Internet User's Awareness and Understanding of Spyware and Anti-Spyware

M.Alshamrani and S.M.Furnell

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

Abstract

Spyware represents one of the main Internet threats. It can secretly compromise and control the devices and the personal data of the individual user or the organization without their knowledge. This research paper examines the level of awareness for Internet users about Spyware threats and Anti-spyware protection services. An online survey was designed and published, with 225 respondents with different backgrounds and experience participating. From the analysed results, the study found that there is a significant lack of awareness amongst Internet users about Spyware threats and Anti-spyware protection services, while the number of Spyware attacks has increased. A quarter of participants had no idea about Spyware threats at all. At least 40% have been attacked by Spyware, and 32% of the respondents do not understand how to use Anti-spyware or the protection system in their PCs. The research found that the lack of training was the main reason for the lack of awareness about Spyware threats and Anti-spyware protection services. Only 31% of the respondents had attended a course or training session about computer security. The trained participants in general are the most aware and protected group of respondents regarding to Spyware threats. However, the study showed that the training sessions are not focusing on or giving sufficient information about Spyware and Anti-spyware. Only 25% of the aware participants received some information about Spyware and Anti-spyware from the training sessions they received from their organizations.

Keywords

Spyware, Anti-spyware, Software, Spyware Training, Information Security

1 Introduction

Spyware represents one of the most significant security threats for individual users and organizational networks. Spyware is a software program which can compromise the covert and the overt of the confidential and non-confidential information from the Internet users' PCs and/or networks (Dinev and Hu, 2007). These programs have the ability to hide in the background on victim's systems or move through the Internet or local networks. Other types of spyware are remotely controlled and directed by its creator commands (Thomson *et al.,* 2006). Spyware can efficiently attack Internet user's privacy by data collecting, system controlling, and/or actions reporting of victims PCs and networks (Cordes, 2005).

While Internet user's awareness of the general Internet threats has been increased over the years, they are still not doing enough to protect themselves, often due to a

false sense of security. An increased number of online attacks have been reported since 1998, which caused huge financial losses estimated to hundreds of millions American dollars in the U.S. which infected companies, organisations, and some governmental agencies, where the worldwide estimated losses were much more (Cavusoglu et al., 2004).

Internet users are targeted by a number of threats that intent to get an unauthorized access to their private and critical data or trying to compromise their system privacy where their systems are often not well protected. Awareness is defined as the extent to which a target population is conscious of an innovation and formulates a general perception of what it entails (Schmidt et al, 2008). Moreover, the number of users of this technology had been increased, which give the above research result an important part for Internet security resolving and improvement.

At the present time, the Internet is joining users from many communities and with different knowledge, experience, background, gender, and ages. These factors have direct effects on the Internet user's attitudes, behaviour, awareness, and reactions against Information security (Furnell, 2008; Dinev and Hu, 2007). The importance of information security and the related awareness of Internet users are the major motivation of this research study. In order to accomplish this, researchers need to have a comprehensive understanding about how Internet user's awareness of Spyware and Anti-spyware have been measured and what level of awareness they have. This study contributes by including some basic aspects about Spyware awareness that have not been investigated yet. The main aims and objectives of this research paper are to demonstrate the actual level of user awareness of spyware and Anti-spyware. This will help to improve the security level against spyware threats by giving the interested security researches and providers a clear realization of Internet user's awareness and practices. In addition, this paper aims to prove the reality of spyware threats in terms of knowledge and practical actions depending on some stated results of some previous research studies.

2 Background

The gradually increasing studies and articles about spyware and the information security awareness are reflecting the massive and the widely distributed threats that spyware could cause. In terms of examining Internet users' spyware awareness, while there is only a limited amount of academic research and other reports, some relevant research has been done.

In the investigation of Internet consumers' awareness about spyware, Zhang (2005) found that the general comprehension and understanding about security, confidentiality, and Spyware are lacking. Moreover, the privacy attacks are not sufficiently noticed by the users, with respondents having limited knowledge about using Spyware removal tools. This research was one of the earliest studies examining Internet users' awareness and its direct relation with spyware threats. Later, Poston et al. (2005) stated that general PC users are aware about security threats in general. However, they are not prompted to react with protecting their systems by using anti-spyware protection system. Schmidt and Arnett (2005) reported that 94% of PC users

know about Spyware threats, while 61% had discovered incidences of spyware infection in their systems.

