at first what the extension was."*
- *"I find the extension useful for people who do not know much about online security, not exactly for me though. The bit about trustworthiness of the website is pretty ok but most browsers these days warn you when visiting untrusted websites."*
- *"I don't know if the actual feedback comes from a trustworthy source, therefore whether believe it or not."*
- *"Avatar feedback looked amazing but maybe make it less creepy."*
- *"I thought the avatar was an interesting idea as it is certainly eye catching but think the addition of colour would be more effective also if the feedback box was slightly transparent to prevent so much of the screen from being obstructed."*
- *"Very helpful, especially for strong passwords."*
- *"Personally I didn't notice anything out of the ordinary/"*
- *"Good to see feedback about password strength and the potential for visiting malicious links. Think the warnings could have been more prominent. I would recommend this to people."*

- *"More in depth explanation of what the extension does or how it differs from normal Firefox would have helped me understand the study better."*

- *"It is fairly large across the bottom of the page, could potentially be made a little smaller and also possibly be a little more obvious when it detects a potentially unsafe site."*

- *"Text and avatar was useful for password entry. Would be very helpful for people without knowledge of internet security to ensure protection of data."*

- *"Shouldn't have plugged the USB in to begin with. Highly reduces threat."*

- *"After taking test it did make me think more about security online."*

- *"I think this is a good idea to raise awareness on online security especially people that are new to technology. A browser extension is a good delivery method because it doesn't require a lot of setup. I like the idea of the colour coded messages and separates colours for warnings or just general tips."*

- *"When concentrating on the questions and the login details, the feedback didn't draw my attention immediately. It was when I looked away that I noticed the colour then the face."*

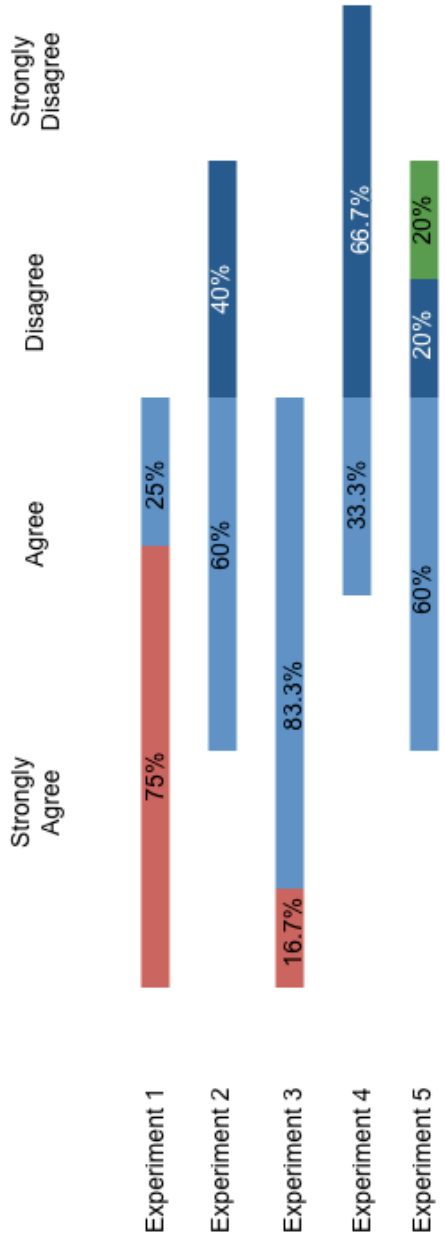
- *"The toolbars at the bottom are clever but I would like to understand the details of why the sites are decided as safe/unsafe. I don't tent to trust statements about security without reasoning."*

- *"There is a need to be very sure about the security nature of any site before giving out some personal information that are not made public."*

