Assessing Protection and Security Awareness amongst Home Users

V-G.Tsaganidi and S.M.Furnell

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

Abstract

Home users have become the most attractive target for cyber criminals as they are more vulnerable and less protected than the rest of the users. As they constitute a mostly inaccessible group the only information they get originates from people in their environment and their exposure to media. Therefore, the amount of information they possess, their awareness about security issues and their security practices play the key role in their protection. This paper presents the findings of a number of interviews with novice UK home users of different ages, educational level and occupation. These interviews were conducted in order to assess their security perceptions, their awareness of threats and security mechanisms, their practices in regard to security and study their opinions and thoughts of security issues in general. The results revealed a satisfying level of threat awareness and security practices which however were not enough to make users feel adequately protected or confident about their actions. They are counting too much on their friends' advice, without wanting to search for more information on their own, thinking that they cannot afford the time and effort required. As a result, they feel somewhat at risk but believe they are taking all the necessary actions to prevent a bad ending.

Keywords

Home users, security practices, security awareness

1 Introduction

Users of the World Wide Web and its services are dealing with the prospect of fraudsters breaching their privacy. In today's online world, the amount of personal information that is exposed, exchanged and exploited is massive. In addition to that, an essential number of other threats is also a hazard for users such as malware including viruses, Trojan horses and worms, spyware and identity thefts by phishing, pharming or other Internet scams. Especially home users are starting to become the primary target for many cybercriminals nowadays. That is because the majority of them lacks the experience to protect their systems or neglect to do so considering themselves not to be possible targets. Since they do not protect their systems properly they are vulnerable to many threats and that makes them an easy pray for hackers and fraudsters. Therefore, security requires immediate attention and a first step to address it is studying the way users think, their actions, the reasoning behind them and how informed they are.

The number of attacks towards home users has been highly increased and the numbers speak for themselves. Symantec's Internet Security Threat Report showed that 93% of all attacks were targeting home users (Symantec, 2007). The equivalent result of the previous 2006 security threat report was 86% (Symantec, 2006). This difference of 7% within the period of 6 months cannot be overlooked as it is extremely forewarning and it indicates how important it is to protect home users. Public is not aware of this new trend, where home users have become the primary target, falsely believing that they are less vulnerable than companies and organizations. However, the threats are multiplying monthly and according to Anti-Phishing Working Group Report (2006) in December 2006 there were 28531 phishing sites, which was increased by two thousand from October. Jaeger et al. (2006) assessed the awareness and understanding of spyware of 205 home users. The findings showed that a high number of the respondents were aware of spyware, being able to define it correctly and identify its risk. However, the users could not accurately recognize which websites have the most chances to distribute spyware. That indicates that home users can be at risk even though they are aware of a threat such as spyware. Home users also have to deal with usability problems when configuring the security settings as it can prove to be very difficult and tricky, and they have to deal with it without help from an expert such as a system administrator (Furnell et al. 2006). From the latter relevant research (Furnell et al. 2007) it was deduced that although the respondents appeared to be aware of the threats and employing security policies and techniques a profound study showed a lack of serious knowledge and understanding. Thus, a more in-depth study was needed to assess not only what users do but also why they do it.

2 Interviewing novice home users

The research was conducted by 20 interviews where all the interviewees were UK citizens as the research aimed at studying the home users exposed to the UK media. Since the last research (Furnell et al. 2007) was focused on advanced users, this study to assess the way the novice home user thinks, feels and reacts with regard to computer security issues, the way they use the Internet, and their awareness of the role they play in the security chain. All the results aimed at studying the user's perceptions, attitudes and customs and what the users think they know and if they believe it is adequate for their protection.

All the interviewees were asked to participate either by word of mouth or by email invitations. They were notified that the research was about novice home users and all the users that classed themselves as such, accepted to participate. Each interview was adjusted to the particular interviewee depending on the answers they provided along the way. Thus, there was no predefined time duration. However, all the interviews lasted at least 15 minutes which was the minimum time needed for covering all the topics. These users did not know that much, did not look that interested in the security topic or they just were not aware of all the advancements in the threats and the security mechanisms. The topics that were chosen to be discussed during the interview were namely, the users' awareness of the various threats and security mechanisms, their knowledge about identity theft and any relevant experiences they had and the sources they use for help and advice. At the end, there were questions regarding their overall opinion about what the interview offered them and if it affected them.

