UDC 004.056:004.738.5
Original Scientific Paper

Factors and Predictors of Online Security and Privacy Behavior

Goran Bubaš *goran.bubas@foi.hr*
University of Zagreb
Faculty of Organization and Informatics Varaždin

Tihomir Orehovački *tihomir.orehovacki@foi.hr*
University of Zagreb
Faculty of Organization and Informatics Varaždin

Mario Konecki *mario.konecki@foi.hr*
University of Zagreb
Faculty of Organization and Informatics Varaždin

Abstract

Assumptions and habits regarding computer and Internet use are among the major factors which influence online privacy and security of Internet users. In our study a survey was performed on 312 subjects (college students who are Internet users with IT skills) that investigated how assumptions and habits of Internet users are related to their online security and privacy. The following four factors of online security and privacy related behaviors were revealed in factor analysis: F1 – conscientiousness in the maintenance of the operating system, upgrading of the Internet browser and use of antivirus and antispyware programs; F2 – engagement in risky and careless online activities with lack of concern for personal online privacy; F3 – disbelief that privacy violations and security threats represent possible problems; F4 – lack of fear regarding potential privacy and security threats with no need for change in personal online behavior. Statistically significant correlations were found between some of the discovered factors on the one side, and criteria variables occurrence of malicious code (C1) and data loss on the home computer (C2) on the other. In addition, a regression analysis was performed which revealed that the potentially risky online behaviors of Internet users were associated with the two criteria variables. To properly interpret the results of correlation and regression analyses a conceptual model was developed of the potential causal relationships between the behavior of Internet users and their experiences with online security threats. An additional study was also performed which partly confirmed the conceptual model, as well as the factors of online security and privacy related behaviors.

Keywords: privacy, security, Internet, user behavior, factor analysis, regression analysis

1. Introduction

Popular assumptions and the reality regarding privacy concerns of Internet users may significantly differ (see [20]): some people are privacy-sensitive, while others don't seem to care much about their privacy in practice; many consumers are more oriented toward fulfilling various needs than interested in retaining their online privacy; even those Internet users who are concerned about their online privacy sometimes act differently online than what they say or believe. A substantial proportion of Internet users have insufficient knowledge about online security and privacy, many of them may not be motivated to regularly update their operating system, some of them do not turn on the real-time monitoring features of antivirus and antispyware systems when they have them on their computers, and most of them do not protect themselves adequately against spyware (see [62]). Even when Internet users try to educate themselves about security and privacy issues the results are mixed because of the difficulty of the subject and technical subtleties that they have to manage [12].

The well known AOL/NCSA Online Safety Study [1] revealed that the assumptions of Internet users about their online safety and privacy are in many cases not consistent with actual virus and spyware/adware infections of their computers. In this study only 6% of Internet users said that they currently had a computer virus on their computer, but a subsequent virus scan revealed that 25% of dial-up users and 15% of broadband users actually had a computer virus (with an average of 2.4 different viruses found on infected computers). It must be noted that an inspection of the computers of all users in this survey revealed that 67% of the users either didn't have antivirus software or that it had not been updated within the past week. The situation was much worse regarding spyware/adware infections. As much as 53% of Internet users in this survey responded that they currently had spyware or adware on their computer, but a subsequent computer scan revealed that the computers of 88% of dial-up and 74% of broadband users were infected by spyware/adware (with an average of 93 spyware/adware components found on their computers). Finally, only 33% of the Internet users in the survey had a firewall set up on their computer.

Online security and privacy have been identified as some of the main concerns of Internet users that affect their online behavior and Internet shopping activity [39], [50]. Various surveys conducted by the Pew Internet and American Life Project over the last few years revealed the following [46]: 84% of Internet users said that they were concerned about businesses and people they didn't know collecting personal information about them; 68% of Internet users reported having problems that could be related to software intrusions over the Internet (spyware, malware etc.); 91% of Internet users said that they had changed at least one activity in their online behavior to avoid intrusions by unwanted programs. However, users make different rationalizations and act diversely in relation to their level of Internet experience and safety involvement: some of them are passive and/or avoidant of certain online activities, others try to protect themselves more actively by responding to specific security and privacy risks, and some are reckless regarding their online safety and privacy [47]. Even though many Internet users think that taking care of their online safety is not their responsibility and that they may not be capable of protecting themselves, the activity of showing (demonstrating) how to behave safely online may result in an increase in their personal responsibility and related online safety behaviors [30].

This paper first provides an overview of selected sources of privacy and security threats. It then turns to its main topic: the survey and the results of factor and regression analyses of the assumptions and habits of college students of Information Systems regarding their online privacy and security behaviors. Finally, the discovered factors of online privacy and security related behaviors are presented, as well as the predictors of virus infection and data loss on home computers.

2. Online security and privacy threats

Computer security is becoming an increasingly more complex problem owing to the amounts and types of information that have to be secured and the growing numbers and types of threats to computer systems. In the past thirteen years there has been a notable increase in the yearly report of new vulnerabilities of computer software (about 20 times more since 1995; see the statistical report of the CERT Coordination Center [2]). In the second half of 2007, Symantec [5] observed as many as 499.811 new malicious code threats, which is an increase of 136% in comparison with the previous observation period. The overall number of identified threats by Symantec was 1.122.311, which meant that almost two thirds of the threats identified were developed during 2007. The increasing numbers of vulnerabilities as well as the growing numbers of malicious code threats are major causes of concern for the security of end users.

It must be emphasized that computer systems security is no longer a problem of a narrow group of experts but rather a global problem affecting private and corporate users of information technology (IT). In modern society IT users need to be both informed and responsible for the security of the computer and information resources they are using. They should also be concerned and active regarding the protection of their right to safety and privacy in the use of computer systems and the Internet. The latest research has revealed the following [14]: 71% of users believe that their computers are safe; users recognize 68% to 99% of threats that are present on the Internet; in many cases diverse forms of system protection are used, from antivirus programs, which are most frequently used form of protection, to firewalls and antispyware/antispam software, which are used least. A special aspect of information security is user privacy. In another recent study [42] 56% of users have shown concern for their privacy when they used the Internet. They were mainly concerned about computer viruses (16.1%), spam (10.5%), spyware (9.9%) and hacker attacks (8%). Furthermore, 73% of the participants in this research reported that they were taking measures to assure their privacy when they were online.

According to the SANS Institute [4], some of the main areas of critical vulnerabilities in 2007 were client-side and server-side vulnerabilities, network devices, security policy and personnel, application abuse and zero day attacks. In our paper we will focus on Windows configuration weaknesses, P2P file sharing applications and other vulnerabilities that were part of the critical vulnerabilities lists and are related to security and privacy assumptions and habits of the subjects in our study (college students with IT skills).

2.1. Vulnerability of computer systems

Computer system vulnerability is a state that enables the attacker to perform activities under the identity of some legitimate user to access data in spite of limitations and restrictions, or hide behind a false identity and disable the system. Vulnerability does not cause damage by itself; it is only a precondition for the realization of some threat [25]. Here is a list of computer system vulnerabilities that are related to computer and network attacks [22]:

- Viruses are referred to as some malicious mobile code that can reproduce itself by infecting other programs [57]. With the growing number of web applications and services, the number of vulnerabilities which can be misused by viruses in order to undermine user security and privacy is also increasing. Therefore a lot of research is focused on discovering new and more efficient methods for the detection and prevention of viral attacks on computer systems (for instance, see [41], [54] and [61]). Executable packing is a popular method for the encryption of benign executables that is often misused by virus writers in order to hide malicious code. According to Lyda and Hamrock [37], more than 80% viruses can be found in some packed variety. Furthermore, there is evidence that more than 50% of recent viruses are nothing but a re-packed version of the existing and known viruses [49]. When viruses are in their packed form, it is very difficult to detect them with anti-virus programs. In order to solve this problem, a new method of pattern recognition based on classification of packed executables is proposed [44].
- Worms are malicious computer programs that actively propagate over a network and replicate independently by sending itself to other systems [3]. Worms can be classified into three main categories which represent different approaches to their development [29]: (a) client application worms that take advantage of user's client (e.g. e-mail, messenger) features to send themselves to other computers; (b) file sharing worms; and (c) traditional worms that exploit application and/or operating system vulnerabilities and thus use alternative ways of replication and propagation. In the history of malware, the year 2003 will be memorized due to the appearance of two most disruptive worms: the *Blaster* and *SQL Slammer* worms. Together they infected over 200,000 systems all over the world and caused damage worth millions of dollars [6]. Nowadays, anti-virus programs and programs for attack detection are not sufficient for efficient protection against self-propagating worms and there is a need for additional mechanisms of defense. One of these alternative types of protection is a method where a worm is transformed into an anti-worm in order to disinfect its original [9].
- A Trojan horse is a malicious program that appears to be benign in order to perform some hidden act and/or to lower the security level on users' computer system [13]. A special type of Trojan horse which has occurred recently is called ransomware or cryptovirus. Ransomware hijacks users' data, encrypts the data and then demands some amount of money in exchange for the decryption key. Trojan horse types of malicious programs represent a great danger for the security of computer systems and therefore new methods and techniques for easier

detection and removal of this type of malware are regularly proposed (see [40], [56]). On the other hand, it is presumed that the most appropriate form of defense against all types of Trojan horse is continual education of end users [36].

• Denial of service attacks (DoS) are attempts to disable the access of legitimate users to the system by reducing the availability of the victim computer [8], [24]. There are two main types of DoS attacks: (1) single-host attacks, which originate from only one source; (2) multi-host (DDos), where the victim client computer is flooded with packages from multiple sources. This kind of attack can cause a potentially large financial loss and there is still a need for the development of techniques that will speed up the process of their detection as well as mechanisms that will serve as a more efficient form of protection. In order to achieve the goal, a framework for automatic classification of DoS attacks has been proposed. This framework is based on interpretation of header content, transient ramp-up behavior and spectral characteristics analysis [23]. Furthermore, a countermeasure called DiDDeM has been developed. It is a distributed mechanism that combines stateful and stateless signatures, speeds up the detection of DoS attacks and enables their prevention [21]. In last few years the number of experimental investigations with the goal of preventing DDoS attacks has increased. Two defensive mechanisms have recently been presented: the first one makes it easier to control overload caused by malicious packages by using Cognitive Packet Network properties for traffic tracking [16] and the other one blocks the sources that are trying to overflood the host with an unusually large number of packages by using the mechanism called targeted filtering that is implemented inside the firewall itself [10].

• Password attacks are aimed at manual guessing of users' password or the use of the so called dictionary attack [32] and are mostly related to user authentication. The most frequently used method of authentication is by user account where the user has to generate a strong password which the attacker will not be able to guess easily. Basic characteristics of quality passwords are [27]: *effectiveness* as a measure of how strong the password is or how hard it would be for the attacker to guess it or break it; the degree of *utilization* which is determined by the ease of use and memorizing of the password; and *satisfaction* of the user as a psychological perception of the degree of effectiveness and utilization of a password. However, users often use common words or names as a password that can easily be broken by the attacker. In addition, users often tend to write their passwords down so that they won't forget them [15] or they generate only one strong password which they use for all of their accounts. In order to avoid the above mentioned security problems, recent research has demonstrated that users are able to generate strong passwords which are very intuitive and easy to remember (see [52], [58]). Even though the authentication method by user accounts is one of the least secure forms of authentication, it is still widely used because of its easy implementation (e.g. [45]).

2.2. Computer system exposure

Computer system exposure is a state in which the system is not vulnerable but it enables gathering of information about the system or from the system (for instance, about the activities of the user) that can later be abused. The main means of computer systems exposure are by spy software, cookies and use of peer-to-peer applications.

• Spy software (spyware, adware) is a software component whose basic purpose is monitoring of victim computer activity and interception or stealing of users' information for some third party [55]. Spyware exists because information has value (e.g., information gathered about the behavior of Internet users has value to advertisers; the potential to show advertisements correlated with user behavior has value to product vendors; gathering information about keystrokes or introducing backdoor vulnerabilities on a host has value to attackers, such as virus writers (for more information see: [48]). In order to lower the probability of computer infection by this kind of malware it is recommended to use an antispyware tool because it enables the detection and removal of spyware and at the same time prevents spyware infiltration into the computer system. Antispyware tools are the most appropriate solution in fighting against spyware in 80% of cases [33]. However, in spite of this fact, one study revealed that only 10% of users aggressively fought against potential spyware infections [17] and another study found that only 40% of users activated their antispyware tool more than once a month [38]. Some of the factors that were found to largely influence the decision to use an antispyware tool are the denial of responsibility, individual's attitude, perceived behavioral control and subjective norms, while the factors like the ease of use, moral obligation and perceived cost were not found to have too much influence [34]. Besides the use of antispyware tools, an alternative form of spyware avoidance behavior is careful reading of the *End User License Agreement* (EULA). According to one study, users don't read EULA before installing desired software and in this way unconsciously expose themselves to the risk that the installed software has a secondary purpose as spyware [18]. A recent study has indicated that EULA-based classification of programs can be used as a preventive mechanism against spyware infection [7].

• Cookies are a special type of data that are stored on user's computer hard drive and are intended to make the user's interaction with the website easier. It must be noted that user-related sensitive information (account or credit card details, recent activities) is sometimes stored in cookie files and transmitted publicly over the Internet. Therefore, cookies can be misused for monitoring, profiling and tracking of the user's activities and can thus be used to undermine their privacy [31]. Because of their properties, cookies are exposed to some serious security threats like cookie-harvesting, as well as end-system and network threats [43]. Solutions for such security and privacy weaknesses are provided in many forms, such as server-managed and user-managed cookie scheme based on symmetric or asymmetric cryptography [28], secure cookie system for mutual authentication between servers and clients [59], and active-cookie dynamic authentication protocol, which can help defend against pharming attacks [26], etc.

• Computer systems that have a peer-to-peer (P2P) application installed have a much greater chance of being infected with malicious code. Also, computers with an installed P2P application that are infected with a computer worm facilitate the spreading of this malicious code and thus create security holes on other computers that are parts of the P2P network (see [35]). In this way, "active worms" can spread over P2P tools and networks much faster and in a rather short time flood the Internet [60]. Besides that, attackers can use a P2P network in order to increase the intensity of DoS attacks [11]. To solve the previously mentioned problems, some security techniques can be of use, such as cryptography, redundant routing and economic methods [53], or auto-adaptive platforms in which nodes warn each other about security threats and thus adapt to their own security policies [51]. Another type of computer protection is firewalls that can be found in hardware or software form and provide protection by intercepting various types of attack through the computer network. The function of a firewall is to examine every incoming or outgoing packet and decide whether to accept or discard it [19]. On the other hand, P2P networks can be positively utilized to significantly reinforce network security by offering substantial help to network members in the protection against malicious applications [51].

3. Problem and hypotheses

The main problem of this research was to determine the factors of behavior of Internet users that affect their online security and privacy and to correlate these behaviors to two common consequences of their disregard of security and privacy protection activities: occurrence of viruses and loss of data on their home computer. The identification of typical behaviors which represent a threat to online security and privacy may help in user education and design of related tools (warning systems and applications for protection from malicious software). For the purpose of our study the behaviors of Internet users were classified into two broad categories: *assumptions* about online security and privacy and *habits* regarding security and privacy related behaviors. However, in our study the data were collected from college students with a good knowledge of information technology (IT) and therefore the conclusions from subsequent data analyses can only be associated with the behavior of information literate and experienced Internet users.

Three hypotheses were defined in relation to the main problem of the study presented in this paper:

- H1: The factors of potentially risky behaviors of Internet users with IT skills can be determined by factor analyses of items related to their assumptions and habits regarding safety and privacy in computer and Internet use.
- H2: The factors of potentially risky behavior of Internet users with IT skills are related to a greater possibility of computer infection with malicious code and the loss of data on their home computer.
- H3: Some specific risky behaviors of Internet users with IT skills can be used as predictors of (a) home computer infections with malicious code and (b) loss of data on their home computer as criteria variables.

