Security and Privacy Related Online Behavior of Experienced ICT Users

Tihomir Orehovački, Mario Konecki, Goran Bubaš
Faculty of Organization and Informatics, Croatia
{tihomir.orehovacki | mario.konecki | goran.bubas}@foi.hr

Abstract
The increase in the number and variety of potential security and privacy threats puts emphasis on the behaviors of Internet users regarding their use of computer systems and the Internet. The assumptions and habits of Internet users have a great influence on the level of their online privacy and security. The identification of typical behaviors which represent a threat to online security and privacy may help in user education and design of warning systems and applications for protection from malicious software. In our survey the data were collected from 312 college students with good knowledge of information technology and with experience in the use of the Internet. The responses of the subjects revealed that most of them regularly updated their operating systems and antivirus software on their computers. However, a substantial percent of the respondents in the survey tended to perform potentially risky or careless online activities like file sharing, visits to "untrustworthy" web pages and alike. Results indicate that, even though there are diverse factors which influence the occurrence of malware/spyware infections on personal computers, the risky and careless behaviors of Internet users could be among the main causes of security and privacy problems of experienced ICT users.

Keywords: privacy, security, Internet, user behavior, survey data, end user threats

1 Introduction

Over the past few years, Internet users have been exposed to a growing number of security and privacy threats and this makes the use of protection mechanisms for computer systems increasingly important. Computers connected to Internet are under potential threat from viruses, worms, Trojans and other types of malicious code. Computer and network attacks are not only increasing in number, but also in sophistication (Hansman and Hunt, 2005). The complexity and poor design of computer systems and user software are some of the causes of vulnerabilities which enable computer and network attacks. According to Computer Emergency Response Team Coordination Center (CERT, 2007) there were 7.236 new vulnerabilities reported in 2007 and the total number of cataloged vulnerabilities is now 38.016 (see Figure 1.). In the first six months of 2007, Symantec observed 212.101 new malicious code threats which is an increase of alarming 185% in comparison with the previous observation period (Symantec, 2007).

There is much advertising regarding computer security and users are often warned about potential threats. However, even though users agree that keeping their computer systems is important, the McAfee-NCSA Online Safety Study (McAfee-NCSA, 2007) has revealed that the assumptions of Internet users regarding their security and privacy do not correspond with the actual condition on their computers. In this study the computer systems of users were

scanned and the results indicated that 54% of users had at least one computer virus or other type of malicious code on their computer. Also, even though 73% of users thought that they had a firewall installed on their computer, only 64% of users actually had a firewall enabled on their computer. Furthermore, 92% of participants in this study said that the anti-virus software on their computer was up to date, but a detailed inspection of computers revealed that only 51% of users had anti-virus program updated within the last week. Finally, 70% of participants stated that they had anti-spyware software on their computer, but only 55% actually had it installed.

