Original scientific paper

Confronting Internet Security Threats

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

Summary

The paper presents the results from the research study of students at the Faculty of Humanities and Social Sciences, University of Zagreb, Croatia about their awareness and exposure to well-known internet security threats as well as their awareness about security threats countermeasures. The results of the research study indicate high level of awareness of students about internet security threats as well as the fact that they are exposed to widely internet security known threats to a certain degree. While students demonstrated knowledge about application of security threats countermeasures, that part of their activities could be improved further. Generally, students need additional and updated knowledge to raise the level of their readiness in order to be able to respond to known and emerging internet security threats. The results of the research will be applied in planning of university courses related to the internet security.

Key words: internet security, security threats, students

Introduction

In today's world, care for computer and other networked devices security has become almost as equally important as the development of information systems themselves. Recent cyber-attacks showed the importance of intrusion prevention by monitoring vulnerabilities and reducing security threats (Abazari, Madani and Gharaee, 2016). Vulnerabilities of computer and other networked devices (like smartphones and other smart devices) consist of "weaknesses in a system which can be exploited by the attackers that may lead to dangerous impact" (Jouini, Rabai and Aissa, 2014, 490). At this moment, there are many active security threats related to the use of the internet (Sherr, 2017; Burgess, 2017; Schroeder, 2017) that could exploit weaknesses in computer and other networked systems and cause substantial financial and other damages. To prevent realization of threats, an individual must be well informed about potential weaknesses in the operating system he or she uses on a computer or other device as well as about weaknesses in applications used in one's daily work. One such group of users of ICT are students which are highly active users of computers, smartphones, tablets and networking. As such they could easily become

victims of different security threats which could end in financial, intellectual, academic, reputation and other damages. To investigate the current level of awareness of students about well-known internet security threats and their exposure to these threats as well as their awareness about security threats countermeasures, a research study was initiated. This paper will present results from this research study.

Security threats

A (computer related) threat is "action or potential occurrence (whether or not malicious) to breach the security of the system by exploiting its known or unknown vulnerabilities. It may be caused by (1) gaining unauthorized access to stored information, (2) denial of service to the authorized users, or (3) introduction of false information to mislead the users or to cause incorrect system behavior (called spoofing)" (Threat). According to Technopedia, "threats are potentials for vulnerabilities to turn into attacks on computer systems, networks, and more". In addition to computer related threats, a category of their own are internet related threats. According to Symantec, 11 most common security threats include virus, spam, spoofing, phishing and farming, spyware, keylogging, adware, botnet, worm, Trojan horse, blended threat (combination of several threats at once), denial of service attack (DOS). In addition to viruses, Vernon included hacks into the list of threats, and hacks have become very frequent in recent periods of time. While some threats aim at a single system vulnerability, other involve multiple exploits (Technopedia) and target both businesses and individuals. The oppose threats, individuals must protect information with the prevention and detection of unauthorized actions by users of a computer (Microsoft). To reach the adequate level of security, one must also apply adequate countermeasures or protective measures. Online literature on internet threats and protective measures is abundant and will be limited to a small selection of references due to the space restrictions: Singh, Kumar, Singla and Ketti (2017) wrote about internet attacks and intrusion detection system; Byrne, Dvorak, Peters, Ray, Howe and Sanchez (2016) investigated user's perspective on risks relative to benefit associated with using the internet; Berriman (2017) wrote about youth using the internet and the governance of their use of the internet; Google introduced a program for teaching safe online exploration (2017); van den Berg and Keymolen wrote about the problem of internet regulation focusing on control vs trust issue; journal Education journal published an article on the internet safety measures (2017). The internet users can inform themselves about the latest internet threats by using many available information resources as the internet security is a topic of high interest to the widest possible circle of users of the internet. In addition to informing oneself about the internet threats and protective measures by using online courses and written, video and audio materials available on the internet, students at the Faculty of Humanities and Social Sciences at the University of Zagreb (who are in focus of this paper)

have a possibility of acquisition of knowledge about internet security. As part of the study program they can take part in courses related to use of ICT such as "Communication technology fundamentals", "Data protection", "Cryptology" and "Internet culture". In addition to the formal study program courses, students can choose short ICT training on site or online courses like "IT security" at the University computer centre in Zagreb, Croatia. The courses are intended primarily for students and teaching staff at the academic institutions in Croatia.

