Online Security: Strategies for Promoting User Awareness

M.Vikharuddin and S.M.Furnell

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

Abstract

This Research paper describes various threats and vulnerabilities the home users face whilst using the services offered by the World Wide Web. It describes the common threats and the way the home users perceive them. Several aspects on online security are discussed that helps home users learn and understand the threats they are posed to. Reports from previous surveys are presented that gives a clear understanding on how the users perceive online security. More the online security perception, the better is the level of security achieved by the home internet users. The main outcome of this research is that the Security guidelines for home users are vast over the internet. Many websites offer simple and very easy to understand guidelines and yet the users are not able to reach those websites. Publishing security information on certain websites is not going to help users and previous survey results shows that the existing media awareness techniques are not succeeded in promoting awareness among home users so it is very important how the cybercrime and online security is presented to the open world. This paper makes a sincere attempt to recommend some new set of online security techniques that could be used to increase the user perceptions and also a solution to improve the existing media awareness techniques so that the governing bodies and software application vendors could reach more users educating them on online safety aspects.

Keywords

Internet Security, Home Users, Security Perception, Media Awareness

1 Introduction

The Internet has become a part of our daily life offering us online banking, shopping, electronic mail, businesses and education. It is a powerful means to establish connections to other computers and users. With the increased use, the internet is no more a safe playground to be dealt with. Information transferred through the Internet could be compromised by various means. Computer security is a vital issue for both home users and business users. Many software applications are available to protect the computers that are connected to Internet. Antivirus applications and Firewall are commonly used to protect computers from hacking, viruses, malicious codes and information theft. The way the home users perceive and protect against the odds plays an important role. Media presentation on the other hand is equally vital as it makes the users aware of the security updates, virus information and protection against them. The governing bodies, software vendors and banks should often perform awareness programs in such a way that the security information reaches

every user. The need for better understanding of the security aspects from a home user point of view was the main motivation to consider this research. This research paper discusses the existing methods on how the home users reach the security guidelines and about the media presentation methods adapted by various banking organizations and software vendors. The research also suggests possible improvements for both user perceptions and awareness programs.

2 Common threats the home users face

Home users often confront threats over the internet that includes viruses, worms, spam, spyware, phishing and hacking. Any of the mentioned threat will lead to the user information being tampered or misused or even the computer being hijacked/attacked.

The most recent noticeable incident in cybercrime is the Trojan attack on the online recruitment website Monster.com. The Trojan used credentials probably stolen from a number of recruiters. It then logged on to the website, searched for resumes and personal details of applicants such as name, surname, email address, home address and telephone numbers were uploaded to a remote server which was under the control of the attackers. 1.6 million job seeker's personal information was stolen (Symantec Report, 2007). Spam mail are unwanted mail the users get which could possibly leads the users to websites involved in installing malware and spyware applications in to the user's computer. The common type of spam in the online threat was related to 'Health products' and 'Commercial products' totaling to 32 % and 30% respectively (Symantec Corporation, 2007). There are many different kinds of threats such as phishing, viruses /worms and Instant messaging are that seriously posing threats to home users. Security is a major concern for home users when they are using the internet services like electronic mailing system, banking, shopping and instant messaging. Protecting home users from this kind of threats personal and drives to discuss the need for online security

3 The Need for Online Security

A survey conducted by comScore in June 2007 concluded that the United Kingdom has the most active online population. On an average, 21.8 million users access the internet everyday and the highest average time spent is 34.4 hours per user per month (comScore, 2004). With the vast number of users connected to the internet, securing their information and computer from being misused is very important and safety measures must be considered to ensure optimum protection. We shall consider the number home users using insecure computers before we talk about the way the users perceive the concept of online security. NetSafe's Home Computer Security Survey conducted in 2005 reveals that 41% of the respondents have an updated firewall and 59% do not use a firewall for computer security at all. 70% of the respondents do not have updated firewall and anti-virus applications (The Internet Safety Group 2005).

According to a survey report from Message Labs conducted in June 2006, one in 101 emails in June contained malware and one in 531 emails comprised a phishing

attack. The global Spam rate was identified to be 64.8% (Message Labs Intelligence, 2006).

According to a survey conducted by AOL and National Cyber Security Alliance 81% of home computers are lacking important computer security applications like Anti-Virus and Firewall applications out of which 64% users were using broadband Internet connection (American on Line/ National Cyber Security Alliance, 2004).

