Improving protection and security awareness amongst home users

P.Bryant, S.M.Furnell and A.D.Phippen

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

Abstract

With increased protection making businesses a much harder target, home users are now becoming targeted more significantly. In the past home users have been somewhat neglected and only in recent years have a few surveys emerged to provide some insight into their level of protection.

This paper reports findings from a survey of 415 home users, examining their knowledge of security issues and the usage and protection of their computer systems. It revealed that while users are generally confident about their security and feel they have heightened awareness about the main threats, protection measures such as firewalls and anti virus are not updated regularly enough to provide sufficient protection. There is also a lack of awareness about phishing threats, and insufficient protection against more recent threats such as spyware. This may have worrying implications for the future, with rising uptake and consequently threats from Instant Messenger and Voice Over IP applications and technologies.

Keywords

Security, Home user, Awareness, Perceptions, Survey.

1. Introduction

Many online security threats can pose a serious risk to both home users and organisations. As Internet and especially broadband connectivity continues to increase, home users are becoming even more vulnerable, especially with the wide use of computers for tasks including communication (e.g. email and instant messenger services, surfing, gaming, file sharing, and storing sensitive and personal information). While their awareness of the threats has increased over the years, what they actually do to protect themselves is generally not enough, leading to a false sense of security. Alongside this, users' machines are holding more sensitive information and online services are inviting them to part with vast amounts of personal and financial information, with shopping, banking, gambling and auctions to name a few.

While organisations are tightening their defences' users are becoming more and more attractive targets, especially with the rise of botnets and related denial of service attacks. "In the first six months of 2005, Symantec identified an average of 10,352 bots per day, up from less than 5,000 per day in December 2004" (Symantec, 2005) and denial of service attacks have an increased by 51% from an average of 927 attacks per day the first half of 2005 to an average of 1,402 attacks by December 2005 (Symantec, 2006). The home user's machine is the ideal candidate for zombies

from which the resources can be utilised for denial of service attacks or the widespread distribution of spam and phishing emails (MessageLabs, 2005).

In order to gauge the extent of current vulnerability, a survey was conducted to assess users' awareness and understanding of ,threats and countermeasures as well as the protection practices they currently follow. The intention of the study was to gain an insight into the vulnerability of users and what might be done to help them.

2. A survey of home user security perceptions

In order to understand the current practices and knowledge of users, an extensive questionnaire-based survey was carried out. The survey included mainly closed option (tick box) questions to provide a high amount of statistical data, but it also included open-ended questions where users could add their own thoughts and input (Fink, 1995). Another essential element was to capture demographic details, such as age and education, to assist in the analysis and conclusions. A maximum of 28 questions (excluding the demographics) were included so as not to overload the participants, while also ensuing that enough information was gathered.

To increase the credibility and distribution of the survey it was placed in its own domain on the Internet at www.securityperceptions.net. This was then promoted via email and word of mouth, but also through a variety of web forums such as ultimatereef.net, ukip.co.uk, allotment.org.uk, webuser.co.uk and the studentroom.co.uk, which gave particular access to home users with differing interests and lifestyles who regularly use the Internet. The research was also supported by the Trustguide initiative (a DTI-funded joint project between British Telecom and Hewlett Packard). In order to have a consistent basis for analysis, the respondents where restricted to UK users, and this requirement was constantly pointed out during the promotion of the survey.

2.1 Respondent demographics and background

The survey received 415 responses, a large majority of which classed themselves as intermediate or advanced users, with 58% stating that their highest level of education was at degree level or higher. Therefore the results could be considered as somewhat unrepresentative of the national population. What this does though mean is that the users who completed the survey could be considered as technically and academically more advanced than the general population. This is supported by the fact that only 8% stated they were novice users, while 43% stated they thought they were advanced users. With this in mind it should be considered that the results would be more positive than normal and show more bias that the home users are more secure than they really are. One other point that should be considered is that a number of respondents were from web forums, and so could be considered to be more experienced (particularly using the Internet) than the average user.

2.2. Vulnerability of users

In terms of assessing their vulnerability the results showed that 87% of the respondents had a broadband connection, much greater than the number of dial-up connections. While the advantage in security terms is that it allows updates to be downloaded fairly efficiently, the systems using broadband are at a severe risk if they do not have the appropriate protection and the users do carry out the required procedures to ensure they are protected. The main reasons for this have been highlighted by Furnell (2005), because of the speed that packets can be transferred over the network and unlike dial up broadband is always on:

- The bandwidth can be harnessed for a denial-of-service attack;
- A mass mailing virus or worm program could be deployed;
- The broadband connection can be used as a spam generator.

