Future Internet **2014**, *6*, 760-772; doi:10.3390/fi6040760

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

Reducing Risky Security Behaviours: Utilising Affective Feedback to Educate Users [†]

Lynsay A. Shepherd [1,*], Jacqueline Archibald [2] and Robert Ian Ferguson [1]

[1] School of Science, Engineering and Technology, Abertay University, Bell Street,
Dundee DD1 1HG, Scotland; E-Mail: i.ferguson@abertay.ac.uk

[2] Dundee Business School, Abertay University, Dundee DD1 1HG, Scotland;
E-Mail: j.archibald@abertay.ac.uk

[†] This article was originally presented at the Cyberforensics 2014 conference. Reference: Shepherd, L.A.; Archibald, J.; Ferguson, R.I. Reducing Risky Security Behaviours: Utilising Affective Feedback to Educate Users. In Proceedings of Cyberforensics 2014, University of Strathclyde, Glasgow, UK, 2014; pp. 7–14.

* Author to whom correspondence should be addressed; E-Mail: lynsay.shepherd@abertay.ac.uk;
Tel.: +44-(0)1382-308685.

External Editor: Mamoun Alazab

*Received: 31 July 2014; in revised form: 22 October 2014 / Accepted: 6 November 2014 /
Published: 27 November 2014*

Abstract: Despite the number of tools created to help end-users reduce risky security behaviours, users are still falling victim to online attacks. This paper proposes a browser extension utilising affective feedback to provide warnings on detection of risky behaviour. The paper provides an overview of behaviour considered to be risky, explaining potential threats users may face online. Existing tools developed to reduce risky security behaviours in end-users have been compared, discussing the success rates of various methodologies. Ongoing research is described which attempts to educate users regarding the risks and consequences of poor security behaviour by providing the appropriate feedback on the automatic recognition of risky behaviour. The paper concludes that a solution utilising a browser extension is a suitable method of monitoring potentially risky security behaviour. Ultimately, future work seeks to implement an affective feedback mechanism within the browser extension with the aim of improving security awareness.

Keywords: usable security; end-user security behaviours; affective computing; user monitoring techniques; affective feedback; security awareness

1. Introduction

A lack of awareness surrounding online behaviour can expose users to a number of security flaws. 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 [1]. This paper aims to identify potential security issues users may face when browsing the web such as phishing attempts and privacy concerns. Techniques developed to help educate users regarding their security awareness have been reviewed, comparing the methods used to engage users, discussing the potential flaws in such tools. Previous research has indicated affective feedback may serve as a successful method of educating users about risky security behaviours [2–4], thus, improving system security. The paper proposes the use of a browser extension to monitor users actions and detect risky security behaviour. Future work seeks to utilise affective feedback to improve the security awareness of end-users, with a view to improving overall system security.

2. Background

Risky security behaviour exhibited by end-users has the potential to leave devices vulnerable to compromise [5]. Security tools are available, such as firewalls and virus scanners, which are designed to aid users in defending themselves against potential online threats however, these tools cannot stop users engaging in risky behaviour. End-users continue to engage in risky behaviour indicating that the behaviour of users needs to be modified, allowing them to consider the security implications of their actions online. This section explores the definition of risky security behaviour, the role of affective feedback and outlines potential threats users may face when browsing the web.

2.1. Risky Security Behaviour

What constitutes risky behaviour is not necessarily obvious to all end-users and can be difficult to recognise. There are multiple examples of behaviour which could be perceived as risky in the context of a browser-based environment, e.g., creating weak passwords or sharing passwords with colleagues [6,7], downloading data from unsafe websites [8] or interacting with a website containing coding vulnerabilities [9].

Several pieces of research have been conducted in an attempt to define and categorise security behaviour. One such attempt was documented in a 2005 paper by Stanton *et al.* [6] where 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 (e.g., hacking into company files, stealing information), detrimental misuse, dangerous tinkering naïve mistakes (perhaps choosing a weak password), aware assurance and basic hygiene. Conversely, in 2012, Padayachee [10] developed a taxonomy, categorising 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.

The scope of behaviour pertaining to this paper relates to general user behaviour, concentrating on user interaction with a web browser. Users face a number of threats online, as discussed in Section 2.3 and may have to deal with these threats in both a home-based or organisational environment.

