Online Security: Strategies for Promoting Home User Awareness

B.Varghese and S.M.Furnell

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

In the current world of advanced technology, the Internet has become a part and parcel of our everyday life, but at the same time threats and vulnerabilities are also increasing rapidly. Studies have revealed that home users are among the primary target of attackers, so the need for better awareness and understanding of the security aspects from the home user point of view is the main idea behind this research. Home users need a good understanding of security guidelines in order to achieve maximum security and to investigate the current awareness and practices of the home user, an online survey was conducted which analysed the user awareness about Internet security, their daily practices and their available support resources. A study was also carried on to observe the quality of the existing security guidelines provided by the reliable sources on the Internet. Based on analysis of results from the online survey, and information's gathered from different investigation, we could observe that majority of home users were unaware about threats and vulnerabilities around them and had poor security practices, this may be because of the home users unawareness about reliable security guidance sources. On this ground home user security guidelines where prescribed for secure computing and also strategies for improving the existing promotional activities regarding home user security were prescribed.

Keywords

Awareness, Internet, Security, Malware

1 Introduction

There has been a rapid increase in the demand for Internet connectivity recorded in the past years. Home users frequently transact various activities over the Internet that involves personal information. These activities include on-line banking, use of e-health services, community websites and engaging in e-commerce, at the same time the Internet is no more a safe play ground due to the vulnerabilities in these new existing technologies. A large number of home users are totally unaware of their exposure to online security risks. Computer security is important to all users and many software applications are available to protect the online users. Antivirus software's, Anti-spyware's and firewall are commonly used to protect the systems from viruses, malicious codes, information theft and hacking. Home Internet users using broadband connections are more prone to these attacks. On the other hand wireless networks offer home users with many benefits such as flexibility, portability, increased productivity and enables users to access to their organisations

without sitting at a fixed physical point at the same time wireless networks are more and more vulnerable to threats than wired networks. There is ample evidence to show that home users are at risk of attack. Indeed, domestic systems present an environment in which malware can thrive, and the recent success of botnets in the UK presents an example of how easily vulnerable machines can be hijacked for misuse. At the same time, home users who lack security awareness can become easy prey for scammers and identity thieves. This research work examines the strategies for promoting home user awareness on online security.

The threats home users frequently face online include viruses, worms, spam, spyware, phishing and hacking. Any of these attacks may misuse or corrupt the user's information or even see the user himself been attacked. These cyber criminal activities affect the main IT security issues like confidentiality which is the prevention of information disclosure to unauthorised persons, Integrity which tells about the correctness of data and it is prevention of unauthorized modification and availability which means usability and access of data whenever and wherever required. According to UK payments association APACS, the cost of Online banking fraud has increased from £22.6m in 2007 to £52.5m in the year 2008 and the total fraud losses on credit and debit cards in UK amounted to £609m which is a 14% increase from the previous year (BBC, 2009).

In 2007 McAfee and National Cyber Security Alliance conducted a survey of 378 home users in the United States regarding online security and awareness and also conducted a technical scan of their systems. The analysis reveals that the 98% agreed it is important to update the security software and 93% of the participants believed their home computers were safe from malware. However, in reality the technical scans revealed that only 24% of the participants had a protected online environment with an anti-virus protection that had received and update within a week and had an enabled firewall and with the anti-spyware software installed. Other facts revealed by the survey were that 54% of the participants reported they had virus on their system and 44% believed that they had spyware on their machines. Another shocking result was 74% of the participants believed they have received phishing emails. And it was sad to see that 9% of the total participants had been victims of online identity theft and all this has taken place due to the knowledge gap and lack in online security awareness. 64% of the participants revealed they were not able to identify if the website is safe or not before visiting (McAfee / NCSA, 2007).

According to Symantec's Internet security threat report, targeted attacks to home users were around 95%. All these facts lead to understanding more about the home user and this leads to investigate the current state of the home user.