Home computers lacking core protections (recently-updated anti-virus software, a properly-configured firewall, and/or spyware protection)	81%
Home computer users who have received at least one phishing attempt via e-mail over the prior two weeks	23%
Home computers lacking current virus protection (not installed or not updated in prior week)	56%
Home computers lacking properly-configured firewall	44%
Home computers lacking any spyware protection software	38%

Table 1: Home users lacking security features (AOL/NCSA Survey Report, 2005)

Above shown table is a summary of the AOL/NCSA survey conducted in 2005. The survey included 225 broadband users and 129 dial-up users. It is apparent from the figures that not many users are able to configure the security software applications. Only 17% of the respondents understood the concept of firewall and how they work and 92% were unaware of spyware applications that were installed in their computers. This survey results discussed above shows the importance of security for home users. From the above results it can be analyzed that most of the home users are not completely aware of how to handle their personal computers. To make the home users aware of how to use the internet, some organizations are trying to provide security guidelines.

4 Security Guidelines

Security guidelines are helpful to reduce the risk of protecting home user's computer, personal and confidential information. Security guidelines for online safety can be found of many websites that educate the users to deploy security principles. Governing bodies and legislation should make sure that the security guidelines are effective and are up-to-date to the present level of threats and vulnerabilities that home users are exposed to. Security principles are useless if they do not reach the home users and media presentation and awareness programs should be tactically presented to educate the users. There are plenty of advisory website where users can

find information about online security including banking websites and security software vendors. Few of the well known sources that offer security information are presented below.

4.1 Get Safe Online: 10 Minute Guide for Beginners (Gets Safe Online, 2007)

This website provides information for home users on how to upgrade the Operating System; it provides series of advices on topics such as firewalls, antivirus, spyware, spam, backups and identity theft etc.

4.2 Symantec Best Practices for Consumers (Symantec Corporation, 2007)

Symantec Corporation has designed a set of guidelines for consumers/home users ensure optimum online security. The following are some of the guidelines that are provided by Symantec. Passwords should be made secure by mixing upper and lower case alphabets and numbers and should not be chosen from a dictionary. Vulnerability checks should be regularly done by using Symantec Security Check at www.symantec.com/securitycheck and user can report cybercrime incidents to get themselves involved in fighting crime.

4.3 Microsoft (Microsoft/ NSCA, 2006)

The National Cyber Security Alliance with the support of Microsoft Corporation has come up with Online Security and Safety Tips, they are as follows. Home users should make use of a firewall application if they did not get it along with the operating system they are using. Along with the firewall application, it is recommended to keep a back up of important documents and files for safekeeping. Parental control applications should be considered if kids are able to access the internet. Anti-spyware applications should be installed to prevent/remove spyware applications. These are some of the safety tips mentioned by Microsoft.

4.4 Discussion

The following tables give a clear picture of the level of information that is offered by Getsafe, Symantec and Microsoft. This table explains how far the users can educate themselves using these sources and decide on which source to rely for future security guidelines.

	Anti-virus	Anti-Spyware	Spam Sense	Backups	Wireless Networks	Online Auction	Identity Theft	Linux/ MAC Users
Getsafe	✓	✓	✓	✓	✓	✓	✓	✓
Symantec	✓	✓	X	X	X	X	✓	X
Microsoft	✓	✓	✓	✓	X	X	✓	X

	Passwords	Parental Control	Intrusion Detection	Vulnerability Assessment	Crime Reporting	OS Updates	E-mail Attachments	Firewall
Getsafe	✓	X	X	X	X	✓	✓	✓
Symantec	✓	X	✓	✓	✓	✓	✓	✓
Microsoft	✓	✓	X	X	X	✓	✓	✓

Table 2: Comparison of Security Guidelines

Getsafe perhaps offers a clear and easily understandable set of guidelines for home users and the website cares for Linux and MAC users too which Symantec and Microsoft fail to. Getsafe and Microsoft guidelines do not concentrate on reporting the security incidents and Microsoft amongst the three sources talks about parental control applications. Getsafe offers assistance in protecting wireless networks and tips for users who do online shopping whereas the other two sources does not mention about it. On the bigger picture, all three sources concentrated on the main aspects that include OS Updates/Patches, Firewall, Anti-virus, Anti-Spyware, Identity Theft, Password Management and Email attachments