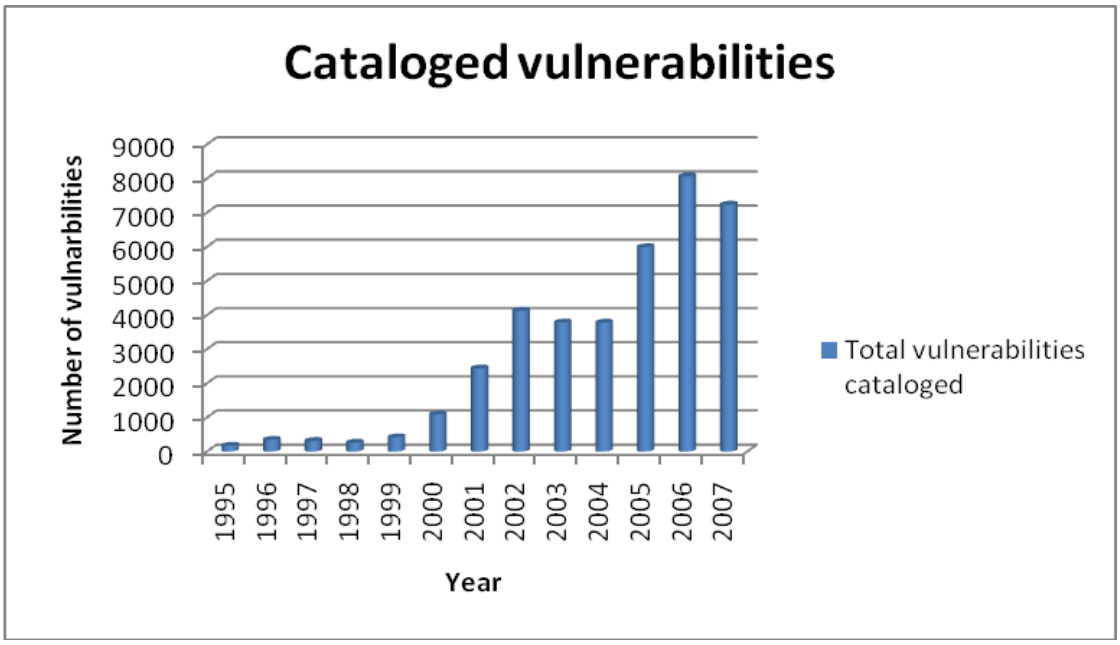

Figure 1: CERT/CC cataloged vulnerabilities of computer systems

Many studies have shown that regardless of the increasing number of security and privacy threats, usage and update of anti-malicious software is not sufficiently present on the computer systems if users. In this paper we will present the results of a survey-based investigation, conducted with the aim of assessing security and privacy behaviors of experienced ICT users.

2 Online security and privacy

In the recent years, Internet has become one of the most powerful sources of information and an important communication and collaboration tool which is widely used in our everyday lives. Even though the Internet enables people to share business ideas, buy goods and services, browse facts, communicate with others worldwide, and perform diverse other activities, it can also be misused for largely undetected data and identity thefts and that makes Internet security and privacy global problems and issues of general concern (Chung and Paynter, 2002).

2.1 Security and privacy related Internet threats

Internet threats can be found in many forms and there are lots of different ways they can infringe users' security and privacy. These types of threats can be categorized in four different groups:

- ***Cookies*** are special type of data that is stored on computer hard drive of web users that are intended to make easier the interaction of the user with the website. However, cookies can be used for tracking of the visitors of web sites and this information can sometimes be linked to personally identifiable information and later sold to and/or reused by unknown parties without the user's knowledge and/or approval (Kierkegaard, 2005). Although cookies are generally placed on the computer hard drive of the user without the users permission, they are voluntarily accepted when the site visitor downloads free applications such as screensavers etc. (Lavin, 2006).
- ***Malware*** is a common term related to parasitic software attacks including viruses, worms and Trojans (for more information see: Kjaerland, 2006). There are many means and routes by which malware can enter and infect the users computer, but the most common are by opening fake e-mail attachments and using peer-to-peer networks.
- ***Password attacks*** are conducted by manual guessing of password or attempting to break into the users account by trying all possible passwords (so-called "dictionary attacks"; Pinkas and Sander, 2002). When users generate passwords they often make two types of mistakes. First, if they generate passwords which are easy to remember, their passwords are an easy target for password attackers who use manual guessing or "dictionary attacks". On the other hand, if users generate passwords that are generally difficult to remember and thus difficult to break, they often make a mistake by storing it in place which is potentially available to an attacker.
- ***Spyware*** refers to malicious software that invades the user's privacy by tracing the victims computer activity and stealing gathered information for some third party (Warkentin et al., 2005). The most common spyware types are adware, browser changer, browser plug-in, bundleware, dialer and keylogger (for more information see: Shukla and Nah, 2005). Spyware infections are most frequent when the user visits "untrustworthy" web sites or engages in file sharing in peer-to-peer networks.

The above mentioned security and privacy threats have one thing in common – they are all much more severe in case of users' risky and careless online behavior. Therefore, we have focused our research on the identification of connections between the behavior of Internet users and the level of their online security and privacy.

