Internet Security: A View from ISPs and Retailers

R.Shams and S.M.Furnell

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

Abstract

This paper describes various the perceptions of internet security for home users from ISPs and Computer Retail stores in the UK. A research survey has been carried out focusing on selected largely subscribed ISPs in the UK and Computer Retailers in Plymouth and Exeter cities. The websites of the ISPs has been analyzed to measure the quality of information they offer with respect to various threats and vulnerabilities the home users are often posed to and also the information of security defense mechanisms the ISPs offer to home users to achieve optimum security. Computer Retailers were approached to measure the quality of IT Security information they offer to their everyday customers who are interested in buying personal computers and internet connections. It has been noticed from the past surveys that the users lack computer security application like Anti-virus, Firewall or Anti-spyware application which weakens the level of security on their home computers and personal information. This research work makes a sincere attempt to analyze the reasons for increase in cybercrime and decrease in the lack of user knowledge on information security. A set of brief media awareness suggestions for ISPs and Retailers has been offered which could perhaps help the home users to easily reach for information related to information security and cybercrime. The main goal of the research however, is to analyze the importance of the ISPs and Computer Retailers' role in making the home users aware of online security.

Keywords

Online Security, Home Users, ISP Surveys, In-Store Survey

1 Introduction

The Internet has become a powerful medium for effective communication, information transfer, online banking and shopping. The fact is that the Internet has made human life easier and simpler but another opposing fact is that it has become a nightmare for people who are not completely aware of its threats. Information exchanged between users over the Internet could get compromised without their knowledge. Securing personal information and computers is often not an easy task to achieve. Possible reasons could be that the users may not be able to understand the security concepts, unaware or cannot reach the security guidelines offered by various sources and may not be interested in investing money for defense mechanisms

2 Common Threats for Home Users

Home users are facing increasing threats in the form of hacking, phishing, viruses, worms, spam etc, which directly compromises confidentially, integrity and

availability. According to a survey conducted by British Computer Society, British citizens are becoming aware of the security threats and they are deploying security measures to protect their information and personal computers. 52% online shoppers are concerned about secure payments and 51% of the users prefer to shop from popular retailer websites which offers them confidence of being secure. Home users are also aware of antivirus and firewall applications to help protect their personal computers from internet threats. 63% per cent of British adults have access to the Internet and 58% of them use it as a medium for shopping and 43% for online banking facilities. 92% of home users consider security applications as safety measures which include antivirus and firewall software applications. These figures, however does not convey that all home users are completely aware of the internet threats.

3 Aims and Objectives

The main aims of this paper are (1) benchmark the existing home user's security measures (2) conduct a survey to investigate the user knowledge on internet security (3) investigate the sources for reliable security guidelines.

Specific objectives of the research are to:

- Analyze the way users reach for security guidelines.
- Analyze and evaluate the guidelines offered in consumer electronic stores.
- Develop a new approach so that the home users could easily reach the information security guidelines.

4 Approach Methods

The study involved two distinct data collection approaches, targeting different potential sources of advice to users. These are discussed in the sub-sections that follow.

4.1 In-Store Survey

Consumer electronic stores like Comet, PC World, Currys and Staples will be approached to respond to the survey questions. Since they are the first point of direct contact for people who buy personal computers, there is a good chance of learning about the way they make the buyers aware of security aspects and defense mechanisms.

4.2 ISP Survey

ISPs, quite similarly to consumer electronic stores, play an important role and form a first point of contact for users who are willing to sign-up for Internet connections. Some of the leading ISPs in the UK were called to check the level of their knowledge with respect to Internet Security and the security mechanism they offer for home users. The list of ISPs that are questioned will be kept disguised throughout the analysis of this research.

5 Internet Security: The ISP Perspective

Internet Service Providers will be the first point of contact for home users who sign-up for internet connections and they play an important role in making the users aware of the internet threats and also about the defending mechanisms against the threats. Most ISPs in Britain have dedicated an area on their websites where users will be able to find information about threats and the ways to defend. How the users are made aware of these defending mechanism plays an important role.

