

Security Usability: A Survey of End-Users

A.Jusoh, S.M.Furnell and D.Katsabas

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

This paper examines the reasons why security technologies are not used correctly by users. It is a major concern in a computer security world if users fail to use tools available to protect their own system and data. To investigate this issue, a survey was conducted to assess the extent to which security features in popular applications are understood by users. A total of 313 respondents were successfully gathered, and it was discovered that users may be simply ignorant of security, or they may not be getting enough information on using the related technologies. The main contributing factors have been discovered which includes users, interface and computer application itself.

Keywords

Usability, Security, Users, Interface, Human Computer Interaction

1. Introduction

Security is an important factor that should be considered when connected to the Internet. Even if users have nothing stored in the system that they consider important, their computer can be a weak link, allowing unauthorised access to the organisation's network and information. The design of interface plays a big role to connect users and the usable functions within the system. In a usability study of PGP 5.0, Whitten and Tygar (1999) stated that security software will not be satisfactory if users do not know how to use it. They had worked on a good user interface but it was still insufficient to give information in an effective manner to non-technical users. The security on wireless network attracted Balfanz et al. (2004) to look at different versions of Public Key Infrastructure (PKI) in terms of providing usable security for users. The traditional PKI deployment was complex, with installation requiring a total of 38 steps within 140 minutes. This was in complete contrast to a user-friendly version, which required just four steps and an average of 1 minute and 39 seconds. It is not surprising if users give up using technologies that require a lot of time and effort to make them functional.

The usability of the systems becomes an issue because many users find it difficult to follow the steps to enable security features in their system. Users should know what type of security features they want to apply and they must be able to find the desired functionality. They also have to be provided with maximum information on how to determine the level of protection and when they should apply the features. A survey has been conducted to gather information about the usability of security. The

purpose of the survey is to focus on users' understanding of the security features available in a range of popular applications: Internet Explorer (IE), Word and Outlook Express. This paper investigates and analyses the factors contributing to why security technologies are not used correctly.

2. Determination of Security Technologies Usability

The survey (entitled *Assessing the Usability of Computer Security Features*) was distributed in paper and web format. Total of 313 responses were gathered, with an almost equal split between male and female. Most of the respondents were aged between 17-29 years, with degree or post graduate education. Thus the majority of respondents were educated persons within an age group that grew up with information technology. From the total responses, it shows nearly all respondents were frequently using a computer either in office or home. Furthermore, most of the respondents classed themselves as either intermediate or advanced users, and generally had a good knowledge of threats and security technologies. In terms of the named threats, 302 respondents were aware of *Viruses*, *Spam* (288), *Spyware* (282), *Hacking* (280), *Worms* (275) and *Phishing* (69). With the percentages of more than 80%, most respondents claimed to know the role of Firewalls, Auto-Updates and Virus Protection. More than 70% of respondents are aware of the security features available in Internet Explorer, but the pattern changes for the other applications, with only 58% of respondents aware of security in Word, and less than 40% awareness for Outlook Express.

The sub-sections that follow examine the responses observed in relation to each of the applications under consideration.

2.1 Internet Explorer

Although users claim they are aware of security features in IE, many of them still do not understand the description of the default security level setting (see Figure 1). They are aware about it but did not spend their time to explore further and get to know the features available.



Figure 1: Security Level setting in Internet Explorer

Option	Respondents	
	Number	Percentage
Yes	197	63 %
No	105	34%
Nil	11	3%
Total	313	100%

Table 1: Understanding the Security Level setting

Furthermore, only 59% of respondents understand the difference between trusted and restricted sites. It is a quite large percentage of respondents who do not know or are not sure about the difference. Tyler (2001) explains the meaning of the both sites:

- Trusted Sites: Users should only use this Web sites pages if they believe it is safe and it will not upload harmful content to the computer. The default security level for this site is Low.
- Restricted Sites: Use this zone for Web sites and pages that users access but do not completely trust because it suspected the sites may send potential harmful content to computer. The default security level is High.

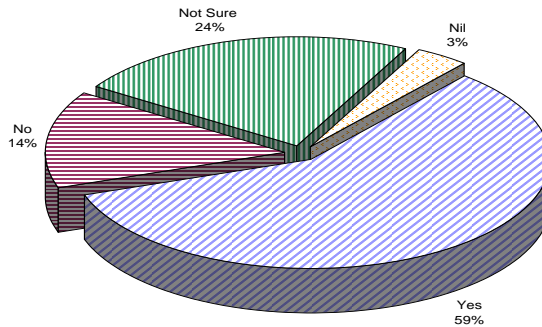


Figure 2: Respondents' understanding of the 'Content Zone'

The same scenario happened when they were asked about ActiveX (see Table 2). Although many of them have heard of it, almost half of these (47%) do not actually know what it means. More than 50% of the respondents said they do not know how to decide if they presented with the option of running active content. It shows that they are exposing themselves to a risk, as their decision could harm the computer.

Option	Respondents	
	Number	Percentage
Yes	128	41 %
No	179	57%
Nil	6	2%
Total	313	100%

Table 2: Knowing how to make decisions with ActiveX content

2.2 Microsoft Word

Word is a popular Microsoft application used by many of the respondents on a daily basis. However, from the result of the survey, it is quite surprising that many do not know about the security features available within the application (see Table 3). As they are not aware, it is reasonable that not many of the respondents use the security features available for their documents.

Security Features	No. of aware respondents
Password	194
Encryption	52
Digital Signature	29
Other	37

Table 3: Awareness of security features used in Word documents

An interesting finding in relation to Word security features is how users interpret the password functionality. Figure 3 shows the dialog box that is presented when a document is password protected to prevent unauthorised modification. Respondents were asked to indicate what they believed this dialog to mean, with the options and their responses listed in Table 4 (the correct answer is that ‘*The document cannot be changed without password*’). 61% answered correctly, 24% of respondents misunderstood the dialog, and another 13% were not sure. 37% of respondents cannot answer correctly although most of them claimed they were using password as the main protection.



