Security Awareness and Affective Feedback: Categorical Behaviour vs. Reported Behaviour

Lynsay A. Shepherd,
Jacqueline Archibald

School of Arts, Media and Computer Games
Abertay University
Dundee, Scotland
lynsay.shepherd@abertay.ac.uk, j.archibald@abertay.ac.uk

This is the accepted version of a paper presented at the International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA 2017), June 19-20, 2017, London, UK which will be published by IEEE

Security Awareness and Affective Feedback: Categorical Behaviour vs. Reported Behaviour

Lynsay A. Shepherd, Jacqueline Archibald
School of Arts, Media and Computer Games
Abertay University
Dundee, Scotland
lynsay.shepherd@abertay.ac.uk, j.archibald@abertay.ac.uk

***Abstract*— A lack of awareness surrounding secure online behaviour can lead to end-users, and their personal details becoming vulnerable to compromise. This paper describes an ongoing research project in the field of usable security, examining the relationship between end-user-security behaviour, and the use of affective feedback to educate end-users. Part of the aforementioned research project considers the link between categorical information users reveal about themselves online, and the information users believe, or report that they have revealed online. The experimental results confirm a disparity between information revealed, and what users think they have revealed, highlighting a deficit in security awareness. Results gained in relation to the affective feedback delivered are mixed, indicating limited short-term impact. Future work seeks to perform a long-term study, with the view that positive behavioural changes may be reflected in the results as end-users become more knowledgeable about security awareness.**

Keywords*— *End-user security behaviour; usable security; affective feedback; user monitoring techniques; user feedback; security awareness; human factors of cybersecurity

I. INTRODUCTION

Risky security behaviour displayed by end-users has the potential to leave devices vulnerable to compromise [1]. Despite the availability of security tools such as firewalls and virus scanners, designed to aid users in defending themselves against online threats, these tools cannot stop users engaging in risky behaviour in the context of a browser-based environment. This indicates a need to assess the current behaviour of end-users, and to educate them regarding the security implications of their actions online. Previous research into educational tools suggest the use of affective feedback as a possible method to utilise in a browser-based environment [2][3][4].

As part of a research project, a prototype Firefox extension named Spengler-Zuul was developed, monitoring user actions, and employing the use of affective feedback as a potential method of user education. This paper outlines a section of a research project whereby a series of experiments have been conducted to gauge how behaviour logged by the aforementioned tool (categorical information) compares to behaviour reported in follow-up questionnaires with the users (reported information). Providing a comparison highlights levels of security awareness in end-users, and aids in demonstrating the potential role affective feedback can have in security education.

II. BACKGROUND

This section will outline risky security behaviours users may encounter when browsing the web. It discusses studies covering methods of measuring risk perception. Owing to the reliance on the internet, several pieces of research have posited the need to educate end-users regarding security behaviour, highlighting areas in which they may be vulnerable online. A number of existing tools are reviewed, prior to a discussion of the role of affective feedback in an educational environment. A novel approach utilising a combined affective feedback and monitoring solution is described, before the disparity between categorical user behaviour versus reported user behaviour is explored.

A. 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 such behaviour can include: interacting with a website containing coding vulnerabilities [5], downloading data from unsafe websites [6] or, creating weak passwords/sharing passwords with colleagues [7][8].

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 [9] to categorise compliant security behaviours and investigated if 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.

In 2005, Stanton et al [7] conducted interviews 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 six identified risky behaviours: intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance and basic hygiene.

Milne et al. [10] investigated risky behaviours in relation to self-efficacy. Participants were asked via a survey if they had engaged in specific risky behaviours online. These suggestions were drawn from previous research into risky behaviours [11][12]. The paper concludes different types of behaviour are exhibited online depending on the demographic and the self-efficacy of the end-user.

Behaviours users were asked about included the use of private email addresses to register for contests on websites, the use of dictionary passwords, and accepting strangers on social networking sites. Allowing their computer to save passwords was the most common risky behaviour participants admitted to (56%).

A lack of perception regarding online security risks can leave users, and their devices vulnerable to compromise.