Out of those with an Internet connection 38% of respondents have a wireless connection, which if unsecure (e.g. without encryption mechanisms so that only the user's machine can connect to it) can provide an additional level of vulnerability. With an insecure connection it can allow another with wireless connectivity within range to connect to the Internet through the network and use the Internet and resources that may become a problem where the victim has a limited download, and the fact that the criminal is getting free Internet access. It is also possible for a hacker to gain access to the user's machine itself, and so use its resources, plus steal or alter files.

2.3 Home Users Security knowledge and practices

The first element to note is that users have a high level of confidence about their security, with 51% indicating that they were 'satisfied' with their security while a further 20% were very confident and additionally 41% felt they understood all the issues and devote time to security. Therefore it is essential to understand how secure these users are to see their level of vulnerability to these threats. The first indication of the level of knowledge possessed by the users was to look at their understanding of the main terminology that is used to explain and refer to the different issues with in security and IT. With this in mind, Table 1 shows a relatively high level of understanding amongst the respondents for what could be considered as the three main issues of Virus, Hacker and Firewall.

	% of Respondents
Virus	99%
Hacker	98%
Firewall	96%
Spyware	89%
Phishing	68%
Identity Theft	92%
Worm	85%
Trojan Horse	83%

Table 1: Respondents' understanding of security terminology

The main area that stands out is that 32% of respondents do not understand what the term 'phishing' means. It is therefore likely that they are unaware of the threat, and so will be unlikely to act in an appropriate manner to ensure they do not become victim of a phishing incident. It can be considered a high proportion when the seriousness of the threat is considered with the possibility that users can be fooled into divulging their personal or financial information, such as bank account details, and the ability for criminals to send vast amounts of phishing emails using botnets and spam. Despite this, however, 92% do understand identity theft so they may be aware in some cases the need to be careful with their information, but again they are not likely to be prepared for a well-designed phishing email that appears legitimate.

Worms and Trojan horses are also a cause for concern where 15% of users still do not understand what the terms mean. This is important when considering that these threats have been in the public eye for at least six years or more, particularly with worms such as the Love Bug in 2000 (BBC News, 2000) and the Slammer worm (Clyde, 2003) that both caused significant damage and were publicised across the world.

There is a significant interest is relating this to the use of firewalls because where only 4% did not know what the term firewall meant, 13% do not have a firewall on their machine. In addition 98% stated that they also knew what the term hacker meant. Therefore the survey tells us that while a number of users understand that there are threats and countermeasures they do not consider the risks sizeable enough to warrant protecting themselves against, and so do not have protection such as a firewall installed. This can also be applied to spyware, where 89% understand what spyware means but only 77% actually have anti-spyware installed on their system, leaving 22% unprotected against spyware threats. Naturally it could be that their understanding of the terms is incorrect or they do not appreciate the threat or alternatively have no knowledge of how to protect themselves against it. Furthermore the fact that only 60% of users have anti-spam installed is not only another indication of the failure to protect themselves, but is closely linked to their lack of understanding of the need for anti spam and the threats. This is highlighted by the fact that only 68% understood the term 'phishing', which is especially linked and distributed principally through spam. A reason for the lack of understanding and protection against spyware, phishing, spam and even to some extent Trojans and worms, is most likely that there is a failure amongst users to keep themselves up to date with the latest threats and countermeasures and integrate this protection into their machines. This suggests a problem for the future if users carry on with this and do not become protected against future threats, especially where the introduction of new technologies provide new opportunities for criminals that users may not be aware of. Instant Messenger (IM) and Voice over Internet Protocol (VOIP) technologies are significant examples of this, where currently 51% of all respondents use IM and 23% already use VOIP. While the current threat posed is not very significant it is predicted that the threats will greatly increase in the future in terms of number and severity, as pointed out in the following quote. "IM-worms are at the initial stage of evolution. And the fact that the vast majority of the worms are written in Visual Basic demonstrates that most of the authors are fairly new to the virus writing scene and are relatively inexperienced programmers" (Gostev, 2005).

Consequently users need to be prepared for the change in the threats which can be done by ensuring that the importance of keeping their knowledge up to date is passed onto users, as there is no point only knowing about the threats in the past. It therefore needs to be emphasised that the threats will change all the time, particularly with the uptake of new technologies, while the means of protecting themselves and their machines will also evolve.

Related to this has to be the fact that not all the respondents fully understood the role of the technologies installed on their machines, at 27%. While 41% had never attempted to configure their firewall thus leaving the possibility that they are left unprotected, with the default settings and this could also cause the firewall to block a significant amount of legitimate traffic, causing frustration for the user. 12% stated that security impedes their use of the computer. A frequent occurrence with firewalls is that it prompts whether the user wants the traffic blocked or not, there is a possibility therefore that users may permit dangerous connections as they may not truly understand what it means. Alternatively users could just turn off the firewall if it becomes too much of a nuisance.

