Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 3159-0040
Vol. 2 Issue 6, June - 2015

Examination on Usability Issues of Security Warning Dialogs

Zarul Fitri Zaaba & Teo Keng Boon
School of Computer Sciences
Universiti Sains Malaysia,
Penang, Malaysia
zarulfitri@usm.my,
tkboon.ucom11@student.usm.my

***Abstract*—This paper examines the usability issues of security warning dialogs from end-users' perception. The study has been carried out in the Universiti Sains Malaysia. The study consists of two parts in order to assess the experience of end users' during the encountering of security warnings – part 1: an online survey study which presented with three different security warning dialogs to examine end-users' understanding and perception, and part 2: an interview study to further understand the issues faced by the end users. The study has gained insights and understanding of the usability issues end-users are facing with the current security warning dialogs. Therefore, this study provided justification for the need of improving security warnings to be more understandable.**

Keywords—security; warnings; usability; Human-computer Interaction; usable security; warnings dialogs.

I. INTRODUCTION

Computer security is gaining increasing concern nowadays as the compromise might bring serious consequences such as information leakage and financial loss. While security warnings have the vital role in the computer security, usability of security warnings has also becoming a concern of the researchers. The concept of security Human-Computer Interaction (HCI-S) was introduced, where the interfaces of security features can be made as usable as possible so users will less likely to make mistake or bypass them [1]. Warnings play an important role in the security aspect, alerting consequences of an action done by user, and remind user to act accordingly. Based on the concept of HCI-S, we can deduce that the security can be improved with usable security warnings. However, evidences have shown that several existing issues of usability of security warnings, such as the lack of information and ease of comprehension, causing difficulties for user to make the appropriate decision.

The issues of security warning had been investigated and classified by previous researchers. In particular attempt to address the usability issues and improve the security warnings dialog, which is the most encountered context of security warning based on [2]. However, based on recent observation there is still lack of empirical evidence on domestic end-users. Therefore, a small focus group study has been carried out in the Universiti Sains Malaysia to investigate and provide insight of the issues of security warnings.

In this paper, an overview of usability issues of security warnings is presented, followed by the discussion of the online survey study that has been carried out. The study followed by a further evaluation by user study with interview method. The findings from the study provide insight of the usability issues faced from the end-user's perspective, and provide justification for the need of improving computer security warnings.

II. OVERVIEW OF USABILITY ISSUES OF SECURITY WARNINGS

The computer security warnings are presented by applications or operating system to inform, alert, and warn the users about the possible unpleasant consequences of an action in advance. The warnings explain that risk might occur and possible precautions should be considered before users proceed with the potentially risk action [3].

Based on the main functions of warnings described by [4], the warnings are important in informing users of the potential risk and provide safety information to avoid the risk. By presenting this information, users can be influenced in a way to differentiate how and what to avoid, and therefore preventing them from the possible undesired consequences. Warnings also act as reminder to the users who already know the risk of their action. The warnings draw attention to what might happen and therefore precaution or wiser decision can be made.

Due to the important role of the computer security warnings played, the usability issues of the computer security warnings are gaining attention from scholars. For the past decade, computer security warnings have been investigated in many context such as browser warnings and virus alert [5][6][7], online banking [8][9], privacy and policy [10][11] and fake security warnings [12][13]. Various common usability issues are found from the studies and researches carried out by scholars and are summarized in Table I.

TABLE I. Usability issues of Computer Security Warnings

Usability issues	Description and findings from past studies
i. Attention towards security warnings	▪ Users did not pay attention to web security cues warning, and easily misidentify small icon warnings [14]. ▪ Users ignored the phishing warnings especially when the web content looked legitimate [15]. ▪ Users ignore web browser warnings in the study done by [16]. They argued that it was influenced by the amount of information displayed by the warnings
ii. Understanding of security warnings	▪ Users were lacking of knowledge to differentiate fake and real warnings [12]. ▪ Users failed to understand the SSL warnings in the browsers [7]. ▪ Users did not understand the meaning of the phishing warnings and the indicators needed to be more distinct [6]. ▪ Users experienced difficulty to understand the context of security warnings [17].
iii. Usage of technical terminologies	▪ Novice users did not understand technical wordings although they were heard about it [18]. ▪ Most of the users do not understand technical terminologies such as the meaning of ActiveX control in Internet Explorer [19]. ▪ User still experienced significant problems on technical jargons used in security warnings [17][20]
iv. Users' motivation	▪ Users ignore security warnings because security warnings are seen as burdens, and offer poor cost-benefit trade off [21].