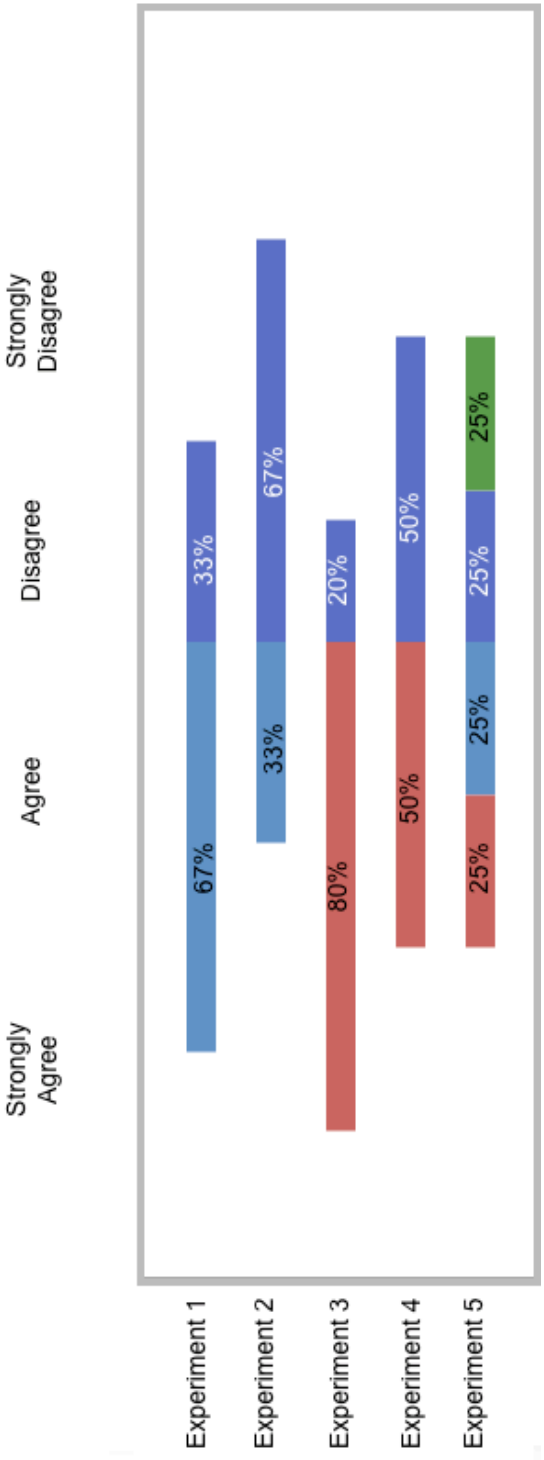
- *"The avatar is creepy."*

Appendix (viii) - diverging bar charts based on Likert data

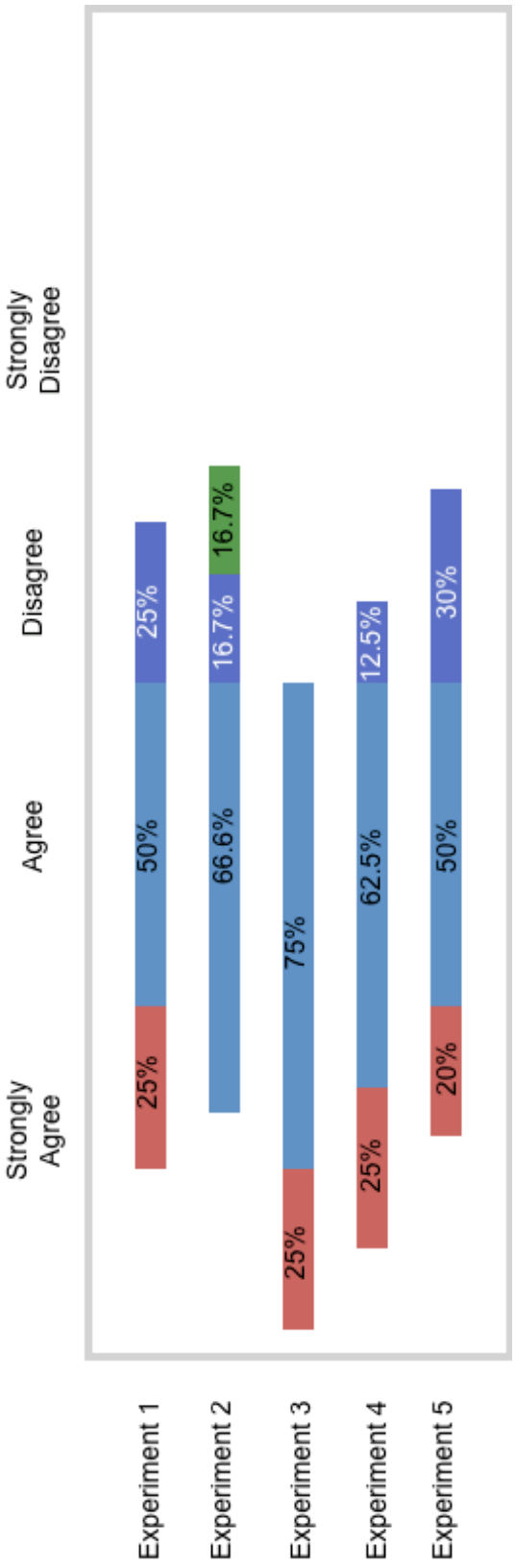
If you received negative password-related feedback, did it make you consider changing your Facebook password?



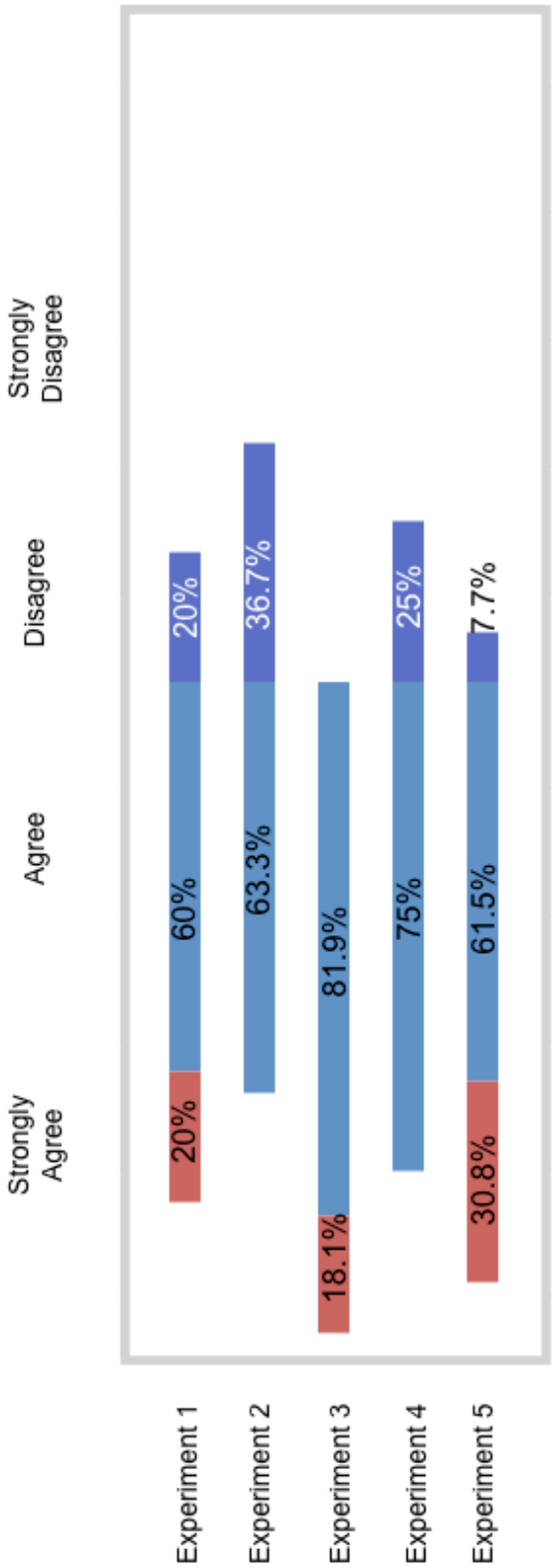
If you received social media-related feedback, did it make you consider the information you share online?



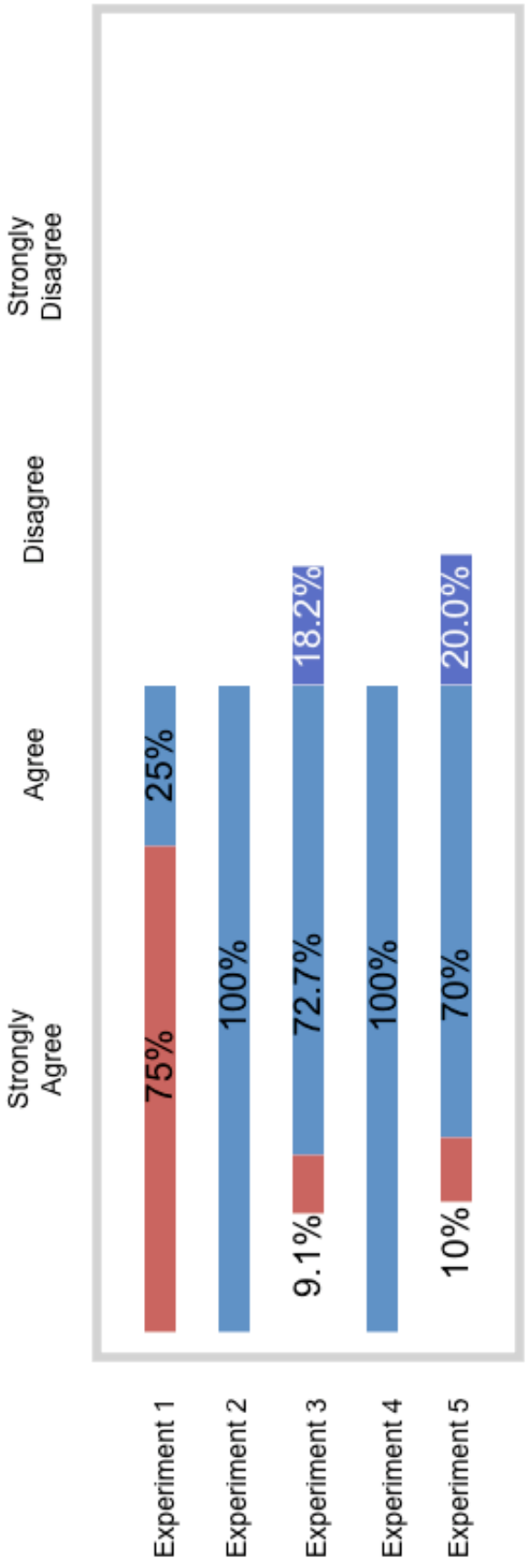
If you received feedback about malicious links on a page, did it make you consider which links you were clicking on?