2.1 Internet Usage

Firstly, interviewees were asked about their Internet activities and then they were asked whether there is an activity they refrain from because it is not secure enough. Some respondents referred to buying online:

> *It does bother me sometimes, cause I think maybe it's not secure but I tend to stick because they have these little padlock symbol and I didn't have any problems with it so far so I just keep going. I wouldn't use sites I've never used before or things that look a bit dodgy and I tend to stay away from them.*
>
> *I always check when I buy things online that they've got the padlock, cause I know it's the secure way of buying things online. I'm quite happy with sites I know, I wouldn't use some random site if I hadn't heard of them or been recommended to them. I'm a bit cautious about using the Internet and paying with my credit card.*

Others were afraid of downloading files from the Internet or doing online banking:

> *I download songs and movies and I don't really think about that, because I think that when I am using the antivirus to scan my computer that this is enough but from what my friends told me it's not...I don't really pay much attention in which websites I am going to.*
>
> *I don't download anything because I am afraid of viruses.*
>
> *I'll buy things and I'll give them my credit card details but I'm still a bit worry about doing my banking online. I'll do it over the telephone but I'm still not too sure about actually doing it over the Internet.*

Even though people are afraid of doing certain things like for example buy things online or download files they will actually do them. Of course some of them will try to assure first that a level of security for that particular action like making sure a website has the padlock symbol or scan a file for malware before opening it.

2.2 Awareness of Threats

The users were asked what threats they know or have heard of, and after they had said all they could remember, they were prompt with some other threats to see if they know them. As the responds showed all the interviewees knew about or had heard of viruses. They all recognized the name, it was the first one mentioned when asked the question and most of them were able to define its impacts on the system and some even identified ways by which a computer can get infected. However, none mentioned the potential data breach where their confidential data could be stolen if their computer was infected by malware. A Trojan horse was the piece of malware less known among the respondents and although most users had heard about phishing they could not provide an exact definition. All of the users receive or have received in the past some junk email but not all of them know its different name, spam. Another observation is that although users were familiar with spyware a couple of them thought that it was a program confusing it with an antispyware. The interviewees after talking about the threats they know or have heard about and learnt about other threats as well they were asked if they were ever faced with any. Fourteen respondents responded positively, with one of them referring to a phishing attempt, six to a Trojan horse and seven to a virus. Three of these 14 respondents were faced with both a virus and a Trojan. From the respondents that admitted having a virus in the past all of them reformatted their computer, with four asking for a friend or relative's help to do it. Only one took their computer to a professional and they reformatted it there. The three respondents that had a Trojan horse were able to solve their problems using their antivirus on their own.

2.3 Security Mechanisms

In order to protect themselves users should take some measurements and use some security mechanisms to do so. Therefore, it was advisable to ask the interviewees which security mechanisms they know, which ones they have and if they would not come up with many then they would be prompt to see if they know any more. The interviewer had in mind the following mechanisms: antivirus, firewall, antispyware and antispam. In order to assess the users' knowledge of other security controls within applications that are not security related they were asked if they have used any of those. None of the users was able to come up with any such security control and thus, they were asked in particular about the security options in Microsoft's Word and their web browser's security adjustments. The results were rather discouraging, as only two have used the first one and four the second one. Almost all of the respondents use an antivirus with only two out of 20 not using one. The rest of the respondents are certain that they have an antivirus where about the firewall, the antispyware and the antispam there were several users that were not sure if they do have them. Those that do not have an antivirus were asked to justify their choice and here is what they replied:

> *I am not cause I am not entering sites such as where you download programs or something. I am just reading newspapers or check things necessary for my coursework. As I said my C drive is totally empty so if something happens I just delete it and that's all.*

> *I just use certain sites to download stuff and buy things, they 2 of each one and I don't think I need an antivirus. I used to have one but it made my computer slow and I didn't like that.*

2.4 Identity Theft

Another important section of questions was referring to identity theft which has drawn a lot of media attention lately. The users that answered positively to the question if they use online payment methods were then asked how they think they protect themselves from identity theft. Since all the interviewees answered they know what identity theft is, they are all aware of it as a threat and therefore were expected to take some kind of a measurement to prevent it. The issue of trust was the first and most common one mentioned. Users interact with websites they trust as they think that if the site is trustworthy they will avoid loosing their identity details:

> *I just use the sites that I trust.*
>
> *If you know the site that you're using, I mean yeah I use different sites but when I want to put my credit card details usually it's a real loyal website like from a train company or an airline company, I don't use it everywhere.*

Others claimed that they only use sites that their friends have recommended and used in the past. Their friends' advice helped them to overcome their fears about identity theft and be able to shop online:

> *I learned from friends about two sites where you can buy things that they are safe and there will be no problem and I only use them.*

Others stated that in order to protect themselves they do certain things regarding the payment methods they use to buy stuff:

> *I use my credit card and we check our credit cards very regularly. We check the bill every month, we got all the receipts.*