III. PART 1: ONLINE SURVEY STUDY

It is useful to gather information from end-user's perspective. The understanding of end-user's perception and comprehensibility lay as the foundation of this research. A survey study has been the preferred tool for initial research to establish the foundation of user studies [8][19][22][23].

. This chapter presents a survey study as a general investigation to examine the perception and usability issues of security warning dialogs. The finding from this survey became the foundation for conducting further investigation in the research.

A. Methodology

This survey focused on the perception and usability issues in relation to security warning dialogs. An online survey using questionnaire has been conducted in November 2014 in order to gain preliminary insight on the usability issues and users' understanding toward contemporary security warning dialogs. The survey was promoted via social networking site (i.e. Facebook roups), E-mail and university community in order to recruit subjects predominantly the current and graduated students from the Universiti Sains Malaysia. The survey consisted of 13 questions, predominantly in the format of closed-ended, which were multiple choice questions and scaled questions.

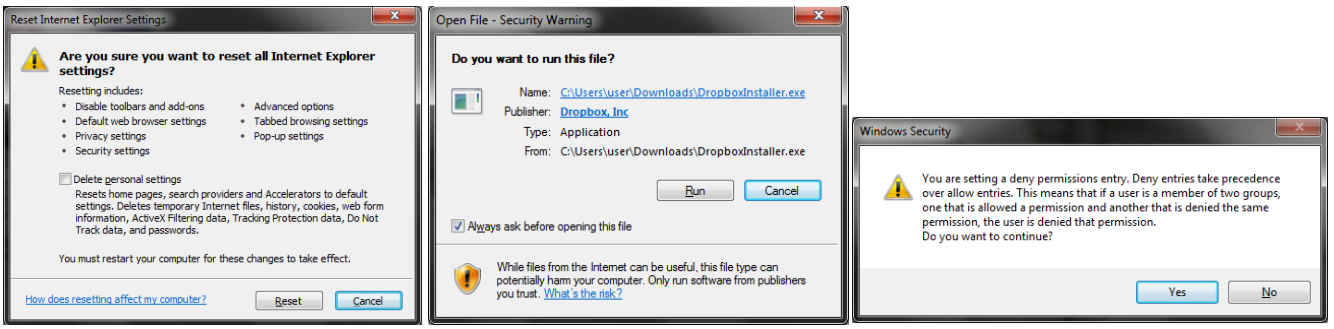
The aim for this survey study is to provide some basis on end-users understanding and perception in relation to computer security warnings. Thus, the results provide useful preliminary insights on how security warnings can be better improved.

B. Results and Discussion

A total number of 55 completed responses were received. Note that due to rounding, the values presented from the results of the study and in some of the later discussion might not add up to exact 100%. All of the figures and percentages reported were based on the proportions of the 55 completed responses. The overview of the profile of the respondents is shown in Table II.