While having the appropriate technologies installed is one thing, they can be considered useless if they are not regularly kept up-to-date with the latest bug fixes, signature lists or patches to fix holes within the code. With regard to the key security applications displayed in Figure 1, a worrying result is that even though the majority of antivirus, firewall and anti-spyware and anti-spam updates are carried out weekly, these figures are still relatively low, with only antivirus getting a positive response from more than half of the respondents (at 63%), while only a further 20% update the antivirus software monthly. This therefore means that a further 16% are very inefficient in updating their antivirus or never do it, thus leaving themselves very vulnerable as it is particularly important to update antivirus frequently to ensure sufficient protection. Even updating the software on a monthly basis can pose a significant risk to the user, as they will be unprotected against any new threats that appear within that period. During this time they may also become victim of a botnet or backdoor program, which can allow a hacker to control their machine.

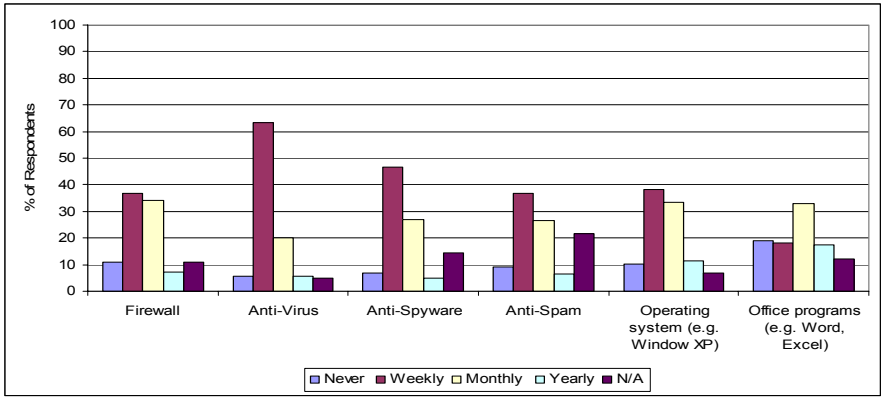

Figure 1: How often do users update applications?

Anti-spyware works in a similar fashion to anti virus software so it is as important to prevent criminals from spying on your behaviour or stealing your data, by ensuring that it is up to date as possible and so prevent new spyware infections. This seems to be another area where user's security is seriously lacking and they are exposing themselves to these dangers as only 47% update on the required weekly basis, while 27% update monthly. This leaves a considerable 26% of respondents who are almost completely unprotected against this threat, by stating that they only update yearly, never or it is not applicable. While it is not as important to update the firewall as regularly, a weekly or monthly basis should provide a basic level of protection for this part. Despite this 29% of users update their firewall either yearly, never or feel it does not apply to them. Thus, only 37% update weekly.

Similarly anti-spam programs do not require the malware list updates of anti-virus and anti-spyware, but the programs may have the requirement to be updated fairly regularly so they can operate at maximum efficiency. Despite this, only 64% of users update their anti-spam on a weekly or monthly basis, subjecting themselves to more spam than necessary which can include phishing emails, while also increasing the possibility that legitimate mail is blocked by the older software.

Additionally security holes within applications that operate on the machine can provide a backdoor past the security technologies, to infect the machine or allow an outsider to spy or even gain control of it and the information within. An essential element for ensuring security is to update these applications with the latest patches as regularly as possible. These exploitable holes occur because of the vast amount of code required to construct the applications, which make it virtually impossible to test the whole system, so it is released with these unknown flaws included. This is especially important with the operating system, which is the backbone for the whole machine and so if it can be compromised in some way then the whole system and everything on it possibly can be as well. Despite this, only 38% updated the operating systems on a weekly basis and a further 33% monthly again leaving 28% of users extremely vulnerable by not updating or only on an annual basis.

Office-type programs, including spreadsheets and word processors, may provide a similar weakness for the system. There is again a deficiency in the percentage of respondents who update their applications on a fairly regular basis at just over half (51%) doing it weekly or monthly. This seems to be an area where there is the least amount of knowledge, as it had the greatest percentage of users who stated that they never update (19%), while 12% put this as not applicable to them.

Another reason that could be used to explain user lack of security could well be the fact that 19% of respondents (second highest response for this question) stated that they felt security packages and services are too expensive. Therefore, it is likely that once an initial subscription with the security software vendor runs out (as its normally supplied when the machine is first purchased) that they do not update this subscription and so are not able to receive new updates.