5 User awareness

Security information is vast and easily available on the internet but how many users are aware of them or at least aware of threats they are posed while connected to the internet? According to the survey by AOL/NCSA in the year 2005 (225 broadband users and 129 dial-up users), only 22% of the respondents felt safe from online threats and 61% were somewhat safe. Some of the other key results of the survey are as follows they are 56% of the respondent had never heard of the word “Phishing”,

61% of them received phishing attempt, 70% felt the phishing mail as legitimate, only 23% knew the difference between a firewall and anti-virus application and only 56% had anti-virus application and 44% had updated within past one week (American on Line/ National Cyber Security Alliance, 2004). The main reason behind this lack of awareness among home users is because of media awareness programs. The organizations are mainly focusing upon the websites to promote awareness, there are no proper TV programs and the security awareness issues are not published in news papers normally, unless or until any attacks on identity thefts has occurred. The only way to learn user about internet security is internet itself, there should be more than one way to know about internet security this should be either mass awareness media such as news papers, posters, which should be displayed in public places. The results shown clearly indicate the need to improve security awareness techniques.

6 Security improvements

Effective ways of making users aware of the internet threats is perhaps the only way to fight the battle against cybercrime. Unfortunately, users are failing to reach the online resources that are meant to help them protect their own information/computer. Unaware of the threats, users are easily being trapped with which cybercrime is rapidly increasing. The role of governing authorities should be more than just making websites to promote awareness amongst the users and create security posters/leaflets. The Information security awareness program should be such a way that it should reach all sorts of home users including the ones who use the internet only to send and receive mail.

According to the European Network and Information Security Agency, information security awareness programs will (European Network and Information Security Agency, 2006):

- Communicate and motivate users to deploy security guidelines/ practices.
- Offer general and specific information about information security risks and controls.
- Make users aware of the responsibilities in securing their information.
- Minimize security breaches and create a stronger culture of information security.

Communication techniques should be very effective so that the users are forced to learn the security guidelines and making them aware that there is nothing important more than securing themselves from online threats. Examples of past security breaches/incident should be presented which users often remember easily and it spreads faster with word of mouth. The effective security awareness program should have the following set of qualities (European Network and Information Security Agency, 2006)

- Reach as much as users as possible ranging from novice users to IT professionals.
- Awareness should not be alarming; users should be educated in a simpler manner.
- It should bring users a good level of confidence.

The awareness being delivered, the media used and the person who is promoting the awareness must be influential and credible. If not, the users may not show good interest in listening.

More than one communication media must be used so that the users can reach the awareness easily.

Banks, community centres, computer dealers, educational institutions, libraries and universities can be used to deliver user awareness.

7 Recommendations

Based upon the following set of principles mentioned by European Network and Information Security Agency, this paper recommends new ways to improve home user perception on online security aspects and the ways the media presentation could be improved by the governing bodies and security software application vendors.

7.1 Perception Improvements

There are several ways in which the existing media awareness techniques can be improved thereby educating the users and making them aware of threats and vulnerabilities they are at which in turn changes the way the users perceive the trends of online security. This paper has made an effort to make some more media awareness methods apart from the ones mentioned by European Network and Information Security Agency, some of the guidelines are as follows:

Text Messaging: Mobile phone service providers should offer regular updates about the latest threats through text messages upon agreeing with the users. This could either be offered free of cost or at a nominal price. Text messages should be short, informative and educative and for more information, users must be advised to check advisory websites like Symantec or McAfee. There are 45 million (84% of the population) mobile phone users in the UK [Mobile ownership in the UK] and upon an agreement with the users and ISP, governing authorities should be able to spread a good awareness on information security as this will reach 84% of the population in the United Kingdom.

Public transport: Public transport vehicles should present the security tips in a simple and easily convincible way so those users who are commuting could have a glimpse of them if they are interested.

Bank Websites: Banking websites should offer security tips just before the users log-on to online banking website. Users should be forced to go through the security guidelines before entering into the website. This however will become annoying for users when they become familiar with security measures. This could be overcome using the *"skip"* option so that the users who are aware of security guidelines can skip the section and process with log-on process.

Comics: Comics usually attract younger generation and this will be an ideal way to implant security awareness from childhood. However, comics will have difficulties to convey complete messages but it is possible to design comics in such a way that it offers complete awareness. Children would read comics and discuss them with their parents through which there is a possibility that the older generation will learn too.