TABLE II. Profile of participants of Part 1 study

Characteristics (n=55)	Frequency Distribution	Percentage (%)
Gender		
Male	35	63
Female	20	37
Age		
18-25	45	82
26-35	6	11
36-45	1	2
46-55	2	4
56 and above	1	2
Education Background		
Pre-U	1	2
Undergraduate	49	89
Postgraduate	5	9
Computing skill (self-rated)		
Beginner	7	13
Intermediate	31	56
Advanced	14	25
Expert	3	6
Computer usage		
Daily	49	89
2-6 times per week	3	6
Weekly	0	0
2-3 times per month	3	6
Monthly	0	0
Security warning encounter frequency		
Every time	14	25
Once a while	26	47
Seldom or never	15	27



Security warning dialog 1 Security warning dialog 2 Security warning dialog 3

Figure 1 Security warning dialogs presented in the online survey study

From the 55 responses, the gender profile can be categorized with 63% of male and 37% of female. Most of the respondents are from the age group of 18-25. Most of the respondents rated themselves as intermediate or advanced computer users. The respondents were asked about their frequency of encountering of security warnings. Half of the users encounter security warnings once a while, and the another half spitted between encounter security warnings every time they use computers, and seldom or never received security warnings equally.

In order to evaluate the comprehension or understanding of respondents toward security warnings, three security warning dialogs were presented as shown in Fig. 1 and respondents were asked to indicate how far they agree with the statements regarding the usability of the security warnings.

The three security warning dialogs chosen are exhibiting some usability issues which were classified in Table I based on the perception and evaluation done by the authors. Therefore, this survey study attempt to evaluate the comprehension of the respondents in relation to these particular issues as well. The evaluation will be discussed in the following paragraphs.

First of all, the three security warnings use the similar yellow icons with exclamation. The icons are the indicator of warnings and attempt to alert the users. Respondents were asked how far the icons being used in the security warning dialogs able to attract their attention, and therefore make them alert of something that they need to make decision. For the three warning dialogs presented, about 30% of respondents claimed that the icons did not attract their attention. On the other hand, 40% of respondents claimed that the icons were able to attract their attention, while the others remain neutral. However, more than 40% of respondents claimed that they generally unaware of the content of the security warning dialogs and leaped to the default decision.

One of the most common usability issues, the usage of technical terminology was also evaluated in the survey. The usage of technical wording is particular noticeable in security warning dialog 2, such as “Accelerator”, “cookies”, “ActiveX”, and etc. In fact, about 40% of respondents rated that they having problem understanding the meaning of technical terminologies. Most of these respondents are come from the group with lower computing expertise. And surprisingly, even some of the respondents who claimed themselves with advanced computing expertise rated that they have certain level of difficulties to understand some of the technical terminologies as well.

When asked about whether the security warning dialogs provide sufficient information for the respondent to make decision, for the three warning dialogs presented; 40% - Security warning dialog 1, 30% - security warning dialog 2, and 30%- security warning dialog 3 of the respondents respectively rated that the information provided was not sufficient. In fact, more than 40% of respondents in every case rated that they are unsure of the most appropriate decision to be made based on the information provided by the warnings. 30% of respondents rated that they are unsure of the risk level of the warnings, and could be the reason of facing difficulties in making the most appropriate decision.

The understanding with the security warnings are dependent on end-users’ knowledge and the information presented in the warnings as well. Either insufficient of information given, or the information given is too complicated which do not aligned with user’s knowledge, will have impact on the comprehensibility. The complicated information (based on the authors’ perception) is found in security warning dialogs 3, where users needed to have related knowledge in the first hand in order to understand.

Respondents were asked to rate their understanding with current security warning dialogs in general. There is only about a quarter of respondents were rated they understand or somewhat understand security warnings, as shown in Fig. 2. This indicate large portion of respondents were not confident of their understanding of security warning dialogs.

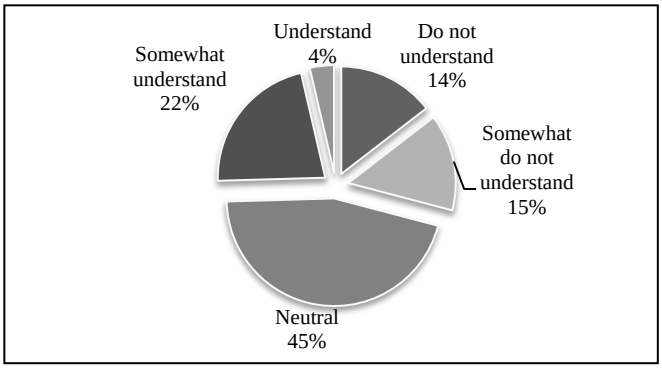


Figure 2 Respondents' Rate of Understanding toward Current Security Warning Dialogs

Finally, 96% of respondents agreed that the current security warnings needed to be improve in order to become more understandable, and therefore enable them to make wiser decision upon the encountering.