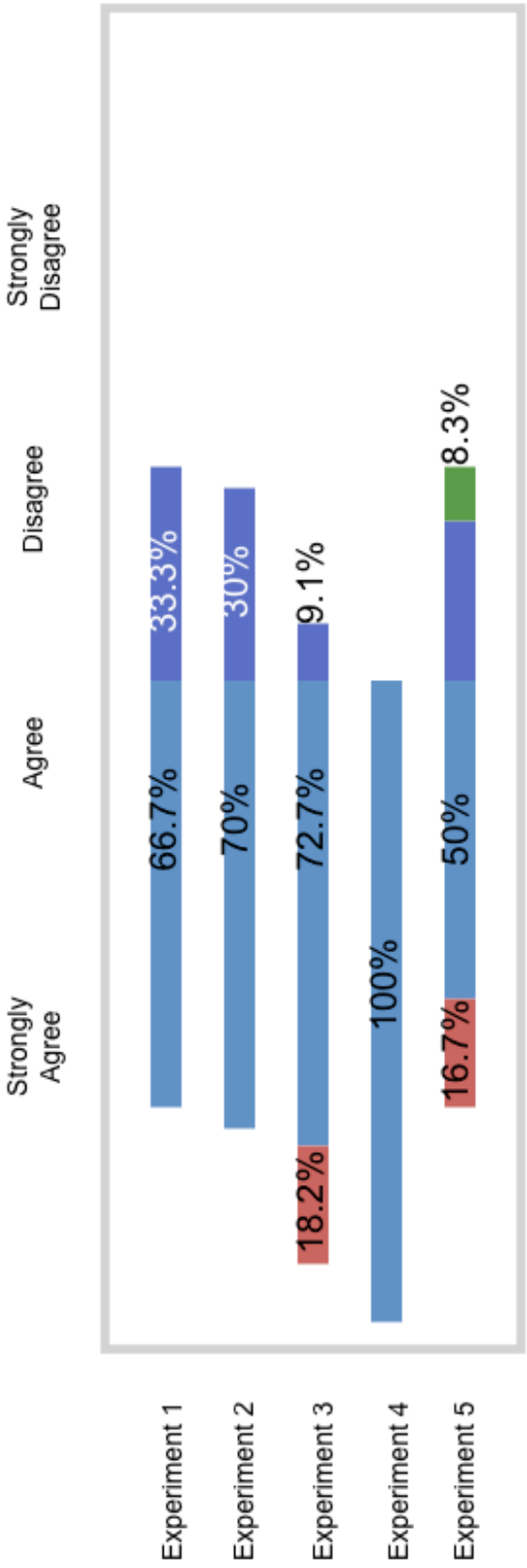
Did the feedback make you hesitate to provide information online?



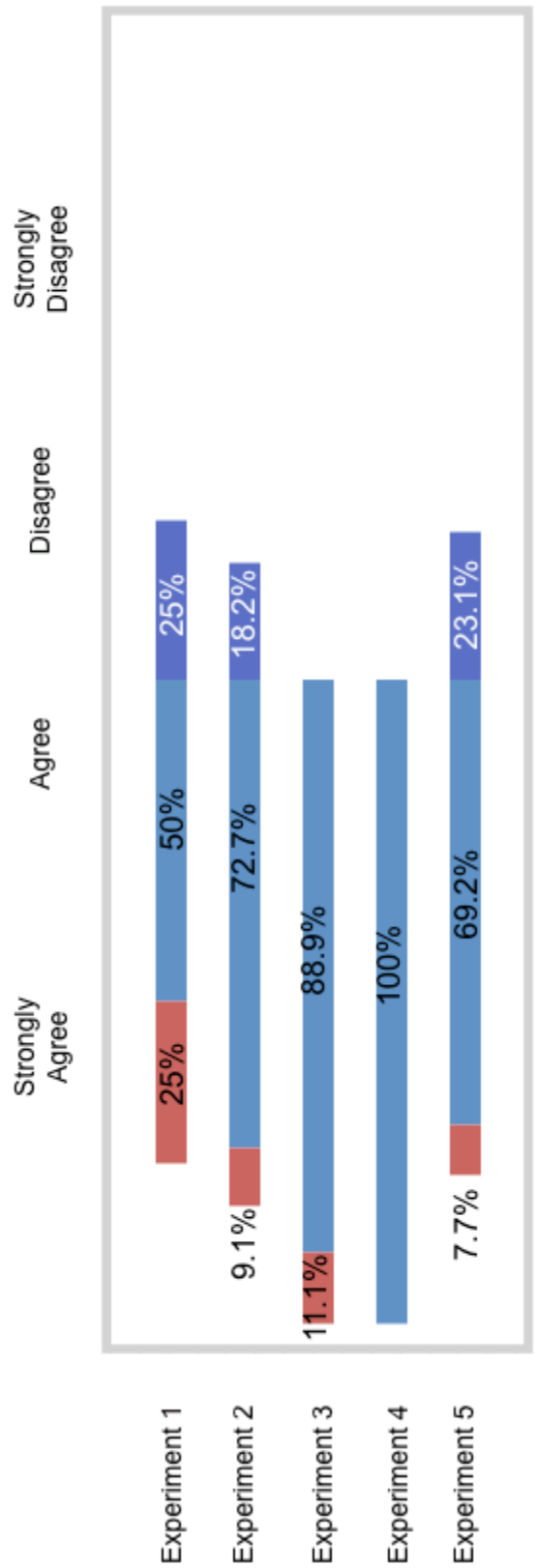
Did the feedback clearly highlight any issues with the page?