2 Methodology to Study Home User Awareness

The main aspects of the research was to analyse the awareness of home users regarding online security, as the target audience were the online home users, it was decided to do a survey with online questionnaire because through an online survey home users could participate from the home Internet at their convenience. Online survey also had few other merits like, the data can be quickly collected and analysed, the cost considered with the online survey is lower compared to other survey

methods and the results will have accuracy and can be easily be transferred to the spread sheets for statistical analysis.

The survey questionnaire was constructed after the intensive literature study and the format and design of the questionnaire mainly included closed option multiple choice questions to provide results for statistical analysis. There were also a few open-ended questions to further analyse the home users' knowledge and so they could share their experiences.

The questionnaire was divided into four parts and started by collecting some demographic details such as education, age, sex, knowledge level and usage level of the participant to support the analysis and conclusions. This was followed by a security awareness survey, which aimed at identifying whether the user is aware of the security facts and the threats around him while using the Internet. For collecting this information certain questions were used like rating the current Internet scenario whether it is safe or not safe, and depicting the user awareness about malware, firewall and usage of wireless networks. Following this, the next part collected information regarding daily practices of the user while using their computer and checking their awareness in different areas like virus, spyware, usage of firewall, usage of email and backups.. To conclude the survey there were some questions to collect information regarding security promotion and daily commercial practices when using the Internet. These questions were designed to capture information from the home user regarding the promotional activities of online security awareness and the sources from where they gain the information and to know how commercially they are using the Internet. The survey was promoted among the home users through social networking communities and through university students.

3 Findings

The online survey received responses from 259 participants, the majority of whom were in the age group of 18 to 35. A major portion of the participants were academically or technically qualified, and 77% classified themselves as intermediate users, while 16% considered themselves as expert users. Overall, 44% of the participants said that Internet is necessary part of their profession or education.

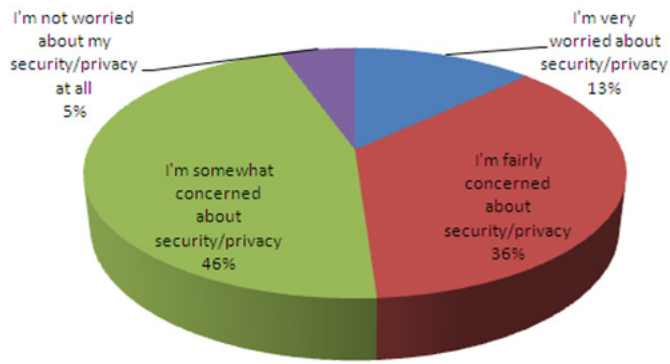

Figure 1: Home User's Concerns about online security & Privacy

From the security awareness investigation we could observe that many of the participants were not sure if the Internet is still a safe place, as shown in Figure 1 below.

When asked if their system was infected with malware 35% of the participants said their systems were not affected and 42% were not sure if their system was affected or not. This actually shows the lack of technical awareness in nearly half of the users and 21% of the participants confidently said their systems were affected with the malware. And 80% of the participants believed that malware would slow down their system performance while 72% of respondents believed it would corrupt or wipe the files in the system. By analysing the user understanding regarding malware, it was possible to see that the user is aware and knows what happens if the system is affected. And in recent years the trend is towards mobile computing and wireless technologies, and when asked with the participants regarding encryption on wireless network 44% did not know about it and just 28% of the participants used encryption on their network.

The next section investigated users daily practices and we could see that around half of the participants update their antivirus daily or weekly and around 20% of the participants did not check or were aware of these updates. 76% believed that antivirus performs regular scan on every file in the system, while 42% of the participant had a misunderstanding that antivirus identifies and prevents hackers. And when the users were asked about spyware, 41% did not know what it is and what it does. Nearly half of the participant's antivirus software also protected spyware, while the rest of the participants were unaware or did not have anti-spyware support. When analysing the participants who did not have anti-spyware, we were able to see that they were victims of some sort of attack. Some of the participants were victims of malware attack and shared there experience, and when analysing these we could analyse that this had happened due to user unawareness and negligence, and once affected it gives big crisis for home user resulting in data loss or even system crash. When the users were asked about how confident they were that their system is free from viruses, 36% replied that their system is okay and 38% believed that they were affectedm, with the rest being unaware of what is happening in their system.