2.2 Privacy concern and behavior of Internet users

Privacy is a term that denotes the right of an individual to determine what information is collected about him/her and how it is used (Kelly and McKenzie, 2002). Research on Internet users privacy concerns and their online behaviors has revealed that the majority of Internet users worry about their online privacy but some of them still don't perform actions to reduce those threats. For example, 70% of American users are concerned about privacy threats (Jupiter, 2002), but only 57% of security professionals in UK, US and EU always delete cookies when they do not need them on their computers because of their privacy concern (Symantec, 2003). It must be noted that personal online behavior can be tracked by the use of cookies which, on the other hand, provide users with a number of benefits and services.

However, when the use of cookies is paired with information about the identity of the Internet user, in wrong hands it can present a serious threat to their privacy.

According to their level of privacy concern, users can be segmented into four distinct groups (Sheehan, 2002): *unconcerned* Internet users are minimally concerned in most of privacy threatening situations; *circumspect* Internet users are slightly concerned with privacy in most of situations; *wary* Internet users show moderate level of concern with most situations; *alarmed* Internet users are highly concerned with privacy in all situations.

3 A survey of security and privacy related behavior

The subjects in our study were 312 college students of information systems aged 18-21 years, of whom 74% were male and 26% female. Most subjects (94% of them) used computers for five or more years and were also Internet users for two or more years. The data in our study were collected with 18 items related to potential *assumptions* and another 18 items related to potential habits of Internet users regarding their online security and privacy, as well as with other items related to demographics and computer/Internet use. The subjects were at the end of their first year of study and, as can be observed from the data presented in Figure 2, more than 90% of them stated that their knowledge of computers and the Internet was in the range from "good" to "excellent".

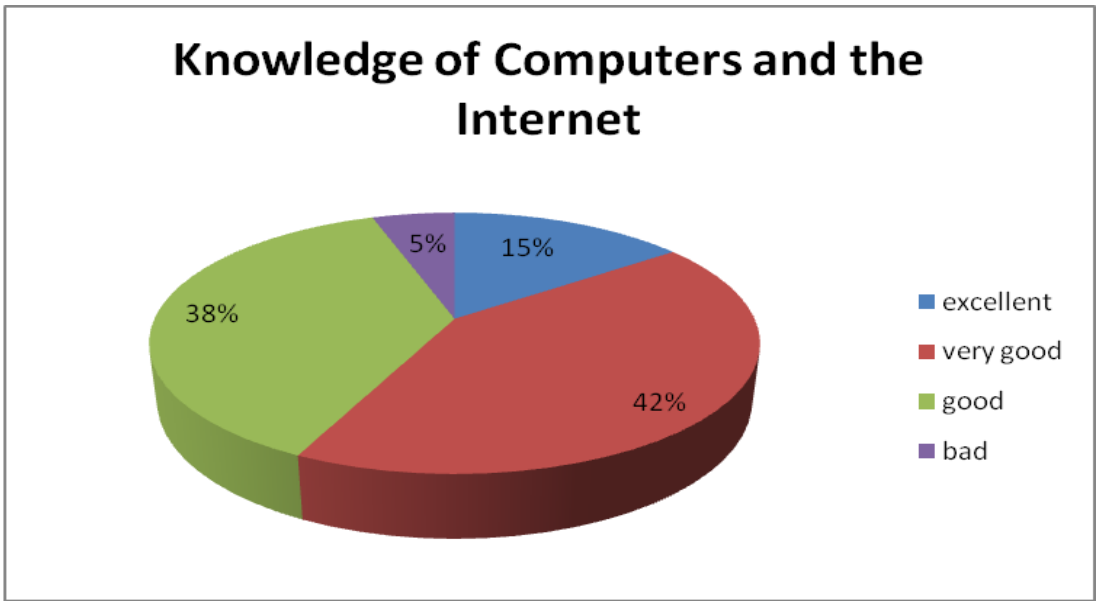

Figure 2: Users' knowledge of Computers and the Internet

The experience of the subjects in our research regarding experienced security and privacy problems in their use of computers is presented in Figure 3. The subjects didn't report having many problems regarding privacy and security threats when they used the computers at faculty. However, they reported experiencing more frequent problems on their home computers. This may indicate that they are using less computer system protection at home than the faculty personnel are using to protect the computers in classrooms and laboratories. Still, the subjects in our research may have been using computers more at home and for

different purpose than at faculty. Another part of our research showed that not all of the subjects in our study (students who were experienced ICT users) used the technologies which could have adequately protected them against various security flaws. As can be concluded from the data presented in Figure 3 the most frequently noticed security or privacy problem was related to malicious software found on home computer.