2.2. Affective Feedback

Affective computing is defined as "computing that relates to, arises from, or deliberately influences emotions" [11]. There are a variety of feedback methods which are considered to be affective. Avatars can provide affective feedback and have been seen to be beneficial in educational environments [2–4]. Robison *et al.* [3] 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. The work highlighted the danger that if an agent intervenes at the wrong time, this may cause a negative impact on how the user learns using the tool.

Work conducted by Hall *et al.* [4] also advocated the use of avatars in providing affective feedback and how they can influence the emotional state of the end-user. Research conducted deployed avatars in a personal social and health education environment, educating children about bullying. Results showed the avatars generated an empathetic effect in children, indicating that the same type of feedback could be used to achieve a similar result in adults.

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 [12]. Dehn and Van Mulken conducted an empirical review of ways in which animated agents could interact with users, and compared avatars against textual information as an affective feedback method. They considered that whilst textual information could provide more direct feedback to users, avatars could be used to provide more subtle pieces of information via gestures or eye contact. Overall, it was noted multimodal interaction could provide users with a greater level of feedback [13]. Colour is also often utilised, with green or blue used to imply a positive occurrence, with red indicating a negative outcome [12]. A combination of sounds, colours and dialogues provided a calming mechanism in a game named "Brainchild" [2] which was designed to help users relax, highlighting the effectiveness of a multimodal approach.

2.3. Potential Threats

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 [8].

Interaction with websites featuring coding vulnerabilities is also risky and users are generally unaware of such flaws [14]. If an application is poorly constructed, users may expose themselves to an attack by simply visiting a site, e.g., vulnerability to XSS attacks or session hijacking. Cross-site scripting (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 [1], 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 [9]. 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 [15,16]. The rise in spear phishing attacks has led the FBI to warn the public regarding this issue [17].

Perhaps one of the most common risky security behaviours involves the misuse of passwords for online accounts which link to personal information. There can be a trade off between the level of security of a password provides and its usability [7]. 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.* [6] 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. Security tools such as virus scanners and anti-malware software can aid users if their machines have been infected with malicious software. If users are educated regarding risky security behaviour, this may prevent their machines from becoming infected in the first instance. A considerable amount of research has been conducted into educating and helping users understand risky security behaviour online, and Section 3 discusses varying approaches.

3. Analysis

This section explores previous research, providing an overview of methods which have been developed in an attempt to keep users safer online. Solutions created to reduce specific types of attack will be discussed, highlighting potential issues these tools fail to resolve.

3.1. Keeping Users Safe and Preventing Attacks

Many users participate in risky security behaviour, particularly when it involves passwords, as highlighted by Stanton *et al.* [6]. 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.* [18] 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. As 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.* [19] 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 five 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.

To demonstrate the strength of a chosen password, Ur *et al.* [12] 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.

Much of the research conducted into keeping users safe online, educating them about risky security behaviour revolves 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.

Dhamija and Tygar [20] produced 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.

Sheng *et al.* [21] 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 three 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.* [22] 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 didn't cause participants to become overly cautious and they continued to click on links in genuine emails however, a longer study is required.

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 [23]. While it has been shown users don't fully understand privacy policies online, the nutrition labels seek to present the information in a format that 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.* [24] 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 focussed on more general warning tools when the user is browsing the web. A Firefox extension developed by Maurer [25] 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.

3.2. Issues with Traditional Security Tools and Advice

Some of the tools discussed in Section 3.1 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 [21]. 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 [26].

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. 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. There are a multitude of common threats online, highlighted in Section 2.3, and there is a requirement that newer tools focus on more than one potential threat area.

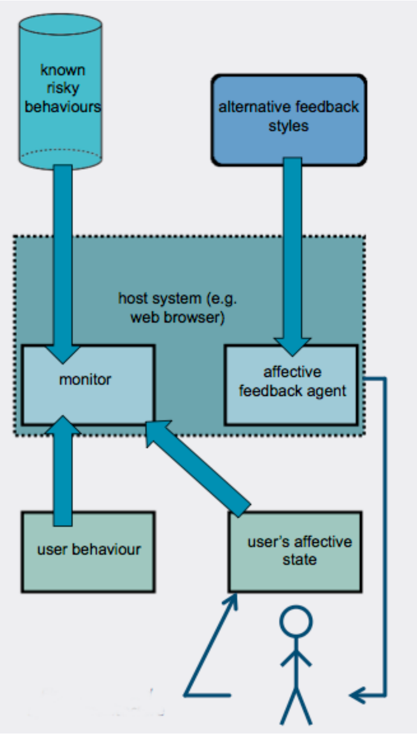
4. Methodology

The research outlined in this section proposes the use of a browser extension to automatically detect risky security behaviour, taking a number of different threats into consideration. Future work seeks to explore the possibility of utilising an affective feedback mechanism in enhancing security risk awareness on detection of risky behaviour within the browser.