4. Method

To test the three previously presented hypotheses a survey was designed with 18 items related to potential *assumptions* and another 18 items related to potential *habits* of Internet users regarding their use of computers and the Internet. These items were supplemented with demographic questions regarding age, gender, year of study, and also with questions associated with students' average grades, knowledge of computers, use of various information technologies (IT), as well as with a list of statements about problems that the students as users of computer systems may have experienced in relation to their information security and privacy.

The items of the survey that addressed the potential *assumptions* of Internet users included statements like: "I think that no person will attempt an unauthorized access to my mailbox, and even if they tried, they could not succeed"; "I don't believe that an unprotected computer which is connected to the Internet using a dial-up (modem) connection for only a day or two is exposed to considerable harmful influences from the Internet". The items that were associated with related *habits* of Internet users included statements like: "I like to download music files (MP3) from the Internet/web or to exchange them over the Internet (for instance, by using peer-to-peer networks for file exchange)"; "From time to time I download diverse unnecessary exec files (games, screensavers) from the Internet/web to my personal computer".

The items of the survey which were used to collect the data for criteria variables were created as answers to the question "*How often have you personally had problems related to information privacy/security?*". The potential responses for the first criterion variable C1 (occurrence of home computer infections with malicious code) and the second criterion variable C2 (occurrence of loss of data on the home computer) were: *never, 1-2 times in many years, 1-2 times per year, 3 or more times per year*.

The subjects in the first part of the study were 312 college students of Information Systems aged 18-22, 74% of whom were male and 26% female. The subjects were at the end of their first year of study and more than 90% of them stated that their knowledge of computers and the Internet was in the range from "good" to "excellent".

The second part of the study was conducted to verify some elements of the theoretical model outlined in Figure 2. A brief survey was administered to 172 college students of information systems aged 18-22 (70% male and 30% female). This survey consisted of demographic questions, two criteria items from the first study, and 16 items that were related to experience with malware (viruses, worms, spyware) and also to factors revealed in the first part of the study: F1– *conscientiousness* in the maintenance of the computer system; F2 – *risky and careless online activities*; F3 – *disbelief* that privacy violations and security threats represent possible problems; F4 – *lack of fear* regarding potential privacy and security threats.

To determine the factors of security and privacy related behaviors the data collected by means of the survey in the first study were analyzed using factor analysis. To investigate the relations of the revealed factors with the criteria variables (security and privacy related problems) the Pearson's coefficient of correlation and regression analysis were used. Finally, the analysis of data collected with the second survey was used to confirm some of the theoretical conclusions related to the first part of the study and also to the conceptual model presented in Figure 2.

5. Results of the first study

The data were collected from 312 subjects with 36 survey items related to assumptions and habits of Internet users regarding their online security and privacy. These were included in factor analysis (principle components method was used with varimax rotation). In the initial factor solution 11 factors were found with eigenvalue above 1.0, which explained 56% of the variance. However, the *Scree test* was used to identify that four factors would be more appropriate for varimax rotation (these four factors explained 33% of variance of the initial factor solution). The five variables (survey items) with largest loading after varimax rotation on each of the four factors are presented in Table 1.

As can be observed from the data presented in Table 1, the first factor (F1) is related to the level of *conscientiousness* regarding the protection of personal online security and privacy that is manifested by regular updating of the operating system and antivirus software. Other items (not presented in Table 1) that loaded predominantly on this factor were associated with security (when using a modem connection) and privacy (regarding potential spyware infection) concerns. The second factor (F2) in Table 1 is associated with *risky online activities* like downloading unnecessary files from the Internet, file sharing, visiting web pages with potentially malicious code, as well as with careless behaviors associated with lack of interest in the preservation of privacy and security of other Internet users. Most of the other items (not presented in Table 1) with predominant loading on this factor were associated with behavior which indicates *lack of care* for personal online privacy. The third factor (F3) in Table 1 is associated with *disbelief* in potential online security threats and privacy violations similar to the popular assumption “why should it happen to me” or “this cannot happen to me”. Finally, the items with a predominant projection on the fourth factor (F4) in Table 1 are mostly related to *lack of fear* of potential security and privacy risks that are associated with the use of the Internet.

The results of the factor analysis that are presented in Table 1 indicate that the assumptions and habits of Internet users which are associated with potential violations of their security and privacy could be grouped into the following categories/factors: *conscientiousness* in the maintenance of the operating system, upgrading of the Internet browser and use of antivirus and antispyware software (F1); engagement in *risky and careless online activities* with lack of concern for personal online privacy (F2); *disbelief* that privacy violations and security threats represent possible problems which need to be dealt with (F3); *lack of fear* regarding potential privacy and security threats with no need for change in personal behavior that would secure greater online security and privacy (F4).

Even though diverse factors influence the occurrence of malware/spyware infections on personal computers, it is reasonable to expect that the risky and/or careless security and privacy related behaviors of Internet users are among the main causes of such problems. Therefore, the factor-scores were calculated (with *regression method*) for the factors presented in Table 1 and correlated with two criteria variables (see Table 2): C1 – occurrence of home computer infections with malicious code; C2 – occurrence of loss of data on the home computer. As can be observed from the data presented in Table 2, the first factor labeled *conscientiousness* (F1) had a statistically significant positive correlation of 0.22 with the criterion C1 (occurrence of home computer infections). This correlation is rather low, but it can be concluded that greater conscientiousness regarding security and privacy related online behavior was associated with more frequent occurrence of computer infections on home computers of Internet users. This may seem paradoxical at first glance, but it is possible that negative users’ experiences regarding problems with malicious code infections as a consequence lead to more careful maintenance of the operating system and proper use of antivirus/antispyware software for protection of home computers connected to the Internet. This finding is of potential use for educational purpose because it indirectly implies that the promotion efforts related to the protection against malicious software could be supported by providing evidence of the potentially negative consequences of the negligence in the maintenance of the operating system, upgrading of the Internet browser and the use of antivirus and antispyware software.

* Only factor loadings of 0.30 or above are displayed. Factor loadings of 0.40 or above are written in boldface.

SURVEY ITEMS	**F1**	**F2**	**F3**	**F4**
I consider myself as a very conscientious person having in mind the regular maintenance of the operating system of my computer and use of antivirus protection.	**.73**			
I am used to performing activities which ensure my privacy and security in using a personal computer and the Internet.	**.67**			
I regularly update (or enable an automatic update) of antivirus protection on my personal computer.	**.67**			
I independently (or with the help of a more experienced person) take care that the newest versions of operating system (for instance of MS Windows) are installed on my computer as well as the necessary "patches".	**.64**			
Whenever possible, I would install the newest version of the Internet browser or download "patches" for the version I am actually using on my personal computer.	**.52**			
From time to time I download diverse unnecessary exec files (games, screensavers) from the Internet/web to my personal computer.		**.57**		
I tend to visit somewhat "untrustworthy" web pages on which malicious programs could perhaps be found.		**.56**		.38
I would continue to perform some potentially risky activities over the Internet (like sharing of music files or playing online games) even if that would endanger the security of other people who are using the same computer resources (e.g., the same computer or a local computer network).		**.52**		**.46**
After the private use of the web from a computer that could be used by other persons I have never cleared the content of the file registering which web pages I have visited ("history") or the locally stored "temporary Internet files".		**.48**		
I like to download music files (MP3) from the Internet/web or to exchange them over the Internet (for instance, by using peer-to-peer networks for file exchange).	.35	**.45**		.32
I think that computers used for professional purposes which do not store any important data should not be specially protected against computer viruses.			**.52**	
I think that no person will attempt an unauthorized access to my mailbox, and even if they tried, they could not succeed.			**.52**	
I don't believe that an unprotected computer which is connected to the Internet using a dial-up (modem) connection for only a day or two is exposed to considerable harmful influences from the Internet.			**.51**	
I rarely take any measure for protection of my privacy when using the Internet because I believe that there is no special reason for privacy violation to happen to me personally.	-.36	.32	**.47**	.36
I assume that the computers which access the Internet from a local computer network of a company, college or some other institution are very well protected from harmful influences from the Internet.			**.40**	
I think that people should be afraid of computer viruses even though many of them do not cause material damage.				**-.58**
I believe that I do not have to change my online behavior because there is a possibility that I could accidentally download spyware programs from the Internet.				**.53**
I suppose that a greater degree of care for the maintenance of the operating system of a computer and updating of antivirus software does not significantly increase my security and privacy on the Internet.			.35	**.51**
I believe that the Internet users should limit their visits to potentially problematic web sites because of the possibility that this could cause them to download unwanted programs on their computers without knowing that they did that.			.30	**-.47**
I always consider the possibility that my personal computer would be infected with some kind of computer virus while I am opening a document or other type of file in the attachment of my e-mail.				**-.45**

Table 1. The results of factor analysis of survey items related to the assumptions and habits of Internet users regarding their online security and privacy (N=312).