ISPs have two strong sources of making home users aware of various Internet threats that the users are often targeted with. The first source is their website and the second one being the technical support they offer over telephone.

6 The role of ISPs

ISP websites offer ample amount of information on security guidelines and the Internet threats they should be aware of. Apart from educating users with security mechanisms like Antivirus, Anti-Spyware, Spam and Firewall, most ISP websites offer hyperlinks to other reliable resources for online security guidelines like GetSafe, Symantec and Microsoft where users will be understand detailed security mechanism that they could deploy to secure their personal information and computers. Apart from educating users, ISPs also offer security mechanisms from their end in both basic and advanced level. In most cases, users will have to spend extra money in order to attach additional security to their subscription. Having said that, this paper would like to present home users security related web pages from some of the leading ISPs in the UK. This research considers a few top rated ISPs with respect to the number of subscribers but not necessarily all the leading top ISPs.

ISP	Free Security Application	Online Help	Virus/ Worms	Phishing	Spyware
Virgin Mobile	PC Guard	✓	✓	✓	✓
Tiscali Broadband	Norton	✓	✓	✓	✓
AOL, UK	McAfee & SpyZapper	✓	✓	×	✓
BT Broadband	Norton	✓	✓	✓	✓
Sky Broadband	McAfee	×	✓	✓	✓
Talk Talk	F-Secure Trial	×	✓	×	✓
Orange	McAfee Privacy Service	×	✓	✓	✓
Vodafone	Norton Security Suite	✓	×	×	✓
O2 Broadband	McAfee Suite	×	×	×	✓

Table 1: Broad comparison between security features on ISPs' websites.

A good comparison between different ISPs can be done taking into consideration the security information and protection they offer. Other popular ISPs include British Telecom, AOL (UK), SKY Broadband, TalkTalk etc. A summary of such details is presented in Table 1.

This paper, earlier had mentioned about the two methods the ISPs deploy in order to promote security measures. The first method was through their website and the second was through the Technical Support they offer over phone for their customers.

This research work approached 6 of the leading ISPs call centers in the UK to analyze the nature of security mechanisms information they offer over the phone. Each ISP was called three to four times during different times of the day to gather few answers for the survey questions. The whole idea behind this was to gauge the level of security awareness that the ISP call centers have and also the security mechanism they offer. The research voids disclosing the names of the 6 ISPs that are surveyed.

6.1 Survey Results

Eighteen responses from ISP Advisors (conducted in 6 ISPs, 3 times each) is the reply to the common threats that the home users should be worried about and taken care of.

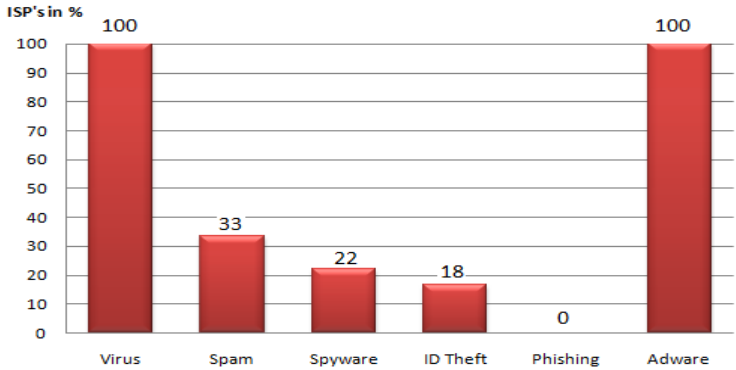

Figure 1: Security Threats the home users should be concerned about.

According to ISPs, the major threat the home users should be worried about is viruses. Spyware and Spam are a concern to some extent where as ID Theft, Phishing and Adware threats are least considered. This could be because the advisors in ISPs were not aware of these threats by themselves which potentially brings down the percentage of home users who are being led into the proper direction of gaining optimum security.

