End-User Perception and Usability of Information Security

Z.F. Zaaba[1,2], S.M. Furnell[1,3] and P.S. Dowland[1]

[1]Centre for Security, Communications and Network Research,
University of Plymouth, Plymouth, United Kingdom
[2]School of Computer Sciences, University Sains Malaysia, Penang, Malaysia
[3]School of Computer and Security Science, Edith Cowan University
Perth, Western Australia
e-mail: info@cscan.org

Abstract

This paper investigates users' understanding of security features and application and examines perceptions relating to usability. The study made use of an online survey consisting of five sections and recruited a total of 564 participants. Respondents were presented with a range of questions designed to measure their experience and knowledge of security. In addition, 2 scenarios were presented to respondents which examined their understanding of security warnings and potential threats, including email phishing and a potentially fraudulent attack through downloading an application. The survey results revealed that end-users are still experiencing significant difficulties with understanding and reacting to current state-of-the-art security applications, messages and potential threats. Furthermore, evidence suggests there is a corresponding need for a novel approach to improve perception and usability of information security.

Keywords

Usability, Security, Interface, Perceptions, Warning, Messages, Human Computer Interaction

1. Introduction

Security features enable users to mitigate security risks by providing protection from potential threats. However, the complex and sophisticated user interfaces hinder an end users' operation of such applications, which can potentially increase the likeliness of incorrect configuration and consequential exploitation. Whitten and Tygar's (1999) assessment of Pretty Good Privacy (PGP) 5.0 was one of the earliest studies on usability issues in the context of security. Proctor et al., (2000) found usability problems existed in third party authentication methods and Wool (2004), determined usability problems in configuring firewalls to selectively filter traffic. These usability problems indicated an essential link between usability and human factors. A lack of usability can cause users to inadvertently change a secure system into an insecure system. Users should be aware of the functionality and be provided with enough information to make informed decisions. In order to investigate the problem in practice, this paper presents findings from a survey assessing users'

understanding of security dialogues within web browsers (i.e. a common end-user application in which security risks can often be found). The discussion begins with an overview of perception and usability issues, before proceeding to outline the research methodology and the associated findings. The study focused upon users' responses to two common security scenarios that can occur during web browsing (namely attempting to visit a potentially fraudulent website and an attempt to download a potentially harmful file). The discussion examines the extent to which the users were supported in understanding and responding to these warnings, and highlights some resulting recommendations for future systems.

2. Overview of perception and usability

According to Nielsen (2003), usability can be referred to as a quality attribute which evaluates how a user interface is being used. It was stated that usability needs to be defined by five quality components, namely: learnability, efficiency, memorability, errors and satisfaction. Usability was also defined by the ISO (1998):

> *"…the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use".*

The interaction between usability and security is essential. The concept of using *design principles* was introduced to improve the security of computer system (Saltzer & Schroeder, 1975). This introduced eight examples of design principles that applied to protection mechanisms. One essential finding was the term *psychological acceptability* which stated that a human interface was designed for ease of use and users should be able to apply the protection mechanism correctly. Consideration of usability can help developers make better decisions and potentially help them to work more effectively (Radle & Young, 2001). Nielsen (2003) identified that usability became a requirement for websites, e-commerce transactions and even the Internet. Schultz (2007) demonstrated that there were significant problems in relation to usability in information security by examining research papers presenting results on the relationship between security and usability. He summarised that there were usability problems in security-related tasks with some rated "severe". Mannan & Van Oorschot (2008) analysed the gap between usability and security in online banking and found that many security requirements were too difficult for general users to follow and were often misled by the marketing related messages on safety and security. Venter et al., (2007) evaluated the usability and security of personal firewalls and concluded that current personal firewalls were generally weak at informing the users and creating security awareness. It was also suggested that the software obstructed the creation of fine-grained rules which is a notable obstacle to usability and security of personal firewalls. Furnell et al., (2007) assessed security perceptions of personal Internet users and found that users' knowledge and understanding are still lacking. Although the problems mostly refer to novice users, they were also applicable to those considering themselves as advanced users. Albrechtsen (2007) conducted a qualitative study on users' view on information security. His findings showed that there is a gap between users' intention and the

