Assessing The Impact of Affective Feedback On End-User Security Awareness

Lynsay A. Shepherd, Jacqueline Archibald and Robert I. Ferguson

School of Arts, Media and Computer Games, Abertay University,
Dundee, DD1 1HG

{lynsay.shepherd, j.archibald,
i.ferguson}@abertay.ac.uk

Abstract. A lack of awareness regarding online security behaviour can leave users and their devices vulnerable to compromise. This paper highlights potential areas where users may fall victim to online attacks, and reviews existing tools developed to raise users' awareness of security behaviour. An ongoing research project is described, which provides a combined monitoring solution and affective feedback system, designed to provide affective feedback on automatic detection of risky security behaviour within a web browser. Results gained from the research conclude an affective feedback mechanism in a browser-based environment, can promote general awareness of online security.

Keywords: End-user security behaviours, usable security, affective feedback, user, monitoring techniques, user feedback, security awareness.

1 Introduction

Risky behaviour exhibited by the end-user may place devices at risk, despite the widespread availability of security tools [1]. This has become a growing concern owing to the reliance on the internet for online banking, e-commerce transactions, consumption of media, and the maintenance of social ties. This paper describes an approach whereby the concept of affective feedback is applied to the domain of a browser-based environment via the use of an extension. The extension has been developed in an attempt to educate users regarding online security, with the end-goal of raising security awareness.

2 Background

Security measures on devices are often seen as restrictive and obtrusive by end-users, potentially limiting users' ability to perform tasks. To circumvent these measures, users may engage in behaviours which are deemed to be risky, placing their devices at risk of compromise.

This section explores previous research, highlighting risky security behaviours users may inadvertently engage in, and perception of risk. Previous attempts at educating the end-user are discussed, before proposing the concept of affective feedback as a possible method to educate the end-user.

2.1 Risky security behaviour

What constitutes risky behaviour is not necessarily obvious to all end-users and can be difficult to recognise. In the context of a browser-based environment there are multiple examples of behaviour which could be perceived as risky, e.g., creating weak passwords/sharing passwords with colleagues [2][3], downloading data from unsafe websites [4] or interacting with a website containing coding vulnerabilities [5].

Attempts have been made to categorise behaviours displayed by users which could be classified as risky, including a 2005 paper by Stanton et al. [2]. 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 defined: intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance and basic hygiene.

Padayachee [6] discussed compliant security behaviours whilst investigating if some users had a predisposition to adhering to security behaviour. A taxonomy developed highlighted elements which have the potential to influence security behaviours in users i.e. 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 security education of employees.

Weak passwords are associated with poor security behaviour and a trade-off exists between the usability of passwords and the level of security they provide [3]. Whilst exploring the issue of security hygiene, Stanton et al. [2] touched on the subject of passwords noting that 27.9% of participants wrote their passwords down and 23% revealed their passwords to colleagues Others have explored the usability of passwords and have acknowledged the difficulties end-users can experience in choosing a password whereby it was determined "*length requirements alone are not sufficient for usable and secure passwords*" [7].

Another risky behaviour category relates to how users perceive technology flaws, e.g. vulnerability to XSS attacks or session hijacking. Social engineering can also be considered to fall into this category: e.g. an attacker could potentially clone a profile on a social networking site and utilise the information to engineer an attack against a target (e.g. via a malicious link) [5]. Such attacks can be facilitated by revealing too

much personal information on social networking sites [8].

A paper by Milne et. al. [9] also investigated risky behaviours and compared this with self-efficacy. The paper concludes that depending on the demographic and the self-efficacy of the end-user, different types of behaviour are 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. These suggestions were drawn from previous research into risky behaviours [10-11].

Specific behaviours users were asked about in the survey included the use of private email addresses to register for contests on websites, selecting 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: 56% of participants admitted to this.

Whilst there has been a number of attempts to categorise risky security behaviours, users may also exhibit a lack of perception regarding risk.

2.2 Perception of risk

A number of research papers have explored techniques to gauge the perception of risk. Farahmand et al. [12] explored the possibility of using a psychometric model originally developed by Fischoff et al. in 1978 [13] in conjunction with questionnaires, allowing a user to reflect on their actions and gauge their perception, providing a qualitative overview.