Figure 1 shows the number if ISP advisors in percentage and the knowledge they were aware of about each of the security threat. All advisors were aware viruses and the defense mechanism against them. 33% of the 18 advisors from 6 ISPs knew about Spam. Spyware information was clearly given only by 22% of advisors and the rest had confused with Antivirus application as a security mechanism against spyware. 18% of the advisors suggested to call the ISPs and report ID Theft activity to them. No clear information was offered about what they are going to do once the user reports it. However, a general information that they will utilize the information to analyze the website where ID theft is supposedly to be happening. Shockingly, none of the advisors knew what phishing was let alone an effective defense mechanism for it. But somehow, users are guided to use Antivirus application in order to prevent phishing attacks. Adware was widely considered as pop-up's from

the web sites and the advisors were aware of the fact that pop-up blocker application would reduce adware being thrown up to the users.

Another important fact that was noticed from the survey is that most advisors in the ISP are confused with anti-spyware and antivirus applications. Below are the summarized details from the outcome of the ISP survey results.

Threat	Description
Virus	Generally advisors are aware of the virus and the threats caused by viruses. This helps home users to implement a basic security mechanism like Antivirus and Firewall applications.
Spyware	Mostly advisors confuse spyware with antivirus. Instead of offering complete Anti-spyware software they offer antivirus and firewall as a solution. This perhaps is not the optimum security a home user should be expecting as the aftermath due to each threat varies a lot.
Adware	Generally advisors have good understanding of adware that it pop-ups unwanted windows and steal personal information for marketing purpose. Advisors often recommend installing a popup blocker application in order to prevent unwanted pop-up's from annoying the users.
Phishing	Home users are advised antivirus as the solution for phishing. Phishing, a relatively new method of stealing personal information is completely misunderstood by the ISP advisors and they are unaware of the fact that an Antivirus application could solve the security vulnerability.
ID Theft	Mostly antivirus and firewalls are proposed as a solution for ID Theft. ID theft relates to phishing attacks for which Antivirus and Firewall applications are not the end solution.
Spam	Most advisors are fairly clear about spam whether it's in the form of email or spam websites.

Table 2: Out come of ISP Survey Results

All the ISPs are very glad to inform about the technical support they offer for various security related questions the home users may have.

The center of gravity is no longer associated with viruses but other major threats like Phishing and ID theft have to be considered as an important issue to be taken care of. Security awareness about these threats including botware and PDF spam should be addressed by ISP and so should the users be made aware of

7 Internet Security: Retail Stores' Perspectives

The paper earlier had mentioned about the two main first point of contact for home user's broadband internet connections as ISPs and computer retailers. ISPs however, have failed to be responsible to educate or make users aware of various threats that the users confront with the broadband connections. This is apparent from the survey that was conducted as a part of this research and also from the past surveys that were conducted by other sources.

Computer Retailers will play an important role in this as every customer could spend a good time in the store learning about the defense mechanisms they could be deploying in order to achieve the best possible level of security. Home users who

make personal computer/laptop purchase will also get a chance to look in to security related applications that are presented in the store.

Five of the following popular retailers in and around the town were approached to participate in this survey as they are the most easily accessible stores for users who plan to buy personal computers and hence were selected.