Research methodology

This research is a follow-up of previous researches on students' perceptions about the internet security threats (Vrana, 2012) and online social networks and security of their users (Vrana, 2013). To find out details about the current awareness and exposure of students to most common and active security threats and their awareness about security threats countermeasures, a research study was initiated. The purpose of this research study was to detect the level of awareness and exposure of students to security threats in order to offer them additional education about security threats countermeasures. The research study aims to answer the following research questions: RQ1: Are students exposed to internet security threats?; RQ2: Are students able to recognize the most common and most frequent internet security threats?; RQ3: Are students applying the basic security threats countermeasures? Online questionnaire with 16 closed type questions was chosen as the research method. While having some drawbacks as a research method, questionnaire is still valuable and applicable research method for researching a large number of potential respondents. The invitation for participation in the research study was sent by students' mailing list at the Faculty of Humanities and Social Sciences in Zagreb (University of Zagreb) in Croatia and it was also published on the main Web page of the same Faculty. The participation invitations were sent on May 9th 2017 with the closing date of May 17th 2017. Convenience sample was used a sampling method to attract as much students as possible for participation in the research study. The research study was closed on May 17th 2017 with 152 answer sets collected.

Research findings

Due to the space restriction, partial research study results will be presented in the following part of the paper.

The following part of results answers two research question; RQ1: Are students exposed to internet security threats? And RQ2: Are students able to recognize the most common and most frequent internet security threats?

Internet security threats recognized and encountered by respondents

Ability to recognize security threats represents an important step towards more secure use of the internet and avoiding well-known and well-documented threats. In this question, the respondents were given an opportunity to select (by

media) frequently announced security threats. The results indicate that the respondents are well acquainted with the most widely known threats except for more sophisticated and more complex threats like farming and spoofing. It is also surprising to see social engineering so low on the list of recognized threats since it quite a common threat. In the second part, the respondents were given the same list of security threats as in the previous question and a possibility to choose the threats they actually encountered. The results show that the majority of threats are spam and classic security threats like viruses, Trojan horses and worms. Adware is also highly ranked as it is present in many free (non-fee based) software applications. On the positive side, it is satisfactory to see phishing and identity theft ranked so low as consequences of their activities could be very severe.

Table 1. Internet security threats recognized by the respondents (multiple answers) (N=151) and internet security threats encountered by respondents (multiple answers) (N=149)

	Threats recognized by respondents		**Threats encountered by respondents**	
	N	**%**	**N**	**%**
Spam	145	96.0	121	81.2
Virus	143	94.7	105	70.5
Identity theft	135	89.4	101	67.8
Trojan horse	132	87.4	74	49.7
Adware	128	84.8	42	28.2
Spyware	123	81.5	27	18.1
Worm	111	73.5	21	14.1
Phishing	84	55.6	11	7.4
DDOS	43	28.5	8	5.4
Man in the middle	28	18.5	5	3.4
Social engineering	27	17.9	5	3.4
Farming	25	16.6	4	2.7
Spoofing	21	13.9	4	2.7
None of the above	1	0.7	1	0.7

Personal data used when signing / logging in into internet services

The choice of login data is usually predetermined by the internet service owner(s) and cannot be chosen / selected by internet users. Personal data protection is increasingly becoming topic of interest as many new online services require entering personal data. While some of the personal data are less secure either because of their shortness (PIN) or because they can sometimes be guessed based on available information about a particular internet user (login or e-mail address), other methods like user's picture are less frequently used (for instance, on smartphones in the process of face recognition) and can be falsified.

Table 2. Personal data used when signing / logging in into internet services (multiple answers) (N=151)

	N	%
E-mail address	139	92.1
Login name consisting of your first and last name	113	74.8
First name	77	51.0
Last name	72	47.7
PIN	56	37.1
Mobile phone number	33	21.9
Your picture	30	19.9
Personal identification number	11	7.3
Some other data	4	2.6

Unlock procedure used when accessing mobile phone

The aim of this question was to detect most commonly used mobile phone unlock procedure as a part of the phone access security. The unlock procedure is also a possible point of attack and must be taken into account when researching the problem of user's secure use of the internet. While PIN remains most popular phone unlock procedure, it is worth noting that not so insignificant number of users do not use any unlock procedure leaving their mobile phone openly accessible to anyone who can get into possession of the phone. The availability of some unlock procedures is directly related with the hardware installed in the mobile phone (for instance, fingerprint scanner), so, they are not available to all respondents.

Table 3. Unlock procedure used when accessing mobile phone (N=151)

	N	%
PIN	42	27.8
None of the above	38	25.2
Screen pattern	36	23.8
Fingerprint	21	13.9
User name or password	14	9.3
Retina scan	0	0.0

Frequency of following URLs sent in e-mail messages

The most recent phishing campaign that happened to Google in May 2017 (Levin, 2017) demonstrated clearly how important is for internet users to recognize valid from invalid URLs in their e-mail sent by hackers. The respondents who always follow URLs are also prone to phishing or virus infections more frequently than those respondents who do not follow URLs in their e-mails.