C. Summary of Findings and Limitation

This survey study provides the useful initial insight of comprehensibility and usability from end-users' perspective toward contemporary security warning dialogs, and became a foundation and justification of further research. The responses indicated there are significant portion of end-users are facing several usability and comprehensive issues with security warnings including lack of sufficient information, usage of technical wording, and inability to perceive risk level. These issues have prevented them to make wise decision confidently. There are rooms for improvement in relation usability issues with the contemporary security warning dialogs. As the goal of HCI-S, the improvement of interface will lead to more secure, robust, and reliable system [1].

One of the constraints of this study was having a small sample. In addition, we only gather respondents from the university environment. Thus, the results might portray from the academic perspective.

IV. PART 2:INTERVIEW STUDY

In the aforementioned section, a survey study was conducted to evaluate common usability issues faced by end-users and provided insight a basic understanding or insight of end-users' perception towards security warning dialogs. Therefore in this section, a more detailed investigation of how end-users dealing with the security warning during practical tasks is presented. This study involves participants to identify perceived security warnings that were encountered during normal system use, and assessed their extent of understanding towards the warning dialogs.

A. Methodology

The interview study focused on the perception of end-users toward security warning dialogs and is carried out in the open-ended interview form. The open-ended approach has been a commonly applied approach in literature for evaluating comprehension and initial clarity of the warnings as recommended by [24]. This form of study provides more information about source of confusion and the types of errors that people make [25].

The interview was conducted in December 2014, targeting the computer users aged 18 years old and above only. The participants was promoted and recruited through word of mouth, E-mail and through social networking site (e.g. Facebook Groups). The participants recruited included students, lecturers and teaching assistants from the Universiti Sains Malaysia (USM). The questions in the interview are predominantly open-ended, that is participants may give any answer they want. Having open-ended type of questions will give more variety answers and it closely reflects to highlight the real problems experience by the end-users. On the other hand, utilizing closed-ended questions are not suitable as the answers were already determined (i.e. users chosen the answers from a list of pre-determined choices). Each interview was recorded in the format of audio, later the scribing was done based on the recording. The scribing was verified by a reviewer hired by the researchers.

B. Results and discussion

The interview had been conducted with 30 participants on one-to-one basis. The participants were recruited from the Universiti Sains Malaysia community, targeting both participants from computing or technical background, and non-computing backgrounds. Note that due to rounding, the values presented from the results of the study and in some of the later discussion might not add up to exact 100%. All of the figures and percentages reported were based on the proportions of the 30 participants. The profile of participants is shown in Table III.

The participants split almost equally from computing background and non-computing background. While participants from computing background claimed that they have at least intermediate computing expertise, many participants from non-computing background claimed that they have only beginner level of computing skills. The profiling of computing expertise was essential in the later examination of usability issues of security warning.

In the first session, two general questions were asked as a warm up questions. This is to gain insight of comprehension and to verify the computing expertise that was claimed by the participants. In addition, this was done to ensure end-users are comfortable so that they aware the questions that they will answers is something that they have experienced beforehand.

1. What web browser do you usually use to access the Internet?

2. What program do you use to read your e-mail?

TABLE III. Profile of participants of Part 2 study

Characteristics (n=30)	Frequency Distribution	Percentage (%)
Gender		
Male	18	60
Female	12	40
Age		
18-25	27	90
26-35	1	3
36-45	1	3
46-55	1	3
Education Background		
Undergraduate	26	87
Postgraduate	4	13
Computing/Technical Background		
Yes	14	47
No	16	53
Computing skill (further self-rated)		
Beginner	10	33
Intermediate	14	47
Advanced	4	13
Expert	2	7

Having said that, it is not surprising, the participants who claimed that they have advanced or expert level of computing expertise do not require any clarification of these questions. However, about 36% of participants, who came from groups with beginner level or intermediate level of computing expertises, have asked of some clarification - in particular, the meaning of the terminologies such as “web browser” and “e-mail program”. Later, in the next session, found that these participants have difficulties understanding technical terminologies used in the security warning dialogs too.