8 Knowledge on security aspects

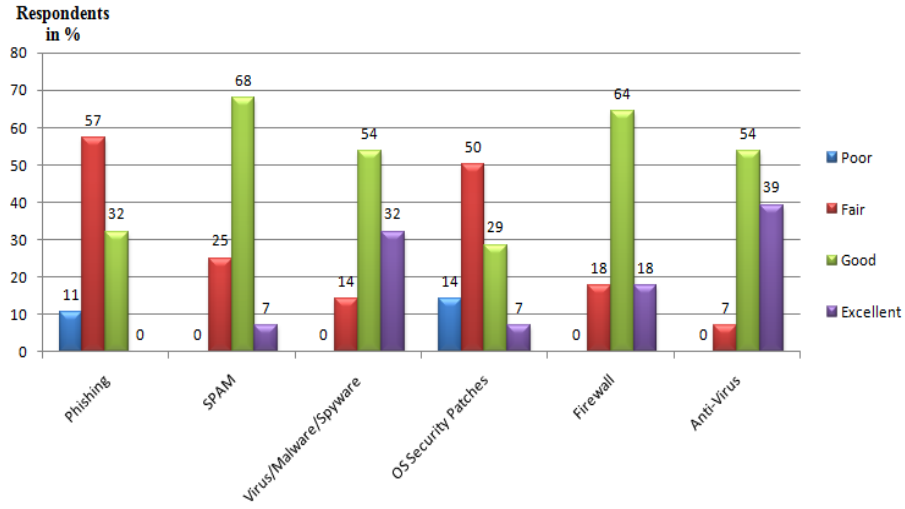

Figure 2: Knowledge on Security Aspects of Store Advisors.

Figure 2 depicts the knowledge level the retail store advisors have on various security aspects like Phishing, spam, virus/malware/spyware, OS security patches, Firewall and Antivirus applications. It is apparent from this chart that 68% of 28 advisors had a good knowledge about Virus/Malware/Spyware, Firewall and Spam and only 53% of them had good knowledge on Antivirus application. However, 54% of them had an excellent knowledge about Antivirus application. Phishing, not surprisingly, 57% of the advisors had fair knowledge and only 10% of them just knew about it. These figures are scarily low as these advisors are meant to educate their customers who whether or not willing to buy a personal computer and/or internet connection from the store.

8.1 Security mechanisms discussed with users

In response to the type of security threat the advisors make the users aware of, 90% of the advisors educate the home users on the advantages they get if they you Antivirus application. 54% and 40% of the advisors offer information about Anti-spam and Firewall applications respectively. Only 7% and 10% of them contribute in making the users aware of ID theft and Phishing activities.

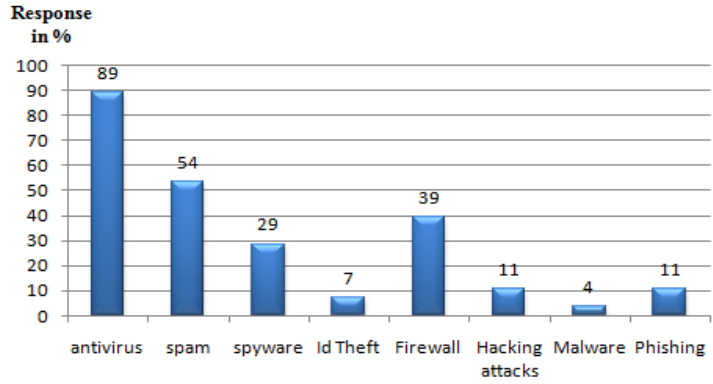

Figure 3: Security Applications discussed with home users.

The Internet, as mentioned earlier throughout this paper, is not safe anymore for home broadband users if there are no proper security defense systems. The usage of security applications like Antivirus, Firewall and Anti-Spyware proves to be very important which is apparent from the various surveys conducted earlier. Home users are aware of security applications to some extent but they have to master the area of total security in order to reduce the crime that originates from the Internet.

9 Recommendations

The fact that the users did not receive any security related information could not be completely pointed out at ISPs. There is plenty of information from reliable sources that the users are not aware of. Media presentation and awareness methods could be the main reason that the home users are not able to cope up with the security demands. If ISPs are not aware of themselves which is apparent from the research work done for this project work, would retail stores from where users purchase personal computers from contribute their help? This is discussed in the following chapter in detail. Possible recommendations for ISPs to enhance the existing security awareness mechanism would include but not limited to:

- → Offering an expert dedicated Internet Security Support team.
- → Design their website to prioritize Internet Security and offer ample amount of information on threats and protection mechanisms.
- → Offering a prompt to learn the latest trends on cybercrime like phishing and ID theft on their IVR Systems.
- → Offering security newsletters and flash news related to cybercrime on their websites.
- → Offering online tools to check the home user computer's vulnerabilities towards various threats.
- → Offering interactive tutorials on security mechanisms targeting novice to expert users.

The above survey summarizes into the fact that both retail advisors and home users are completely unaware of the modern day threats specifically with phishing.