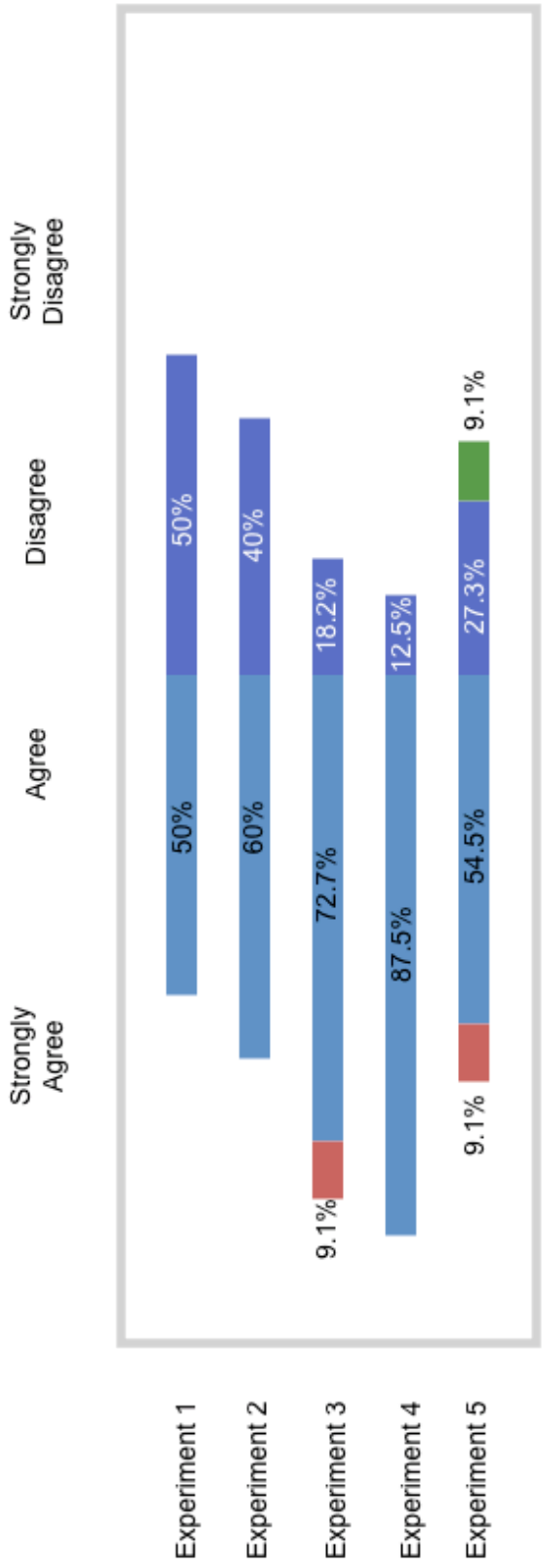
Do you think the feedback provided helped to increase your security awareness?



Did you find the feedback useful?



Did the feedback encourage you to learn more about online security?



Appendix (ix) - publications

Below is a list of publications generated as a result of the research project:

- Shepherd L. A., Archibald J., Ferguson R. I. Reducing Risky Security Behaviours: Utilising Affective Feedback to Educate Users. Future Internet. 2014; 6(4):760-772.

- Shepherd, L. A. Archibald, J. and Ferguson, R. I. (2014). Reducing risky security behaviours: utilising affective feedback to educate users, Proceedings of Cyberforensics 2014, University of Strathclyde, Glasgow, pp7-14, 2014

- Shepherd, L. A. Archibald, J. and Ferguson, R. I. (2013). Perception of risky security behaviour by users: survey of current approaches. Human Aspects of Information Security, Privacy, and Trust: Lecture Notes in Computer Science, 8030, pp176-185

Appendix (x) - completed ethics form

REAS

School of Engineering, Computing and Applied Mathematics

Staff and Research Student

Form REAS

ETHICS

Please complete all sections as required and follow instructions at end of form.

A - Personal Details -

Summary Information

Project Leader/Research Student (Name)
Ms Lynsay Shepherd

Proposed work	
A generic programme of research with similar ethical issues	
• Individual researcher	No
• Research Centre	No
An individual programme of research	
• Individual Postgraduate Research Student	Yes
• Individual Staff Researcher	No

Others involved in work on project (name(s)):
• UAD Staff- Dr Jackie Archibald and Dr Ian Ferguson

B - Project Details

Project title: Enhancing security risk awareness in end-users via affective feedback

Proposed start date and duration: 1st September 2012. 3 year project.

Main Aim of Study:
• Ascertain the most unobtrusive way to direct affective feedback to an average computer user • Determine if a monitoring agent with affective feedback can be used to enhance system security

Creator: CES/AMG Joint Research Ethics Committee; **approved by**: CES/AMG Joint Research Ethics Committee; **approval date**: 30/6/2011 **activity/task**: research/research ethics; **review date**: next review 29/06/2012
Macintosh HD:Users:lynsay:Documents:Lynsay's Stuff:University Stuff:Important Documents:Ethics Form and Supporting Docs:EthicsStaffResearchStudents.doc

*Has the proposal been considered by:	Yes/No
Peer review by an external sponsor Internal peer review A Local Ethics Committee? Date of consideration: If yes to any of above please attach a copy of the external report and decision.	Yes Yes No 15/06/12

Is the research externally funded?: If Yes was the ethics approval for the research grant application: • Full (considered and fully approved by SREC prior to submission) • Interim (SREC Chair approved subject to full consideration at a later date) • Rejected	Yes (SICSA) Yes

C – Proposal

On a separate page (not more than two sides of A4 in total) please state:

- the background to the project and the need for the project to be undertaken
- where the research will be undertaken
- the methods or procedures to be used
- the anticipated outcome(s)

D - Ethical Issues

What ethical issues do you think this research raises?

Experiments are to be carried out with test subjects, therefore potential ethical issues would pertain the rights of these subjects. The code of good practise outlined in section F of this document will be adhered to at all times during the experiments, upholding the rights of subjects.

Specifically, the research will employ the use of a Firefox extension to monitor user behaviour, therefore some information about the way a user interacts with a site will be collected. The information collected will not identify users however when they are browsing a site, it will be used to provide real-time feedback.

E – Type of Research

What type of research approach will you undertake?

Table : E1

	Yes/No
Literature Based	Yes
Survey	Yes
Experiment	Yes
Qualitative	Yes
Other (please specify):	

Will you use any of the following research methods ?

Table : E2

	Yes/No
Questionnaires	Yes
Interviews	No
Observation overt (open observation)	Yes
Observation covert (concealed observation)	No
Other :	

User behaviour will be monitored via the use of a Firefox extension, as explained in section D.

F – Human Subjects

Does this research involve human subjects ? Yes/No | Yes

If the answer is **YES**, you must complete this section fully
If the answer is **NO** please go directly to section **G - Declaration**

Please state the intended number of research subjects : 100

Who are the intended research subjects ? (generally, not by name) :

Students who may use computers on a daily basis but do not study the subject i.e. average users. In terms of the university, this means students outwith SECAM and AMG.

How do you intend to recruit these subjects ?

Placing a notice on the university portal.