4.1. Proposed System Overview

The research proposed seeks to develop a software prototype, in the form of a Firefox browser extension, which monitors user behaviour. The prototype will contain feedback agents, several of which will utilise affective feedback techniques. Should the user engage in potentially risky security behaviour whilst browsing, e.g., entering a password or credit card number into a form, an affective feedback mechanism will trigger, warning users regarding the dangers of their actions. Feedback mechanisms have been explored in previous research and will 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 [27]. 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. The success of the software will be gauged via a series of end-user experiments followed by a questionnaire utilising a Likert scale. Figure 1 attempts to summarise how the software prototype (browser extension) will work. When the user is interacting with a web browser, the tool will monitor these interactions, and compare them to a knowledge base of known risky behaviours. If a risky behaviour is detected, an affective feedback agent will be triggered, providing suitable feedback to the end-user in an attempt to raise awareness of risky behaviour.

Figure 1. Overview of system architecture.



4.2. Technical Details

Following a comparison between XUL-based Firefox extensions (XML User Interface Language) and those created by Mozilla's Add-on SDK, a prototype solution was constructed using a XUL-based extension. This method allows for extensive customisation of the user interface, which a tool of this type requires and additional functionality can be gained via the links to the XPCOM (cross platform component object model) [28]. When developing Firefox extensions to capture user behaviour and provide feedback to users, a number of files are required. Extensions follow the same basic structure, with several files, which must be included. In terms of modifying an extension in an attempt to monitor user behaviour and provide cues to modify the behaviour, particular files are very important.

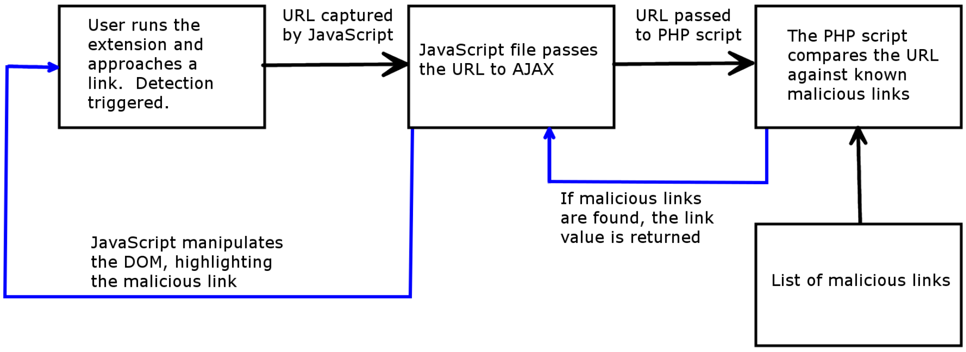
The browser.xul file within the content folder contains a number of links to other required files and is essentially the foundation for the whole extension. This file has the ability to link to JavaScript files, including the jQuery library, should it need to be embedded in an extension. The file also allows additional XUL constructs to be added, allowing the menus and toolbars within Firefox to be modified e.g., adding a link into a menu to allow the user to run an extension.

Another file, which can be modified extensively, is the JavaScript file within the content folder. It can call a number of functions, including referencing the jQuery library and can make use of the Mozilla framework. The file can manipulate the DOM (document object model) of the website displayed in the browser e.g., attach event listeners to all links on a page or modify anchor tags. Additionally, the file can utilise AJAX, passing data back and forth between a web server and the JavaScript file.

To provide a full example of how a Firefox extension may be developed to monitor user behaviour and provide appropriate feedback, details of the Link Detector extension are outlined (Figure 2). The Link Detector extension is designed to warn users about malicious links. When the user starts the Firefox extension, the browser.xul file makes a call to the JavaScript file to run the initial function. The DOM is then manipulated, using JavaScript to add event listeners to all links on a given website. If a user approaches a link with the cursor, an event is triggered. JavaScript passes the link value to a PHP script via AJAX, and is checked against a list of known malicious links. The list of malicious links is sourced from a third-party database, which is managed and updated by Malwarebytes, the company with the anti-malware tool of the same name [29]. The AJAX request then returns a value indicating if the link is known to be malicious. If the link is flagged as being potentially dangerous, the JavaScript file then manipulates the DOM, highlighting the malicious link in red. This is repeated for each link a user approaches.

