Making the Internet a safer place: students' perceptions about Internet security threats

Radovan Vrana
Faculty of Humanities and Social Sciences
University of Zagreb
Ivana Lučića 3, 10000 Zagreb, Croatia
rvrana@ffzg.hr

Abstract. *Today's generations of students are among most frequent users of the Internet. During use of the Internet, students' computers are exposed to different types of security threats. To find out more about students' perceptions of this topic, a research at the FHSS in Zagreb was carried out. Results of the research show that respondents successfully recognized most common security threats, however they do not employ all the necessary basic protective measures available to them. They also feel that they are not fully capable of protecting their computers on the Internet, so they need more education in this area.*

Keywords. Internet security, user study, students

1 Introduction

Rapid spreading of the Internet has changed significantly many aspects of our lives from education, business, medical care, free time to making changes to individuals' life style.[1] Over the years, the Internet has become an environment which "(...) enables real-time dynamic interaction, facilitating global opportunities such as rapid communication, socialising, information and data sharing, banking, the sale and purchase of goods, and a vast array of business activities and information services."[2] As this global network attracts more and more new users, it has become evident that its users are more and more frequently exposed to numerous security threats. Currently, there are around 2.4 billion users on the Internet[4], and not all of them are benevolent and these users make the Internet extremely vulnerable to outside interference.[3] Such malevolent Internet users are best described as "(…) unscrupulous individuals with the opportunity to exploit and prey on the opportunities on offer in a 'cyber' world."[2] Their activities are qualified as cybercrime, which is "(…) a general term of convenience and is considered a subset of 'digital' or 'hi-tech' crime and as a generalisation for criminal and undesirable or harmful behaviour that is assisted or enabled by networked technology."[2] The results of activities of these malevolent user groups or individuals are usually called security threats. To prevent and avoid security threats or to successfully employ countermeasures, a regular Internet user must be appropriately educated. This will also make him/her a responsible user who will be able to protect his own computer and data from activities of malevolent individuals or groups. Nowak criticized irresponsible user behaviour which leads to less secure Internet environment and pointed out that "(...) many people regard the Internet as a service they can use as they please without assuming any responsibility. This view is reinforced by the fact that the Internet has no governmental structure, nor any central authority from which such rights and responsibilities might emanate."[5] Most popular Internet services are usually most frequently exposed to security threats, and this also has become the fact for Web 2.0. Because of its popularity, Web 2.0 has already attracted cybercriminals who transformed Web 2.0 into an environment which is sometimes very insecure for regular users and their personal data. Turner pointed out that "Web 2.0 has not itself created a new threat but rather increased the rate of potential exposure and highlighted the more complex threat environment that has developed."[6] Global trends such as social networking, cloud computing, and virtualization make situation more complex because they introduce new types of security threats and many aspects of these new threats are still unknown or less research. With each new Internet service and each new electronic device capable of connecting to the Internet, number of security threats on the Internet will increase. US National Intelligence Council foresees that "By 2025 Internet nodes may reside in everyday things: food packages, furniture, paper documents, and more. Today's developments point to future opportunities and risks that will arise when people can remotely control, locate, and monitor even the most mundane devices and articles."[7] All Internet users regardless of their age, education, job and position should be educated about risks as well as about their rights and responsibilities regarding the use of the Internet in order to make it a reasonably safe environment. This paper will focus on one group of intensive Internet users - students, and it will present results from the survey of students of the Faculty of Humanities and Social Sciences in Zagreb (FHSS) about their perception of the most common security threats and countermeasures that can be employed to make use of the Internet safer.