Ask school offices to email students, requesting their participation in experiments

Could any of your research methods cause your subjects discomfort, anxiety, stress or embarrassment ? if so, how do you intend to minimise this ? **Yes/No** | No

Please confirm that you intend to adopt the following good practice when dealing with your research subjects :	**Yes/No**
The subjects will be provided with a written / oral explanation of the project.	Yes
The subjects will be asked to complete a consent form.	Yes
The subjects will be advised that they may not benefit from this study.	Yes
It will be made clear to the research subjects that they can withdraw from this study at any time.	Yes
The subjects will be offered a guarantee of confidentiality.	Yes
The subjects will be offered a guarantee of anonymity.	Yes
The Data Protection Act will be adhered to.	Yes
The health and safety of the researcher will be taken into consideration.	Yes
The subjects will be advised of any potential health and safety risks involved in taking part in this study.	Yes

The subjects will be provided with contact details of a member of the research team.	Yes
You will indicate to your subjects how and when they will hear the outcome of this research.	Yes

G - Declaration

I agree that :	**Agree Yes/No**
Where relevant, I have discussed with my supervisory team the use of Human Subjects in this research project.	Yes
I agree to discuss all the necessary permission forms/questionnaires/interview questions relating to this application with my supervisory team.	Yes

Name : Lynsay Shepherd

Date : 04/03/13

What to do next :

Submit electronically to ces@abertay.ac.uk for consideration by the School/Institute Research Ethics Sub Committee. All correspondence regarding this application should be conducted by email to above address.

*This normally relates to medically related research.

Creator: CES/AMG Joint Research Ethics Committee; **approved by**: CES/AMG Joint Research Ethics Committee; **approval date**: 30/6/2011 **activity/task**: research/research ethics; **review date**: next review 29/06/2012
Macintosh HD:Users:lynsay:Documents:Lynsay's Stuff:University Stuff:Important Documents:Ethics Form and Supporting Docs:EthicsStaffResearchStudents.doc

Appendix (xi) - ethical approval email

From: **Snedden, Ruth**
Subject: Ethics Approval No 1739
Date: 18 March 2013 at 14:47
To: Shepherd, Lynsay

Hello Lynsay
Ethics Approval – Application No 1739– 2012/13
Enhancing security risk awareness in end-users via affective feedback
Your Application to the School Research Ethics Committee has now been Approved, and your Letter is here for you at Reception, Level 4 to collect.
Kind regards

References

Abeyratna, S., Paramei, G. and Tawfik, H. 2010. An affective interface for conveying user feedback. *KSim2010 - UKSim 12th International Conference on Computer Modelling and Simulation*, pp.369–374.

Adams, F. M., and Osgood, C. E. 1973. *A cross-cultural study of the affective meanings of color. Journal of cross-cultural psychology*, 4(2), pp. 135-156.

Al-Ameen, M. N., Wright,M., and Scielzo, S. 2015. Towards Making Random Passwords Memorable: Leveraging Users' Cognitive Ability Through Multiple Cues. [online]. *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, pp. 315–2324.

Alexa (2016). *The top 500 sites on the web*. [online]. http://www.alexa.com/topsites/category/Computers/Internet/On_the_Web/Online_Communities/Social_Networking [Accessed 10 May 2016].

Alkaldi, N., and Renaud, K. 2016. Why do People Adopt, or Reject, Smartphone Security Tools?. *Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016).* Pp. 135-144

ANEW. 2015. *ANEW Message*. [online]. http://csea.phhp.ufl.edu/media/anewmessage.html [Accessed 10 May 2016].

Arguedas, M., Xhafa, F., Daradoumis, T. and Caballe, S. 2015. An Ontology about Emotion Awareness and Affective Feedback in Elearning. *2015 International Conference on Intelligent Networking and Collaborative Systems, Taipei*. pp. 156-163.

ARS Technica UK. 2016*. Firefox trundles past Microsoft browsers for first time- Chrome remains king*. [online]. http://arstechnica.co.uk/business/2016/05/firefox-overtakes-microsoft-internet-explorer-edge-browsers-first-time-statcounter/. [Accessed 30 May 2016].

ARS Technica UK (2012). *Firefox fights back, holds on to second place in world browser share*. [online]. https://arstechnica.com/information-technology/2012/07/firefox-fights-back-holds-on-to-second-place-in-world-browser-shares/). [Accessed 30 May 2016].

Arvolaa, A., Vassallob, M., Deanc, M., Lampilaa, P., Sabab, A., Lähteenmäkia, L., Shepherd, R. 2008. Predicting intentions to purchase organic food: the role of affective and moral attitudes in the theory of planned behaviour. *Appetite* 50:2. pp. 443-454.

Kralik, J.D. 2011. Stop On Red! The Effects of Color May Lie Deep in Evolution…. [online]. http://www.psychologicalscience.org/index.php/news/releases/stop-on-red-a-monkey-study-suggests-that-the-effects-of-color-lie-deep-in-evolution.html

Avey, J.B., Wernsing T.S., and Luthans, F. 2008. Can positive employees help positive organizational change? Impact of psychological capital and emotions on relevant attitudes and behaviors. *The Journal of Applied Behavioral Science* 44:1. pp. 48-70.

Balduzzi, M. 2011. Attacking the privacy of social network users. [online]. HITB. http://conference.hitb.org/hitbsecconf2011kul/materials/ D1T1%20%20Marco%20Balduzzi%20-%20Attacking%20the%20Privacy% 20of%20Social%20Network%20Users.pdf [Accessed 30 April 2014].

Basnet, R.B. and Doleck T. 2015. Towards Developing a Tool to Detect Phishing URLs: A Machine Learning Approach. *2015 IEEE International Conference on Computational Intelligence & Communication Technology*, Ghaziabad. pp. 220-223.

Beale, R, and Creed, C. 2009. Affective Interaction: How emotional agents affect users. [online]. *In : International Journal of Human-Computer Studies*, 67, pp.755-776.

Besmer, A. 2009. Social Applications: Exploring A More Secure Framework. *In: Symposium On Usable Privacy and Security (SOUPS 2009),* pp.1- 10.

Bicakci, K., Yuceel, M., Erdeniz, B., Gurbaslar, H. and Atalay, N. 2009. Graphical Passwords as Browser Extension: Implementation and Usability Study. *In: Symposium On Usable Privacy and Security (SOUPS 2009).* pp.1-17.

Bradley, M.M. and Lang, P.J. 1999. Affective norms for English words (ANEW): Instruction manual and affective ratings. Technical Report C-1. *The Center for Research in Psychophysiology.*

Bubaš, G., Orehova, T. and & Konecki, M. 2008. Factors and Predictors of Online Security and Privacy Behavior. *Journal of Information and Organizational Sciences*. 32 (2), pp.79–98.

Ciampa, M. 2013. A comparison of password feedback mechanisms and their impact on password entropy. *Information Management & Computer Security*. 21:5. pp. 344–359.

Canova, G., Volkamer, M. Bergmann, C. Reinheimer, B. 2015. Nophish app evaluation: lab and retention study. *In: NDSS workshop on usable security.*

Cegan J., Soukal J., Drasar, M., and Vykopal J. 2012. PhiGARo – tool for phishing incident processing. Masaryk University. [Online]. Available from: http://www.muni.cz/ics/services/csirt/tools/phigaro [Accessed 02 April 2017].