The Link Detector is a small prototype browser extension, exploring the possibility of raising awareness regarding risky security behaviours in end-users via the use of affective feedback. As such, this may aid in preventing users revealing information to websites, which have been hijacked via an XSS attack. The final prototype developed will not be restricted to scanning for dangerous links only, and seeks to tackle a number of the threats outlined in Section 2.3.

Figure 2. Overview of the Link Detector extension.


User runs the extension and approaches a link. Detection triggered.
URL captured by JavaScript
JavaScript file passes the URL to AJAX
URL passed to PHP script
The PHP script compares the URL against known malicious links
If malicious links are found, the link value is returned
List of malicious links
JavaScript manipulates the DOM, highlighting the malicious link

5. Discussion

A key challenge involved in the development of a Firefox extension which monitors user behaviour, was the consideration of how to capture user behaviour within the confines of a web-browser. The prototype in development seeks to target average users, *i.e.*, those who may use IT at work or home to access the Internet but lack a computing-based background. As such, these users may not have a clear understanding of security issues, and implications. Previous studies have investigated the use of multimodal approaches to capture user behaviour, using a combination of eye movements [30] and video footage of test subjects [31], in addition to task-based analysis. Average computer users may only have a simple PC, therefore the final tool created should not require any additional hardware such as cameras to record data. In this respect, monitoring user behaviour, within the restrictions of the browser environment is a major developmental challenge. There is the risk users may become habituated when using the system: to combat this, there is the potential to allow users to develop a personalised local profile on their system. This would store their preferences relating to how they react to certain warnings displayed.

There are concerns regarding whether users may be suspicious of the use of a tool similar to the Link Detector, which generates a local profile, and if users would actually use the tool. Research has indicated users prefer using software they are familiar with, rather than a separate tool [26]. The final software prototype developed during the research will be unobtrusive: it will be part of the Firefox browser in the form of an installed extension, therefore it will be part of a familiar environment. Additionally, the use of Firefox extensions are commonplace and many require the use of a local profile [32] which is hidden.

Section 4.2 demonstrated that JavaScript contains the necessary low-level event-driven functionality to detect user interaction on a webpage, and can therefore be used to monitor security behaviour. Section 3.1 highlighted that a number of successful tools consisted of browser extensions, and therefore, a similar approach has been utilised. It became apparent that implementing a JavaScript system within a Firefox extension might be a potential solution. Using JavaScript to access the DOM of the webpage displayed in the browser window meant it was possible to run the script against any website, rather than one coded specifically for the research. Though Firefox security extensions are widely implemented, currently available solutions are yet to explore the impact of affective feedback, particularly when educating users about security awareness.

Affective feedback has been used to educate users in the past and as such, may be a suitable method when educating users regarding security awareness. An empirical review conducted by Dehn and

Van Mulken [13] considered ways in which animated agents interacted with users, providing a comparison between the role of avatars and textual information in human-computer interaction. Though it was hypothesised that users gained more direct feedback from textual information, avatars provided more subtle cues through specific gestures. Robison *et al.* [3] successfully utilised avatars in an intelligent tutoring system, helping students learn about microbiology. This indicates that potentially, affective feedback may show similar results when aiding users in considering their security behaviour [2].

In the link detector extension, red has been chosen as the colour used to highlight the malicious links. There are currently two reasons for this: in the UK red is generally seen as a warning colour and in the research conducted by Ur *et al.* [12] red is used to indicate that a password is weak. The final extension is to be improved, detecting the background colour of the page prior to highlighting the malicious link. Currently, if the background colour of the page being scanned is red, it would be extremely difficult for users to see highlighted links. It should be noted that the warning colour-scheme would need to be modified for the extension to work effectively for colour-blind users.

Research is currently in the early stages and as such, a series of preliminary Firefox extensions have been developed to test the methodology, concentrating on capturing user behaviour. Affective feedback agents will be added at a later date. The Link Detector is an extension designed to warn users about malicious links, and has been outlined in detail in Section 4.2. An additional extension was developed to determine what a user is typing on a given website. Utilising jQuery, keystrokes are written to a log file on a server, along with a timestamp. Essentially, the extension passes keypress information to a PHP file via AJAX. The PHP script separates the contents of the keypress array and attaches an appropriate timestamp. This raises the issue of privacy concerns. Potentially, data stored on the server could be encrypted to protect the data. An alternative solution would involve storing the data on the users' local machine rather than a remote server.