In the main session, the comprehension of participants toward security warning dialogs was evaluated. In the previous study, five security warnings were presented to participants in order to gain clear understanding of users’ mental model [26]. While in another study, only one scenario was described to the participants [27]. However, in this study two scenarios of warnings were presented to users in order to provide sufficient information yet able to meet the time constraint. The scenarios presented are shown in Table IV.

A series of questions were asked in order to understand how far the participants understand the security warnings. In particular, participants were asked where the security warnings came from, this is to gain preliminary insight of the participants’ knowledge towards given security warnings.

TABLE IV. Security Warnings that have been used in the interview study

Security warnings	Description
	The security warning user received when tried to open an application from unknown publisher.
	The security warning user received when tries to download an application from web in Internet Explorer.

TABLE V. The comprehensibility of participants towards the icon in the security warnings

Icons	Correct meanings and descriptions	Some wrong / inaccurate answers given by participants	% participants who answered correctly	% participants who answered wrongly / inaccurately	% participants who did not know the meaning
	Error: something is wrong, high possibility of unsafe	Certificate, *“cannot open”*.	37	27	37
	Warning: Alert, may be dangerous, be careful	Defender *“can ruin everything”*.	53	23	23
	Applications / exe file	Windows OS, system file	53	20	27

For the security warning dialog 1, 1/3 of the participants identify correctly where it was given by the operating system. However, another 1/3 misidentify it as the warnings encountering when try to download a program, or the usual acknowledgement during installation of a software. Some thought it was the warning from antivirus. The last 1/3 was not knowing or unsure of where the warnings came from.

On the other hand, for security warning 2, only 10% of participants identify the warning was given by IE. This could be due to the decreasing usage of IE over time [28], when users are switched to other browser. Most of the participants gave other answer. Based on the scenario given, many participants thought it was a fake security warning on the webpage that prompt them to download junk applications.

Participants were asked to describe the meaning of the respective security warning dialogs, and their understanding to specific elements in the security

warnings. Generally, most of participants who identified the prompts were security warnings have gave the correct meanings or answers which were near to the correct meanings. Others have given inaccurate response or do not know the meaning of the warnings.

Icons are the useful elements in security warnings. During the interview, participants were asked to describe what they understand about the icons in the given security warnings. The results are shown in Table V. About 20-30% of the participants failed to explain the meaning of each icon accurately. Some of the wrong or inaccurate answers given are shown in Table III as well. While 20-30% of participants never understand or notice specific meaning of the icons. From the result, we can deduce that the icons used in the security warnings do not give meaningful information to many end-users.

From the perspective of human computer interaction, the signal cues (i.e. icons and words) should be able to comprehend the users with the context of warnings that they are dealing with. For instance, the unidentified program icon (white background) did not convey anything to end-users. No information or explanation was given and it had been used in many security warnings before [17].

On the other hand, the participants' understanding of technical terminologies was also evaluated, by requiring them to describe what they know of the term "digital signature" found in the security warning dialog 1. The participants who gave minimal description were assumed as have at least some knowledge of what is digital signature. Overall, the participants who were able to explain and those who were not split into about 50:50. Almost all participants from beginner level of computing expertise unable to explain the meaning of digital signature. Yet surprisingly, there were participants who claimed that they have advanced level of computing expertise have not idea of what is digital signature.

For scenario 2, the participants were asked about the differences of the "Run" and "Save" decisions. It can be found that participants who ever used Internet Explorer as their web browser tend to understand the differences between the two decisions. From here, we can deduce that the understanding of security warnings is also depends on users' experience.