Representatives in retail stores must have a good understanding on various threats and possible ways to fight against them. Home users also have an impression that the security applications which are the most important defense mechanism are expensive. There are plenty of reliable sources for home users to learn and educate themselves with the various internet threats and also the guidelines to safeguard their home computers and personal information. But, most the users are not able to reach those resources. Retailers should not only be a computer selling medium but also act as a medium to make home users aware of the threats and defense techniques against cybercrime. They must implement effective media awareness methods and a few recommendations are to:

- → Offer brochures/booklets like the Virgin Media's "Play Safe: Internet safety made easy" which has all the necessary information the users need to learn about cybercrime and the ways they could protect themselves against it.
- → An Information Security expert in each store who could explain the technical terms/jargons to every user, make them understand the importance of security and most importantly convince them to use security applications.
- → Instead of displaying "Ice Age" or "National Treasure" on the HD TV in the stores, projecting useful information on information security could be an effective way to enhance media awareness.

10 Conclusion

The Internet, as mentioned earlier throughout this paper, is not safe anymore for home broadband users if there are no proper security defense systems. The usage of security applications like Antivirus, Firewall and Anti-Spyware proves to be very important which is apparent from the various surveys conducted earlier. Home users are aware of security applications to some extent but they have to master the area of total security in order to reduce the crime that originates from the Internet.

ISPs and retail stores were presumed to play an important role in spreading the awareness which eventually is a wrong assumption according to the survey results. In a search conducted in the year 2005, home users think that ISPs should take of the entire security for the internet connections they are subscribing and about 60% of the survey respondents were willing to spend a few extra pounds to having their information and computers secured. ISPs with some extra money from the customers can only offer affordable or free security applications to the users but how about the guidelines about threats and vulnerabilities? As analyzed in this research, some ISPs consider spreading the awareness through their websites but not all them consider media awareness techniques which are aimed at educating the home users. There is a similar situation with the retail stores too. They are selling security applications in their stores but offering a free booklet or brochure that contains the information about internet threats, prevention and protection techniques could help the users educate themselves. Just giving away for free or selling a few security applications does not necessarily mean that the users are completely aware of all the threats. Usability in security applications have a considerable affect on encouraging the user in deploying them. Human computer interaction with these security applications proves to be a vital concept. Human computer interaction is defined as *"the past of a user interface which is responsible for establishing the common ground between a*

user and the security features of a system". Security application designers must consider easy to understand interfaces in their applications so that even a novice user should be able to install and manage them. According to Whitten, a security application incorporates a good usability if:

- → It educates the user with the security task that they have to perform.
- → It includes easy guide to achieve the mentioned tasks.
- → It has a easy to understand and comfortable interface and
- → It does not show error messages that are strange to the users.

Usable security applications that are affordable to home users would have great impact to achieving optimum security there by achieving the goal "Every users is safe user".

11 References

British Crime Survey, (2003). *"Fraud and technology Crimes"*, http://uk.sitestat.com/homeoffice/homeoffice/s?rds.rdsolr3405pdf&ns_type=pdf&ns_url=%5Bhttp://www.homeoffice.gov.uk/rds/pdfs05/rdsolr3405.pdf%5D

Browse the Web Safely, Symantec Corporation. http://www.symantec.com/norton/security_response/browsewebsafely.jsp

Getsafeonline, (2007). *"10-minute guide for beginners"*, http://www.getsafeonline.org/nqcontent.cfm?a_id=1179

Johnston J, Eloff J H P and Labuschagne L. (2003), *"Security and Human Computer Interfaces"*, Computers and Security Journal, Vol 22, No 8.

Microsoft Corporation. Security at home,. http://www.microsoft.com/protect/default.mspx

Virgin Broadband Handy Booklet on Online Safety, http://allyours.virginmedia.com/websales/service.do?id=2

Whitten A. and Tygar J.D. (1998), *"Usability of Security: A Case Study"*, Carnegie Mellon University, USA. http://reports-archive.adm.cs.cmu.edu/anon/1998/CMU-CS-98-155.pdf