Takemura [14] 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 there was a risk of being infected by a virus. 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%. This displays a wide range of attitudes towards risk perception.

San-José and Rodriguez [15] 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 and results showed that the antivirus software created a false sense of security and they were unaware of how serious certain risks could be.

In a different study, Hill and Donaldson [16] proposed a methodology to integrate models of behaviour and perception. The research attempted to assess the perception of security the system administrator possessed. It also created a trust model, reducing 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.

Understanding the level of risk perception a user possesses can help identify the best methods to educate users regarding security behaviour.

2.3 Tools to educate end-users

Since there is the potential for end-users to inadvertently engage in behaviours deemed risky, many tools have been developed to help users.

Furnell et. al. [17] conducted a study in 2006, 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.

Much of the research conducted into keeping users safe online, educating them about risky security behaviour revolves around phishing attacks. Various solutions have been developed to gauge how to educate users about the dangers of phishing attacks, with the view that education will reduce engagement in risky security behaviours.

Dhamija and Tygar [18] proposed a method to enable users to distinguish between spoofed websites and genuine sites. A Firefox extension was developed providing users with a trusted window in which to enter login details. A remote server generated a unique image 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.

Sheng et. al [19] 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 [20] 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 didn't cause participants to become overly cautious.

Similarly, an Android app called NoPhish has been developed to educate users about phishing on mobile devices [21]. The game features multiple levels where users are presented with a URL and are asked if 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.

Besmer et. al [22] 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 users' 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.

In addition to security tools which have been developed to target privacy issues on social networking sites, studies have also focused on more general warning tools for the web. A Firefox extension developed by Maurer [23] 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. [24] 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.

Despite the number of tools created to help protect users online, users continue to engage in risky security behaviour. The tools developed span a number of years, indicating users still require security education. Therefore, this suggests that a different approach is needed when conveying information to end-users. Ongoing research is described and explores the use of affective feedback as a suitable method of educating the end-user, raising security awareness.

2.4 Affective feedback

In terms of computing, this is defined as *"computing that relates to, arises from, or deliberately influences emotions"* [25]. Types of affective feedback include, specific text or phrases, and avatars with subtle facial cues. Such feedback has previously been beneficial in educational environments [26-28].

Several methods can be employed to inform the user that they are exhibiting risky behaviour. Ur et al. [29] 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 to increase 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. Affective properties of colour were highlighted by Osgood and Adams in 1973 [30], and colours such as red signify danger in Western culture. 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.

Multimedia content such as the use of colour and sound can also be used to provide feedback to the user. In a game named "Brainchild" developed by McDarby et al. [26], 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.

Textual information provided via the GUI can be used to communicate feedback to the user. Dehn and Van Mulken [31] conducted an empirical review of ways in which animated agents could interact with users. 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 could be utilised when aiding users in considering their security behaviour online, since it can detect and help users alter their internal states [26]. Work conducted by Robison et al. [27] 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.

Hall et al. [28] 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 potentially be used to achieve the same result in adults.

2.5 The relationship between security behavior, education, and affective feedback

Although there's a number of security tools available which have been designed to help the end-user, people are still falling victim to online attacks. This suggests that perhaps a different approach is required. The ongoing research discussed in the following sections offers the application of affective feedback in the context of a browser-based environment, in attempt to raise the security awareness of end-users.

3 Methodology

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 has the potential to serve as a suitable method to educate users regarding risky security behaviours [26-28]. Within the scope of the browser environment, on detection of risky security behaviour, the browser is used as a delivery mechanism for affective feedback, warning users about their actions.

3.1 Testing harness overview

The research project proposed the creation of a testing harness, in the form of a XUL (XML User Interface Language) browser extension for Mozilla Firefox, including the ability to monitor user behaviour and provide suitable affective feedback (Fig. 1). The

extension developed was named Spengler-Zuul, and utilises several feedback agents. Should the monitoring system detect a user engaging in a known, potentially risky security behaviour whilst browsing the internet e.g. entering a commonly used password into a website, an affective feedback mechanism triggers, warning users regarding the dangers of their actions.