Figure 3: A Password dialog in Microsoft Word

Option	Respondents	
	Number	Percentage
The document cannot be opened without a password	75	24 %
The document cannot be changed without a password	191	61%
Not Sure	41	13%
Nil	10	2%
Total	313	100%

Table 4: Understanding of the Password dialog from Figure 3

Apparently respondents might use the security technologies inappropriately since they could not understand them properly. Because the ‘open read only’ sentence is at the same line as ‘Enter password to modify’, users thought they also need password to enable them to open and read the document.

As Sutcliffe (1995) has indicated, the issue of HCI design analyses what people do with the computer systems and their interfaces to understand the user’s task and the requirements. Designing of application should help user to fulfil and match the system characteristics. Sutcliffe identifies seven of basic principles of HCI which are consistency, compatibility, predictability, adaptability, economy and error prevention, user control and structure interface.

2.3 Microsoft Outlook Express

The worst results were in relation to Outlook Express, where most of the answers show respondents know nothing about security features available in it. More than 60% of them do not understand the Digital ID, Encryption, the Advanced Security setting and also they are not using the Sign and Encrypt option when sending messages. From the comments added by some of the respondents, they said they rarely use the application and some did not use it at all. Since they do not use the application, they do not notice the use of security features available to protect them. However, they should also acknowledge the use and function of each security features available in case they need to use them in the future.

Option	Digital ID	Encrypt	Advanced Security
Yes	82 (26%)	87 (28%)	85 (27%)
No	209 (67%)	196 (63%)	211 (68%)
Nil	22 (7%)	30 (9%)	17 (5%)
Total	313 (100%)	313 (100%)	313 (100%)

Table 5: Understanding the options available for Digital ID, Encrypt and Advanced Security settings



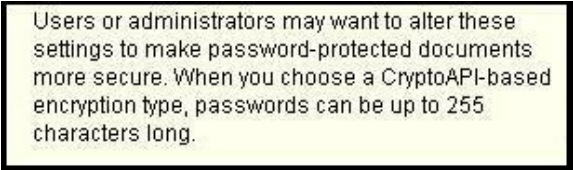
Figure 4: Sign and Encrypt options while Sending Message

3. Contributing Factors

Factors of users, interface and the application itself all play a part in determining the usability of security technologies. The tendency of users to ignore, neglect and take things for granted will lead to a very bad situation for the future of security technologies. Users with a bad behaviour will contribute nothing to the usability of security technology when they could not use the tools correctly. They were aware of the security features available in each of the applications, but awareness is just not enough to make computer safe without taking any further action. Those who have an IT department in their company may normally leave all of the computer responsibilities to the IT personnel. However, they should not forget the fact that all the basic settings and security features are often the user's own responsibility. Users should learn how to protect their own computers so that they are safe from any threats. They should realise they are the main contributing factors that could harm the computer and probably affect the system of an organisation.

An unfriendly interface presents a big problem to the usability of security technologies. If users interpret the interface wrongly, they will get a wrong idea about the security features as well. As a result, they may use the security technologies inappropriate way. Wording used in any application must be as simple as possible and easily to understand by users. Furthermore, the layout of the application must also be designed in such a way that it will not be so complicated to be understood.

The application itself should give more help functions to users to make it easy to understand how to use the security features. Many of the current help functions are not helping users to understand certain features much better. If users utilise the 'help' system in the hope that it will explain what something means, they will often be very disappointed as the help function will give only a very brief description. An example is the context-sensitive help in Microsoft Word when choosing the encryption type. It is not helping much in giving clues to users on how to determine the type of encryption. It explains only basic information on what the page is all about. The '?' function should play an important role in helping users understand the features available more detail and precise. If the information could be delivered in a very short, compress and efficient, it will help users a lot in understand the security technologies in a correct way.



Users or administrators may want to alter these settings to make password-protected documents more secure. When you choose a CryptoAPI-based encryption type, passwords can be up to 255 characters long.

Figure 5: Context-sensitive help for the Encryption Type in Microsoft Word

4. Conclusion

This paper has discussed the usability of security technologies based on a survey distributed to 313 respondents. The features in Internet Explorer, Word and Outlook Express have been analysed to obtain assessments for each application. The results give insights into how users perceive the security technologies based on their awareness. It seems that some of the applications are consequently lacking in terms of usability since users do not understand them.

The contributing factors have been recognised in an attempt to understand and clarify why the security technologies are not used correctly, and consist of users, interface and the application. If users could use the security technologies in appropriate and right manner, the usability of security will not be an issue anymore in any computer application.

5. References

- Balfanz, D., Durfee, G., Smetters, D.K. and Grinter, R.E. (2004), “In Search of Usable Security: Five Lessons from the Field”, *Security and Privacy*, Vol. 2, No. 5, pp. 19-24.
- Faulkner, C. (1998), *The Essence of Human – Computer Interaction*. Prentice Hall, Cornwall, UK.
- Sutcliffe, A. G (1995), *Human – Computer Interface Design* (2nd Ed.) Macmillan Press Ltd. London, England.
- Tyler, D. (2001), *Windows XP – Home and Professional Editions*. SYBEX Inc. USA.
- Whitten, A and Tygar, J.D. (1999), “Why Johnny can not encrypt: A usability evaluation of PGP 5.0”, in *Proceedings of the 8th USENIX Security Symposium*, Washington, D.C., USA, August 23–26, 1999.