The participants were asked about possible consequences if choose to proceed in the given security warnings. Most of the responses were the risk of infected by malware. However, when asked about the decision they will make, the responses are summarized in Table VI below. The responses worth discussed is that many participants choose to cancel the running or download because they are unsure of the consequences, and therefore choose to play safe. In fact, the security warning 2 is the regular warning that will be given when downloading an executable file (.exe) with Internet Explorer, while the file might not be necessary something harmful. However, many participants make the decision to cancel the download simply because of the uncertainty. If the downloads is actually legit, this in turn is not a wise decision, and deter normal download operation. Table VII below quotes some of the response from participants in this case.

TABLE VI. DECISION MAKE BY THE PARTICIPANTS AND THE REASONS

	% participants		
Decision	**Scenario 1**	**Scenario 2**	**Reasons**
Proceed	37	3	• Need the software • Rely on antivirus to protect • Confident in own knowledge/skills to resolve computer problems
Cancel	43	90	• Recognize the risk of infected by malware • Afraid of the unknown consequence • Past experience of getting junk software • Suspicious scenario
Depend	20	7	• Whether recognize the source of the software • Depend on the recommendation and review of others

TABLE VII. The Quote/responses from the Participants

Users	Responds
A	*"Cancel. Because it's a potential threat, and I don't want it harms my computer. Because I don't know what this is about."*
B	*".if the message tells me something I cannot understand and I feel not comfortable then I would not run. I'm afraid to run if I don't understand."*
C	*".because this 'potentially harm' looked very dangerous, so if I no trust this one I would just click Cancel."*

TABLE VIII. Opinion of Participants towards Improvement of Security Warnings

	Beneficial	Not beneficial
Reasons	• Able to increase understanding especially for users who have lower computing expertise • Able to make wiser decision instead of simply based on assumption and experience	• Current security warnings are already understandable • Current security warnings have their status quo and new security warnings might not be recognizable • People who act in ignorance do not get benefit for improvement of security warnings

Finally, the participants were asked what they think if the security warnings can be improved or changed to a better version that can be suited or personalized based on their level of comprehension. For both cases, most of the participants said that it will be beneficial if the security warnings being more understandable instead of using technical jargons. The participants will be able to make wiser decision instead of simply based on assumption and experience. Some opinions on how to improve security warnings were received and added into account in further work in improving security warnings. However, there were about 26% of participants did not see benefit from the improvement on comprehensibility of security warnings. The responses received are summarized in Table VIII below. The majority on the other hand still think the need on the improvement of security warnings.

D. Summary of findings and Conclusion

This interview study has provided better understanding of usability issues faced by the end-users. The participants were encouraged to share their thought and what they understand from the security warnings during the interview.

From the results, the usability and comprehensive issues that were classified by scholars are still presented in contemporary security warnings. The study found that 50% of participants do not know the meaning of the term “digital signature”, this show that the usability issue in the aspect of usage of technical wordings is significant. Some elements in security warnings such as the icon and description given do not provide much meaningful information for the end-users to make proper decision, 40-60% of participants from this study unable to appreciate and to understand the meaning or information provided by the icons in the security warnings.

The problem or challenges in security warnings studies are not only significant among the end-users with lower computing expertise, but also found within the so called advanced computer users. Also found that most of the end-users largely depend on their past experience and intuition. Some participants (see Table VII) have mentioned that the not understandable warnings make them afraid, and simply make the ‘safe’ decision to cancel due to the uncertainty.

Generally, the finding of this study affirm the result from the part 1 study, where many end-users are facing usability and comprehensive issues with the security warnings, and have provided more information of the users’ perception and thought during the encountering of the security warnings.

Therefore, there are still plenty of rooms for improvement in the usability aspects of security warnings. In fact, 74% of the participants are looking forward for the improvement of security warnings to be done, if possible aligned to their level of understanding in order to enable them to make wiser decision.