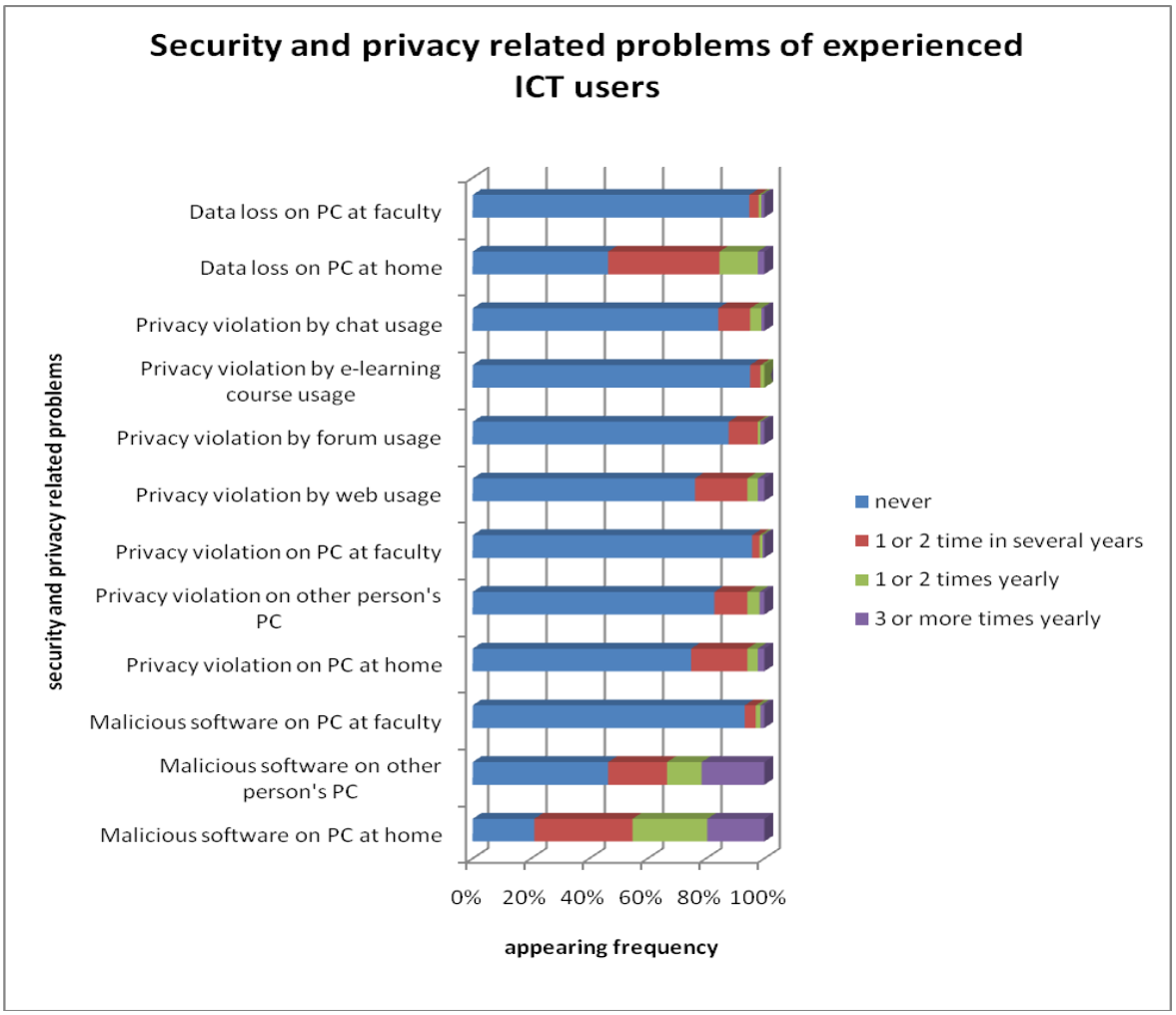

Figure 3: Security and privacy related problems of experienced ICT users

The responses of the subjects in our survey indicated that most of them intended to or actually performed regular upgrading/updating of their operating system and antivirus software and that their attitudes and habits in those fields did not considerably endanger their computer systems. However, the data collected on the assumptions and habits regarding their online behavior revealed that a substantial percent of the subjects in our study disregarded or were unaware of potential online security and privacy threats. The data presented in Table 1 uncovers various online security and privacy related behaviors (assumptions and habits) of experienced ICT users. These data reveal that a substantial percent of subjects disregarded or were unaware of potential online security and privacy threats.

As can be observed from the responses to survey items which are presented in Table 1, some of the experienced ICT users, who were subjects in our research, tend to underestimate the potential security and privacy threats related to Internet use. For instance, 42% of the subjects responded with "Totally true" or "Mostly true" to the survey item *"I believe that I don't have to change my online behavior because of the possibility to unintentionally download spyware from the Internet to my computer."* Furthermore, 43% of the subjects used the same responses to provide answer to the survey item *"I tend to visit somewhat "suspicious" web pages on which malicious code could perhaps have been placed."* Also, 42% of the subjects responded with "Totally true" or "Mostly true" to the survey item *"From time to time I download diverse unnecessary executing programs (e.g. a game, a screensaver, etc.) to my computer."* Finally, as many as 66% of the subjects responded positively to the following statement: *"I like to download music files (MP3) from the Internet/web or to share them using file sharing network services."* These findings indicate that, despite the considerable threats and risks of the previously mentioned online activities, even the experienced ICT users with good knowledge of computers and the Internet are not sufficiently aware of Internet threats or motivated to alter their online behavior to better protect their online security making themselves more exposed to potential risks of data loss, computer breakdown due to malicious code, or privacy invasion.