The second factor (F2) related to engagement in *risky and careless online activities* was in low but statistically significant positive correlation of 0.14 with the criterion C1, and at the same time in somewhat higher statistically significant positive correlation of 0.23 with the criterion C2 (occurrence of loss of data on the home computer). This finding is not surprising since it can be expected that those Internet users who engage in *risky and careless online activities* are more likely to experience problems with malicious code infections of their home computers, and at the same time are also more likely to suffer from data loss on their home computers. However, this finding also indicates that the second factor (F2) is related to external criteria variables, which is an indirect proof its validity. Furthermore, this finding indicates that the education and promotion efforts aimed at prevention against malware attacks should focus on this type of user activity.

The correlation of the third factor (F3), which is associated with *disbelief in potential severity of security and privacy threats*, with criterion C1 (occurrence of home computer infection) was rather low (r=-0.17), but statistically significant. This could mean that Internet users who on average had experienced fewer occurrences of home computer infection were also likely to believe less in the potential severity of online security and privacy threats. This finding may have also been expected and it suggests that the education and promotion efforts related to the prevention of malware attacks should try to change this type of perception of the users who have not experienced or are not aware of serious security or privacy related intrusions into their computer systems. Finally, the fourth factor (F4), which is related to *lack of fear of online security and privacy threats*, was not in a statistically significant correlation with either of the two criteria variables (C1 or C2).

** p<0.01; p<0.05	F1 Conscientious behavior	F2 Risky/careless online activities	F3 Disbelief in severity of threats	F4 Lack of fear of online threats
C1 – home computer infection	.22**	.14*	-.17**	-.03
C2 – data loss on home computer	-.02	.23**	-.08	.03

Table 2. Correlation of factors of online security and privacy related behaviors with criteria variables (N=312)

To further analyze the relation of online security and privacy related behaviors of Internet users with security and privacy problems a regression analysis was performed. The 18 items of the survey associated with the assumptions and another 18 items of the survey related to habits of Internet users were used as predictor variables in regression analyses. The criteria were the variables *occurrence of home computer infections* (C1) and *occurrence of data loss on the home computer* (C2).

The results of the regression analysis for the first criteria variable are displayed in Table 3. According to the data presented in Table 3 the occurrence of home computer infection with malware/spyware was related to greater measures taken for protection of online privacy, reflection on the possibility of computer virus infection when opening files in e-mail attachment, avoidance of the use of business computers for private needs or activities, fear of unauthorized people accessing private mailbox, and tendency to visit "untrustworthy" web pages with possible malicious programs. Even though these variables are considered as *predictors* in regression analysis, semantically most of them resemble a *consequence* of previously experienced online safety and privacy violation(s), except for the predictor variable related to visiting "untrustworthy" web pages. It must be noted that the multiple regression coefficient with these predictors explained 18% of variance of the criterion variable (R=0.43).

The results of the regression analysis in relation to the second criteria variable *occurrence of data loss on the home computer* (C2) are displayed in Table 4. It must be noted that the three predictor variables in Table 4 explained only 6% of the variance of the criterion variable (R=0.24). It can be concluded that, among other predictor variables, the reported occurrence of data loss on the home computer in our study was predominantly associated with behaviors like visiting "untrustworthy" web pages, use of a business computer for private needs and non-business activities, and disregard for personal privacy after the use of the web from a computer used by other people. The variables associated with the maintenance of the operating system, the use of antivirus, antispyware or similar programs, were not identified as predictors of this criteria variable in this regression analysis perhaps because the subjects in this study were IT literate Internet users who took rather good care of these aspects of their online security and privacy. In fact, 69% of the subjects in our study stated (with a response "true" or "mostly true") that they regularly updated the antivirus protection of their computer and 62% considered themselves conscientious regarding the maintenance of the operating system of their computer. Furthermore, 72% of the subjects stated that they would install "patches" for their web browser or upgrade to the latest version of web browser, and 58% of them said that they were used to performing activities which ensure greater online security and privacy. However, many of the subjects in this study were also used to performing risky and careless online activities like visiting "untrustworthy" web pages, downloading MP3 files and file sharing. According to the data presented in Table 3 and Table 4, the latter were probably the dominant causes of security and privacy violations that were experienced by the IT literate subjects in our survey.

* β – beta coefficient of regression; T – test of significance; p – level of significance

PREDICTOR VARIABLE	β	T	p
I rarely take any measure for protection of my privacy when using the Internet because I believe that there is no special reason for privacy violation to happen to me personally.	-.20	-3.56	.00
I always consider the possibility that my personal computer may be infected with some kind of computer virus while I am opening a document or other type of file in the attachment of my e-mail.	.16	3.03	.00
I very rarely (almost never) use a business computer for my private needs or non-business activities over the Internet.	.16	3.01	.00
I think that no person will attempt an unauthorized access to my mailbox, and even if they tried, they could not succeed.	-.13	-2.53	.01
I tend to visit somewhat "untrustworthy" web pages on which malicious programs could perhaps be found.	.13	2.19	.03

Table 3. Results of stepwise regression analysis in relation to the criteria variable *occurrence of home computer infections* (C1; R=0.43; N=312)

* β – beta coefficient of regression; T – test of significance; p – level of significance

PREDICTOR VARIABLE	β	T	p
I tend to visit somewhat "untrustworthy" web pages on which malicious programs could perhaps be found.	.15	2.70	.00
I very rarely (almost never) use a business computer for my private needs or non-business activities over the Internet.	-.13	-2.32	.02
After the private use of the web from a computer that could be used by other persons I have never cleared the content of the file registering which web pages I have visited ("history") or the locally stored "temporary Internet files".	.13	2.28	.02

Table 4. Results of stepwise regression analysis in relation to the criteria variable *occurrence of data loss on the home computer* (C2; R=0.24; N=312)

6. Conceptual model of security and privacy related online behaviors

The factors of security and privacy related behaviors of Internet users with IT skills that are presented in Table 1, the correlation analysis in Table 2, and regression analyses in Table 3 and Table 4 indicate only a small interaction between occurrence of malicious code and data loss on home computers of Internet users (as predictor variables C1 and C2) with specific (types of) behaviors of Internet users. This can be at least partly explained by the characteristics of the predictor variables. For instance, the disbelief in severity of threats to online security and privacy (see factor F3 in Table 1) could lead to a greater chance of experiencing security and privacy violations. However, the actual experience of such problems could in turn result in greater belief that such threats exist and also in a more cautious behavior in order to prevent these threats which would subsequently result in less frequent occurrence of malicious code infections and consequent data loss on the home computer. Therefore, within a population of subjects (and also in the convenience sample in our study) there could be users who had not experienced much online security and privacy violations when using a home computer and who therefore disbelieve in the severity of threats (↓C1 & ↑F3 subjects). At the same time, there could be subjects who have experienced security and privacy violations when using a home computer and believe in the severity of threats (↑C1 & ↓ F3 subjects). The fact that this assumption is close to reality is confirmed by the data graphically represented in Figure 1. As can be concluded from the data presented in Figure 1, the first group of subjects (↓C1 & ↑F3 subjects; 21% of the sample) who stated that they had never experienced a malware infection on their home computer had higher factor scores for their disbelief in the severity of threat regarding their online security and privacy (these factor scores were calculated for factor F3 in Table 1; average factor scores for various subgroups of subjects were in the range from 0.41 to -0.18). On the other hand, the group of subjects who stated that they had experienced three or more occurrences of malware infections on the home computer had lower factor scores for their disbelief in the severity of threat regarding their online security and privacy (↑C1 & ↓F3 subjects; 20% of the sample).