Freeman and Urbaczewski (2005) provided considerations of the damaging effects of spyware and investigated why people hate Spyware. In addition, the study reported that users' privacy and service performance are very important concerns. Furthermore, the report mentions that Internet users presume that governments and IT industries are responsible about controlling and defending them from spyware threats. In addition, the results showed that most of the respondents felt that they are not having to be responsible about protecting themselves. However, there are different points of views about the awareness and who is really responsible, where users, vendors, governments, organizations, or industries are all have to share within this mission.

Awad, and Fitzgerald (2005) investigated the Internet users' negative thoughts about Internet security. They showed four illusory behaviours were appreciably related to the this feeling: the variable nature of PC system settings, slowing and crashing of the system, installing un-approval protection system, and spyware downloads.

Kucera et al. (2005) reported about the presence of spyware in many of the popular freeware and shareware that may download from Internet websites. Once it downloaded, it has been found that this software has the ability to gather various forms of victims' personal information.

Meanwhile, Lee and Kozar (2005) identified 3 types of factors that had significant impacts upon Internet users' adoption of anti-spyware protection. Firstly, they determined two user attitude factors; namely users' compatible morals and relative advantages of anti-spyware usages. Secondly, they determined two social influence factors; namely the visibility and image of Spyware threats. Finally, they stated two behavioural control factors; computing capacity and the ability to test/try the protection product.

Dinev and Hu (2007) studied the main factors that effect users' actions against spyware threats. They concluded with four main determination factors driven from their research study results: Users' awareness of spyware, and the perceiving of the usefulness, the controllability, and the simplicity of use.

Another important result related directly with the research area, Jaeger and Clarke (2006) formed a survey that examined the level of awareness and understanding of home PC users to spyware threats. They found that the majority of home users understand about spyware. However, they found a lack of understanding of the needed protection system to securing their PCs against spyware threats. The survey showed that about 20% of 205 respondents are not using any Anti-spyware system. In addition, the research found that respondents are considering spyware as a "High/Some Threat" where 72% of the respondents had changed their browsing habits and accessing behaviour due to pervious expert, infections, and media/news articles.

A research study by Sipior and Ward (2008) investigated the perceptions of users related to considerations of trust, privacy, and legal protection in using application software that containing embedded spyware. The study reveals further results about the direct influences of the overall trust of a software vendor according to the examination of trustworthiness. The research stated three important factors that affect the software vendor trustworthiness; multi-dimensional construct, reveals trustworthiness-integrity, and trustworthiness-ability. The research results are providing software vendors and regulatory agencies of governments a useful guidance and recommendations in indicating the related concerns of Spyware.

3 Methodology

In order to accomplish the research aims, there are different methods that can be taken on. For instance, the research can interview a group of Internet users, monitoring their practices, and recording their information. However, these methods might not be very effective for the research approach. The personal interview by the researcher with the respondents is very difficult, as it is time consuming and requires a lot of effort to reach the targeted participants in different countries, locations, and with different backgrounds. In addition, it provides limited numbers of respondents for monitoring their practices and recording their feedback. The online survey uses an anonymous way of collecting the data, which encourages the respondents to participate in the survey and give more truthful answers. Nevertheless, the study needs to investigate Internet users who are involved with the research topic which needs to find respondents who are using the Internet service. Thus, the best method that helps to reach different users in different places is by conducting a survey and publishing it by using the online survey.

Such a survey is a cost effective method as it does not require printed papers to be distributed with to target respondents. It can also provide the researcher qualitative, quantitative, and very productive analysis approaches. It helps the researcher to display, retrieve, represent, and modify the collected data of the survey.

The main objectives of this survey were to investigate the Internet user' consciousness and understanding about spyware threats and anti-spyware services. In addition, the research investigated aspects of respondents' wider practices around Internet usage and information security.