Table 4. Frequency of following URLs sent in e-mail messages (N=151)

	N	%
Seldom	70	46.4
Never	42	27.8
Occasionally	30	19.9
Often	8	5.3
Always	1	0.7

The next part of the research answers the following research question: RQ3: Are students applying the basic security threats countermeasures?

Informing oneself about internet security threats and informing oneself about internet security threats countermeasures

Informing oneself about the most recent and most dangerous internet security threats is a priority in establishing the behavior patent that helps in secure use of the internet. The aim of this questions was to discover sources of information the respondents use to inform themselves about the internet security threats. The most frequently chosen information sources are those at hand: friends and the university. It is interesting to see that some respondents use some other ways to inform themselves, however, some of them provided answers in which they state that they do not inform themselves at all. Similarly, to the first question, the question about and informing oneself about internet security threats countermeasures aimed at discovering sources of information for the respondents about internet security threats countermeasures. Except the most frequently chosen answer (friends), other answers differ from the previous question showing that the respondents seek information about countermeasures from professional sources which indicates that they are aware of existence of such sources and their potential quality when dealing with security threats.

Table 5. Informing oneself about internet security threats (N=150) and informing oneself about internet security threats countermeasures (N=149)

	Informing oneself about internet security threats		**Informing oneself about internet security threats countermeasures**	
	N	**%**	**N**	**%**
At the university	47	31.3	36	24.2
Internet security companies Web sites	30	20.0	45	30.2
Courses outside the university	4	2.7	2	1.3
Daily newspapers	16	10.7	11	7.4
Friends	81	54.0	80	53.7
General purpose news Web portals	38	25.3	28	18.8
Other ways of informing	63	42.0	47	31.5
Popular computer and internet related magazines	29	19.3	26	17.4
Radio	12	8.0	2	1.3
Relatives	30	20.0	30	20.1
Safe internet use specialized Web portals	45	30.0	62	41.6
TV	31	20.7	13	8.7
Weekly magazines	2	1.3	1	0.7

Solving internet security threats

In addition to being informed, the respondents have to also be able act for themselves in order to resolve the security threat issue. A significant number of them help themselves while other seek help from friends, experts and relatives. Dealing with the security threats by themselves indicate that these respondents are confident in their own knowledge and skills.

Table 6. Solving internet security threats (N=150)

	N	%
By myself	60	40.0
By the help of friends	33	22.0
By the help of experts	27	18.0
By the help of relatives	25	16.7
Other ways of solving threats	5	3.3

Antivirus software installed

Today, when there are free of charge antivirus software applications available globally, there is no excuse why one wouldn't have such a software installed on the device intended for access to the internet. The results in this question (N=151) indicate that 90,1% (N=136) have antivirus software installed on their device while 9,9% (N=15) of the respondents still do not have such a protection which could lead to security problems.

Frequency of operating system (OS) and application update on a device most frequently used for access to the internet; frequency of creating a backup copy of content on a device most frequently used for access to the internet

Software update is one of the most common and straightforward defense methods against security threats. Most recent OS-es and application offer automatic check-up for availability of updates and their installation thus helping users to avoid security holes in OS and applications they frequently use. With every new update, new safety features are added as it was evidently necessary in case of the most recent global ransomware attack (Hern, 2017.). The results (N=151) show that OS is updated occasionally and applications (N=151) often which is good as it raises the level of security. A more frequent application of updates would improve the security even more. Finally, creating a backup copy (N=151) of user data and applications is another critical activity in achieving the necessary level of security of computer and other networked systems. Unfortunately, the respondents are creating backup copies only occasionally and seldom which put them in danger of data and applications loss.

Table 7. Frequency of operating system (OS) and application update and frequency of creating a backup copy of user data (N=151)

	Operating system update		Applications update		Creating backup	
	N	%	N	%	N	%
Never	4	2.6	4	2.6	34	22.5
Seldom	22	14.6	15	9.9	43	28.5
Occasionally	53	35.1	38	25.2	46	30.5
Often	33	21.9	53	35.1	15	9.9
Always	39	25.8	41	27.2	13	8.6

Frequency of change of passwords in internet services one uses

Frequent password change is one of the best methods of protections against user account intrusion. The consequences of not doing so could lead to sever consequences as showed by the resent publication of a database with 560 million of user passwords on the internet (Broida, 2017). The answers to this questions indicated poor management of user accounts protected by passwords as almost one fifth of the respondents do not change passwords at all, while almost half of them do it less than once a year. Very few respondents change their passwords once in three months or even more frequently, which should be the standard procedure.