B. Measuring perception of risk

Over the years, a variety of techniques have been utilised in an attempt to measure the perception of risk which the end-user possesses. Hill and Donaldson proposed a methodology integrating models of behaviour and perception [13]. The research examined the perception of system security the system administrator possessed. This created a trust model, engaging system administrators, and reducing the threat from malicious software. By quantifying the risk of threats, a triage system was developed to deal with issues.

In a different scenario, Ur et al. [14] 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.

Ng, et al. [15] devised a health belief analogy when explaining the perception of risk in terms of cyber security. 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.

San-José and Rodriguez [16] measured perception of risk using a multimodal approach. In the study, an antivirus program was installed in 3000 households with internet connected PCs. These machines were scanned for viruses on a monthly basis. The software was supplemented by quarterly questionnaires, therefore scan results could be compared against perception of risk information gathered from the questionnaires. Results showed a false sense of security was created by the antivirus software, and users were unaware of the seriousness of risks.

C. Education and awareness of risky security behaviours

A variety of tools have been developed to address differing aspects of risky security behaviours, and these are outlined in this section.

One such example is the password strength meters used in research by Ur et al. [17]. These meters were placed next to password fields and improved the security and usability of passwords. 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, there were potential issues with retention, and 38% of participants admitted to writing down their password from the previous day.

Other research has explored the education of users with regards to phishing attempts. Such tools have included Anti-Phishing Phil by Sheng et. al [18] which attempt to gamify the subject. After playing the game, 41% of participants viewed the URL of the web page, checking if it was a genuine site. Results showed that some participants became overly cautious, and a number of false positives were produced.

Kumaraguru et. al [19] developed a phishing training tool, PhishGuru. This was developed to discourage people from revealing information in a phishing attempt. A cartoon message is presented if a user clicks on a link in a suspicious email, whereby they are warned about the dangers of phishing. A short-term study was conducted, and it was found that the cartoon message proved to be effective: participants retained the information after 28 days.

A newer tool, NoPhish has been developed as an Android application. The tool seeks to provide education about phishing attempts via mobile devices [20]. The game features multiple levels and users are presented with a URL. They are asked to determine if it is a legitimate link, or a phishing attempt. After playing the game, participants gave significantly more correct answers when asked about phishing. A longer-term study showed participants still performed well however, their overall performance decreased.

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 [21]. Labels seek to present the information in an easily readable format, aiding users to understand privacy policies online. 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.

A Firefox extension developed by Maurer [22] provides alert dialogs when users are entering sensitive data e.g. credit card information. By providing large JavaScript warnings, the extension seeks to raise security awareness. It was noted that the use of certain colours made users feel more secure.

Volkamer et al. developed an add-on for Firefox called PassSec. This extension attempted to help users detect websites which provided insecure environments for entering a password [23]. The extension significantly reduced the number of insecure logins, and therefore raised security awareness.

The tools discussed in this section span a number of years, and some of the research may seem outdated. However, the range, and age of the research tools developed indicates there is still a problem with effectively educating users regarding

security awareness. This suggests a different approach is required for user education: the use of affective feedback is a potential approach.

D. Affective feedback and risky behaviours

Affective feedback is defined as "*the process of using technology to help people achieve and maintain specific internal states*" [2] i.e. using signals to alter user behaviour. Previous research has indicated affective feedback may serve as a successful method of educating users about risky security behaviour [2][3][4]. 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 positively impact upon the security awareness of the end-user.

Virtual human characters, avatars, and textual content [24] and the use of colour and sound [2] have been used to influence state. Avatars provide affective feedback and have been seen to be beneficial in educational environments [2][3][4]. Textual information and the use of specific words has the potential to alter a user's state/behaviour e.g. a password described as "weak" can encourage them to create a stronger password [17]. Colour is also often utilised, with green or blue used to imply a positive occurrence, with red indicating a negative outcome [17].

To further the argument for use of affective feedback Wixon [25] 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 [26] in their overview of emotional simulations. Affective feedback has the potential to be utilised in the field of security education, thus the application of such a mechanism in this research project.