A series of tests using the keypress extension were run on a desktop machine, producing some interesting results. The extension successfully logged keystroke information when the word "hello" was typed and if a website included a form with an input password field, the extension continued to log the information. Sample websites could be developed for users during the testing phase, mitigating the need to reveal real password information. Eventually, the keypress extension will detect the name of the form field a user is entering information into. If the 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.

6. Conclusions and Future Work

Despite the number of tools proposed to help end-users reduce risky security behaviours, it is apparent that users are still falling victim to online attacks. Various tools created focus on educating and warning users regarding one specific type of threat, e.g., phishing attacks. A different approach, integrating warnings concerning multiple types of threats to modify user behaviour may be a potential solution. Specifically, these warnings would utilise affective feedback, with previous research indicating that this type of feedback may be suitable in an educational context.

Future work seeks to continue the development of Firefox extensions, which monitor and detect risky security behaviour, and provide affective feedback to discourage such behaviour. The monitoring solution is to be expanded, detecting the information users are revealing online, with a view to preventing users from disclosing sensitive information. Feedback agents will be created, featuring differing affective feedback techniques such as text-based feedback using specific terms, colour-based feedback and avatars using subtle cues and gestures. Ultimately, the prototype software developed will seek to investigate if security risk awareness in end-users improves through the use of affective feedback, with the potential to also improve overall system security.

Acknowledgments

Work presented in this paper has been funded via a Scottish Informatics and Computer Science Alliance (SICSA) prize scholarship.

Author Contributions

Lynsay A. Shepherd, Jacqueline Archibald and Robert Ian Ferguson designed the study and developed the methodology. Lynsay A. Shepherd designed the software and wrote the manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Kaspersky Lab. Kaspersky security bulletin 2013. Available online: http://media.kaspersky.com/pdf/KSB_2013_EN.pdf (accessed on 27 April 2014).
2. McDarby, G.; Condron, J.; Hughes, D.; Augenblick, N. Affective feedback. Media Lab Europe (2004). Available online: http://medialabeurope.org/mindgames/publications/publicationsAffectiveFeedbackEnablingTechnologies.pdf (accessed on 22 May 2012).
3. 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, The Netherlands, 10–12 September 2009; pp. 37–42.
4. 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.
5. Li, Y.; Siponen, M. A call for research on home users information security behaviour. In Proceedings of PACIS 2011, Brisbane, QLD, Australia, 7–11 July 2011.
6. Stanton, J.M.; Staim, K.R.; Mastrangelob, P.; Jolton, J. Analysis of end user security behaviors. *Comput. Secur.* **2005**, *24*, 124–133.
7. Payne, B.; Edwards, W. A brief introduction to usable security. *IEEE Inter. Comput.* **2008**, *12*, 13–21.
8. Fetscherin, M. Importance of cultural and risk aspects in music piracy: A cross-national comparison among university students. *J. Electron. Commer. Res.* **2009**, *10*, 42–55.