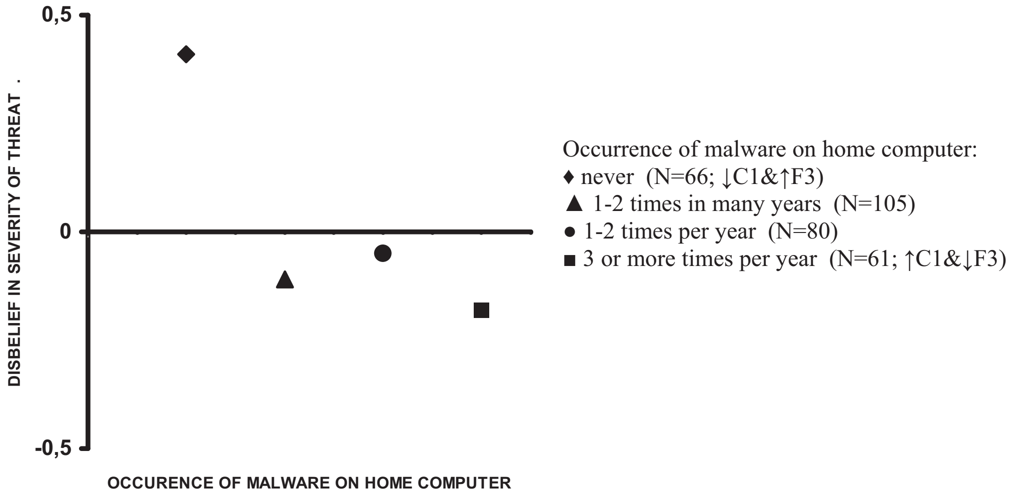

Figure 1. The relationship between the disbelief in the severity of threat to online security and privacy (represented by average factor scores for factor F3) and the occurrence of malware on the home computer for four groups of subjects

The previously outlined type of relationship is also expressed numerically by the statistically significant but rather low correlation of -0.17 between factor F3 and criterion C1 presented in Table 2. However, another reasonable supposition could be that those who disbelieve in the severity of online security and privacy threats should experience more occurrences of malware on their personal computer because they probably behave less cautiously in relation to prevention of those threats. Since the two tendencies regarding the relationship of occurrences of malware on the home computer and disbelief in severity of threats to security and privacy obviously work in opposite directions, the expected correlation between these two variables cannot be high.

The hypothetical duality in the influences between experienced security and privacy violations on the one side, and the behavior factors of Internet users which affect their online security and privacy on the other, is depicted in Figure 2. Whereas conscientiousness in the maintenance of the operating system, upgrading of the Internet browser and the use of antivirus and antispyware software should be associated with less experience with security and privacy violations, the correlation between the two related variables in Table 2 (F1 and C1) is oriented in the opposite direction. That is because more experience with malware on the home computer could also result in more care devoted to the protection of online security and privacy. The same type of duality of influences was mentioned earlier regarding disbelief in the severity of threats (factor F3) and probably also exists regarding risky online behaviors (factor F2) and fear of online threats (factor F4).

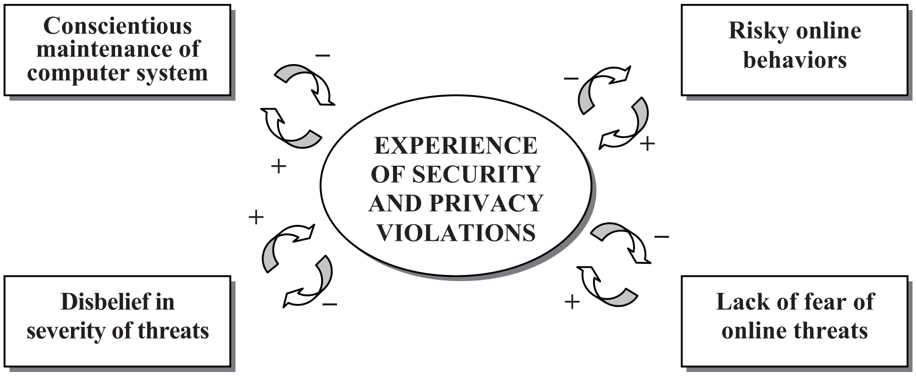
Conscientious maintenance of computer system
Risky online behaviors
EXPERIENCE OF SECURITY AND PRIVACY VIOLATIONS
Disbelief in severity of threats
Lack of fear of online threats
–
+
–
+
+
–
–
+

Figure 2. The conceptual model of the dual influences of experienced security and privacy violations with the factors of related behaviors of Internet users

There are probably other elements which may cause a low correlation between specific online behaviors and occurrence of malware/spyware on the home computer as one of the potential criteria in research of security and privacy related online behavior of Internet users. One of them may be unawareness of actual computer infections or of intrusions over the Internet in cases when a computer is inadequately protected. The AOL/NCSA Online Safety Study [1] revealed that a substantial percent of Internet users were not aware that their computers were actually infected by malware/spyware, which was revealed by a computer scan after they had provided answers to the survey questions. It is possible that less careful Internet users who are not afraid of online threats or disbelieve in them and therefore engage in risky online behaviors may also register less computer infections even though their computers are in fact infected by malware/spyware.

7. Results of the second study

In the second survey another group of 172 subjects were asked questions related to the conceptual model presented in Figure 2. The presumption that experience of security and privacy violations influences the conscientiousness in the maintenance of the computer system was tested with the survey question *"My previous problems with computer viruses, worms, spyware and alike motivate me for the protection of my computer."* It must be noted that 48% of the subjects in this second study responded with "much" and "very much" to this question. Similarly, it was found that 42% percent of the subjects responded with "much" and "very much" to the survey item *"I am more conscientious in the protection of my computer* *after I have experienced problems related to viruses, worms or spyware."* This confirms that the experience of security and privacy problems has a strong influence on the behavior of a substantial percentage of computer/Internet users (subjects in our second study) regarding the protection of their computer systems. Another assumption would be that other computer/Internet users take better care of their computer systems because they are conscientious individuals. In fact, 43% of the subjects in the second study responded with "much" or "very much" to the survey question *"I perceive myself as a very conscientious person and because of this trait I take more care of the maintenance of my computer and of my online security and privacy."*

To test if there are users who engage in risky activities because they have not experienced computer virus infections or spyware problems (or are unaware of them), the following survey statement was formulated in the second study: *"I engage in risky activities over the Internet (visits to potentially harmful web pages, downloading of executable code or file sharing) because I haven't had unpleasant experience with online malicious programs."* Such behavior was characteristic of 26% of subjects who responded with "much" or "very much" to that item of the survey. However, only 18% of the subjects have assessed themselves as risk-prone and used that type of response to the survey item *"I believe that I am a person who tends to take risks in various fields and therefore I behave the same way when it comes to visiting potentially harmful web pages, downloading of executable code and file sharing over the Internet."* It must be emphasized that 18% of the subjects also responded with "much" or "very much" to the survey question *"I believe that I am generally a brave person, i.e., it is difficult to scare me, and therefore I am not so concerned about how I could protect my computer and avoid unsafe activities while I am using the Internet."*

As many as 58% of the subjects in the second study stated that they felt quite confident when using the Internet because they had no bad experience with malware (they responded with "much" or "very much" to the survey item *"When I use the Internet, I feel relaxed regarding the protection of my computer because I have had no particularly unpleasant experience with viruses and alike."*). However, there were far fewer of those subjects who generally disbelieved in the potential online threats since only 13% of the subjects responded with "much" or "very much" to the survey item *"I believe that nothing can happen to me when I use the Internet, regarding my online privacy and security, because nothing has happened to me until now."*

To investigate whether some of the factors related to the conscientious and risk-prone use of computers and the Internet that were discovered in the first study could be confirmed, in this separate and additional study the method of factor analysis was again used to analyze the data collected with the 16 items of the second survey. The principal components factor analysis revealed four factors with eigenvalues greater than 1.0, which explained 59% of the variance. The Scree test also indicated that four factors should be preferred for varimax rotation. The results of the factor analysis of the items used in the second study are presented in Table 5 (only 13 factor markers with an especially dominant projection on a single factor are displayed in this table). It can be concluded from the semantic content of the items in Table 5 that the first factor (F1) in this factor analysis is related to *cautiousness after experience of problems with malware*. The second factor (F2) in this analysis could be labeled *conscientiousness in the maintenance of the computer system in relation to the protection against malware threats*. The third factor (F3) in Table 5 could be interpreted as *risk-prone behavior regarding online privacy and safety*. Finally, the fourth factor (F4) revealed in our second study could be interpreted as *relaxed use of the Internet without fear of malware infections because of no previous unpleasant experiences of that kind.*

The factors revealed in the second study are in concordance with the conceptual model of the dual influences on Internet users of their experiences of security and privacy violations and of the factors of online safety behaviors (assumptions and habits) that is presented in Figure 2.