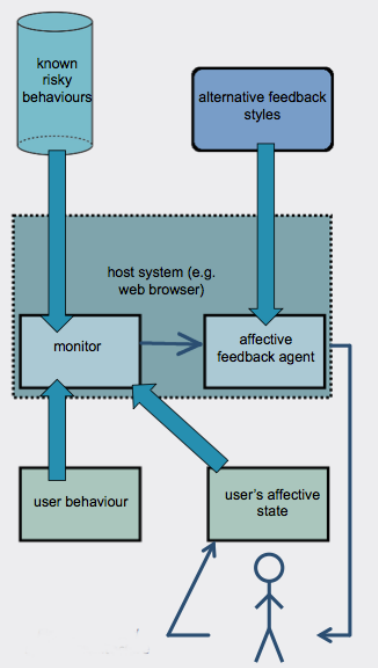

Fig. 1. Overview of the Spengler-Zuul extension

3.2 Monitoring solution

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.

Research conducted by Bubaš, Orehova and & Konecki [32] and, Milne, Labrecque and Cromer [9] define specific risky security behaviours. A smaller subset of these behaviours were chosen for implementation, owing to their suitability for monitoring in the context of a web browser. Checks for these behaviours were built into a monitoring solution:

- Commonly used words in a password
- Password contains personal information
- Password length
- Malicious links found on page
- Current page is a malicious link

- Site is served via HTTP
- Current page is a top 20 social media site

When the user interacts with the browser, the information is encrypted, and processed on the server. As an example, processing the information on a server allows the URL of a current site to be compared against a known database of malicious sites [33]. Detection of a malicious site can then trigger the affective feedback mechanism, delivering some form of information to the end-user.

The development of a monitoring solution required a method of logging user actions. Previous research conducted by Fenstermacher and Ginsburg [34] noted the use of an XML log file generated by users' actions within a particular application. Drawing inspiration from this approach, a logging system was developed for the monitoring solution whereby a unique log is generated on a server for each user, and their actions are recorded. In terms of future work, this can be used to build-up a local profile of the end-user, determining common mistakes they may engage in.

3.3 Affective feedback delivery

Following the implementation of the monitoring system, an affective feedback delivery system was put in place. Risky behaviours triggered a form of affective feedback within the browser, using weighted sentences constructed from an affective word list [35], colour, and avatars to alert users to possible risks.

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 security decisions. 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. The 3 affective methods chosen were colours, avatars and text. The following section will discuss each type of feedback in more detail.

Text-based feedback

Research highlighted text-based feedback as an appropriate form of affective feedback for disseminating information to the end-user. When Ur et al. [29] investigated password strength meters, text-based feedback was also applied to describe users' passwords e.g. "*weak*". Other research, such as the work conducted by Dehn and Van Mulken [31] concluded that textual information provided more direct feedback to end-users.

The Spengler-Zuul extension developed required a word list in order for affective sentences to be constructed, with an indication as to the whether they were positively or negatively weighted.

The AFINN database developed by Finn˚Arup Nielsen at DTU Informatics, Technical University of Denmark [35] was chosen for this purpose. 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 during the experimental design process. The wordlist was specifically developed for microblogs e.g. services such as Twitter where users post short messages. This concept fits in with this re-

search project as the affective feedback solution aims to regularly updates end-users with short messages depending upon their actions.

Text-based feedback has been split into 3 sections, or bars: password information, general information, and malicious site information.

The final pieces of affective text integrated into the Spengler-Zuul 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 triggers e.g. if a user visited a safe site or a malicious site.

In the case of unencrypted sites (HTTP) and social media sites, users were provided only with a general warning. It is possible to visit a social media site and stay safe, provided you are mindful regarding the information you are sharing with others. Similarly, you can visit an unencrypted website and behave in a completely safe way e.g. not entering sensitive information.

When writing affective phrases, care was taken to provide balanced text. As an example, the malicious links message telling users they are safe has a positive rating of 2. Conversely, the negative message for the opposing trigger has a 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. Within 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 final affective phrases for the malicious links are as follows-

- Positive text: "*Links found on the page have been validated and deemed safe.*"
- Negative text: "*Harmful links have been found on the page.*"

Colour-based feedback

Another method of providing affective feedback to the end-user involves the use of certain colours in a bid to influence users. To provide an example, in Western culture, the colour red has long been associated with danger. Research carried out by Kralik, J.D. et. al. [36] has even proposed that the link between the colour red and dangerous situations may be rooted in evolutionary psychology.