2 Most common security threats on the Internet and responsible user behaviour

Since the advent of the Internet, its users have witnessed many changes which re-defined their the way they use this global network. The Internet is "(...) most popular and useful communication and information infrastructure" today.[8] By becoming being very popular, the Internet has also become a platform for different criminal activities. During the years, cybercrime has become a very serious problem. The total damage created by cybercrime in 2011 was estimated to 388 billion US dollars, while over 1 million users every day (50 000 people every hour, 820 people every minute and 14 people every second) are victims of cybercrime.[8]

Today, most common security threats on the Internet are "(…) fraud, identity theft and theft of intellectual property rights. Cyber criminals are utilising a wide range of techniques including spamming, phishing, viruses, malicious code, hacking, denial of service attacks, network intrusion and the distribution and supply of illicit data to commit acts of both criminality and undesirable behaviour."[2] Furthermore, "(...) failure to secure and update the necessary protective applications, which now include spyware scanners, spam filters, firewalls, pop-up blockers, and browser hijack erasers as well as anti-virus software."[9] can cause serious damage as well as inadequate "(…) network configuration settings, to set our security and privacy preferences, manage cookies and spam filters, and close open ports that pass through firewalls on home networks."[9] As we can see, there are many ways in which cybercriminals as well as irresponsible Internet users can create damage to other Internet users. The first line of defense for users on the Internet are usually Internet service providers.

In attempt to protect their users, Internet service providers offer different types of security services such as antivirus software, antispam software, firewalls etc. either as a mandatory feature or as an option for users which like to set the level of security by themselves. However, not all Internet service providers offer necessary level of computer security to their users. As a result, Internet service providers are sometimes responsible for computer security related problems. Some of them ignore to protect their users as they decide not to offer secure delivery of their services because such effort would create additional cost for them.[10] Another reason for emergence of Internet security problems are security features Internet service providers do offer to their users, but which are often not enabled by default because "(...) there is nearly no explicit demand for them from the average, i.e., rather security unaware user."[10] Inexperienced users with no sufficient knowledge and skills about use of the Internet could often find themselves in situations in which they can suffer damage created by other Internet users. Kritinzger and von Solms think that "(...) many personal Internet users do not possess the information security knowledge to understand and protect their PC and therefore their personal information."[11] Furnell, Bryant and Phippen investigated home users to assess their perceptions of security issues, and their attitudes towards the use of related safeguards and they discovered segments that were lacking awareness and accompanying safeguards especially among novice users of the Internet who "(...) did not know how to protect themselves and were not aware of initiatives that may help them."[12] The Internet users, both experience and inexperienced, should be aware about the most common risks and threats that can influence their activities on the Internet and how to apply countermeasures to make their use of the Internet much safer. "It is therefore essential that all users understand the risks of using Internet, the importance of securing their personal information and the consequences if this is not done properly."[11]

University students are among most frequent users of the Internet, and, as such, they encounter different threats during their daily use of this global network. Some of the security threats are imposed to students by other users of the Internet, while some of them are provoked by students themselves because of insufficient knowledge, skills and experience about safe use of most popular Internet services. According to the latest Cisco Connected World Technology Report, college students demonstrated risky behaviour on the Internet because they are not very concerned about protecting passwords and they allow other people, even strangers, to use their computers and devices.[13]

Appropriate use of the Internet in an university environment is sometimes regulated by university policies or some other documents which state the rules of conduct in digital information environment. If a university does not have such a written document, it can be copied from the corporate environment and modified as appropriate. In his paper on IT security Turner suggested a list of guidelines for introducing and policing an effective IT policy which include a selection of steps. Some of them are:[6] the role of policy is to ensure the security of users (in his case, employees in a company, in case of this paper students at a university), messages written in the policy should promote flexibility regarding use of social media to ensure that security threats are contained, there should be a training program available, at least once a year which would demonstrate rules of conduct on the Internet, enforce the policy and review the policy as necessary etc.

It is almost impossible to avoid all the existing security threats while using the Internet, however, common sense and up to date knowledge about how to avoid certain types of unwanted behaviour could help students and other user categories to use the Internet more safely. Most security threats on the Internet could be prevented or avoided by preparing students to become more responsible users. The Internet itself offers numerous Web sites that offer guidelines for safe use of the Internet. For LaRose, Rifon and Enbody, it is "(...) possible to improve safety behavior by emphasizing the user’s personal responsibility."[14] According to Davinson and Sillence "Practicing secure behaviour is expected to be affected by perception of a threat being present and whether enacting a secure behaviour will actually reduce the threat."[15] The following part of the paper will present research about students' perceptions about security threats on the Internet.