Research conducted in the following section seeks to utilise an affective approach, deploying the use of a monitoring solution with an integrated affective feedback delivery system, in an attempt to improve end-user security awareness.

III. Methodology

A. Prototypes developed

A XUL-based Firefox extension was developed for the research project, named Spengler-Zuul [27]. This incorporated a monitoring solution capable of detecting potential security risks such as if a page contains malicious links, or a password entered is too short. These risky behaviours were drawn from previous research [10][11][12][28] and were chosen as they could apply to the context of a browser-based environment. When the user interacts with the browser, information gathered is encrypted, and processed on the server. As an example, processing the information on a server allows the URL of a website to be compared against a database of known malicious sites [29]. Detection of a malicious site triggers the affective feedback mechanism, delivering information to the end-user. A unique log file is generated for each browser session, and records risky security behaviour triggers e.g. if a user visited a malicious site.

Three methods of affective feedback were chosen: colours, avatars and text. 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 advice because of their behaviour, negative advice, or a mixture of both positive and negative.

The sentences contained in the Spengler-Zuul extension came from text in an affective word list named AFINN [30]. The avatars were chosen in relation to Ekman's six basic emotions [31]. Specifically, the happy and sad avatars used in this research project were drawn from work conducted by the Swiss Center for Affective Sciences [32]. Finally, colours used were chosen due to their usage in previous research projects [17][2]. The final colours chosen were: red (#CF4250), yellow (#EBA560), and green (#78BF60), producing a traffic-light system.

Multiple versions of the Spengler-Zuul extension were developed, allowing differing combinations of affective feedback to be tested against a control environment:

- Spengler-Zuul (none)- monitors users, no on-screen feedback.
- Spengler-Zuul (text)- monitors users, displays text-based affective feedback.
- Spengler-Zuul (text, avatar)- monitors users and displays text-based affective feedback, and an avatar
- Spengler-Zuul (text, colour)- monitors users and displays text-based affective feedback, and colour
- Spengler-Zuul (text, colour, avatar)- monitors users and displays text-based affective feedback, and colour. Additionally, an avatar is situated in the bottom right of the screen (Fig 1).

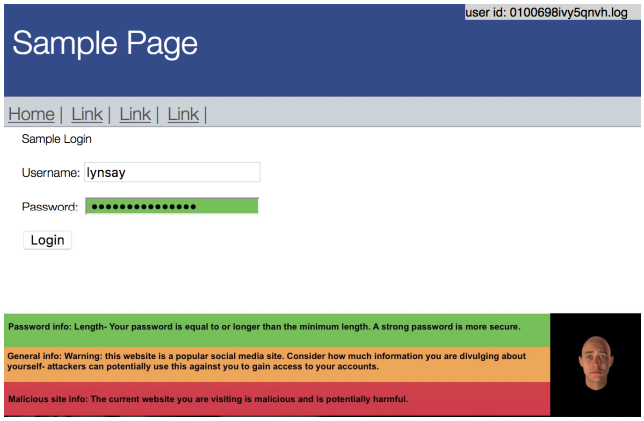

Fig 1. Screenshot of the Spengler-Zuul (text and colour and avatar) extension

B. Experimental phase

During the experimental process, participants were initially given an "Information For Participants" handout, noting that

the experiment was testing a Firefox extension. Security awareness and behaviour were not mentioned, in relation to the experiments, in an effort to eliminate bias. Participants were then given a random USB stick, labelled with a number from 1-5 and each USB stick contained a portable version of the Firefox browser, with a version of the monitoring solution/affective feedback mechanism add-on pre-installed (Table 1). After signing the consent form, participants were asked to work their way through an instruction sheet, visiting specific websites.

Table 1. Different versions of feedback included in each experiment.

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

Participants were asked to visit a number of predefined sites, some with false positives to trigger appropriate feedback on-screen e.g. fake malicious links to trigger warnings. During the experimental process, participants were also asked to complete a web form, asking them personal information such as hobbies. Completing this form was entirely optional however, revealing such information could have been deemed a risky security behaviour.

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 any feedback shown on-screen. In the background, the users' actions on the computer-based part of the experiment were logged, meaning the information provided in the questionnaire can be corroborated against the information in the unique log files.