Colour Lovers. 2016. http://www.colourlovers.com/. [online]. http://www.colourlovers.com/ [Accessed 30 April 2016].

Computerworld. 2010. *Mozilla confirms infected Firefox add-ons slipped through security*. [online]. http://www.computerworld.com/article/2520691/networking/mozilla-confirms-infected-firefox-add-ons-slipped-through-security.html [Accessed 30 April 2016].

Daniel Miessler. 2014 . 10k_most_common.txt. [online]. https://github.com/danielmiessler/SecLists/blob/master/Passwords/10k_most_common.txt [Accessed 30 April 2016].

De Carné De Carnavalet, X. and Mannan M. 2015. A Large-Scale Evaluation of High-Impact Password Strength Meters. *ACM Transactions. Information. Systems. Security*. 18(1), Article 1.

Dehn, D. and Van Mulken, S. 2012. The impact of animated interface agents: a review of empirical research. [online]. *International Journal of Human– Computer Studies*. 52 (1), pp.1-22.

Derose, Steven J. 2005. *The Compass DeRose Guide to Emotion Words*. [online]. http://www.derose.net/steve/resources/emotionwords/ewords.html [Accessed 30 April 2016].

Dhamija, R. and Tygar, J. 2005. The Battle Against Phishing: Dynamic Security Skins. In: *Symposium On Usable Privacy and Security (SOUPS 2005).*, pp.1-12.

Doubleday, A., Ryan, M., Springett, M. and Sutcliffe. (1997). A comparison of usability techniques for evaluating design. [online]. *In: Proceedings of the 2nd Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, DIS 1997, pp.101–110.

Ekman, P. 1999. Basic emotions. [online]. *Cognition*. http://doi.org/10.1002/0470013494.ch3

Egelman S., Sotirakopoulos A., Muslukhov, I., Beznosov, K., and Herley, C. 2013. Does my password go up to eleven?: the impact of password meters on password selection. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, Paris*. pp. 2379–2388.

Farahmand, F., Dark, M., Liles, S., Sorge, B. 2009. Risk perceptions of information security: A measurement study. *In: Proceedings of the 2009 International Conference on Computational Science and Engineering, CSE 2009*. pp.462–469.

Farahmand, F., Atallah, M.J., and Spafford, E.H. 2013. Incentive Alignment and Risk Perception: An Information Security Application. *In: IEEE Transactions on Engineering Management, vol. 60, no. 2*. pp. 238-246.

Farter. 2011. *Using localStorage in Firefox Extensions for Persistent Data Storage*. [online]. http://fartersoft.com/blog/2011/03/07/using-localstorage-in-firefox-extensions-for-persistent-data-storage/ [Accessed 30 April 2016].

FBI. 2013. *FBI Warns Public That Cyber Criminals Continue to Use Spear-Phishing Attacks to Compromise Computer Networks*. [online]. Retrieved from: http://www.fbi.gov/sandiego/press-releases/2013/fbi-warns-public-that-cyber-criminals- continue-to-use-spear-phishing-attacks-to-compromise-computer-networks. [Accessed 30 April 2016].

Fenstermacher, K.D. and Ginsburg, M.A. 2002. Lightweight framework for cross-application user monitoring. [online]. *IEEE Computer*. pp.51–58.

Fetscherin, M. 2009. Importance of cultural and risk aspects in music piracy: A cross-national comparison among university students. *Journal of Electronic Commerce Research.*

Fischoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B. 1978. How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sciences*. 9 (2), pp.127–152.

Furnell, S., Jusoh, A. and Katsabas, D. 2006. The challenges of understanding and using security: a survey of end- users. *Computers & Security*, 25 (1), pp.27-35

Furnell, S., and Thomson, K. 2009. Recognising and addressing 'security fatigue'. *Computer Fraud & Security*. pp. 7-11.

Gievska, S., Koroveshovski, K. and Chavdarova, T. 2014. A Hybrid Approach for Emotion Detection in Support of Affective Interaction. *International Conference on Data Mining Workshop*. pp.352-359.

Gulz, A., Ahlner, F. and Haake, M. 2007. Visual Femininity and Masculinity in Synthetic Characters and Patterns of Affect. *ACII 2007, LNCS*. pp.654–665.

Hadnagy, C. 2011. *Social engineering: the art of human hacking*. Indianapolis, Wiley Publishing.

Hall, L., Woods, S., Aylett, R. and Paiva, A. 2005. Achieving empathic engagement through affective interaction with synthetic characters. *In: TAO, J., Tan, T., Picard, R.W., (ed.). ACII 2005, Heidelberg, LNCS Springer*. pp 731–738.

Heishman, R., Duric, Z. and Wechsler, H. 2007. Understanding cognitive and affective states using eyelid movements]. *In: First IEEE International Conference on Biometrics: Theory, Applications, and Systems, BTAS 2007*. pp.1-6.

Herath, T. and Rao, H.R. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Syst, 47 (2). pp.154–165.

Herley, C. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. *Proceedings of the 2009 workshop on New security paradigms workshop. ACM, 2009.*

Hernandez, J., Paredes, P., Roseway, A. and Czerwinski, M. 2014. Under Pressure: Sensing Stress of Computer Users. *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems - CHI '14.* pp.51–60.

Hibshi, H., Breaux, T.D. and Broomell, S.B. 2015. Assessment of risk perception in security requirements composition. *2015 IEEE 23rd International Requirements Engineering Conference (RE), Ottawa, ON, 2015*. pp. 146-155.

Hilbert, D. and Redmiles, D.F. 2000. Extracting Usability Information from User Interface Events. *ACM Computing Surveys*. pp.384-421.

Hill, R. and Donaldson, D. R. 2015. Bridging the Trust Gap: Integrating Models of Behavior and Perception. *NSPW '15 Proceedings of the 2015 New Security Paradigms Workshop*. pp.148-155.

Hini, D., Gendall, P., and Kearns, Z. 1995. The link between environmental attitudes and behaviour. *Marketing Bulletin*. 6.3. pp. 22-31.

Hoffman, L. 2011. Risky business. Communications of the ACM, 54 (11). pp. 20-22.

HpHosts. 2016. [online]. http://www.hosts-file.net/ [Accessed 30 April 2016].

Husák, M. and Cegan J. 2014. PhiGARo: Automatic Phishing Detection and Incident Response Framework. *2014 Ninth International Conference on Availability, Reliability and Security, Fribourg.* pp. 295-302.

Iovane, G., Salerno, S., Giordano, P., Ingenito, G. and Mangione, G.R. 2012. A Computational Model for Managing Emotions and Affections in Emotional Learning Platforms and Learning Experience in Emotional Computing Context. *2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems, Palermo*. pp. 873-880.

Imdb.Com. 2016. *Ghostbusters*. [online]. http://gb.imdb.com/title/tt0087332/ [Accessed 30 April 2016].