3 Research

To find out more about students' perceptions about Internet security related issues, a research project was developed. The purpose of the research is to raise the level of awareness among the students at the Faculty of Humanities and Social Sciences in Zagreb about the necessity of being a responsible user of the Internet. The main hypothesis of this research was that students although frequent users of the Internet still lack knowledge and skills necessary for safe use of the Internet. An online survey was chosen as a method for this research. An e-mail invitation was sent to students' mailing list at the Faculty of Humanities and Social Sciences in Zagreb on March 6th 2012. and students of the first year of study of information sciences were asked directly to participate in the since they were not members of the students' mailing list. The survey was closed at March 23rd 2012 with total of 355 students who participated in the survey.

4 Findings and discussion

First two questions aimed at collecting data about sex of the survey participants and the year of the study at the Faculty of Humanities and Social Sciences in Zagreb. 267 (75,4%) female respondents, and 87 (24,6%) male respondents participated in this survey. The structure of the respondents was as follows:

Table 1. Academic structure of the respondents (N=355)

Year of study	N	%
First year of the undergraduate study	52	14,6%
Second year of the undergraduate study	31	8,7%
Third year of the undergraduate study	32	9%
Fourth year of the undergraduate study	8	2,3%

First year of the graduate study	58	16,3%
Second year of the graduate study	146	41,1%
Postgraduate/doctoral study	15	4,2%
Student of the old "Pre-Bologna" programs of study	13	3,7%

Most respondents who participated in this research are student of the graduate studies (senior students), followed by freshmen, while students of the second year and of the third year of the undergraduate study are less represented. Postgraduate students and students of the old "Pre-Bologna" programs of study are least represented in these results. The fact that not all students at the Faculty of Humanities and Social Sciences are members of the students' mailing list affected the structure and number of the respondents. It will also affect the possibility for students to receive news about security issues sent by the FHSS IT department and information about courses organized for them to overcome these issues at the Faculty or at the University.

Table 2. Electronic devices used to access the Internet (multiple answers) N=(354)

Electronic device	N	%
Desktop computer	129	36,4%
Portable computer	293	82,8%
Family computer	190	53,7%
Computer owned by a friend	141	39,8%
Computer in a public institution (library etc.)	313	88,4%
Computer installed in a public space	26	7,3%
Tablet computer	8	2,3%
Mobile phone (old generation)	88	24,9%
Mobile phone (smartphone)	131	37%
TV set	12	3,4%
DVB-T receiver with LAN capability	15	4,2%
Some other electronic device	0	0%

Most respondents in this research use personal computers in public institutions such as libraries to access the Internet. The FHSS has a new library building with approximately 200 PCs, all connected to the Internet. Respondents in this research also use portable computers to access the Internet. Significant number of respondents use computers which they share with other family members or friends. This situation can create certain security risks if all users of these shared computers are not aware about principles of safe use of the Internet. In addition to desktop computers and portable computers for which there are many software applications which serve to protect users from security threats, smartphones are third most used category of devices used for access to the Internet which is still less covered with antivirus and other security software although such software exists. So, respondents are therefore potentially more exposed to security threats when using smartphones to access the internet although the number of known threats for this platform is still rather low. This may change in near future.

Table 3. Security threats respondents recognize (multiple answers) N=(355)

Security threat	N	%
Social engineering	69	19,4%
Phishing	177	49,9%
Spoofing	54	15,2%
Farming	49	13,8%
Identity theft	341	96,1%
Spyware	285	80,3%
Adware	182	51,3%
Trojan horse	342	96,3%
Virus	350	98,6%
Worm	304	85,6%
Spam	306	86,2%
DDoS	76	21,4%
I don't recognize any threat on the list	0	0%

According to results in this part of the survey, respondents successfully recognized most common security threats on the Internet in the following order (first five): viruses, Trojan horses, identity theft, spam and worms. One can conclude that respondents at this non technical Faculty demonstrated that they were well informed about most common security threats.