Some choose to use cards that have a limited amount of money on them in order to lose the minimum amount of money in case of an identity theft:

> *I prefer not to use my credit card online and that means I have to se my debit card instead but I think that's safer because.. it's not like they're gonna steal a lot of money, it's less damage.*
>
> *The only good thing is that even if I use the credit card it has a low limit so he is gonna get a small amount of money.*

Unfortunately for e-commerce's bloom, there were some respondents that stated they refrain as much as they can from using their credit cards as they feel vulnerable to identity theft:

> *I don't use that much the credit card that's why* (identity theft) *because some day maybe someone gets my card and everything.*

> *I am not using it a lot* (the credit card) *because I'm afraid they can steal my passwords and they can charge me but ok, sometimes when I am obliged to use it, I use it.*

There was even a case where an interviewee stated refraining entirely from online shopping was his only option. An important observation is that none of the interviewees felt very confident in using their credit cards. From the 18 users reporting that they shop online, some of them tried to avoid shopping whenever they could and the rest tried to be as cautious as possible. However, there was not a single person saying that they were not at all afraid of identity theft. Despite their fear though, many of them were not discouraged and continue buying stuff online on a regular basis.

2.5 Social Engineering

The interviewees had various jobs and a scenario of using a computer at work did not apply for all of them. However, because all the users were familiar with using a username and a password for an account, they were able to picture a scenario of them working for a company, having a username and a password to login to their work computers. They were first described a case of a social engineering attack by the phone, using a similar example of that described by Granger (2001). Then they were asked how they would react and whether they would divulge their login details. Even though the majority of the respondents would at least think about it before sharing these details over the phone, there were 5 people that would:

> *Yes, I would provide my details, what can you say to someone superior? I won't tell you?*
>
> *I think I would that only if I knew the person* (even their name).

There were many respondents who said that in order to avoid divulging such important information they would use a number of ways to obtain some kind of confirmation about the caller's identity. There were a couple of respondents that were more negative about giving away such information and only one that looked certain about not divulging her login information. Some stated that they would ask the caller's number to call them back themselves or they would ask somebody else in their working environment or even ask the caller to come over himself to get the details:

> *I feel like giving away some information could be vital and important, so I may not give, I may ask some questions or ask to call back in a couple of minutes, so that I ask some other people that are working around.*
>
> *I don't think so. I would tell him I will be in the office in a while, I will give it to you myself or something, face to face I mean.*

2.6 Phishing

The interviewees were asked what they would do if they received a phishing email and also if they had any ideas about how they could tell if the email or the link or the website itself were legitimate. They were encouraged to share their thoughts in order to see if they possessed indeed the knowledge to spot a phishing attempt or at least a dodgy element that would prevent them from divulging their personal data. Some of the interviewees also talked about phishing emails they did actually receive but no one fall for them even if a couple of them almost did. Here are some of their thoughts:

> *I've never accepted any but I don't think I would know how to tell if it's legitimate so I would visit the website from the link.*
>
> *I would visit the website but on my own, not from the link.*

2.7 Sources for help

In order to evaluate at a small scale the advice shops offer when people buy their new computers the interviews were asked if they receive any advice when they bought their computers but none had. When it comes to if they felt they needed any at that time their answers differed. Some thought they did not and some others said they can always use some more information. Then the interviewees were asked who they turn to for help when they are facing a problem with their computer and 12/20 answered friends. However, one of those 12 answered that would also consult a relative, and three more would also visit websites. In addition three of those 12 would go to an expert if their problem insisted. Two of the rest answered they would ask for a relative's help only and two others mentioned a colleague from their IT department at work. As observed by their answers, there is a trust issue even with the professionals that solve problems with computers because users cannot judge for themselves if the price they pay for their services is fair or if they are being overcharged. Moreover, if they can avoid the whole procedure of finding the right person to fix it and then pay any price they will charge them, they prefer to ask friends who can always trust and rely on. After that the interviewees answered if they know about the websites that provide information about security topics and guidelines and they were given the example of Getsafeonline. From the 17 users that were asked this question, only two knew about their existence but have not visited them and four others stated they have used other websites like Microsoft's or AOL's. The respondents then were asked whether they would visit these websites if they knew their web addresses. Seven respondents replied that they would probably visit them with three rating free time as the only constraint. Additionally, four respondents explicitly expressed their refusal to visit these websites. Two of them said explicitly:

> *Because I don't care. I mean it's not that I had severe problems with viruses in the past, to be that afraid to look for information all day long.*

> *It's such a waste of time for me, it's a good thing though… but the thing is that I have a few friends in my circle, who are good in computers and if I ask them I know they are the best guides so there is no point.*

The interviewees were asked who they think is responsible for online security with 13 replying the end user is responsible too. It was really encouraging to hear that users think they have a share of the responsibility. Some respondents also mentioned companies and Internet or software providers and only 3 named the Government because they think the Internet is too wide, chaotic and shared across the world to be secured which is rather concerning.