From the responses received it was possible to observe that 74% of participants had firewall installed on the machines. Of these, 38% claimed to have manually checked their firewall configurations, while 61% had not done so. When asked the reason for this behaviour, more than half believed that the default configuration is sufficient to protect them against vulnerabilities.

When the home users were asked about spam mails, 63% indicated that they receive spam regularly, 42% were not interested in using spam filters while 19% were totally unaware what the spam filter is. One of the important reasons for an increase in spam may be that 76% were not interested to report it. This means that the spam providers are getting support from the user itself.

In this world of online insecurity, backups are very important and when, analysed with the responses it was able to observe that 55% do backups while 12% were

ignorant about it. From the participants who did backup we were able to analyse that nearly half of the users did not have a regular practice. Nowadays a good backup culture needs to be developed in the home users so that they will be ready to face any uncertainty.

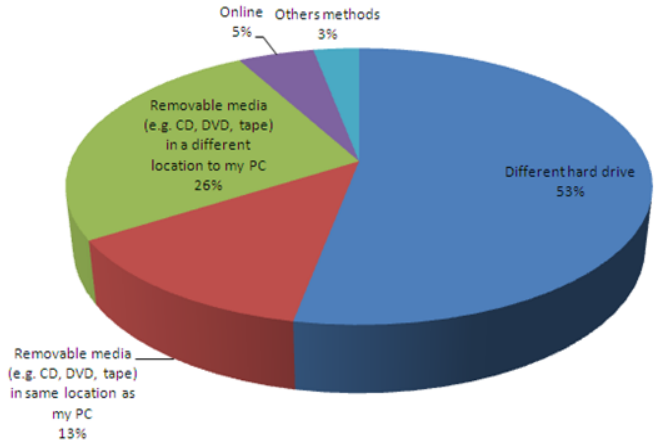

Figure 2: User Data Backup

As Figure 2 shows more than half of the participants preferred different hard drive to have their backup, and it is interesting to see nowadays a small percentage of users willing to have their backup online. When how many of the have successfully restored their back, only 33% of the participants have restored it while 47% of the participants did not have occasion to use their backups.

The reason for the flaw in security is the home user unawareness. When we analyse the resources of home user support as shown in Figure 3, we could analyse that

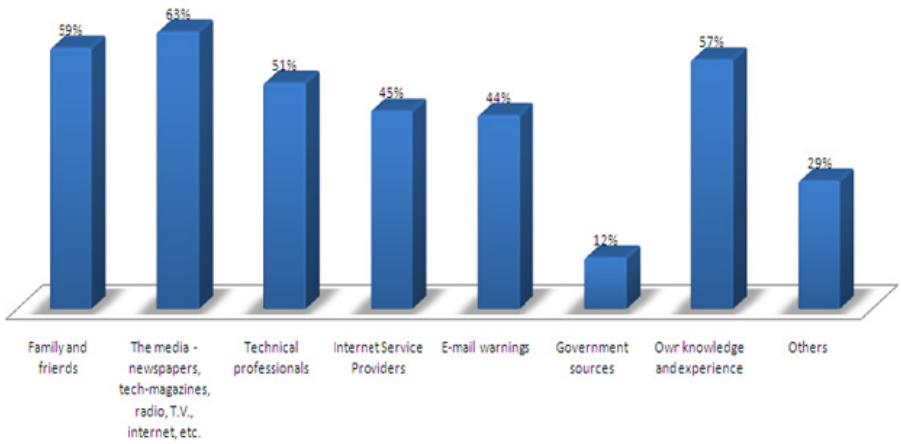

Figure 3: Sources of Technical Support to Home Users

Media like newspapers, tech-magazines, radio, TV and the Internet were the primary sources of knowledge support, followed by the family and the friends circle. The problem is that if the family and friends did not have adequate knowledge or had a misconception it will be passed on the user too, and these wrong practices will then continue. Looking at Figure 3, government sources were clearly the least rated by the user. Governments should take more imitative to promote these security techniques as it safe guard the nation too. Even though government had some of the reliable resources it is not promoted effectively, so that the home users are unaware of it. When user were asked for their common support website these were some of the responses.