actual users' behavior as users did not perform many individual security actions. Having said that, there is clearly a need to pay much more attention to human factors in information security tasks, this paper presents an initial study which was aimed to get a better understanding of user's perception and usability of security features and applications.It is clearly futile to build an effective user interface if the user still ignores warnings or does not understand how to use the system correctly (in a secure manner). User feedback can help developers to create better, more understandable and more usable systems. However, according to Coffee (2006), many software developers lack the interest or technical skill to develop secure systems. They consider security as part of the non-functional requirements – i.e. security is not fully integrated into the development lifecycle process (Mouratidis et al., 2005). Security should be considered during the whole development process, if it is ignored or only emphasised after the implementation stage, conflicts will rise and it could lead to future problems. It is essential that developers are now slowly beginning to realise that information security is essential even if their primary function is not related to security (Tondel *et al.*, 2008).

3. Methodology

In order to determine users' perception and usability issues in information security, an online survey was conducted to investigate preliminary insights from users regarding their level of understanding of particular issues in relation to the security of their computer system. The survey was conducted online between February-March 2010, and promoted to the end user community via e-mail, snowball sampling and news entry information on the university's internal staff/student websites. This survey consisted of 41 questions offering both open and closed responses. Respondents were not obliged to answer all questions as some of the questions were conditional. Overall, 784 responses were submitted to the website however, only 564 responses were fully completed which represented a 72% completion rate. All of the figures and percentages reported were based upon the results of a simple statistical analysis on the proportions of completed responses in this study.

4. Results and discussion

From the 564 responses, there was an almost equal gender balance with 49% male responses and 51% female. Most of the respondents were aged between 17-30 years, with at least degree level education and been using computers for more than 5 years. This showed that the vast majority of respondents had considerable familiarity with computing technology. Respondents were primarily staff/students from the authors' university together with individuals from the public/private sector. Most respondents rated themselves as intermediate/advanced users and indicated that they were concerned with regards to issues relating to computer security. In terms of security software usage, 86% were using some form of protection at home or work leaving 14% who did not use it (or were unsure). Before proceeding with further investigation, the survey asked respondents to describe the types of problem that they regularly encounter whilst using their computer. Incidents of malware, problems with Internet connection, problems in understanding help functions, complex

security features and user interface difficulties were the main concerns. 70% of respondents indicated that they were at concerned regarding issues of security in their computer with only 5% indicating they were not concerned at all. This finding provided an interesting baseline to assess the real situation of how end users' perceived the security features of information system. Indeed, the following responses from surveyed respondents highlight the issues:

> *"I do not have to use any security software because I am using Mac. I believe there is no virus at all so I don't have to use any of those"*
>
> *"I am using Linux. It is free from any malware attack. I don't have to spend money to get antivirus software"*
>
> *"I do not care whether I have the antivirus or not as I believe it's not my responsibility. It's my company's asset anyway"*

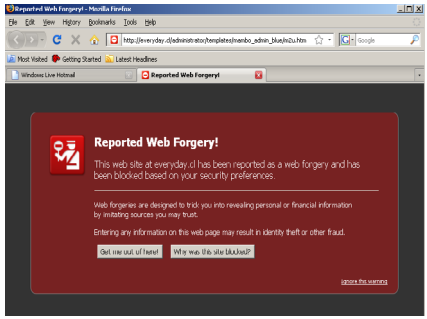
End users' behaviour might lead them to a significant problem if they become a victim of a malware attack. In the next sub-sections two scenarios are presented considering how users understand the usability of security features and how this can lead them to make a security-relevant decision. Scenario 1 focuses on security warnings relating to possible phishing sites, while Scenario 2 looks at warnings that are issued when downloading executable files. These scenarios are used to assess a user's ability to understand security features, usability and issues of security in their daily routine whilst using computer.