V. Conclusion and Future Work

This survey study provides the useful insight of comprehensibility and usability from end-users’ perspective toward contemporary security warning dialogs, and became a foundation and justification of further research. The responses indicated there are significant portion of end-users are facing several usability and comprehensive issues with security warnings including lack of sufficient information, usage of technical wording, and inability to perceive risk level via the survey and interview questions. These issues have prevented them to make wise decision confidently. There are rooms for improvement in relation usability issues with the contemporary security warning dialogs. As the goal of HCI-S, the improvement of interface will lead to more secure, robust, and reliable system [1]. One of the constraints of this study was having a small sample. In addition, we only gather respondents from the university environment. Thus, the results might portray from the academic perspective only. Having difficulties to find a fully commitment of participants is one of the challenging issues.

In conclusion, the result of the survey and interview studies has become the foundation to understand the challenging aspects of security warnings. These bases will be used to further enhance the current security warning presentation so that the warnings will be able to communicate the risk accordingly. From one perspective, it helps the general public and researchers within this domain to understand the usability issues of security warnings.

Security warning should be able to help end-users to act with secure manner actions. Warnings itself should be able to convey the risk and warn the users on possible actions to take. For the future works, suitable framework will be used to improve security warnings utilizing the results of the survey and interviews. A prototype will be developed to test end-users in comparing the existing warnings and the new

warnings. Therefore, it will open a new dimension on how security warnings can be improved and help the society to act in a safe behavior.

REFERENCES

[1] J. Johnston, J. H. P. Eloff and L. Labuschagne. “Security and human computer interfaces”. *Computers & Security*, vol. 22, no. 8, pp. 675-684, 2003.

[2] Microsoft. “Windows User Experience Interaction Guidelines”. Available online at: http://msdn.microsoft.com/en-us/library/aa511440.aspx (Accessed: 18/02/2013)

[3] Z. F. Zaaba. "Enhancing Usability using Automated Security Interface Adaption (ASIA)". PhD Thesis, University of Plymouth, 2014.

[4] M. S. Wogalter. “Purposes and Scope of Warnings”. In Wogalter*, M.S. (ed.) Handbook of Warnings*. USA: Lawrence Erlbaum Associate, 2006, pp. 3-9. ISBN 0805847243.

[5] R. Dhamija, J. D. Tygar and M. Hearst. "Why phishing works", *Proceedings of the SIGCHI conference on Human Factors in computing systems*. Montreal, Quebec, Canada, pp. 581-590, 2006.

[6] S. Egelman, L. F. Cranor, and J. Hong. "You've been warned: an empirical study of the effectiveness of web browser phishing warnings", *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*. Florence, Italy, ACM, pp. 1065-1074, 2008.

[7] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri and L. F. Cranor. "Crying wolf: An empirical study of ssl warning effectiveness", *Proceedings of the 18th Usenir Security Symposium*. Montreal, Canada, pp. 399-410, 2009.

[8] M. Mannan and P. C. Van Oorschot. "Security and usability: the gap in real-world online banking". *Proceedings of the 2007 Workshop on New Security Paradigms*. New Hampshire, ACM, pp. 1-14, 2008.

[9] C. S. Weir, G. Douglas, M. Carruthers and M. Jack. "User perceptions of security, convenience and usability for ebanking authentication tokens", *Computers & Security*, vol.28, 1-2, pp. 47-62, 2009.

[10] R. Reeder, C. M. Karat, J. Karat, C. Brodie, C. Baranauskas, P. Palanque, J. Abascal, and S. Barbosa. "Usability Challenges in Security and Privacy Policy-Authoring Interfaces Human-Computer Interaction – INTERACT 2007". Springer Berlin / Heidelberg, pp. 141-155, 2007.

[11] B. Lampson. "Privacy and security: Usable security: how to get it", *Communication of ACM*, vol. 52, no. 11, pp. 25-27, 2009.