All this shows that the awareness of updating non-security applications is particularly lacking, with the idea that security only resides with these applications, supported by the results about user awareness of security features. A significant part

of managing user's security is the ability to personalise and ensure that the security settings that exist within a number of programs can be used by the user. For one, most Internet browsers have security features where users are able to manage different aspects of their security and things that they are subject to when browsing the Internet, such as content filtering or more importantly cookie management. Without these they may be less secure than they think. Despite this, only 40% actually know that the security features exist within web browsers, while more importantly only 22% actually understand how they work. Given that 97% use the Internet for web browsing, this is a significantly low proportion, particularly in relation to the amount of users who understand the features.

Other types of programs show a similar picture, with only 39% knowing that security features in office programs and email clients exist, while 37% know about the operating systems features. Moreover 25% of all respondents actually understand the security of office programs, 24% the features in email clients and a lowly 21% who actually understand the security features of the operating system (OS).

Further issues to do with the usability of security come down to the fact that 11% of users stated they do not have time to deal with security issues, and 12% feel that security impedes the use of their computer. This may be considered a small proportion, but if this was taken to apply to the whole population, then 11% is a large number of users from the 62% of the UK population who use the Internet.

3. Discussion

The survey has been able to reveal interesting conclusions that while the majority of users are confident about their security and feel they have heightened awareness about the main threats, there are areas where there practices and knowledge to protect themselves is insufficient. Particularly, while firewalls and anti viruses are installed on their systems, they are generally not updated regularly enough to provide sufficient protection. There is a specific problem in considering malware that even disables these applications, leaving the users extremely vulnerable if they do not update their virus lists in time before becoming infected.

There is also a lack of awareness about phishing threats, and insufficient protection against other more recent threats such as spyware. This may have worrying implications for the future with rising uptake and consequent threats from Instant Messenger and Voice Over IP applications and technologies. More importantly, users are taking large risks by not updating the other applications on their machines on a regular basis. Key to this is the operating system and Office style programs, where coding errors and bugs have been exploited in the past by malware writers and hackers to spy on the user, corrupt or steal their data or control their machine. This is particularly important where a backdoor is created past the anti virus or firewall protection, rendering them useless, while the user has no knowledge and still feels safe while using sensitive information or data on their machine.

Therefore users are not doing enough to protect themselves, so there is a need to significantly improve home user awareness and protection. Additionally, this is

particularly important when considering the increase of the threat financially and especially to individuals: "Attackers appear to be moving away from threats that destroy or compromise data and toward the theft of confidential, financial and personal information for financial gain." (Symantec, 2006).

4. Conclusion

The survey has provided an insight into home users' security knowledge and practices of which there are areas that still need to be improved especially concerning knowledge about more recent threats and updating of their applications. It is worth again pointing out that the majority of respondents were advanced or experienced users, and so for the results to be applied to the population of home users the bias towards suggesting greater security awareness and protection needs to be taken into account.

The survey also assessed areas such as what users use their computers and the Internet for, where they might go for security advice and in particular whether users had any knowledge or experience of information sources that are designed to assist the home users, as well as their understanding about reporting security incidents. These elements are under further investigation and have not been covered by this paper.

Particular areas which could be further investigated include how users gain their security knowledge and whether they feel it is useful. An investigation could be applied to all sorts of information sources from the websites to retail stores and even from friends and relatives to understand if this information is appropriate and understandable for different types of home users needs. It is important to know how they learn, and to improve the advice that is given, in order to subsequently improve their protection.

5. References

BBC News (2000), "Papers fall for Love Bug", Friday 5th May 2000, http://news.bbc.co.uk/1/hi/uk/736570.stm, (Accessed 3rd September 2006)

Clyde, R (2003), "Inside the Symantec Internet Security Threat Report", Summer 2003, Issue 19, Symantec Corporation, http://www.symantec.com/symadvantage/019/report.html#read (Accessed 28th September 2006)

Fink, A, (1995), "The survey kit / Vol.2, How To Ask Survey Questions", Sage Publications, London

Furnell, S (2004), "Hacking begins at home: are company networks at risk from home computers?", *Computer Fraud & Security*, Volume 2004, Issue 1, January 2004, Pages 4-7

Gostev, A, (2005), "Malware Evolution: January - March 2005", April 2005, http://www.viruslist.com/en/analysis?pubid=162454316#mobile (Accessed 1st September 2006)

MessageLabs, (2005), "Intelligence 2005 Annual Security Report: Cyber-criminals narrow their focus", http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/intelligence_reports/2005_annual_security_report/DA_123230.chp.html, (Accessed 31st August 2006)

Symantec Corporation (2006), "Symantec Internet Security Threat Report IX", March 2006, http://www4.symantec.com/Vrt/offer?a_id=22651, (Accessed 31st August 2006)