4.1. Scenario 1

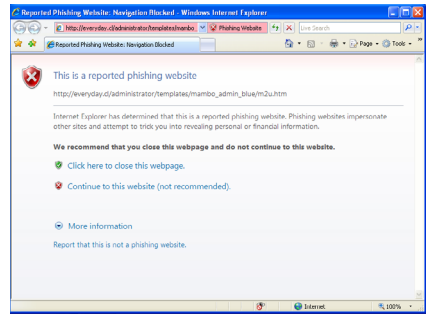
In order to gauge the level of understanding of the usability of security features in a web browsing context, respondents were asked to indicate their preferred web browser. As each browser has different methods of presenting security warnings, respondents were then shown a screenshot based on their chosen browser. In this scenario, respondents were asked to imagine they had received an email from their bank and were asked to re-activate their online banking account by clicking the hyperlink within the email. Respondents were then asked what they would do next. The six images are depicted in Figure 1.

The *best practice* actions were chosen by the majority of users as depicted in Figure 2, although a small proportion of respondents indicated that they would have ignored the warning and proceeded with the transaction. Had this been a genuine email/website, it is likely that they would have become a victim of a phishing site that could result in their personal or financial information being passed to an unknown party. Although 13.3% indicated they would attempt to get more information about the meaning of the message, if they did not understand the information needed, it would also be possible for them to become victims. This survey revealed that there were clear distinctions in the way that security warnings were presented by each browser (see Table 1). This study focussed on 5 elements, namely: usage of help function, colours, icons, choices and terminology. Based on

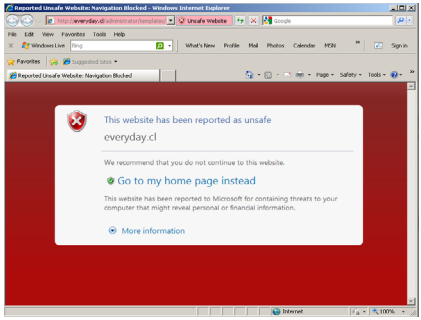
these features, this study revealed that there were no specific standards to present security warnings, messages or notifications. Each vendor had their own style or preference to present such warnings. Currently, Microsoft (2011), had more specific guidelines for users that covered issues on controls, command, text, messages, interaction, windows and visual. This documentation will guide them to create a standard and more meaningful outcome in relation of usability.



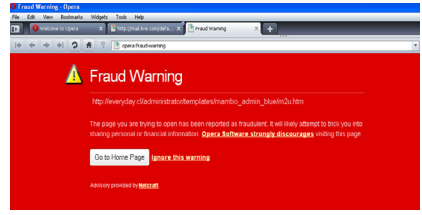
Mozilla Firefox



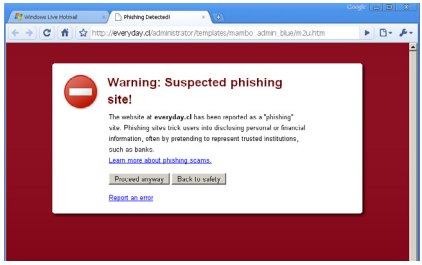
Internet Explorer 7



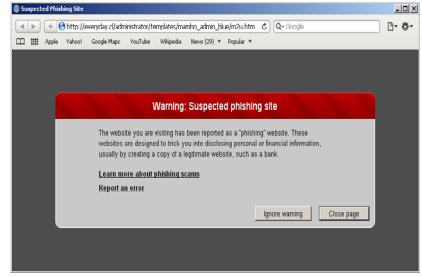
Internet Explorer 8



Opera



Google Chrome



Safari

Figure 1: Screenshots from various web browsers showing a security warning having detected a possible phishing website