4 Results

The group of participants (totalling 225 respondents) gave high reliability to the results of the online survey (See Figure 1, 2 and 3). The participants been invited through the invitation emails and the educational portal of the University of Plymouth. A notable finding is the lack of attendance for computer security training sessions (See Figure 4). Also, the security topics of the attended training sessions or courses were very general in terms of informative and practical contents. Some of the trained participants are still suffering from different Internet attacks, as well as unawareness of the important threats and security tools. The survey showed that the trained participants in general are the most aware and protected group of respondents

regarding to spyware threats. However, the study showed that the training sessions are not focusing or giving sufficient information about spyware and anti-spyware. Only 25% of the aware participants received some information about spyware from the training sessions they received from their organizations.

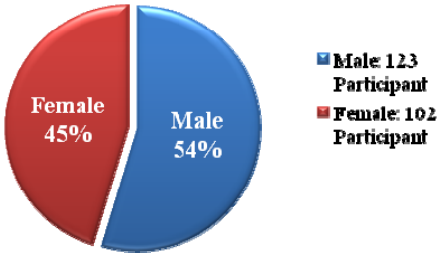

Figure 1: Gender balance of respondents (n=225)

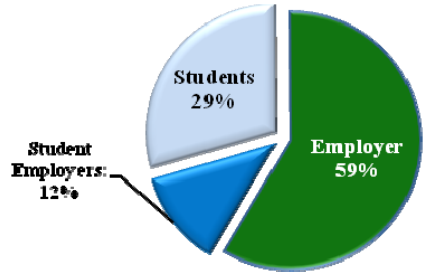

Figure 2: Current employment and/or student status

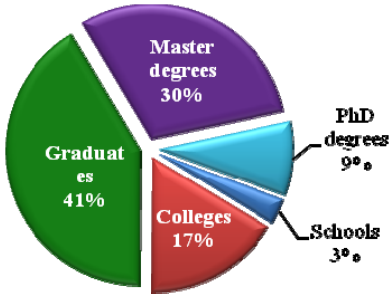

Figure 3: Level of education

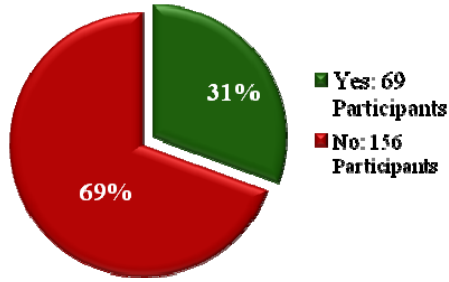

Figure 4: Attendance for any computer security course or training session

The findings have shown that the number of Internet attacks is significant (see Figure 5) and the level of awareness of the average Internet user is still a concern. However, the majority of the Internet users have shown real interest in attending training sessions and receiving instructions about Internet security in general and spyware in particular. Some organizations are providing their users effective protection tools but the training and awareness side is still poor and very limited.

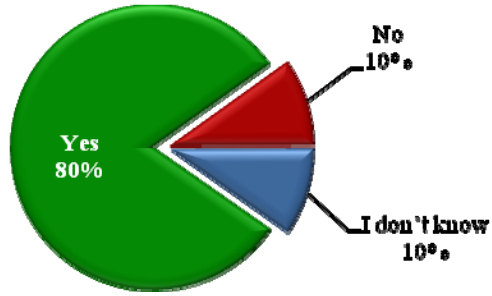

Figure 5: Experience of being attacked through the Internet

The research investigations showed that at least 2 from every 5 respondents have been attacked by spyware (see Figure 6), which represents a high number of attacks. In terms of awareness, 72% of the participants mentioned they knew about spyware threats and malicious activities while 28% of them did not. This result shows that for every four participants, there is at least one participant that had no idea about spyware at all (see Figure 7).