Table 1. Responses of experienced ICT users (N=312) to survey items associated with the assumptions and habits regarding online security and privacy

	Totally true	Mostly true	Niether true, or untrue	Mostly untrue	Totally untrue
I believe that I don't have to change my online behavior because of the possibility to unintentionally download spyware from the Internet to my computer.	18%	24%	25%	21%	12%
I assume that all computers that access the Internet from a local network of a company, college or some other institution are well protected.	7%	25%	30%	21%	7%
I believe that Internet users should limit their visits to potentially problematic/harmful web sites because of the possibility to unwantingly download an undesired program on their computer.	18%	37%	27%	14%	4%
I don't believe that an unprotected computer which is connected to the Internet via a modem (telephone line) for only a day or two is exposed to considerable potentially malicious wrongdoing from the Internet.	3%	10%	25%	32%	30%
I would continue performing some potentially risky activities over the Internet, like sharing of music files or playing online games, even if this would endanger the security of other people who are using the same computer resources (the same computer or a local network).	11%	17%	28%	27%	17%
I rarely conduct safety measures for protection of my privacy while using the Internet because I suppose that there are no reasons for a privacy violation to happen to me personally.	4%	19%	23%	30%	24%
I tend to visit somewhat "suspicious" web pages on which malicious code could perhaps be placed.	13%	30%	26%	18%	14%
I don't have a habit of regular erasing of cookies placed on my computer by the Internet browser (e.g. MS Internet Explorer) that I use.	17%	25%	25%	14%	19%
I like to download music files (MP3) from the Internet/web or to share them using file sharing network services.	35%	31%	14%	11%	9%
From time to time I download diverse unnecessary executing programs (e.g. a game, a screensaver, etc.) to my computer.	13%	28%	20%	21%	19%
I have never erased the content of the file that stores information of visited web sites ("history") or temporarily stores Internet files.	11%	18%	30%	22%	19%
I regularly erase from my mailbox the messages which should not be kept because of their sensitive content (very private or confidential).	19%	26%	23%	20%	12%