In terms of cyber security, a number of studies have been conducted, into the use of colour-based feedback including Ur's 2012 paper [29] on password meters.

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. [26] which attempts to help users relax.

During the development of the extension, the following colours were chosen for inclusion to denote affect: a shade of red (#CF4250), yellow (#EBA560), and green (#78BF60), producing a traffic-light system.

Avatar-based feedback

Avatar-based feedback may be an appropriate form of affective feedback when attempting to educate users. Again the Brainchild tool by McDarby et. al. [26] indicated affective feedback can help users alter their internal states. Avatars have been used to good effect in intelligent tutoring systems [27], with Hall et. al. [28] agreeing that the use of avatars may prove effective in influencing the emotional state of the end-user, thus forming part of this research.

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. [37]. The paper makes reference to the previously identified 6 basic emotions [38]: happiness, anger, sadness, fear, disgust, and surprise, and also includes a neutral avatar, devoid of any such emotion. The 2 avatars selected for inclusion in this research project were happiness and sadness, to denote positive and negative feedback accordingly.

Research has shown that people are uncertain about emotions displayed in expression sequences in comparison to simple static images [37]. Due to this finding, static images of avatars were implemented into the Spengler-Zuul extension.

Combining feedback

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 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 and commonality. A password may be short (bad) however, it may be a non-dictionary word (good). To prevent the system from providing users with positive feedback when they have failed any of the password security checks, the password flags are checked and provide an override. So whilst users may have an uncommon, yet short password, they are still shown negative affective text, colours and avatars. They will only be shown positive feedback when they meet all 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.

Spengler-Zuul extension developed

A number of versions of the final tool, named the Spengler-Zuul extension were developed, allowing the impact of different combinations of affective feedback to be tested against a control environment. 5 versions of the tool were created:

- 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 (see Fig. 2).

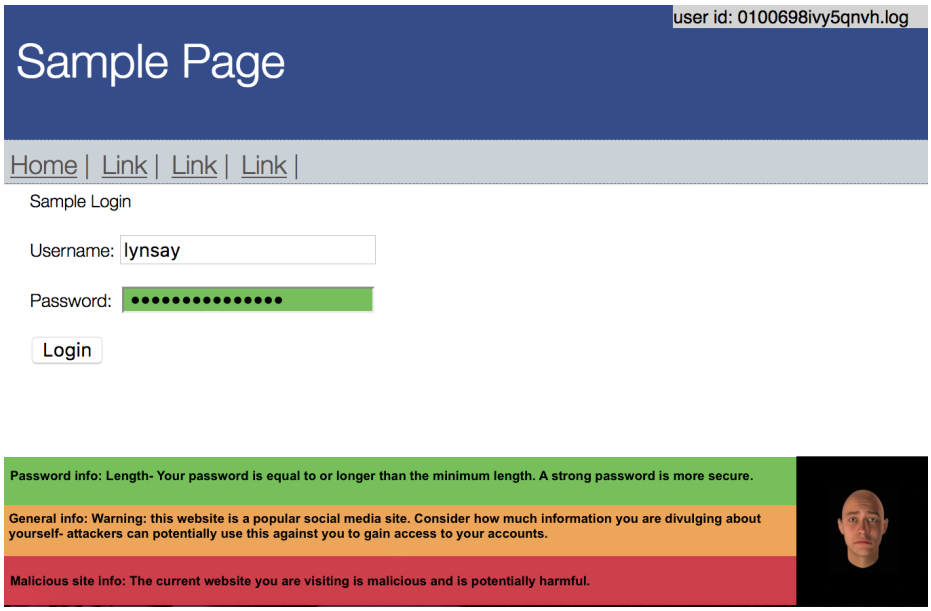

Fig. 2. Affective feedback displayed in the browser via the Spengler-Zuul extension

3.4 Experiments

Participants were initially given a briefing handout, outlining the experimental process. Participants were drawn from Abertay University, and many had a computing background. No reference was made to the type of feedback which would be provided. The fact that risky security behaviours and awareness were also being measured was omitted from the information for participants, in order to avoid bias.