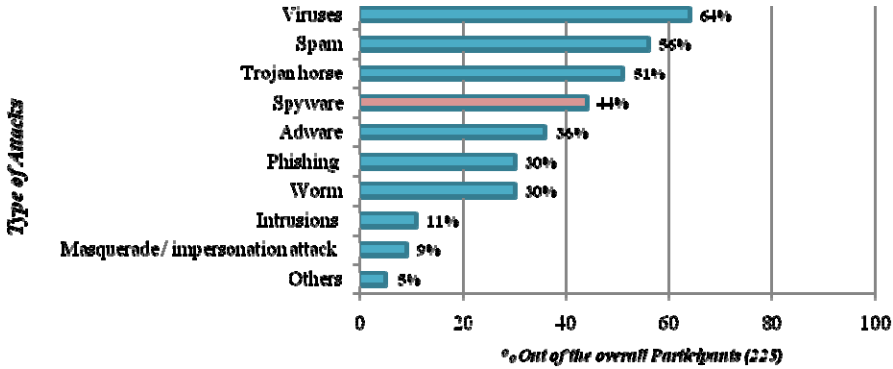

Figure 6: The type of attack that participants had experienced

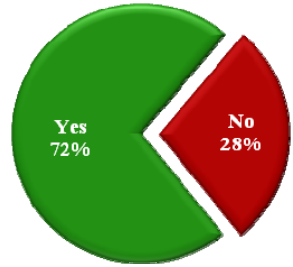

Figure 7: Knowledge about the malicious activities and threats of spyware

Regarding the participants' considerations of protecting, preventing, and cleaning their computer from spyware, the vast majority (79%) mentioned it is a very important issue (see Figure 8). While 18% of the respondents are feeling that spyware is representing a low or middle importance security issue. Further analysis revealed that most of those 18% did not attend any computer security course or training session while the majority of them had been attacked at least one time through the Internet.

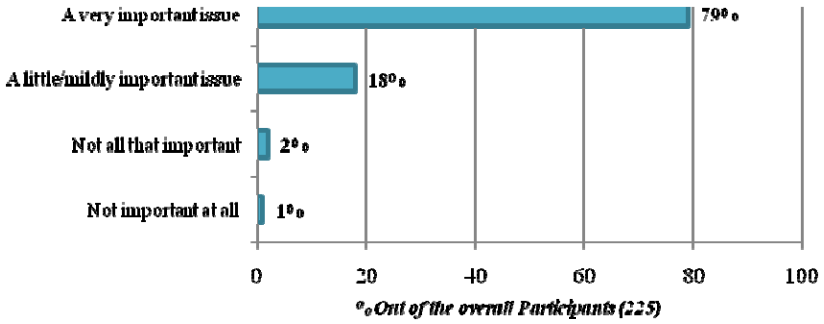

Figure 8: Importants of protecting, preventing and cleaning their PCs from spyware

The majority of Internet users depend on their antivirus systems for protecting themselves against spyware threats, whereas (68%) indicated that they are using specific anti-spyware (see Figure 9). It would seem from the results that a large proportion of these users cannot differentiate between viruses and spyware and between anti-virus and anti-spyware..

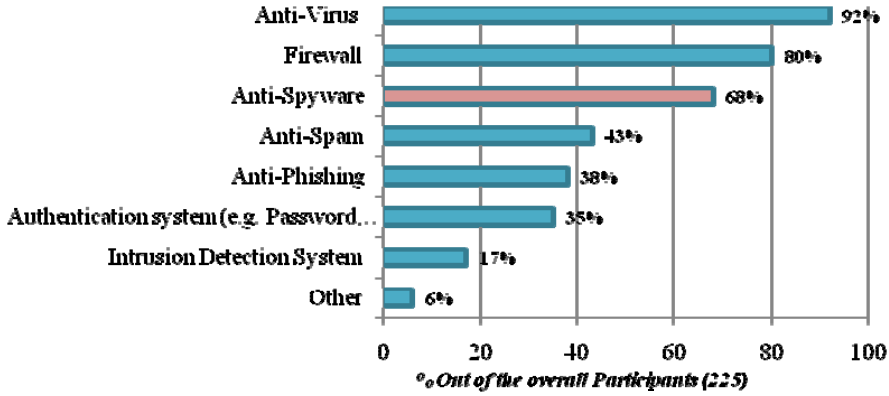

Figure 9: The protection that participants are using for their PCs

5 Conclusion

The findings of this research study provide some useful further information for this area of security interest. The increased number of spyware attacks and the lack of

user awareness about the threats and related protection were the main findings of the research study. Users' awareness in these areas is still very poor and they need to take more efficient steps to enhance their knowledge. The main cause was the lack of efficient training. The trained participants in general are the most aware and protected group of respondents regarding spyware threats. Nonetheless, the investigations still showed that some of the training sessions had not included any sufficient information about spyware threats and protection. Also, the educational courses of computer security had shown some derelictions for its awareness mission about computer and Internet security in general, and spyware threats and Anti-spyware awareness in particular. The Internet users' investigations had shown a good level of acceptance to know about the common Internet threats and the usages of the protection software by attending training sessions or by receiving information on the topic.