Even though they were highly information literate, some of the subjects in our survey probably were insufficiently informed of certain types of vulnerabilities of their computer systems. For instance, 13% of them responded with "Totally true" or "Mostly true" to the survey item *"I don't believe that an unprotected computer which is connected to the Internet via a modem (telephone line) for only a day or two is exposed to considerable potentially malicious wrongdoing from the Internet."* In fact, having an unprotected personal computer connected to the Internet for an hour or two via a modem is considered as risky behavior, and it is recommended that before connecting a computer system to the Internet for the fist time a firewall and anti-virus software is installed while the system is still offline.

In some other areas the subjects in our research may have simply been unconcerned or too positive about potential threats. For instance, 23% of the subjects responded with "Totally true" or "Mostly true" to the statement *"I rarely conduct safety measures for protection of my privacy while using the Internet because I suppose that there are no reasons for a privacy violation to happen to me personally."* Positive thinking regarding privacy and security risks and belief that others are taking care of their online safety was also revealed in the 33% of the affirmative responses to the item *"I assume that all computers that access the Internet from a local network of a company, college or some other institution are well protected."* In fact, a personal firewall, updated operating system and up-to-date antivirus and antispyware protection is necessary even when the Internet is accessed through an institutional local area network.

In relation to several aspects of their online privacy it looks like some of the subjects in our survey were simply negligent or sloppy. As many as 42% of them responded with "Totally true" or "Mostly true" to the item *"I don't have a habit of regular erasing of cookies placed on my computer by the Internet browser (e.g. MS Internet Explorer) that I use."* Also, 29% of them gave the same response to the statement *"I have never erased the content of the file that stores information of visited web sites ("history") or temporarily stores Internet files."*

It must be noted that in our research the highest correlation of 0.26 ($p<0.001$) was found between malicious software found on home computer of the subjects in our research and their online behavior measured by the responses to the survey item *"I tend to visit somewhat "suspicious" web pages on which malicious code could perhaps be placed."* This is another indication that risky online behavior is one of the major causes of current security and privacy violations.

The other results of our survey (not presented in Table 1) related to privacy indicate that a half (52%) of subjects thought that it is important to carefully select passwords for access to their online resources but on the other hand 19% of them were unwilling to change their passwords after they once have chosen them and they did that only when it was absolutely necessary. It is encouraging that only 5% of subjects had shared their passwords for no reason with their friends and that only 7% of subjects had used the simplest passwords for their online accounts. Also, only 13% of the subjects stated that they did not check their computer systems for possible infections by spyware or adware. Regarding online security, only 9% of the subjects thought that the effort to have latest versions of antivirus software was a waste of time and only 9% of them had stated that they would not make effort to have the latest version of web browser (with "patches") installed on their computer. Finally, only 12% of the subjects

admitted that they were not very conscientious regarding regular maintenance of their operating system and antivirus software.

Results of the survey that was conducted in our study show that experienced ICT users were aware of many potential risks and threats, but also that some of them were insufficiently concerned regarding the need to protect them selves when using the Internet. In all cases of security and privacy related behaviors there was a fair percentage (at least 5-10%) of those whose statements indicated that that did not care enough about these issues. In fact, several things were present in online behavior of a relatively large percent of the subjects in our survey that could lead to serious security and privacy attacks like not erasing cookies on personal computer, visiting untrustworthy web sites and downloading of potentially suspicious content. They subjects in our study probably visited suspicious web sites and downloaded potentially malicious files/code to satisfy their curiosity or some need, even though they were at least partially aware of potential privacy and security threats.

There is obviously a need for further and constant education and rise of awareness about the issues presented in this paper. The fact that this research was conducted among students of information systems leads to the assumption that the results of the same study among students who do not study ICT related subjects and other less computer literate Internet users would be even more problematic.