* Only factor loadings of 0.30 or above are displayed. Factor loadings of 0.40 or above are written in boldface. (N=172)

SURVEY ITEMS	F1	F2	F3	F4
I am more conscientious in the protection of my computer after I have experienced problems related to viruses, worms or spyware.	**.75**			
I am afraid that my computer could get infected with a virus, worm or spy software when connected to the Internet because I have previously had similar unpleasant experiences.	**.74**			
My previous problems with computer viruses, worms, spyware and alike motivate me for the protection of my computer.	**.73**	.31		
The problems which other people had with computer viruses, worms and alike motivate me to protect my computer from the threats that are related to the activities with the Internet.	**.68**	.34		
I make effort to have the latest version of antivirus software on my computer.		**.78**		
I take care of the maintenance of the operating system on my computer (for instance, by installing the latest version and “patches”).		**.77**		.38
I try to protect my computer from spy software and check it regularly.	.36	**.70**		
I perceive myself as a very conscientious person and because of this trait I take more care of the maintenance of my computer and of my online security and privacy.		**.58**	-.31	
I believe that I am a person who tends to take risks in various fields and therefore I behave the same way when it comes to visiting potentially harmful web pages, downloading of executable code and file sharing over the Internet.			**.74**	
I engage in risky activities over the Internet (visits to potentially harmful web pages, downloading of executable code or file sharing) because I have had no unpleasant experience with online malicious programs.			**.71**	
I believe that I am generally a brave person, i.e., it is difficult to scare me, and therefore I am not so concerned about how I could protect my computer and avoid unsafe activities while I am using the Internet.			**.63**	
I believe that nothing can happen to me when I use the Internet, regarding my online privacy and security, because nothing has happened to me until now.				**.79**
When I use the Internet I feel relaxed regarding the protection of my computer because I have had no particularly unpleasant experience with viruses and alike.				**.70**

Table 5. The results of the factor analysis of the second study which revealed the following types of behavior in the use of computers/Internet: cautious / affected with malware (F1), conscientious (F2), risk-prone (F3), and relaxed / unaffected with malware (F4)

The dual influences can be observed in relation to the first factor (F1), which is associated with cautiousness after experiencing problems with malware, as well as the fourth factor (F4), which was interpreted as a relaxed use of the Internet without fear of malware infections because of no previous unpleasant experiences of that kind. It must be noted that, according to the data presented in Table 6, in our second study the first factor (F1) was in small but statistically significant positive correlation with the occurrence of home computer infection (criterion C1), and that the fourth factor (F4) was in statistically significant negative correlation with both the occurrence of home computer infection (C1) and data loss on the home computer (C2). This confirms the influence of non /experience with malware infection of a computer system on the security and privacy related behavior. Even though these results may appear as “common sense” outcomes of research, it is important to identify such tendencies in user behavior, as was done in our first study, and to confirm them (at least indirectly), as was performed in our second study, so that proper interventions could be designed at the level of user education toward the change in the attitudes and habits of computer/Internet users regarding their online safety and privacy.

Most of the factors of safety and privacy related behaviors that were identified in the first study had semantically comparative factors in the results of factor analysis of the second study. The factor labeled *conscientiousness* in the maintenance of the operating system, upgrading of the Internet browser and use of antivirus and antispyware software (F1) that was revealed in the first study (see Table 1) is comparable to the factor *conscientiousness in the maintenance of the computer system in relation to the protection against malware threats* (F2) that appeared in the second study (see Table 5). Also, the factor labeled engagement in *risky and careless online activities* with lack of concern for personal online privacy (F2) in the first study (see Table 1) is similar to the factor *risk-prone behavior regarding online privacy and safety* (F3) that was revealed in the second study (see Table 5). Finally, the factor identified in the first study as *lack of fear* regarding potential privacy and security threats with no need for change in personal behavior that would secure greater online security and privacy (F4 in Table 1) could be associated with the factor *relaxed use of the interned without fear of malware infections because of no previous unpleasant experiences of that kind* (F4 in Table 5). Even though the subjects were different and there were also somewhat different items in the second study, it can be concluded that the second study indirectly confirmed the results of the first factor analysis presented in Table 1.

** p<0.01; p<0.05	F1 Cautious / affected	F2 Conscientious	F3 Risk-prone	F4 Relaxed / unaffected
C1 – home computer infection	.18*	.04	.08	-.15*
C2 – data loss on home computer	.13	-.03	.11	-.28**

Table 6. Correlation of factors of online security and privacy related behaviors with criteria variables (N=312)

8. Discussion

The data presented in Table 1 confirm the first hypothesis (H1) in this research that the factors of potentially risky behaviors of Internet users with IT skills can be determined by factor analyses of items related to their assumptions and habits regarding safety and privacy in computer and Internet use. The following factors of security and privacy related online behavior of Internet users were revealed in our first study (see Table 1): F1 – *conscientiousness* in the maintenance of the operating system, upgrading of the Internet browser and the use of antivirus and antispyware programs; F2 – engagement in *risky and careless online activities* with lack of concern for personal online privacy; F3 – *disbelief* that privacy violations and security threats represent possible problems; F4 – *lack of fear* regarding potential privacy and security threats with no need for change in personal online behavior. However, the second hypothesis (H2) was only partly confirmed and the results of this study were mixed regarding the relationship of factors of potentially risky behavior of Internet users with IT skills on the one side, and greater possibility for computer infection with malicious code and loss of data on their home computer as criteria variables on the other. The factor of risky and careless online activities that was found in our first study (F2; Table 1) was in low but statistically significant positive correlation with the two related criteria variables (C1 and C2; see Table 2), and the factor of disbelief in the severity of online security and privacy threats (F3; Table 1) was in significant negative correlation with the first criterion (C1), which partly confirms the second hypothesis (H2). However, no correlation was found between the fourth factor (F4; Table 1) related to lack of fear regarding online security and privacy threats and both criteria variables (C1 and C2). Furthermore, the correlation of the first factor (F1; labeled *conscientiousness* in the maintenance of the operating system, upgrading of the Internet browser and the use of antivirus and antispyware programs; see Table 1) with the first criterion (C1) was in the opposite direction than hypothesized. To explain this phenomenon, a conceptual model of security and privacy related behaviors of Internet users was developed (see Figure 2). Finally, the third hypothesis (H3) was also only partly confirmed in our first study because there were mixed results in the use of regression analysis (see Table 3 and Table 4) for identifying specific risky behaviors of Internet users with IT skills that can be used as predictors of home computer infections with malicious code (C1) and loss of data on their home computer (C2).