Participants were then given a USB stick labelled with a number from 1-5. Each USB stick contained a portable version of the Firefox browser, and a version of the Spengler-Zuul extension. The types of feedback delivered corresponded to the numbers 1-5, and are outlined in Table. 1. Participants were asked to visit a number of pre-defined websites, following on-screen instructions. Some of the websites were chosen to purposely trigger feedback e.g. a HTTP warning. On completion of the computer-based part of the experiment, participants were asked to complete a paper-based questionnaire utilising Likert Scales. This allowed participants to assess their response to the on-screen feedback received. Participants were only allowed to take part in the experiments once only, regardless of the experiment group they were in.

Table. 1. Experiment groups and feedback types

Group	Feedback type	Participants (n)
1	Control	12
2	Text	13
3	Text, avatar	16
4	Text, colour	14
5	Text, colour, avatar	17

4 Results

A control group was used during the experimental phase, and received no on-screen feedback, however they were asked to visit the same websites. Questions in the study were conditional to allow for the control group to be compared against those who received some form of affective feedback. The questions sought to assess the potential impact of affective feedback on awareness of risky security behaviours. By analysing responses to the Likert Scale questionnaire, a p-value was gained via the use of the Mann-Whitney U test to indicate statistical significance (Table. 2).

Table. 2. Control group vs. affective feedback results

Statistical significance- question vs. experiment				
Question	**Group 1 vs. 2**	**Group 1 vs. 3**	**Group 1 vs. 4**	**Group 1 vs. 5**
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 participants feel 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 behavior 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 group. Other results were mixed, with text and avatar-based feedback proving successful in eliciting a hesitant response in participants when they were clicking on links, and when they were asked to provide information online.

5 Discussion

Participants were asked to answer 8 questions during the study relating to on-screen feedback, in an effort to determine the potential impact of affective feedback on security awareness. 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 positive, statistically significant results for all affective experiments. This indicates that no form of affective feedback delivered out-performed the other. In this study any form of affective feedback (text, colour, avatars) had an impact on overall awareness.

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.

When participants were asked "*Do you think the feedback provided helped to increase your security awareness?*", all affective experiment questionnaire results produced a positive, statistically significant result when compared to the control group questionnaire data. This indicates that in this study, 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 experiment questionnaire results produced a positive, statistically significant result when compared to the control group questionnaires. 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 to the need for education: in this instance it appears the participants were eager to learn.

Again, 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?" were interesting as no form affective feedback delivered surpassed the other in terms of the impact on the end-user. This is an interesting result as a separate part of the questionnaire asked participants which type of affective feedback they felt had the largest impact. Raw results gained from this question indicated participants felt colour had the largest impact, though it was only used in 2 of the experiment groups.

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 raw results in another part of the questionnaire, 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, again highlighting a potential 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.

In terms of the affective feedback delivered, some participants left free-form comments on the questionnaire, stating some participants thought 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*".

As of August 2015, Mozilla announced XUL-based extensions would be deprecated, and they would move to a new API named WebExtensions [39]. In addition to this, at the start of 2017, Mozilla started to integrate warnings (text-based) in Firefox regarding password entry on a non-HTTPS website [40]. This is a feature which was integrated into the Spengler-Zuul extension in 2015, and highlights the importance of security awareness in the context of a browser-based environment.

6 Conclusion/Future work

To conclude, this research study found that the delivery of affective feedback within the confines of a browser-based environment enhanced users' general awareness of security risks online, though it didn't have an impact on specific behaviours such as the information they shared on social media websites. 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 allows users to consider whether their online behaviours could be perceived as risky.

This piece of research was a preliminary study to investigate if it was plausible to apply affective feedback in the context of a browser-based environment. If affective feedback was delivered over a longer period of time, on a regular basis, this has the potential to reflect positive behavioural changes as end-users become more knowledgeable regarding the subject matter. Future work seeks to investigate the impact of a long-term study in this area, utilising varying affective agents e.g. differing word-lists and avatars.

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 [41]. Regardless of the users' age, 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 become yellow, distorting colours [42] could provide another avenue for investigation. Similarly, the affective feedback delivered could be modified to appeal to children, helping to educate them about staying safe online from a young age, enhancing their security awareness.