4 Conclusion

Information has become an important resource and use of computer systems is a major factor of productivity in many areas. This places great importance on security and privacy issues and makes it necessary to identify problems related to the risky behavior of Internet users in this area and not allow such problems to escalate. One way to do this would be by raising awareness regarding security and privacy risks which are today highly associated with the use of the Internet. Our research has shown that experienced ICT users are mostly aware of the problem and they perform some actions to protect themselves but, in spite of that, there is a large area where the actions of some of them are insufficient. Some users even deliberately ignore risks when it suits them and they sometimes think that it takes too much time or effort to assure security and privacy in their use of computers and the Internet. With new and evolving threats the end-user remains one of the weak points in security protection for organizations (IBM, 2007). Proper and constant education in this area is needed even for expert users and much more for new users to properly develop their habits so that their work and life online would be more protected and secure.

References

CERT/CC, (2007): Vulnerability Remediation Statistics [Online Report], Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, U.S.A., Retrieved January 21 2008, URL: http://www.cert.org/stats/vulnerability_remediation.html

Chung, W., Paynter, J., (2002): Privacy Issues on the Internet. Proceedings of the 35th Annual Hawaii International Conference on System Sciences, January 7 - 10, IEEE Computer Society, Washington, DC, USA

Hansman, S., Hunt, R., (2005): A taxonomy of network and computer attacks, Computers & Security, Vol. 24, No. 1, pp. 31 - 43.

IBM (2007). The Evolving Threat: Combat Training for the New Era of Malicious Code [Online Report]. IBM Corporation, IBM Global Technology Services, Somers, NY, U.S.A. Retrieved January 21 2008, URL: http://www.iss.net/documents/whitepapers/Evolving_Threat_Whitepaper_04-16-07.pdf

Jupiter Research, (2002): Security and Privacy Data [Online], Consumer Survey, Jupiter/The NPD Group, Retrieved January 23 2008, URL: http://www.ftc.gov/bcp/workshops/security/020520leathern.pdf

Kelly, G., McKenzie, B., (2002): Security, privacy, and confidentiality issues on the Internet, Medicine and the Internet: The Essential Guide for Doctors, B.C. McKenzie (ed.), Oxford University Press, pp. 127-136.

Kierkegaard, S.M., (2005): How the cookies (almost) crumbled: privacy & lobbyism, Computer Law & Security Report, Vol. 21, No. 4, pp. 310-322.

Kjaerland, M., (2006): A taxonomy and comparison of computer security incidents from the commercial and government sectors, Computers & Security, Vol. 25, No. 7, pp. 522-538.

Lavin, M., (2006): Cookies: What do consumers know and what can they learn?, Journal of Targeting, Measurement and Analysis for Marketing, Vol. 14, No. 4, pp. 279-288.

McAfee, National Cyber Security Alliance, (2007): McAfee-NCSA Online Safety Study, Retrieved January 21 2008, URL: http://staysafeonline.org/pdf/McAfee_NCSA_analysis.pdf

Pinkas, B., Sander, T., (2002): Securing passwords against dictionary attacks, Proceedings of the 9th ACM conference on Computer and communications security, November 18-22, ACM, Washington, DC, USA, pp. 161-170.

Sheehan, K.B., (2002): Toward a Typology of Internet Users and Online Privacy Concerns, The Information Society, Vol. 18, pp. 21-32.

Shukla, S., Nah, F.F-H., (2005): Web browsing and spyware intrusion, Communications of the ACM, Vol. 48, No. 8, pp. 85 – 90.

Symantec Corporation, (2003): Privacy: A Study of Attitudes and s in US, UK and EU Information Security Professionals [Online Report], Cupertino, CA, U.S.A., Retrieved January 20 2008, URL: http:// www.symantec.com/avcenter/reference/privacy.attitudes.s.pdf

Symantec Corporation, (2007): Symantec Internet Security Threat Report: Trends for January – June 07 [Online Report], Cupertino, CA, U.S.A., Retrieved October 16 2007, URL: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf

Warkentin, M., Luo, X., Templeton, G.F., (2005): A framework for spyware assessment, Communications of the ACM, Vol. 48, No. 8, pp. 79-84.