The proposed methods to improve the existing media awareness techniques will reach more audience at all age and with varying knowledge on computers and information security. The governing bodies, security software vendors and the media should come to a common understanding in promoting internet security amongst home user and implement them so as to bring the cybercrime activities down.

7.2 Security Guidelines

The research paper would like to present few improvements that could perhaps increase the level of user awareness about online security. Some of the improvements are mentioned below:

Shareware/Freeware/File sharing applications: These applications are often bundled with viruses, worms and Trojan horses which will get installed along with the application the user is looking for. This will be usually mentioned in the end-user agreement that is displayed during the installation process. User must read the agreement completely, carefully and if they feel they are at risk the application should not be used and instead look for a similar application from a well known source that is free from threats.

Phishing websites: User should clearly understand the techniques used in phishing attacks and be able to easily differentiate legitimate and phishing websites.

Spam: Users should learn what spam and how spam mail looks like. They should be careful whilst dealing with mail that may be spam and delete them if the mail is not from a known source.

The above mentioned set of security guidelines will serve the need to secure user's information that are exposed to the internet threats and also to help protect their computer system. Users will learn the security aspects when they make themselves available for the media that are promoting security awareness. The mixed combination of security applications like anti-virus, anti-spyware and firewall will offer a highly secure internet experience

8 Conclusions

Security guidelines for home users are vast over the internet. Many websites offer simple and very easy to understand guidelines and yet the users are not able to reach those websites. The relatively new threat Phishing, is getting unnoticed among home users and they are tactically forced to submit their personal and banking details. Home users have their own perception theory when it comes to submitting their banking details over the internet. Trust plays an important role in online transactions and some users are even ready to take risk. Media presentation and awareness plays an important role for users to understand the "Do's and Don'ts". The recommended security guidelines would perhaps strengthen the existing levels of security the home users deploy. Users should educate themselves from the resources available as it is their own responsibility to secure their information.

Future work would be to implement the recommended set of media awareness methods that will help users learn and educate themselves with online security techniques that are mentioned earlier in the report. Knowledge on Phishing could be made aware of into a greater depth to a group of people and later conducting a survey to evaluate their perception on phishing websites. A similar approach could be used to evaluate the home user's perception on spyware and malware after they are made aware of them. Key points for future are, making users aware of spyware applications and phishing websites and evaluate their perception, media awareness can be implemented with the new methods proposed and evaluate the effectiveness of the same and Web applications like the Internet Explorer and mail clients like MS Outlook could be designed in such a way that they are more secure and flexible giving the users more freedom and security.

9 References

American on Line/ National Cyber Security Alliance, "*AOL/NCSA Online Safety Study*", 2004. www.staysafeonline.info/pdf/safety_study_v04.pdf. Date Accessed 18/03/07

BBC Presentation, *"Life of Crime Part 5"*, 2001. http://news.bbc.co.uk/hi/english/static/in_depth/uk/2001/life_of_crime/cybercrime.stm, Date Accessed: 21/05/07

ComScore, *"Review on pan-European Online Activity"*, 2007. http://www.comscore.com/press/release.asp?press=1459 Date Accessed: 18/07/07

European Network and Information Security Agency: "A User's guide: How to Raise Information Security Awareness", 2006.

Gets Safe Online, *"10-minute guide for beginners"*, 2007. http://www.getsafeonline.org/nqcontent.cfm?a_id=1179 Date Accessed: 23/06/07

The Internet Safety Group, *"NetSafe Survey"*, 2005 http://www.netsafe.org.nz/Doc_Library/download/2005_ISG_home_computer_security_survey_summary.pdf. Date Accessed 12/05/07

Message Labs Intelligence, "*Going Up, Going Down!", 2006.* http://www.messagelabs.co.uk/mlireport/2006_annual_security_report_5.pdf Date Accessed: 16/06/07

Microsoft/ NSCA, "Online Security & Safety Tips", 2006 http://www.staysafeonline.org/basics/resources/MicrosoftHomeUserGuidebook.pdf Date Accessed: 13/06/07

Mobile ownership in the UK, http://www.dhaliwalbrown.com/knowledge/UK_Mobile_Market_Statistics_2006 Date Accessed: 20/07/07

Symantec Report, *"A Monster Trojan"*, 2007. http://www.symantec.com/enterprise/security_response/weblog/2007/08/a_monster_trojan.html Date Accessed: 20/08/07

Symantec Corporation, *"Symantec Internet Security Threat Report"*, 2007. http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf Date Accessed: 26/07/07