"Microsoft, Symantec, Getsafe online"
"help from microsoft, help from google", "security help from google seach results"

Considering the U.K national average of 49.5% of online banking users, we had a response of 59% of the participants who use online banking. This difference may be because we have a greater participation of academically and technically qualified users in our online survey. And to briefly consider the security precautions taken by the user, users password characteristics were analyzed and it was able to see that a major percentage of users and practice good password policy.

4 Discussion

The survey responses provided information regarding how home users think, act and react to the vulnerabilities. While most of the users considered themselves as intermediate or above, half of them were totally unaware and did not know whether there system is affected by malware or not. Moreover, some of the users had incorrect ideas about malware, and at the same time a major portion of the home users were totally unaware of encryption on wireless network, which can lead the intruders to having access on their network. This makes the user extremely vulnerable and can lead to further problems. There are areas where the home user awareness has to be increased like antivirus, anti-spyware and firewall, because in the current scenario even though this software is installed on the user machines, they are generally not enabled or regularly updated to provide good protection to the users.

Many home users assumed that antivirus will prevent them from hackers and online frauds. Many studies say the home users are the target of attackers because hackers capitalize upon their unawareness. Many users did not use proper security applications like anti virus software, ant spyware and firewall and the common problems they faced were corruption of data, change in system settings, decreased system performance, and change in browser settings. Two thirds of the home users did not check the configurations of the firewall and they believed that the default configuration is sufficient to protect them from all these threats. So it is advisable that if the vendors and the developers a good standard of default setting it will be very beneficial for the novice users. As email has made communication easier, it has also enabled that transportation of spam. Nowadays spam levels are increasing day by day and e-crimes are also increasing rapidly, but many users are totally unaware where to report against these activities if they become the victims of it. From our

survey 76% of users replied they are not interested in reporting these complaints. These types of attitudes could be changed only by promoting proper awareness to the home users.

A good backup culture should be developed with the home users so that in case of any data loss the user will be able to retrieve their data. More awareness should be increased with home users so that they do not need to suffer a major loss. The major source of technical support for the home users was the media followed by friends and relatives. If the friend or the relative is not a technical expert, the home users knowledge will be limited which leads to more risk. The home users mostly relied on websites of Microsoft and security vendors for technical advice while the users were totally unaware of the government run websites specifically targeting home users security like Get safe online and IT safe. These may be due to the lack of promotion from the government and other security organizations. Home users are not willing to waste time and effort to find out these sources and expand their knowledge; they just need the things to be done.

5 Conclusion

After a careful study, this research paper has given some important security guidelines and promotion methods of available technical resources to increase the security and awareness among the home users.

Security guidelines included updating the antivirus frequently, and enabling the firewall applications and making sure that it is working fine. Anti-spyware software should be installed and updated regularly and the operating systems needs to be updated frequently with the newly available updates and patches. Users should develop the ability to recognise the genuine and fake websites and take care of their personal credentials. Users should be advised to follow strong password characteristics and should make sure the file and the print sharing should be disabled when not in use. User should be taken more precaution no to open mails of unknown senders and always rely on reliable security sources for help and advice.

Government and other security organization can take more initiatives to promote the security awareness programmes and websites, so that home users can have the full benefit of these resources. More promotional activities can be carried on televisions advertisements, print media, radio advertisements, commercial websites, through mobile communication and by educating from schools.

6 References

BBC, 2009, '*Big jump in online banking fraud'*, http://news.bbc.co.uk/1/hi/business/7952598.stm, [Date Accessed: 08-08-2009]

McAfee / NCSA, 2007, '*McAfee/NCSA Cyber Security Survey'* http://209.85.229.132/search?q=cache:zlc0shdbMFcJ:download.mcafee.com/products/manuals/en-us/McAfeeNCSA_Analysis09-25-07.pdf+mcaffe/ncsa+2007&cd=1&hl=en&ct=clnk&gl=uk, [Date Accessed: 19-08-2009]

Symantec Corporation,2007. "*Symantec Internet Security Threat Report*", http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf [Date Accessed: 26-1-2009]