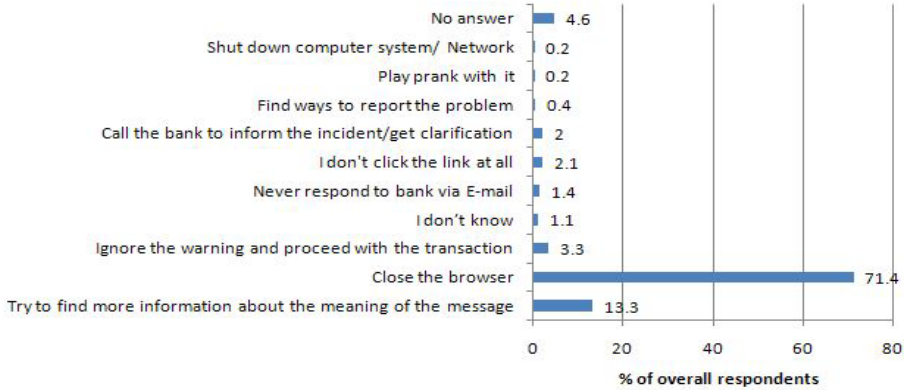


Figure 2: Users' preferred action when presented with the phishing security warning (Scenario 1)

After assessing the users' response towards the phishing warning, the next question attempted to assess users' general understanding of the security warning presented. 75% responses understood the warning with the remainder unsure how to interpret the information presented. From this group, 13% chose try to find more information about the meaning of the message. Of most concern were a small percentage of respondents with 1% claiming to understand the depicted screenshot but still ignored the warning and proceeded with the transaction. From the respondents who did not understand the phishing warnings, there were 3 main issues identified; technical terminology (62%), nature of the event being described (55%) and choices available (25%). No attempt was made to further question the elements that they did not understand as the question was only presented in a general context.

Browsers	Usage of Help Function	Usage of Colours	Usage of Icon	Available choices	Terminology used
Mozilla Firefox	• Providing information on why the website is blocked	• Using a red background colour scheme to get attention	• Using 2 types of warning icon	• Ignore this warning • Get me out of here • Why was this site blocked	• Reported as web forgery
Internet Explorer 7	• Providing more information about the incident	• Address bar changing to red colour with Phishing website connotation	• Error warning icon	• Continue to website(not recommended) • Close the webpage • More information about phishing • Report that it is not phishing website	• Reported as phishing website
Internet Explorer 8	• Providing more information about the incident	• Address bar changing to red colour with Unsafe website connotation	• Error warning icon	• Go to my homepage instead • More information about phishing • Report this site does not contains threats • Disregard and continue (not recommended)	• Reported as unsafe website
Google Chrome	• Providing more information about phishing scams	• Using a red background colour scheme to get attention	• No entry warning icon	• Proceed anyway • Back to safety • Report an error • Learn more about phishing scams	• Suspected as phishing site
Safari	• Providing more information about phishing scams	• Using a red highlighted header colour	• No icon	• Learn more about phishing scams • Report an error • Ignore warning • Close page	• Suspected as phishing site
Opera	• No details	• Using a fully red background colour scheme	• Warning icon	• Go to homepage • Ignore this warning	• Fraud warning

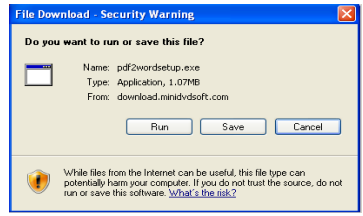
Table 1: Comparison of the security warnings from various web browsers