The organizations showed a good level of interest of supporting its staff and members with the protection tools and services. However, the training efforts are not sufficient and need to provide more effective training for their group of users. This training should give the attendant information about the common security threats. The training should also give practical advice for using the protection software, such as the ways of updating it, fixing and modifying the protection settings, use of the self-support options, etc.

The protection software usability and price were amongst the main barriers that prevented some of the Internet users from adopting them, while other users are using freeware and unlicensed products. Most of the licensed products that individuals use are related to organizations that provide them with the licensed protection services. The vendors need to offer a more efficient, usable, and informative awareness system about spyware and other common threats. Including such awareness-raising within the protection software will give users more ability to improve their awareness about spyware threats and anti-spyware protection services corresponding to the level of protection that they receive.

6 References

Awad, N.F. and Fitzgerald, K. (2005). "The Deceptive Behaviors that Offend Us Most about Spyware" *Communications of the ACM*, 48(8): 55-60.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). "A model for evaluating IT security investments". Communications of the ACM, 47(7).

Poston, R., Stafford, T.F., Hennington, A. 2005. "Spyware: A View from the (Online) Street" *Communications of the ACM*, 48(8): 96-99.

Cordes, C.S,. (2005) "Monsters in the Closet: Spyware Awareness and Prevention". EDUCAUSE Quarterly Magazine, Volume 28, Number 2, 2005.

Davis, F.D. (1989). "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, 13(3): 319-340.

Delio, M. (2004). "Spyware on my machine? So what?" Wired News, December 06, 2004.

Dinev, and Hu, Qing. (2007) “The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies”. Journal of the Associaton for Information Systems (JAIS),Volume 8, Article 2, pp. 386-408, July 2007.

Freeman, L.A. and Urbaczewski, A. (2005). “Why Do People Hate Spyware?”. Communications of the ACM. August 2005/Vol. **48**(8): 50-53 .

Furnell, S., Gennattou, M. and Dowland, P. (2002). ”*A prototype tool for information security awareness and training*”. Logistics Information Management. Vol.15 No.5/6 pp.352.

Furnell. S, Tsaganidi, V. and Phippen, A. (2008). “Security beliefs and barriers for novice Internet users", *Computers & Security* **27**(7-8): 235-240.

Hu, Q. and T. Dinev, (2005). “Is Spyware an Internet Nuisance or Public Menace?” *Communications of the ACM*, 48(8): 61-66.

Jaeger, M. and Clarke, N. (2006).” The Awareness and Perception of Spyware amongst Home PC Computer Users”. SCISSEC

Lee, Y. and Kozar, K.A. 2005. “Investigating Factors Affecting the Adoption of Anti-Spyware Systems,” *Communications of the ACM*, 48(8): 72-77.

Mazliza, O. and Rodziah, L. (2006). "Women in computer science: no shortage here!" Commun. ACM 49(3): 111-114.

Schmidt, M.B. and Arnett, K.P. (2005). “Spyware: A Little Knowledge is a Wonderful Thing” Communications of the ACM, 48(8): 67-70.

Schmidt, MB.; Johnston, A.C., Arnett, K.P., Chen, J.Q. and Li, S. (2008). “A Cross-Cultural Comparison of U.S. and Chinese Computer Security Awareness” September 03, 2008, IGI Global Magazine for IT professionals.

Sipior, J.C. and Ward, B. (2008) “User perceptions of software with embedded spyware” Journal of Enterprise Information Management, Vol.21, No.1, pp: 13-23.

Thomson, K. Von Solms, R. Louw, L. (2006). ” Cultivating an organizational information security culture”. Computer Fraud & Security. Vol. 2006, Issue 10,Pages 7-11.

Zhang, X. (2005). “What Do Consumers Really Know about Spyware?” Communications of the ACM, 48(8): 44-48.