[12] D. Sharek, C. Swofford, and M. Wogalter. "Failure to Recognize Fake Internet Popup Warning Messages". *Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting*, pp. 557-580, 2008.

[13] B. Stone-Gross, R. Abman, R. Kemmerer, C. Kruegel, D. Steigerwald and G. Vigna. The Underground Economy of Fake Antivirus Software. In Schneier, B. (ed.) Economics of Information Security and Privacy III. Springer New York, pp. 55-78. ISBN 1461419808, 2013.

[14] T. Whalen and K. M. Inkpen, K. M. "Gathering evidence: use of visual security cues in web browsers". *Proceedings of Graphics Interface 2005. Victoria, British Columbia Canadian Human-Computer Communications Society*, ACM, pp. 137-144, 2005.

[15] M. Wu, R. C. Miller and S. L. Garfinkel. "Do security toolbars actually prevent phishing attacks?" *Proceedings of the SIGCHI conference on Human Factors in computing systems*. Montreal, Quebec, Canada ACM, pp. 601-610, 2006.

[16] C. Seifert, I. Welch and P. Komisarczuk. "Effectiveness of security by admonition: a case study security warnings in a web browser setting", *secure Magazine*, pp. 1-9, 2006.

[17] Z. F. Zaaba, S. M. Furnell, P. S. Dowland and I. Stengel. "Assessing the usability of application-level security warnings", *Proceedings of the 11th Security Conference (Security Assurance & Privacy)*, Las Vegas, USA, 2012.

[18] C. Bravo-Lillo, L. F. Cranor, J. S. Downs and S. Komanduri. "Bridging the Gap in Computer Security Warnings: A Mental Model Approach". *Security & Privacy,* IEEE, vol. 9, no. 2, pp. 18-26, 2011.

[19] S. M. Furnell, A. Jusoh, D. Katsabas, and P. S. Dowland. "Considering the Usability of End-User Security Software", *Proceedings of 21st IFIP International Information Security Conference (IFIP SEC 2006)*. Karlstad, Sweden. Springer Boston, pp. 307-316, 2006.

[20] Z. F. Zaaba, S. M. Furnell, and P. S. Dowland. "End-User Perception and Usability of Information Security", *Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA)*. London, pp. 97-107, 2011.

[21] C. Herley. “So long, and no thanks for the externalities: the rational rejection of security advice by users”. *Proceedings of the 2009 workshop on New security paradigms workshop*. Oxford, United Kingdom, ACM, pp. 133-144, 2009.

[22] J. M. Stanton, K. R. Stam, K. R., Mastrangelo and J. Jolton. “Analysis of end user security behaviors”. *Computers & Security*, vol. 24, no. 2,pp. 124-133, 2005.

[23] L. A. Jones, A. I. Anton and J. B. Earp. "Towards understanding user perceptions of authentication technologies". *Proceedings of the 2007*

ACM workshop on Privacy in electronic society. Alexandria, Virginia, USA, ACM, pp. 91-98, 2007.

[24] S. Leonard, H. Otani and M. Wogalter. "Comprehension and memory". *Warnings and risk communication*, pp. 149-187, 1999.

[25] J. S. Wolff and M. S. Wogalter. “Comprehension of pictorial symbols: Effects of context and test method”. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 40:173{186(14), 1998.

[26] C. Bravo-Lillo, L. F. Cranor, J. S. Downs, and S. Komanduri. "POSTER: What is still wrong with security warnings: a mental models approach". *SOUPS'10: Proceedings of the 6th Symposium on Usable Privacy and Security*, 2010.

[27] F. Raja, K. Hawkey, S. Hsu, K. L. C. Wang, and K. Beznosov. "A brick Wall, a Locked Door, and a Bandit: A physical Security Metaphor For Firewall Warnings", *Proceedings of the Seventh Symposium on Usable Privacy and Security*. Pittsburgh, USA, 2011, pp. 1-20.

[28] W3Schools "Browser Statistics". Available at: http://www.w3schools.com/browsers/browsers_stats.asp (Accessed: 27/02/2015).