Table 4. Security threats respondents encountered N=(350)

Security threat	N	%
Phishing	47	13,4%
Identity theft	58	16,6%
Spyware	179	51,1%
Adware	141	40,3%
Trojan horse	272	77,7%
Virus	308	88%
Worm	155	44,3%

Spam	284	81,1%
Some other security threat not listed here	13	3,7%

This question was oriented towards collecting data about security threats respondents actually encountered while using the Internet. As expected, respondents encountered security threats that are at high on the list of most common security threats of many major Internet security companies (first five): viruses, spam, Trojan horses, spyware, worms. Some of these threats are less destructive for computer data than others, which is good. It would be interesting to know what these 58 respondents who claim that they suffered from identity theft actually encountered or did on the Internet to feel that their personal data were compromised in the described way. Since this survey was anonymous, it is impossible to get such answer at the moment.

Table 5. Personal data respondents use for access to different Internet services (multiple answers) N=(351)

Personal data	N	%
User name	330	94%
Password	310	88,3%
debit/credit card PIN	41	11,7%
First and last name	244	69,5%
Home address	142	40,5%
OIB	52	14,8%
Phone number	106	30,2%
E-mail address	316	90%
Personal Web site URL	22	6,3%
Personal Blog URL	19	5,4%
Facebook profile URL	57	16,2%
Bank account number	29	8,3%
Credit card number or other means of electronic payment	63	17,9%

In addition to encountering different security threats, respondents are exposed to misuse of their personal data i.e. data about themselves and their private life. Different Internet services require different data for signing up and using their services, for which they offer different security levels. Most frequently provided data by students in this research for access to different Internet services (academic, library, banking, etc.) were user names, e-mail addresses and passwords. It should be mentioned that some data are less likely to be requested from users such as details about bank accounts etc. and that Internet sites requesting such type of data must provide solid explanation for requesting such type of personal data.

Table 6. Following URLs sent by email by other users N=(355)

Frequency	N	%
Never	28	7,9%
Seldom	143	40,3%
Occasionally	117	33%
Often	59	16,6,%
Always	8	2,3%

One of the most common ways of Internet users deception is sending URLs which will take users (i.e. their browsers) to different Web addresses which may contain malicious code. According to results, a significant number of respondents follow URLs sent to them by other Internet users occasionally and often. Modern Web browsers will partially protect users from Web sites known for security threats such as phishing by blocking access to such Web sites this decreasing the rate of security incidents created by users unaware of this type of problem.

Table 7. Ways of informing respondents about Internet security threats and countermeasures (multiple answers)
A= Information about security threats
B= Information about countermeasures

	A		B	
	N	%	N	%
I read articles in daily newspapers	161	97,6%	95	57,6%
I read articles in weekly newspapers	47	95,9%	25	51%
I read articles in scientific journals	33	82,5%	35	87,5%
I read articles in popular IT magazines	85	88,5%	85	88,5%
I read news at Web pages of IT security firms	93	80,9%	98	85,2%
I receive information from friends	270	95,1%	253	89,1%
I receive information from relatives	99	88,4%	82	73,2%
I receive	112	93,3%	95	79,2%

information in classes at the Faculty				
I attend courses outside the Faculty	8	100%	4	50%
I watch TV broadcasts	127	97,1%	79	60,8%
I listen to the radio broadcasts	34	97,1%	21	60%
I read news at IT related Web portals	192	91,4%	179	85,2%
I found out about Internet security threats and countermeasures in some other way	83	88,3%	79	84%

Most respondents in this survey chose friends and Web portals publishing IT related news as most frequently used information resources which helped them to become familiar with information related to security threats and ways of overcoming security related problems. These two categories of answers together with IT security related organizations, TV broadcasts and university courses represent most available information resources that respondents trust in case of Internet security problems. These results are not coming as a surprise because respondents are in close and frequent contact with their friends with which they exchange information about IT related news. Because of their high availability IT related news portals are excellent resource of current information about Internet security related issues.