IV. Results

The log files gained from the monitoring solution were compared with data from the questionnaire participants answered. By comparing these approaches, an understanding of user awareness of risky security behaviour can be developed i.e. do the log files reflect what users said they actually did in the questionnaires? This multi-modal approach is comparable with work by San-José and Rodriguez [16], whereby they compared virus scan log data against questionnaire data.

To produce descriptive statistics from the data gained from the log files, databases and questionnaires 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 test was utilised. 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. The main difference Table 2 highlights 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 (categorical information) in the log files vs. those who reported they revealed personal information in the questionnaire in experiments groups 1 (control) and 3 (text and avatar-based feedback). This potentially highlights a lack of security awareness in end users who haven't realised the level of information they divulged. This could also explain the similar results for "*Did user enter email address?*" in groups 4 (text, colour-based feedback) and 5 (text, colour, avatar-based feedback), and "*Did user visit a malicious site?*" in groups 1 (control) and 2 (text-based feedback).

Table 2. Experimental results- log files vs. questionnaire data

Question	Group 1 (Control)	Group 2 (Text)	Group 3 (Text, avatar)	Group 4 (Text, colour)	Group 5 (Text, colour, avatar)
User revealed personal information	Yes	No	Yes	No	No
User entered private email address	No	No	No	Yes	Yes
Entered a common password	No	Yes	Yes	Yes	Yes
User had personal details in password	No	No	No	No	No
User visited a malicious site	Yes	Yes	No	No	No

V. Discussion

When the questionnaire results (reported information) were compared to the log files (categorical information) there was one key question regarding risky security behaviour which produced a statistically significant result.

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 similar results are seen across all experiments containing affective feedback, it suggests the delivery of the affective 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 [33]. One interpretation of the result is that participants may not have been aware of the term *"dictionary word"* in relation to passwords. Additionally, they may not have been aware that dictionary words in passwords contribute to poor password hygiene [10].

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 reported revealing information about themselves (as per the questionnaire data), in comparison to the number of participants who categorically revealed personal information about themselves, as revealed by the appropriate log files.

In experiment 1 (control) and experiment 3 (text and avatar-based feedback) there was a significantly higher proportion of participants who categorically revealed personal information about themselves in the log files, in comparison to those who reported 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.

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 log files were simple 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.

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 categorically visited malicious sites (according to the log files) than reported visiting malicious sites in the questionnaire. Since experiment 1 does not contain any form of affective feedback whereas experiment 2 does, therefore 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 again highlights participants either chose to divulge sensitive information, or that they actively engaged in risky security behaviour by failing to read the page properly.

There are a number of limitations regarding the study. In relation to the experimental design, end-users were aware they were taking part in an experiment therefore, they may have assumed all websites they were asked to visit were safe. Additionally, the experiments took place on a lab machine therefore, participants may have been less careful when clicking on links, as they weren't on a personal machine.

VI. Conclusions

Affective feedback did not appear to have an impact on the behaviour of users as recorded by categorical information in the log files. 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 positive result, where fewer participants in experiment 5 divulged information and this suggests affective feedback may have made a difference.

However, given that all other results were insignificant, it is more plausible that the particular group of participants already possessed a good knowledge of risky security behaviours. Overall, it has been concluded affective feedback did not have an impact on participant behaviour, as per the log files.

The results gained still highlight an interesting point. In comparing categorical behaviour (log files) and reported behaviour (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.

This research project involved a small-scale experiment. Potentially, 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.

VII. Future Work

Future work would involve changing some of the affective feedback which was delivered to the participants during the experiment, and potentially modifying the positioning to find the optimal placement. 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. [34] and have the potential to be applied to the realm of cyber security. Consideration could also be given to the specific phrasing and the wordlist used. There are also a number of other wordlists available- running a comparison in terms of risky security behaviours could aid in establishing which is the most efficient and appropriate list to use when interacting with average end-users on the internet.

Results gained 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.

REFERENCES

[1] Li, Y. and Siponen, M (2011). A call for research on home users information security behaviour. In: PACIS 2011, Proceedings,.