Imperva. 2016. *Cross-Site Scripting*. [online]. http://www.imperva.com/Resources/Glossary?term=cross_site_scripting [Accessed 30 April 2016].

Jameson, A. and Riedl, J. 2011. Introduction to the transactions on interactive intelligent systems. *ACM Transactions on Interactive Intelligent Systems (TiiS).* 1 (1), pp.1-6.

Kaspersky Lab A). 2013. *Kaspersky Lab report: 37.3 million users experienced phishing attacks in the last year*. [online]. http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year [Accessed 30 April 2016].

Kaspersky Lab. 2013. *Kaspersky security bulletin 2013*. [online]. http://media.kaspersky.com/pdf/KSB_2013_EN.pdf [Accessed 30 April 2016].

Kelley, P. 2009. A “Nutrition Label” for Privacy. *In: Symposium On Usable Privacy and Security*. pp.1-12.

Kumaraguru, P., Cranshaw J., Acquisti, A., Cranor, L., Hong, J.,Blair, M. and Pham, T. 2009. School of Phish: A Real-World Evaluation of Anti-Phishing Training*. In: Symposium On Usable Privacy and Security (SOUPS 2009)*. pp.1-12.

Kumi, R., Conway, C.M., Limayem, M and Goyal, S. 2013. Research Article Learning in Color: How Color and Affect Influence Learning Outcomes. *IEEE Transactions on Professional Communication*. Vol. 56, no. 1, pp. 2-15.

Labunets, K., Massacci, F., Paci, F. and Tran, L.M.S. 2013. An Experimental Comparison of Two Risk-Based Security Methods. *2013 ACM / IEEE International Symposium on Empirical Software Engineering and Measurement, Baltimore, MD*. pp. 163-172.

Larose, R., and Rifon, N. J. 2007. Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *[Journal of Consumer Affairs*, 41 (1), pp.127-149.

Li, Y. and Siponen, M. 2011. A call for research on home users information security behaviour. *In: PACIS 2011, Proceedings,.*

Lottridge, D., Chignell, M. and Jovicic. 2011. Affective Interaction: Understanding, Evaluating, and Designing for Human Emotion. *In: Reviews of Human Factors and Ergonomics*. pp.197-237.

Lund Research Ltd. 2013. *Mann-Whitney U Test using SPSS Statistics*. [online]. https://statistics.laerd.com/spss-tutorials/mann-whitney-u-test-using-spss-statistics.php. [Accessed 30 April 2016].

Maurer, M., De Luca, A. and Kempe, S. 2011. Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness. *In: Symposium On Usable Privacy and Security (SOUPS 2011)*. pp.1-13.

Mcdarby, G., Condron, J., Hughes, D. and Augenblick, N. 2004. *Affective feedback*. Media Lab Europe. [online].. http://medialabeurope.org/mindgames/publications/publicationsAffectiveFeedbackEnablingTechnologies.pdf. [Accessed 30 April 2016].

Measuring Usability Llc. 2016. *A/B Test Calculator*. [online]. http://www.measuringu.com/ab-calc.php. [Accessed 30 April 2016].

Milne, G. R., Labrecque, L. I. and & Cromer, C. 2009. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*. 43 (3). pp.449–473.

Milne, G. R., Rohm, A. J. and Bahl, S. 2004. Consumers' Protection of Online Privacy and Identity. *Journal of Consumer Affairs*. pp.217–232.

Mostyn, B. 1978. *The attitude behaviour relationship*. Available from: https://dspace.lib.cranfield.ac.uk/bitstream/1826/2968/1/MCRC%2015.PDF. [Accessed 02 February 2017].

Mozilla A). 2015. *History of the Mozilla Project*. [online]. https://www.mozilla.org/en-US/about/history/details/. [Accessed 30 April 2016].

Mozilla B). 2015. *Frequently Asked Questions*. [online]. https://addons.mozilla.org/en- us/faq. [Accessed 30 April 2016].

Mozilla C). 2015. *Code Snippet*. [online]. https://developer.mozilla.org/en-US/Add-ons/Code_snippets/On_page_load. [Accessed 30 April 2016].

Mozilla D). 2015. *Local Storage*. [online]. https://developer.mozilla.org/en-US/Add-ons/Overlay_Extensions/XUL_School/Local_Storage#Logging. [Accessed 30 April 2016].

Mozilla E). 2015. *The Future of Developing Firefox Add-ons*. [online]. https://blog.mozilla.org/addons/2015/08/21/the-future-of-developing-firefox-add-ons// [Accessed 30 April 2016].

Mozilla Developer Network A). 2015. *Security best practices in extensions*. [online]. https://developer.mozilla.org/en-US/Add ons/Security_best_practices_in_extensions. [Accessed 30 April 2016].

Mozilla Developer Network. 2015. *SDK and XUL Comparison*. [online]. https://developer.mozilla.org/en-US/Add-ons/SDK/Guides/SDK_vs_XUL. [Accessed 30 April 2016].

Myers, D. 2004. *Social Psychology with SocialSense, chapter 4*. Available from: http://highered.mheducation.com/sites/dl/free/0070952027/363504/Ch04_Myers3Ce.pdf [Accessed 02 February 2017].

Nalisnick and Baird. 2013. Character-to-Character Sentiment Analysis in Shakespeare's Plays. *Proceedings of the 51st Annual Meeting of the Association for Computational Linguistics*. pp.479–483.

Ng, B., Kankanhalli, A. and Xu, Y. 2009. Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46 (4), pp.815–825.

Nielsen, F. 2011. A new ANEW: evaluation of a word list for sentiment analysis in microblogs. *Proceedings of the ESWC2011 Workshop on 'Making Sense of Microposts': Big things come in small packages. Volume 718 in CEUR Workshop Proceedings*, pp.93-98.

Novak, D., Nagle, A. and Riener, R. 2014. Linking Recognition Accuracy and User Experience in an Affective Feedback Loop. *IEEE Transactions on Affective Computing*. Vol. 5, no. 2, pp. 168-172.

Nyman, R. 2009. *How to develop a Firefox extension*. [online]. https://robertnyman.com/2009/01/24/how-to-develop-a-firefox-extension/. [Accessed 30 April 2016].

Office For National Statistics. 2016. *Internet users in the UK: 2016*. [online]. http://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2016#recent-internet-use-is-on-the-increase-for-those-aged-65-and-over. [Accessed 3 August 2016].

Olson, J.M., and Zanna, M.P. 1993. Attitudes and attitude change. *Annual review of psychology*. 44(1) pp. 117-154.

OWASP. 2016. *Password length & complexity*. [online]. https://www.owasp.org/index.php/Password_length_&_complexity. [Accessed 30 April 2016].

Ozdemir, C. and Bergler, S. 2015. A Comparative Study of Different Sentiment Lexica for Sentiment Analysis of Tweets. *Proceedings of Recent Advances in Natural Language Processing*. pp.488–496

Padayachee, K. 2012. Taxonomy of compliant information security behavior. *Computers & Security.* 31 (5), pp. 673–680.