Because some of the hypothesized relations of online safety and privacy related behaviors with criteria variables were not identified, a conceptual model of the dual influences of experienced security and privacy violations on the one side, and factors of related behaviors of Internet users, on the other, is introduced (see Figure 2). It can be concluded from this model that the predictor variables of online safety and privacy related behaviors should be used with criteria variables associated with *subsequent* and not *antecedent* experiences of security and privacy violations on their home computer. In other words, the previous experiences of the occurrence of malware/spyware and data loss on home computers influence the current online security and privacy related behaviors of Internet users and therefore may not be suitable criteria for regression analyses performed to identify potential causal relationships, as was intended in our first study. However, the correlation and regression analyses reported in our first study did confirm the association of risky and careless online behavior with the occurrence of malware/spyware on home computers of Internet users with IT skills.

To evaluate the conceptual model of the dual influences of experienced security and privacy violations and factors of related behaviors of Internet users (presented in Figure 2), a second study was conducted which confirmed the influence of experience regarding malware threats on the attitudes and behaviors related to protection against security and privacy threats. It appeared that while those users who have experienced unpleasant malware infiltrations on their computer systems tended to protect themselves better while using their computer and the Internet, those who had no previous unpleasant experience with malware were inclined to be less cautious and concerned.

9. Conclusion

Research into typical behavior patterns that affect online security and privacy of Internet users can be used for educational and promotional purposes, as well as for the design of reminders and warning systems that could reduce the occurrence of computer infections with malware and spyware. In this paper the factors of security and privacy related online behaviors of Internet users with IT skills were identified. It must be noted that somewhat different factors may have been revealed if a different set of survey items had been used (as was partly demonstrated in our second study) and if the sample consisted of users with less IT skill and Internet experience.

The factors revealed in our study partly reflect the categorizations of Rifon et al. [47], who have defined Internet users as *Newbies* (unsure of Internet dangers and do not know how to protect themselves), *Brave Surfers* (consider the Internet as a dangerous place but can cope with that), *Confident Surfers* (believe that the Internet is safe because they can protect themselves), or *Reckless Surfers* (think that the Internet is dangerous but do not care). However, their categorization was developed only for the purpose of forming focus groups and was not verified by means of factor analyses. Since no similar factor analyses were found, the results of our two studies may be the first attempt to produce an empirically founded categorization of safety and privacy related behaviors of computer and Internet users.

This study could be extended with further efforts to verify the factors presented in Table 1 and Table 5, as well as with additional studies that use criteria variables which measure the occurrence of security and privacy problems some time after a survey is performed that collects data on the online behaviors (assumptions and habits) of Internet users. This could be supplemented with actual virus/spyware scans of their computers or with the diary method for collecting data on malware intrusions.

Finally, some remarks should be made regarding aspects of computer security which the user should take care of: the use of antivirus and other protection programs as well as their regular updates; firewall use; careful approach towards unknown e-mails and their attachments; careful usage of programs that have been written by some unknown author; regular updates of the operating system; turning off user's computer or logging off and disconnecting from the network when it is not used; disabling of execution of mobile code (ActiveX, JavaScript, Java) whenever possible; disabling of scripting possibilities in e-mail clients; usage of strong passwords; taking care of safe password storage, and constant education about security flaws and ways of their prevention and protection against them.

References

[1] *** *AOL/NCSA Online Safety Study* [Online Report]. America Online and the National Cyber Security Alliance, 2004. Retrieved 30 September 2007, URL: http://staysafeonline.org/pdf/safety_study_v04.pdf

[2] *** *CERT Coordination Center Vulnerability Remediation Statistics* [Online Report]. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, U.S.A., 2008. Retrieved 8 October 2008, URL: http://www.cert.org/stats/vulnerability_remediation.html

[3] *** *F-Secure Malware Code Glossary* [Online]. F-Secure Corporation, Helsinki, Finland. Retrieved 30 September 2007, URL: http://www.f-secure.com/glossary/eng/malware-code-glossary.shtml

[4] *** *SANS Top-20 Internet Security Attack Targets (2007 Annual Update)* [Online Report]. The SANS Institute, 2007. Retrieved 8 October 2008, URL: http://www.sans.org/top20/2007/top20.pdf

[5] *** *Symantec Internet Security Threat Report: Trends for July – December 07* [Online Report]. Symantec Corporation, Cupertino, CA, U.S.A., 2008. Retrieved 8 October 2008, URL:http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_Internet_security_threat_report_xiii_04-2008.en-us.pdf

[6] Bailey, M; Cooke, E; Jahanian, F; Watson, D; Nazario, J. The Blaster Worm: Then and Now, *IEEE Security & privacy*, 2005, pp. 26 – 31.

[7] Boldt, M; Jacobsson, A; Lavesson, N; Davidsson, P. Automated Spyware Detection Using End User License Agreements. *Proceedings of the International Conference on Information Security and Assurance*, Busan, 2008, pp. 445 – 452.

[8] Carl, G; Kesidis, G; Brooks, R.R; Rai, S. Denial-of-service attack-detection techniques. *Internet Computing*, Vol. 10, No. 1, 2006, pp. 82-89.

[9] Castaneda, F; Sezer, E.C; Xu, J. WORM vs. WORM: Preliminary Study of an Active Counter-Attack Mechanism, *Proceedings of the 2004 ACM workshop on Rapid malcode*, Washington, DC, 2004, pp. 83 – 93.

[10] Chen, S; Tang, Y; Du, W. Stateful DDoS Attacks and Targeted Filtering. *Journal of Network and Computer Applications*, Vol. 30, No. 3, 2007, pp. 823 – 840.

[11] Dumitriu, D; Knightly, E; Kuzmanovic, A; Stoica, I; Zwaenepoel, W. Denial of Service Resilience in Peer-to-Peer File Sharing Systems, *ACM SIGMETRICS Performance Evaluation Review*, Vol. 33, No. 1, 2005, pp. 38 – 49.

[12] Flinn, S; Lumsden, J. User perceptions of privacy and security on the web. *Third Annual Conference on Privacy, Security and Trust (PST 2005)*. St. Andrews, New Brunswick, Canada, 2005. Retrieved 30 September 2007, URL: http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-48251.pdf

[13] Franz, M. Containing the ultimate Trojan Horse. *Security & Privacy Magazine*, Vol. 5, No. 4, 2007, pp. 52-56.

[14] Furnell, S.M; Bryant, P; Phippen, A.D. Assessing the security perceptions of personal Internet users. *Computers & Security*, Vol. 26, No. 5, 2007, pp. 410-417.

[15] Gehringer, E.F. Choosing passwords: security and human factors. *Proceedings of IEEE 2002 International Symposium on Technology and Society*, IEEE, Piscataway, NJ, U.S.A., 2002, pp. 369-373.

[16] Gelenbe, E; Loukas, G. A self-aware approach to denial of service defence, Computer Networks, Vol. 51, No. 5, 2007, pp. 1299–1314.

[17] Girard, J. A field guide to spyware vibrations, *Gartner Research*, 2004.

[18] Good, N; Grossklags, J; Thaw, D; Perzanowski, A; Mulligan, D; Konstan, J. User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware. *Journal of Law and Policy for the Information Society*, Vol. 2, No. 2, 2006, pp. 283 - 344.

[19] Gouda, M.G; Liu, A.X. Structured Firewall Design. *Journal of Computer Networks*, Vol. 51, No. 4, 2007, pp. 1106-1120.

[20] Gray, P. Privacy concerns: Perception versus reality. In: Cei staff (Eds.), T*he Future of Financial Privacy: Private Choices versus Political Rules*. Competitive Enterprise Institute, 2000, pp. 76-92. Retrieved 30 September 2007, URL: http://www.cei.org/pdf/2378.pdf

[21] Haggerty, J; Shi, Q; Merabti, M. Early Detection and Prevention of Denial-of-Service Attacks: A Novel Mechanism With Propagated Traced-Back Attack Blocking. *IEEE Journal on selected areas in communication*, Vol. 23, No. 10, 2005, pp. 1994 – 2002.

[22] Hansman, S; Hunt, R. A taxonomy of network and computer attacks. *Computers & Security*, Vol. 24, No. 1, 2005, pp. 31-43.

[23] Hussain, A; Heidemann, J; Papadopoulos, C. A Framework for Classifying Denial of Service Attacks, *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, Karlsruhe, Germany, 2003, pp. 99 – 110.