[2] McDarby, G.,et al. (2004). Affective feedback. Media Lab Europe. [online]. http://medialabeurope.org/mindgames/publications/publicationsAffectiveFeedbackEnablingTechnologies.pdf

[3] Robison, J., McQuiggan, S., Lester, J. (2009). Evaluating the consequences of affective feedback in intelligent tutoring systems. [online]. In: Proceedings of International Conference on Affective Computing and Intelligent Interaction, ACII 2009, pp. 37–42. http://www4.ncsu.edu/~jlrobiso/papers/acii2009.pdf

[4] Hall, L., et al. (2005). Achieving empathic engagement through affective interaction with synthetic characters. [online]. In: Tao, J., Tan, T., Picard, R.W., (ed.). ACII 2005, Heidelberg, LNCS Springer, p 731–738.

[5] Hadnagy, C (2011). Social engineering: the art of human hacking. Indianapolis, Wiley Publishing.

[6] Fetscherin, M (2009). Importance of cultural and risk aspects in music piracy: A cross- national comparison among university students. [online]. Journal of Electronic Commerce Research,. http://www.csulb.edu/journals/jecr/issues/20091/Paper4.pdf

[7] Stanton, J.M (2005). Analysis of end user security behaviors. [online]. Computers and Security 24, pp.124–133.

[8] Payne, B. and Edwards, W (2008). A brief introduction to usable security. [online]. Internet Computing, 12 (3), pp. 13–21.

[9] Padayachee, K (2012). Taxonomy of compliant information security behavior. [online]. Computers & Security, 31 (5), 673–680. http://dx.doi.org/10.1016/j.cose.2012.04.004

[10] 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

[11] 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 Con- sumer Affairs, 41 (1), pp.127-149. 10.1111/j.1745-6606.2006.00071.x

[12] 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

[13] 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. 10.1145/2841113.2841125

[14] Ur, B. et al. (2016). Do Users' Perceptions of Password Security Match Reality? [online]. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16, pp.3748–3760. http://doi.org/10.1145/2858036.2858546

[15] Ng, B., Kankanhalli, A. and Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. [online]. Decision Support Systems, 46 (4), pp.815–825. http://dx.doi.org/10.1016/j.dss.2008.11.010

[16] San-José, 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

[17] 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.

[18] 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

[19] 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

[20] Canova, G. Volkamer, M. Bergmann, C. Reinheimer, B. 2015 Nophish app evaluation: lab and retention study. In: NDSS workshop on usable security

[21] Kelley, P (2009). A "Nutrition Label" for Privacy. [online]. In: Symposium On Usable Privacy and Security, pp.1-12. http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf

[22] 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

[23] 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

[24] 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

[25] Wixon, D (2011). Measuring fun, trust, confidence, and other ethereal constructs: it isn't that hard. [online]. Interaction, 18 (6), pp. 74-77. http://dx.doi.org/10.1145/2029976.2029995

[26] 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. http://www.sciencedirect.com/science/article/pii/S107158 1909000573

[27] 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

[28] Shepherd L.A., Archibald J., Ferguson R.I. (2013) Perception of Risky Security Behaviour by Users: Survey of Current Approaches. In: Marinos L., Askoxylakis I. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2013. Lecture Notes in Computer Science, vol 8030. Springer, Berlin, Heidelberg

[29] HpHosts. 2016. [online]. http://www.hosts-file.net/

[30] 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 Mi- croposts': Big things come in small packages. Volume 718 in CEUR Workshop Proceed- ings, pp.93-98.

[31] Ekman, P. (1999). Basic emotions. [online]. Cognition,. http://doi.org/10.1002/0470013494.ch3

[32] 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

[33] Hoffman, L (2011). Risky business. [online]. Communications of the ACM, 54 (11), pp. 20- 22. http://dx.doi.org/10.1145/2018396.2018404

[34] Gulz, A., Ahlner, F. and Haake, M. (2007). Visual Femininity and Masculinity in Synthetic Characters and Patterns of Affect. [online]. ACII 2007, LNCS, pp.654–665. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.452.887&rep=rep1&type=pdf