4.2. Scenario 2

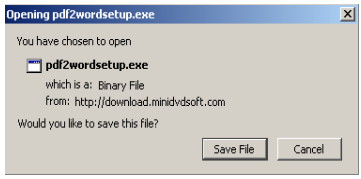
Using the respondent's preferred browser, a second scenario was presented in which the user was presented with a security warning following a click on a link to install software (Figure 3). Most respondents indicated they would save the file and then scan for viruses (35%). Surprisingly, 29% of respondents who used Internet Explorer 7 decided to cancel or quit from the process. This could be caused by the rather specific warning within the dialogue (indicating that the files could possibly contain malware), although Internet Explorer 8 used an identical prompt. It is also notable that almost 10% of respondents would run the application straightaway without virus scanning it first (although it is possible that these users were under the impression that their anti-virus product would automatically scan the file before execution). It has to be remembered that this may not accurately represent users' real intentions as this scenario was effectively simulated. However, this demonstrated that users may be at risk by running applications directly from the source without scanning it. One interesting finding from this survey was that a small

percentage of users would not download the software if they used their own laptop or computer.

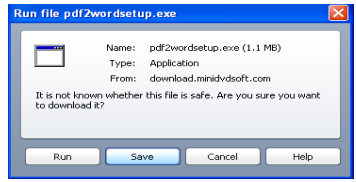
Internet Explorer 8



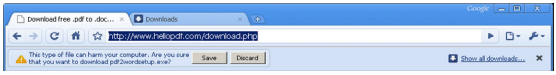
Internet Explorer 7



Mozilla Firefox



Opera



Google Chrome

Safari

Figure 3: Security warning in various web browsers

By showing the six security warning messages in Figure 3, it can be noted that there was a clear method on how each security warning was presented except from the two versions of Internet Explorer. Internet Explorer used the footnote area to provide additional explanation and access to the help function whist others did not use it at all. The usage of security icons was partially consistent except for Safari and Google Chrome. There were no warning icons used at all in Mozilla Firefox and Opera. When displaying the list of available choices (options) for users, each browser had a similar method. Opera represented the help function via a button whilst Internet Explorer 7 and 8 used a link to provide help. Surprisingly, Mozilla Firefox, Google Chrome and Safari did not provide a help function for the security warning. In terms of the title or header of the message, Internet Explorer and Safari used the same message, indicating "File Download-Security Warning" whilst the others presented the downloaded file name instead. When asked if they were satisfied with the level of information provided for the warning messages 43% were satisfied whilst 54% agreed that the information given was not enough. A somewhat interesting finding related to respondents who felt they had enough information based on the depicted warning, 17% decided to cancel or quit from the process whilst 9% decided to run the application straightaway. These users claimed that the information was enough

for them to make a decision however they were still unable to demonstrate secure behaviour

When asked for additional content that would be useful when making such decisions, 38% would like to have details of the consequences if they were to proceed to run the application, 33% wanted to have confirmation of the legitimacy of the download, 27% wanted confirmation that their action was free from any kind of malware attack and 17% wanted to have provision of a proper help function. Some of the responses suggested that the computer should have a strict defence process, more understandable features and automatic virus scanning. Some of the respondents indicated they would like to see information of the provider of the application in order to gauge their trust level. They wanted to download only if it were from the provider that was well known and secured for them. A further option considered by some users was to present historical information, indicating the choices made by previous visitors to the site (when presented with the same warning).

5. Conclusions and future work

Respondents were clearly concerned and aware of the security issues however, they were still unsure of the appropriate action to take when presented with certain security events. Respondents had demonstrated that they had used security technologies to help them to mitigate the risk of attacks (e.g. Antivirus, Internet Security etc). Usage of security technologies is fundamental but understanding how to use it and the risks or the threats they are facing is far more essential.

The results from the survey also revealed that users agreed that more appropriate information should be provided in security messages. Although such information will not directly solve the problem, it will give more meaningful support to help users' to make secure decisions and mitigate the risk of becoming a victim. Security features are expected to help users in making a decision but are still beyond the comprehension of users with a basic level of understanding. Users interact with computer with some purpose, when they have to cope with security features this can distract them from what they intend to do. The less security related activities interfere with their actions, the more likely they are to use the system. Yet, it is still not a guarantee for the users to use it correctly. Simply putting such functionality in software/systems without proper guidelines and user friendly features will lead to end user misunderstanding.