2.8 The users' perception of their security knowledge

In order to assess the users' opinions about how much they know about security they were asked if they think they know enough about it. Eleven out of 20 answered that they do not know enough, seven answered that they do, although some were not very confident about it. Even the respondents that think they know enough are not blindly believing that they know everything. They are just happy with how things are so far, and they continue trying to be as cautious as they can, protecting their systems and their personal data. Here is what some of them said:

> *No I think I know a little it and I am aware enough not to give out passwords and usernames and give out too many like credit card details when I am not fully confident in what I am doing but I don't really know.*
>
> *I know preliminary stuff but at least I can secure myself.*

2.9 Impact of the Interview

A very important question was one of the last ones asked to the interviewee, whether the discussion informed them or changed their view in any way. It was expected that users, being novice, would think that the information provided in the interview, would be considered as a plus and could signal their quest for more information. However, only ten felt that it was informative, eight thought it was somewhat informative since it provided some definitions about threats or the reference to the websites and two thought it made no difference to them. Here are some of their opinions:

> *Yeah, it raises my awareness about what is there and how you have to be alert all the time, about how resourceful people can be in social engineering and in tricking you.*
>
> *Yes it made me think a little bit more about security on my computer.*
>
> *No, it's made me realize I am doing what I should be.*

3 Conclusions

Most of the respondents were aware of threats. Even though they did not know much about all of them, they knew that they could cause a lot of damage to their computers. However, none mentioned the probability of a loss of personal information. Still, if the user knows that there are a lot of risks it is more possible to protect more their system. That is why some of them, the ones that after the interview answered they were informed, decided to change some of their habits. If the user is uninformed and thus unaware, then they have a false sense of security that prevents them from protecting more their computer. During the interview, many respondents were keen on knowing more about the threats and listened carefully while these were being explained to them. Of course there were others that looked as if they did not care about knowing more and thought since they did not have so far any problems, they were alright with what they knew up until now. As it can be concluded from their answers, the respondents tend in general to avoid anything redundant because they want to cope with everything they have in their possession. Some of them would like to know more and act more but without having to search for themselves for information.

Regarding phishing emails the majority of the interviewees expressed even simple ideas on how to check the e-mail's genuineness which is really encouraging because as more people are getting aware of phishing, their checks will become more thorough and more demanding. Of course there were also users that would not check at all and they admitted it, even though the nature of the question encouraged them to think something and say it at that time. The interviewees did actually mention some important things that should be noticed but will they indeed think about them each time they go into their inboxes?

The fact that none of the interviewees received any advice when their purchased their computers is very concerning and should be the subject of a different research that will focus on the quantity and quality of the advice shops offer if they actually offer any. Shops could play a very important role in informing the users about the various threats and the risks associated with the use of computers and the Internet, as well as the ways of dealing with them. Overall, the interview provided some interesting findings that can be used to find the right way to approach the home users and help them in the difficult task of protecting their systems, themselves and thus, the other users. Especially them who are the most vulnerable since they are relying on their own power and actions to protect themselves. First of all they need to be educated, informed, alarmed and equipped with the right tools to ensure their computer's security. But the users have to understand why it is important to maintain their security and then what they should be careful about, what they should be afraid of and how they can achieve their protection.

4 References

Anti-Phishing Working Group (2006) "Phishing Activity Trend, Report for December 2006" http://www.websense.com/securitylabs/resource/PDF/apwg_report_december_2006.pdf (Accessed 26/07/2007)

Furnell, S. M., Bryant, P. and Phippen, A., D. (2007) "Assessing the security perceptions of Personal Internet Users" *Computers & Security*, Vol.26, Issue 5, p. 410-417

Furnell, S. M., Jusoh, A. and Katsabas, D. (2006) "The challenges of understanding and using security: A survey of end-users" *Computers & Security*, Vol. 26, Issue 1, p. 27-35

Granger, S. (2001) "Social Engineering Fundamentals, Part I: Hacker Tactics" Security Focus http://www.securityfocus.com/infocus/1527 (Accessed 24/05/2007)

Symantec, (2006) "Symantec Internet Security Threat Report- Trends for January 06-June 06" Volume X, Symantec Enterprise Security

Symantec, (2007) "Symantec Internet Security Threat Report- Trends for July-December 06" Volume XI, Symantec Enterprise Security