Next six questions were related to actual measures respondents take in attempts to protect their computers and content stored on these computers from malevolent users on the Internet.

Table 8. Use of antivirus software on computer used to access the Internet N=(354)

	N	%
Yes	338	95,5%
No	12	3,4%
I don't know what antivirus is	4	1,1%

Almost all respondents use antivirus software as a means of protection from viruses and similar malicious software that users may download to their personal computers. Antivirus software is not expensive, and there are also a few free of charge respectable antivirus software packages students can use on their computers. Such a high percentage of respondents using antivirus software is encouraging and it proves that respondents are well informed about viruses and protective software.

Table 9. Use of firewall on computer used to access the Internet N=(353)

	N	%
Yes	297	84,1%
No	36	10,2%
I don't know what firewall is	20	5,7%

Similar protective software is a firewall which is also part of system of protection in most popular operating systems and it can be integrated in the operating system. However, users are sometimes unaware of its existence. According to the results in this research, respondents were well protected from different types of intrusion into their computers.

Table 10. Upgrading OS as a security threat countermeasure N=(350)

Frequency	N	%
Never	37	10,6%
Seldom	53	15,1%
Occasionally	102	29,1%
Often	52	14,9%
Always	106	30,3%

Upgrading operating system has become an automated procedure which helps users to stay current by applying different security related patches to their computer systems. However, less than one third of the respondents update operating system of their computer always, which enables malicious program code to infect students' computers. Upgrading the operating system has become mandatory and it is mostly done automatically. If this automatic procedure is disabled, the computer could become vulnerable.

Table 11. Upgrading software application as a security threat countermeasure N=(351)

Frequency	N	%
Never	25	7,1%
Seldom	61	17,4%
Occasionally	92	26,2%
Often	68	19,4%
Always	105	29,9%

Another way of protecting one's computer is to upgrade application code as to become less exposed to security threats. Again, less than one third of respondents update frequently applications they use which creates a risk for users of such software.

Table 12. Creating backup copies of important data N=(353)

Frequency	N	%
Yes	183	51,8%
No	170	48,2%

Only a little more than a half of respondents created backup copies of their important data which is an unsatisfactory result. Creating a backup copy is one of the most basic security procedures which offers users safety and availability of their personal data in future and prepares them for possible loss of data on their computer. This result should have been better.

Table 13. Frequency of change of passwords of Internet services respondents use N=(353)

Frequency	N	%
Never	105	29,7%
Less than once a year	122	34,6%
Once a year	58	16,4%
Once in 6 months	34	9,6%
Once in 3 months	30	8,5%
Once a month	3	0,8%
Several times a month	1	0,3%
Once a week	0	0%
Several times a week	0	0%
Every day	0	0%

Another basic measure for protecting user data is frequent change of password for access to Internet services. This is a known problem, and it seems that respondents in this research don't follow common security recommendations which usually suggest changing password every few weeks.

Last two questions were dedicated to assessment of respondents' abilities to respond to security threats on their own.

Table14. Assessment of respondents' knowledge about Internet security N=(355)

	N	%
Insufficient	87	24,5%
Sufficient	84	23,7%
Good	116	32,7%
Very good	57	16,1%
Excellent	11	3,1%

Most of the respondents assessed their level of knowledge about Internet security as good, and almost one half of the respondents assessed their knowledge as barely sufficient or insufficient. This result calls for immediate action and students should receive additional education about computer and Internet security either by enrollment in optional university preparatory/introductory courses or in courses outside university which will explain them employment of best methods of computer and personal data protection.