9. Hadnagy, C. *Social Engineering: The Art of Human Hacking*; Wiley Publishing: Indianapolis, IN, USA, 2011; pp. 23–24.
10. Padayachee, K. Taxonomy of compliant information security behavior. *Comput. Secur.* **2012**, *31*, 673–680.
11. Picard, R.W. *Affective Computing*; MIT Press: Cambridge, MA, USA, 1997; p. 15.
12. Ur, B.; Kelly, P.G.; Komanduri, S.; Lee, J.; Maass, M.; Mazurek, M.L.; Passaro, T.; Shay, R.; Vidas, T.; Bauer, L.; *et al*. How does your password measure up? The effect of strength meters on password creation. In Proceedings of Security 2012 the 21st USENIX Conference on Security Symposium, Bellevue, WA, USA, 8–10 August 2012; USENIX Association: Berkeley, CA, USA, 2012.
13. Dehn, D.; van Mulken, S. The impact of animated interface agents: A review of empirical research. *Inter. J. Hum. Comput. Stud.* **2000**, *52*, 1–22.
14. Imperva. Cross-Site Scripting. Available online: http://www.imperva.com/Resources/Glossary?term=cross_site_scripting (accessed on 27 April 2014).
15. Schechter, S.E.; Dhamija, R.; Ozment, A.; Fischer, I. The emperor's new security indicators. In Proceedings of 2007 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 20–23 May 2007.
16. Kaspersky Lab. Kaspersky Lab Report: 37.3 Million Users Experienced Phishing at-Tacks in the Last Year. 2013. Available online: http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year (accessed on 27 April 2014).
17. FBI. FBI Warns Public That Cyber Criminals Continue to Use Spear-Phishing At-tacks to Compromise Computer Networks. Available online: 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 on 4 April 2014).
18. Furnell, S.M.; Jusoh, A.; Katsabas, D. The challenges of understanding and using security: A survey of end-users. *Comput. Secur*. **2006**, *25*, 27–35.
19. Bicakci, K.; Yuceel, M.; Erdeniz, B.; Gurbaslar, H.; Atalay, N.B. Graphical passwords as browser extension: Implementation and usability study. In Proceedings of Symposium on Usable Privacy and Security (SOUPS 2009), Mountain View, CA, USA, 15–17 July 2009; ACM: Pittsburgh, PA, USA, pp. 1–17.
20. Dhamija, R.; Tygar, J. The battle against phishing: Dynamic security skins. In Proceedings of Symposium on Usable Privacy and Security (SOUPS 2005), Pittsburgh, PA, USA, 6–8 July 2005; pp. 1–12.
21. Sheng, S. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In Proceedings of Symposium on Usable Privacy and Security (SOUPS 2007), Pittsburgh, PA, USA, 18–20 July 2007; ACM: New York, NY, USA; pp. 1–12.
22. Kumaraguru, P.; Cranshaw, K.; Acquistic, A.; Cranor, L.; Hong, J.; Blair, M.A.; Pham, T. School of phish: A real-world evaluation of anti-phishing training. In Proceedings of Symposium on Usable Privacy and Security (SOUPS 2009), Mountain View, CA, USA, 15–17 July 2009; ACM: New York, NY, USA; pp. 1–12.

23. Kelley, P.A. “Nutrition Label” for privacy. In Proceedings of Symposium on Usable Privacy and Security (SOUPS 2009), Mountain View, CA, USA, 15–17 July 2009; ACM: New York, NY, USA, 2009; pp. 1–12.
24. Besmer, A. Social applications: Exploring a more secure framework. In Proceedings of Symposium on Usable Privacy and Security (SOUPS 2009), Mountain View, CA, USA, 15–17 July 2009; ACM: New York, NY, USA, 2009; pp. 1–10.
25. Maurer, M.; de Luca, A.; Kempe, S. Using data type based security alert dialogs to raise online security awareness. In Proceedings of Symposium on Usable Privacy and Security (SOUPS 2011), Pittsburgh, PA, USA, 20–22 July 2011; pp. 1–13.
26. Wu, M.; Miller, C.; Little, G. Web wallet: Preventing phishing attacks by revealing user intentions. In Proceedings of Symposium On Usable Privacy and Security (SOUPS 2006), Pittsburgh, PA, USA, 12–14 July 2006; pp. 1–12.
27. Shepherd, L.A.; Archibald, J.; Ferguson, R.I. Perception of risky security behaviour by users: Survey of current approaches. In Proceedings of Human Aspects of Information Security, Privacy, and Trust, Las Vegas, NV, USA, 21–26 July 2013; Volume 8030, pp. 176–185.
28. Mozilla Developer Network. SDK and XUL Comparison. Available online: http://developer.mozilla.org/en-US/Add-ons/SDK/Guides/SDK_vs_XUL (accessed on 4 April 2014).
29. Ur I.T. Mate Group. hpHosts Online—Simple, Searchable & FREE! Available online: http://hosts-file.net/ (accessed on 4 April 2014).
30. Heishman, R.; Duric, Z.; Wechsler, H. Understanding cognitive and affective states using eyelid movements. In Proceedings of First IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2007, Crystal City, VA, USA, 27–29 September 2007; pp. 1–6.
31. Doubleday, A.; Ryan, M.; Springett, M.; Sutcliffe, A. A comparison of usability techniques for evaluating design. In Proceedings of the 2nd Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques, Amsterdam, The Netherlands, 18–20 August 1997; Coles, S., Ed.; ACM: New York, NY, USA, 1997; pp. 101–110.
32. Mozilla Developer Network. Local Storage. Available online: https://developer.mozilla.org/en-US/Add-ons/Overlay_Extensions/XUL_School/Local_Storage (accessed on 19 October 2014).