Parkin, S., Krol, K., Becker, I. and Sasse, M.A. 2016. Applying Cognitive Control Modes to Identify Security Fatigue Hotspots. Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association.

Payne, B. and Edwards, W. 2008. A brief introduction to usable security. *Internet Computing*. 12 (3), pp. 13–21.

Pfleeger and Caputo. 2012. Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*.

Picard, R. 2000. *Affective Computing*. MIT Press.

Ranieri, C.M. and Romero, R.A.F. 2016. An Emotion-Based Interaction Strategy to Improve Human-Robot Interaction. *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR), Recife*. pp. 31-36.

Robison, J., McQuiggan, S., Lester, J. 2009. Evaluating the consequences of affective feedback in intelligent tutoring systems. *In: Proceedings of International Conference on Affective Computing and Intelligent Interaction, ACII 2009*. pp. 37–42.

Sacharin, V., Sander, D. and Scherer, K. R. 2012. The perception of changing emotion expressions. *Cognition & Emotion.* pp.1273–1300.

Salvi, S. M., Akhtar, S., and Currie, Z. 2006. Ageing changes in the eye. *Postgraduate Medical Journal, 971*. pp.581–587.

San-José, P. And Rodriguez, S. 2011. Study on information security and e-Trust in Spanish households. *In: Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS 2011*. pp.1-6.

Schechter, S.E., Dhamija, R., Ozment, A. and Fischer, I. 2007. The Emperor's New Security Indicators. *Proc. 2007 IEEE Symposium on Security and Privacy*.

Schneier, B. 2008. *The psychology of security*. [online]. Available: http://www.schneier.com/essay-155.html [Accessed 3 August 2016].

Selmi, M., Aïmeur, E. and Hage, H. 2013. Privacy Framework for Peer Affective Feedback. *2013 International Conference on Signal-Image Technology & Internet-Based Systems, Kyoto*. pp. 1049-1056.

Shahriar, H., Weldemariam, K., Lutellier, T. and Zulkernine, M. 2013. A Model-Based Detection of Vulnerable and Malicious Browser Extension. *In: Software Security and Reliability (SERE), 2013 IEEE 7th International Conference on.* pp.1-17.

Shay, R. Komanduri, S., Durity, A., Huh, P., Mazurek, M., Segreti, S., Ur, B., Bauer, L., Christin, N., Cranor, L.. 2016. Designing Password Policies for Strength and Usability. *ACM Transactions on Information and System Security*. 18 (4).

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. and Nunge, E. 2007. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. *In: Symposium On Usable Privacy and Security (SOUPS 2007)*. pp.1-12.

Shepherd, L. A., Archibald, J. and R.I., Ferguson. 2014. Reducing Risky Security Behaviours: Utilising Affective Feedback to Educate Users. *Future Internet*, 6 (4), pp.760-772.

Shepherd, L.A., Archibald, J. and Ferguson, R. I. 2013. Perception of Risky Security Behaviour by Users: Survey of Current Approaches*. Human Aspects of Information Security, Privacy, and Trust, 8030*. pp.176- 185.

Siegle, G. 1994. *Genanew*. [online]. http://www.pitt.edu/~gsiegle/wordlist/index.htm [Accessed 3 August 2016].

Stangroom, J. 2016. *Mann-Whitney U Test Calculator.* [online]. http://www.socscistatistics.com/tests/mannwhitney/Default2.aspx. [Accessed 3 August 2016].

Stanton, J.M (2005). Analysis of end user security behaviors*. Computers and Security* 24, pp.124–133.

Stanton, B., Theofanos, M., Prettyman, S. and Furman, S. 2016. Security Fatigue*. IT Professional*. 18(5) pp. 26-32.

Stats Direct. 2016. *P Values*. [online]. http://www.statsdirect.co.uk/help/basics/pval.htm [Accessed 3 August 2016].

Steinbart P.J, Keith, M.J., and Babb, J. 2016. Examining the Continuance of Secure Behavior: A Longitudinal Field Study of Mobile Device Authentication. *Information Systems Research*.

Straub, D., and Welke, R. 1998. Coping With Systems Risks: Security Planning Models for Management Decision Making. *MIS Quarterly* (22:4), pp. 441-469.

Suggi, R. and Freeman, N. 2009. *Abusing Firefox Extensions*. [online]. https://www.defcon.org/images/defcon-17/dc-17-presentations/defcon-17-roberto_liverani-nick_freeman-abusing_firefox.pdf [Accessed 3 August 2014].

Takemura, T. 2011. Empirical analysis of behavior on information security. *In: Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, ITHINGSCPSCOM*, pp.358–363.

The R Foundation. 2015. *The R Project for Statistical Computing*. [online]. https://www.r-project.org/ [Accessed 5 August 2016].

United States Computer Emergency Readiness Team. 2011. Using Caution with USB Drives. [online]. https://www.us-cert.gov/ncas/tips/ST08-001 [Accessed 3 August 2014].

Ur, B., Bees, J., Segreti, S., Bauer, L., Christin, N, and Cranor, L. 2016. Do Users' Perceptions of Password Security Match Reality? *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16,* pp.3748–3760.

Ur, B., Kelley, P., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N. and Cranor, L. 2012. How does your password measure up? The effect of strength meters on password creation*. In: Security 2012 Proceedings of the 21st USENIX Conference on Security Symposium.*

Urban Dictionary. 2016. http://www.urbandictionary.com/. [online]. http://www.urbandictionary.com/ [Accessed 5 August 2016].

Vance A., Eargle D., Ouimet K., and Straub, D. 2013. Enhancing password security through interactive fear appeals: A web-based field experiment. *In System Sciences (HICSS), 2013 46th Hawaii International Conference on. IEEE, Hawai'i*, 2988–2997.

Volkamer, M., Renaud, K., Canova, G, Reinheimer, B, and Braun, K. 2015. Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness. *Trust and Trustworthy Computing: 8th International Conference, TRUST 2015*, pp.104–122

Volkamer, M., Renaud, K., and Reinheimer, B. 2016. TORPEDO: TOoltip-poweRed Phishing Email DetectiOn*. IFIP International Information Security and Privacy Conference*. Springer International Publishing.

Willison, R., and Warkentin, M. 2013. Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS quarterly* 37(1): pp. 1-20.

Wixon, D. 2011. Measuring fun, trust, confidence, and other ethereal constructs: it isn't that hard. *Interaction*, 18 (6), pp. 74-77.

Wu, M., Miller, C. and Little, G. 2006. Web Wallet: Preventing Phishing Attacks by Revealing User Intentions. *In: Symposium On Usable Privacy and Security (SOUPS 2006)*. pp.1-12.

Xu, M., Ong, V., Duan, Y. and Mathews, B. 2011. Intelligent agent systems for executive information scanning, filtering and interpretation: perceptions and challenge. *Information Processing and Management: an International Journal*, 47 (2), pp.186- 201.