[24] Hussain, A; Heidemann, J; Papadopoulos, C. Identification of repeated denial of service attacks. *Proceedings of 25th IEEE International Conference on Computer Communications (INFOCOM 2006)*, Barcelona, Spain, 2006, pp. 1-15.

[25] Hutinski, Ž; Zlatović, M; Balaban, I. Identification of the frequency and the intensity of the threats in the function of development of the information system. *Journal of Information and Organizational Sciences*, Vol. 30, No. 1, 2006, pp. 63-81.

[26] Juels, A; Jakobsson, M; Stamm, S. Active Cookies for Browser Authentication, *Proceedings of the 14th Annual Network and Distributed System Security Symposium*, San Diego, CA, 2007.

[27] Keith, M; Shao, B; Steinbart, P.J. The usability of passphrases for authentication: an empirical field study. *International Journal of Human-Computer Studies*, Vol. 65, No. 1, 2007, pp. 17-28.

[28] Khu-Smith, V; Mitchell, C.J. Enhancing the security of cookies. *Lecture Notes in Computer Science: Information Security and Cryptology* (*ICISC 2001*), Springer Berlin / Heidelberg, Vol. 2288, 2002, pp. 197 - 230.

[29] Kienzle, D.M; Elder, M.C. Recent worms: a survey and trends. *Proceedings of the 2003 ACM workshop on Rapid malcode*, Washington, DC, USA, 2003, pp. 1-10.

[30] LaRose, R; Rifon, N.J; Wirth, C. Online safety begins with you and me: getting Internet users to protect themselves. *Annual conference of the International Communication Association (ICA 2007)*, San Francisco, CA, USA, 2007. Retrieved 30 September 2007, http://www.msu.edu/~isafety/ica07.pdf

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

[32] Lee, K-C; Mikhailov, L. Intelligent intrusion detection system. *Proceedings of 2nd International IEEE Conference on Intelligent Systems*, Varna, Bulgaria, 2004, pp. 497-502.

[33] Lee, Y; Kozar, K.A. Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, Vol. 48, No. 3, 2005, pp. 72–77.

[34] Lee, Y; Kozar, K.A. An empirical investigation of anti-spyware software adoption: A multitheoretical perspective, *Information & Management*, Vol. 45, No. 2, 2008, pp. 109–119.

[35] Li, T; Guan, Z; Wu, X. Modeling and analyzing the spread of active worms based on P2P systems. *Computers & Security*, Vol. 26, No. 3, 2007, pp. 213-218.

[36] Luo, X; Liao, Q. Awareness Education as the Key to Ransomware Prevention. *Information Systems Security,* Vol .16, No. 4, 2007, pp. 195–202.

[37] Lyda, R; Hamrock, J. Using entropy analysis to find encrypted and packed malware. *IEEE Security & Privacy*, Vol. 5, No. 2, 2007, pp. 40–45.

[38] Lopez, M.D; Charron, C. Spyware threat goes unchecked. *Forrester Research*, 2005.

[39] Miyazaki, A.D; Fernandez, A. Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, Vol. 35, No. 1, 2001, pp. 27–44.

[40] Moffie, M; Cheng, W; Kaeli, D; Zhao, Q. Hunting Trojan Horses. *Proceedings of the 1st workshop on Architectural and system support for improving software dependability*, 2006, pp. 12-17.

[41] Morales, J.A; Clarke, P.J; Deng, Y. Characterizing and Detecting Virus Replication. *Proceedings of Third International Conference on Systems*, Cancun, 2008, pp. 214-219.

[42] Paine, C; Reips, U-D; Stieger, S; Joinson, A; Buchanan, T. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, Vol. 65, No. 6, 2007, pp. 526-536.

[43] Park, J.S; Sandhu, R. Secure cookies on the web. *IEEE Internet Computing*, Vol. 4, No. 4, 2000, pp. 36-44.

[44] Perdisci, R; Lanzi, A; Lee, W. Classification of packed executables for accurate computer virus detection, *Pattern Recognition Letters*, Vol. 29, No. 14, 2008, pp. 1941–1946.

[45] Pinkas, B; Sander, T. Securing passwords against dictionary attacks. *Proceedings of the 9th ACM conference on Computer and communications security*, ACM, Washington, DC, USA, 2002, pp. 161-170.

[46] Rainie, L. Privacy Online: How Americans feel… the ways they are responding to new threats … and why they are changing their online behavior [Congressional Internet Caucus]. Pew Internet and American Life Project, Washington, D.C., U.S.A., 2005. Retrieved 30 September 2007, URL: http://www.pewInternet.org/PPF/r/50/presentation_display.asp

[47] Rifon, N; Quilliam, E.T; LaRose, R. Consumer perceptions of online safety. *Annual conference of the International Communication Association (ICA 2005)*, New York City, New York, U.S.A., 2005. URL: http://www.msu.edu/~isafety/papers/ICApanelfg.htm

[48] Shukla, S; Nah, F.F-H. Web browsing and spyware intrusion. *Communications of the ACM*, Vol. 48, No. 8, 2005, pp. 85 – 90.

[49] Stepan, A. Improving Proactive Detection of Packed Malware. *Virus Bulletin Ltd.*, Retrieved 7 October 2008, URL: http://www.virusbtn.com/virusbulletin/archive/2006/03/vb200603-packed.dkb

[50] Udo, G.J. Privacy and security concerns as major barriers for e-commerce: a survey study. *Information Management & Computer Security*, 2001, Vol. 9, No. 4, pp. 165-174.

[51] Vlachos, V; Androutsellis-Theotokis, S; Spinellis, D. Security applications of peer-to-peer networks. *Computer Networks*, Vol. 45, No. 2, 2004, pp. 195-205.

[52] Vu, K-P.L; Proctor, R.W; Bhargav-Spantzel, A; Tai, B-L; Cook, J; Schultz, E.E. Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, Vol. 65, No. 8, 2007, pp. 744-757.

[53] Wallach, D.S. A Survey of Peer-to-Peer Security Issues. *Lecture Notes in Computer Science: Software Security – Theories and Systems*, Vol. 2609, 2003, pp. 253 – 258.

[54] Wang, T-Y; Wu, C-H; Hsieh, C-C. A Virus Prevention Model Based on Static Analysis and Data Mining Methods, *Proceedings of IEEE 8th International Conference on Computer and Information Technology Workshops*, Sydney, 2008, pp. 288-293.

[55] Warkentin, M; Luo, X; Templeton, G.F. A framework for spyware assessment. *Communications of the ACM*, Vol. 48 , No. 8, 2005, pp. 79-84.

[56] Wu, N; Qian, Y; Chen, G. A Novel Approach to Trojan Horse Detection by Process Tracing. *Proceedings of the 2006 IEEE International Conference on Networking, Sensing and Control*, 2006, pp. 721-726.

[57] Xu, D; Li, X; Wang, X.F. Mechanisms for spreading of computer virus on the Internet: an overview. *Proceedings of 8th International Conference on Control, Automation, Robotics and Vision (ICARCV 2004),* Kunming, China, 2004, pp. 601-606.

[58] Yan, J; Blackwell, A; Anderson, R; Grant, A. Password memorability and security: empirical results. *Security & Privacy Magazine*, Vol. 2, No. 5, 2004, pp. 25-31.

[59] Yang, J.P; Rhee, K. H. A New Design for a Practical Secure Cookies System. *Journal of Information Science and Engineering*, Vol. 22, 2006, pp. 559-571.

[60] Yu, W; Boyer, C; Chellappan, S; Xuan, D. Peer-to-Peer System-based Active Worm Attacks: Modeling and Analysis. *Proceeding of the IEEE International Conference on Communications*, 2005, pp. 295 – 300.

[61] Zhang, B; Yin, J; Hao, J; Zhang, D; Wang, S. Using Support Vector Machine to Detect Unknown Computer Viruses, *International Journal of Computational Intelligence Research*, Vol. 2, No. 1, 2006, pp. 100 - 104.

[62] Zhang, X. What do consumers really know? *Communications of the ACM*, Vol. 48, No. 8, 2005, pp. 44-48.