Table15. Ability to protect one self's computer N=(355)

	N	%
Yes	193	54,5%
No	162	45,6%

A little more than a half of the respondents think that they are able to respond to security threats on their own and to protect their computers from known security threats. While this result may seem satisfactory, especially for students of humanities and social sciences, results in previous questions suggest rather low level of knowledge necessary for actual implementation of computer security measures. Students should improve their abilities to recognize security threats and to protect their computers and other devices they use to access the Internet.

5 Conclusion

The Internet is one of the most interesting and most successful human inventions of all times. As such, it equally attracts both men and women, layman and experts, children and elderly, students and scholars. Unfortunately, not all of the Internet users are benevolent, and other Internet users are forced to protect themselves from individuals and groups on the Internet who are jeopardizing safety of their computers and content stored on these computers. Students are also frequent users of the Internet, and as such, they are exposed to different security threats on a daily basis. Because of this, they must be well educated about possible computer related security threats and countermeasures they can employ to protect their computers. To find out more about the current state of awareness of student at the Faculty of Humanities and Social Sciences in Zagreb about computer related security threats and safe use of the Internet, a research project was developed. Students who participated in this research project showed that they are informed about most common computer related security threats about which they receive information from their friends and from news on IT related Web portals. Most of them employ basic protection measures and tools on their computers such as antivirus software and firewalls, but they do no update their operating system code or applications code too often. They also change their passwords and make backup copies of their personal data occasionally which make them targets for security threats. Finally, based on their current knowledge and abilities to protect their computers and personal data, students feel they are still not able to protect their computers and personal data on their own. The main hypothesis of this research that students although frequent users of the Internet still lack knowledge and skills necessary for safe use of the Internet was confirmed. As a result of this situation, students should be offered additional education about safe use of the Internet and responsible behavior on this global computer network.

References

[1] Takemura, T, Umino, A: **A quantitative study on Japanese Internet users' awareness to information security: necessity and importance of education and policy**, World Academy of Science, Engineering and Technology, 2009, 638-644.

[2] Hunton, P: **The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model**, Computer Law & Security Review, 2009, 528–529.

[3] Smirnov, S: **Privacy on the Internet,** Russian Politics and Law, 2001, 51-63.

[4] **Key ICT indicators for developed and developing countries and the world (totals and penetration rates),** available at `http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html`, Accessed 25th February 2007.

[5] Nowak, G: **Taming the cyber frontier**, Computer Fraud & Security 2011, 2011, 5/9.

[6] Turner, R: **A new focus for IT security?**, Computer Fraud & Security 2011, 2011, 7-11.

[7] **Disruptive Civil Technologies Six Technologies with Potential Impacts on US Interests out to 2025**, available at `http://www.dni.gov/nic/confreports_disruptive_tech.html`, Accessed 28th February 2012.

[8] **Norton cybercrime report 2011**. available at `http://www.symantec.com/content/en/uk/home_homeoffice/html/cybercrimereport,`/, Accessed 28th February 2012.

[9] LaRose, R, Rifon, N, Liu, X, Lee, D: **Understanding online safety behavior: A multivariate model**, International Communication Association, New York, US, 2005.

[10] Völker, L, Noe, M, Waldhorst, O, Werle, C, Sorge, C: **Can Internet users protect themselves? Challenges and Techniques of Automated Protection of HTTP Communication**, Computer Communications, 2011, 457-467.

[11] Kritzinger, E, von Solms, SH: **Cyber security for home users: A new way of protection through awareness enforcement**, Computers & Security, 2010, 840–847.

[12] Furnell, SM, Bryant, P, Phippen, AD: **Assessing the security perceptions of personal Internet users**, Computers & Security, 2007, 410–417.

[13] **Cisco 2011 annual security report**, available at http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf , Accessed 28th February 2012.

[14] LaRose, R, Rifon, NJ, Enbody, R: **Promoting personal responsibility for Internet safety**, **Communications of the ACM**, 2008, 71-76.

[15] Davinson, N, Sillence, E: **It won't happen to me: Promoting secure behaviour among Internet users**, Computers in Human Behavior, 2010, 1739-1747.