Current findings suggest that information provided in messages or warnings should use less technical terminology, offer sufficient provisional help to explain the circumstances and any further actions to be taken, and enough appropriate choices for the user. These results show the importance of usability as part of the design challenge. This study utilised scenarios to simulate computer security events, created based on the experience of dealing with computers as part of a daily routine and it was expected that most end-users dealt with similar issues. The current study was unable to determine the importance of the features as depicted in Table 1 (with the aim of developing a meaningful feature to help end-users). It is expected that

practical experiment study will be conducted so that the end-user can face the real situation and be able to express what they really understand and need in relation to usability issues and their perception towards it. The results will be able to clarify the effectiveness of current security implementations and enhancement can be done to suit users' needs.

6. References

Albrechtsen, E. (2007), 'A qualitative study of users' view on information security', *Computers & Security*, vol.26, 4, pp.276-289.

Coffee, P. (2006) 'Security Onus Is on Developers'. (Online). Available at: http://www.eweek.com/c/a/Application-Development/Security-Onus-Is-on-Developers/ (Accessed: 03/03/11).

Furnell, S. M.,Bryant, P. & Phippen, A. D. (2007), 'Assessing the security perceptions of personal Internet users', *Computers & Security*, vol.26, 5, pp.410-417.

ISO (1998) 'ISO 9241 Part 11: Guidance on usability'. (Online). Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=16883 (Accessed: 04/03/11).

Mannan, M. & Van Oorschot, P. C. (2008) '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.

Microsoft (2011) 'Windows User Experience Interaction Guidelines'. (Online). Available at: http://msdn.microsoft.com/en-us/library/aa511440.aspx (Accessed: 03/04/2011).

Mouratidis, H., Giorgini, P. & Manson, G. (2005), 'When security meets software engineering: a case of modelling secure information systems', *Information Systems*, vol.30, 8, pp.609-629.

Nielsen, J. (2003) 'Usability 101: Introduction to Usability'. (Online). Available at: http://www.useit.com/alertbox/20030825.html (Accessed: 01/03/11).

Proctor, R. W., Lien, M.-C., Salvendy, G. & Schultz, E. E. (2000) A Task Analysis of Usability in Third-Party Authentication. *Information Security Bulletin*, 5, (W3schools), pp. 49-56.

Radle, K. & Young, S. (2001), 'Partnering usability with development: how three organizations succeeded', *Software, IEEE*, vol.18, 1, pp.38-45.

Saltzer, J. H. & Schroeder, M. D. (1975), 'The protection of information in computer systems', *Proceedings of the IEEE*, vol.63, 9, pp.1278-1308.

Schultz, E. E. (2007), 'Research on usability in information security', *Computer Fraud & Security*, vol.2007, 6, pp.8-10.

Tondel, I. A., Jaatun, M. G. & Meland, P. H. (2008), 'Security Requirements for the Rest of Us: A Survey', *Software, IEEE*, vol.25, 1, pp.20-27.

Venter, H.,Eloff, M.,Labuschagne, L.,Eloff, J.,von Solms, R.,Herzog, A. & Shahmehri, N. (2007) 'Usability and Security of Personal Firewalls'. *New Approaches for Security, Privacy and Trust in Complex Environments*. Springer Boston, pp 37-48.

Whitten, A. & Tygar, J. D. (1999) 'Why Johny can't encrypt: a usability evaluation of PGP 5.0', *Proceedings of the 8th USENIX Security Symposium*. Washington D.C, pp. 169-184.

Wool, A. (2004), 'The use and usability of direction-based filtering in firewalls', *Computers & Security*, vol.23, 6, pp. 459-468.