References

1. Li, Y and Siponen M, A call for research on home users information security behaviour, 2011, PACIS 2011, Proceedings, paper 112
2. Stanton, J.M., et al.: Analysis of end user security behaviors. Elsevier. Computers and Security 24, pp.124–133 (2005)
3. Payne, B., Edwards, W.: A brief introduction to usable security. Internet Computing, IEEE (Volume:12 , Issue: 3) pp. 13–21 (May/June 2008)
4. Fetscherin, M.: Importance of cultural and risk aspects in music piracy: A cross-national comparison among university students. Journal of Electronic Commerce Research (January 2009), http://www.csulb.edu/journals/jecr/issues/20091/Paper4.pdf
5. Hadnagy, C.: Social engineering: the art of human hacking, pp. 23–24. Wiley Publishing, Indianapolis (2011)
6. Padayachee, K.: Taxonomy of compliant information security behavior. Computers & Security 31(5), 673–680 (2012), http://dx.doi.org/10.1016/j.cose.2012.04.004
7. Shay, R., et al. (2016). Designing Password Policies for Strength and Usability. [online]. ACM Transactions on Information and System Security, 18 (4),. http://doi.org/10.1145/2891411
8. Balduzzi,M.:Attackingtheprivacyofsocialnetworkusers.HITBSecconf2011Malaysia (2011), http://conference.hitb.org/hitbsecconf2011kul/materials/ D1T1%20%20Marco%20Balduzzi%20-%20Attacking%20the%20Privacy% 20of%20Social%20Network%20Users.pdf (accessed September 21, 2012)
9. Milne, G. R., Labrecque, L. I. and & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. [online]. Journal of Consumer Affairs, 43 (3), pp.449–473. http://doi.org/10.1111/j.1745-6606.2009.01148.x
10. Larose, R., and Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. [online]. Journal of Consumer Affairs, 41 (1), pp.127-149. 10.1111/j.1745-6606.2006.00071.x

11. Milne, G. R., Rohm, A. J. and Bahl, S. (2004). Consumers' Protection of Online Privacy and Identity. [online]. Journal of Consumer Affairs, 38, pp.217–232. 10.1111/j.1745-6606.2004.tb00865.x
12. Farahmand, F., et al. (2009). Risk perceptions of information security: A measurement study. [online]. In: Proceedings of the 2009 International Conference on Computational Science and Engineering, CSE 2009, 3, pp.462–469. http://dx.doi.org/10.1109/CSE.2009.449
13. Fischoff, B., et al. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. [online]. Policy Sciences, 9 (2), pp.127–152.5
14. Takemura, T. (2011). Empirical analysis of behavior on information security. [online]. 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. http://dx.doi.org/10.1109/iThings/CPSCom.2011.8
15. San-Jose, P. and Rodriguez, S. (2011). Study on information security and e-Trust in Spanish households. [online]. In: Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, BADGERS 2011, pp.1-6. http://doi.acm.org/10.1145/1978672.1978673
16. Hill, R. and Donaldson, D. R. (2015). Bridging the Trust Gap : Integrating Models of Behavior and Perception. [online]. NSPW '15 Proceedings of the 2015 New Security Paradigms Workshop , pp.148-155. 10.1145/2841113.284112
17. Furnell, S. et al. (2006). The challenges of understanding and using security: a survey of end- users. [online]. Computers & Security, 25 (1), pp.27-35. http://dx.doi.org/10.1016/j.cose.2005.12.004
18. Dhamija, R. and Tygar, J. (2005). The Battle Against Phishing: Dynamic Security Skins. [online]. In: Symposium On Usable Privacy and Security (SOUPS 2005)., pp.1-12. http://cups.cs.cmu.edu/soups/2005/2005proceedings/p77-dhamija.pdf
19. Sheng, S. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. [online]. In: Symposium On Usable Privacy and Security (SOUPS 2007)., pp.1-12. http://cups.cs.cmu.edu/soups/2007/proceedings/p88_sheng.pdf
20. Kumaraguru, P. et. al. (2009). School of Phish: A Real-World Evaluation of Anti-Phishing Training. [online]. n: Symposium On Usable Privacy and Security (SOUPS 2009)., pp.1-12. http://cups.cs.cmu.edu/soups/2009/proceedings/a3-kumaraguru.pdf
21. Canova, G. Volkamer, M. Bergmann, C. Reinheimer, B. 2015 Nophish app evaluation: lab and retention study. In: NDSS workshop on usable security
22. Besmer, A. (2009). Social Applications: Exploring A More Secure Framework. [online]. In: Symposium On Usable Privacy and Security (SOUPS 2009), pp.1- 10. http://cups.cs.cmu.edu/soups/2009/proceedings/a2- besmer.pdf
23. Maurer, M., De Luca, A. and Kempe, S (2011). Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness. [online]. In: Symposium On Usable Privacy and Security (SOUPS 2011), pp.1-13. http://cups.cs.cmu.edu/soups/2011/proceedings/a2_Maurer.pdf
24. Volkamer, M. et. al (2015). Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness. [online]. Trust and Trustworthy Computing: 8th International Conference, TRUST 2015, pp.104–122. http://doi.org/10.1007/978-3-319-22846-4_7
25. Picard, R.W. Affective Computing; MIT Press: Cambridge, MA, USA, 1997; pp. 15.
26. McDarby, G.; Condron, J.; Hughes, D.; Augenblick, N. Affective feedback. Media Lab Europe (2004). Available online:

http://medialabeurope.org/mindgames/publications/publication AffectiveFeedbackEnablingTechnologies.pdf (accessed on 22 May 2012).
27. Robison, J.; McQuiggan, S.; Lester, J. Evaluating the Consequences of Affective Feedback in Intelligent Tutoring Systems. In Proceedings of International Conference on Affective Computing and Intelligent Interaction (ACII 2009), Amsterdam, Netherlands, 10–12 September 2009; pp. 37–42.
28. Hall, L.; Woods, S.; Aylett, R.S.; Newall, L.; Paiva, A.C.R. Achieving Empathic Engagement through Affective Interaction with Synthetic Characters; Tao, J., Tan, T., Picard, R.W., Eds.; Springer: Heidelberg, Germany, 2005; Volume 3784, pp. 731–738.
29. Ur, B., et al. (2012). How does your password measure up? The effect of strength meters on password creation. [online]. In: Security 2012 Proceedings of the 21st USENIX Conference on Security Symposium,
30. Adams, F. M., & Osgood, C. E. (1973). A cross-cultural study of the affective meanings of color. Journal of cross-cultural psychology, 4(2), 135-156.
31. 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. http://dx.doi.org/10.1006/ijhc.1999.0325
32. Bubaš, G., Orehova, T. and & Konecki, M. (2008). Factors and Predictors of Online Security and Privacy Behavior. [online]. Journal of Information and Organizational Sciences, 32 (2), pp.79–98.
33. HpHosts. 2016. [online]. http://www.hosts-file.net/
34. Fenstermacher, K.D. and Ginsburg, M.A. (2002). Lightweight framework for cross- application user monitoring. [online]. IEEE Computer, pp.51–58.
35. Nielsen, F (2011). A new ANEW: evaluation of a word list for sentiment analysis in microblogs. [online]. 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.
36. Association For Psychological Science (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
37. Sacharin, V., Sander, D. and Scherer, K. R. (2012). The perception of changing emotion expressions. [online]. Cognition & Emotion, pp.1273–1300. http://doi.org/10.1080/02699931.2012.656583
38. Ekman, P. (1999). Basic emotions. [online]. Cognition,. http://doi.org/10.1002/0470013494.ch3
39. Mozilla (2015). The Future of Developing Firefox Add-ons. [online]. https://blog.mozilla.org/addons/2015/08/21/the-future-of-developing-firefox-add-ons/
40. Mozilla (2017). Designed to protect your privacy. [online]. https://www.mozilla.org/en-GB/firefox/desktop/trust/
41. Office for National Statistics (2016). Internet users in the UK: 2016. [online]. http://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2 016#recent-internet-use-is-on-the-increase-for-those-aged-65-and-over
42. Salvi, S. M., Akhtar, S., and Currie, Z. (2006). Ageing changes in the eye. [online]. Postgraduate Medical Journal, 971, pp.581–587. http://doi.org/10.1136/pgmj.2005.040857