Table 8. Frequency of change of passwords in internet services one uses (N=151)

	N	%
Never	29	19.2
Less than once a year	64	42.4
Once a year	26	17.2
Once in 6 months	23	15.2
Once in 3 months	5	3.3
Once a month	3	2.0
Once a week	0	0.0
Daily	1	0.7

Estimation of students' knowledge about internet security

The final question aimed at receiving estimation of the respondents' knowledge about internet security in general. Almost half of the respondents showed that their knowledge is insufficient or sufficient which should be immediately improved given the situation with the severe security incidents occurring every week. Levels of knowledge stating good and very good could be also improved.

Table 10. Estimation of students' knowledge about internet security (N=152)

	N	%
Insufficient	37	24.3
Sufficient	38	25.0
Good	46	30.3
Very good	26	17.1
Excellent	5	3.3

Conclusion

Internet security is important at the university and outside of it. Students are very active users of the internet because university study programs require from them participation of ICT related activities. At the same time, they are also very exposed to every kind of internet security threats as almost any other group of frequent users of the internet services. Students inform themselves about the newest security threats as much as possible through various available channels of communication and by mediation of different people to remain up to date with the current internet security developments. The research study successfully provided answers to all three research questions: RQ1: the research study confirmed that students were exposed to internet security threats; RQ2: students were able to recognize the most common and most frequent internet security threats; RQ3: students were applying the basic security threats countermeasures. All three special hypotheses of the research study were confirmed: H1: students are well acquainted with the existence of most common and frequent security threats some of which they encounter in their daily academic activities; H2: students possess knowledge about the basic security threats countermeasures; H3: the level of knowledge of students about internet security is still low. To improve the situation, students should be offered additional courses which would enable to acquire additional theoretical and also hands-on knowledge about the internet related security.

References

Abazari, F.; Madani, A.; Gharaee, H. Optimal Response to Computer Network Threats. // 8th International Symposium on Telecommunications (IST'2016), IEEE, 2016, 729-734.

Berriman, L. Framing internet safety: the governance of youth online. // Information, Communication & Society. 20 (2017), 1829-1830.

Broida, R. 560 million more passwords were exposed -- was yours?. 16.5.2017. https://www.cnet.com/how-to/protect-yourself-from-the-latest-database-breach/ (18.5.2017.)

Burges, M. Another large cyberattack is underway and it could be worse than WannaCry. 18.5.2017. http://www.wired.co.uk/article/adylkuzz-cyberattack-malware (19.5.2017.)

Byrne, Z. S.; Dvorak, K. J.; Peters, J. M.; Ray, I.; Howe, A.; Sanchez, D. From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet. // Computers in Human Behavior 59 (2016), 456-468.

Communication technology fundamentals. http://inf.ffzg.unizg.hr/index.php/en/38-instruction/instruction-undergraduate-study/583-information-technology-fundamentals (13.5.2017.)

Data protection. http://inf.ffzg.unizg.hr/index.php/en/38-instruction/instruction-undergraduate-study/561-data-protection (13.5.2017.)

Google program teaches safe online exploration. // American School Board Journal. 204 (2017), 20.

Hern, A. How to protect your computer against the ransomware attack. (16.5.2017.) https://www.theguardian.com/technology/2017/may/15/windows-xp-patch-wannacry-ransomware-wecry-wanacrypt0r (18.5.3027.)

Internet culture. http://inf.ffzg.unizg.hr/index.php/en/39-instruction/instruction-graduate-study/576-internet-culture (13.5.2017.)

Jouini, Mouna, Rabai, Latifa Ben Arfa, Aissa, Anis Ben. Classification of security threats in information systems. // Procedia Computer Science. 32 (2014), 489–496.

Levin, S. Google Docs users hit with sophisticated phishing attack in their inboxes. 3.5.2017. https://www.theguardian.com/technology/2017/may/03/google-docs-phishing-attack-malware (18.5.2017.)

New drive on internet safety. // Education Journal. (2017), 7.

Schroeder, S. There's another hacking attack right now, and it's making more money than WannaCry. 18.5.2017. http://mashable.com/2017/05/18/adylkuzz-wannacry-attack/#riLJeC185Eqm (19.5.2017.)

Security Threats. https://msdn.microsoft.com/en-us/library/cc723507.aspx (18.5.2017.)

Singh, R.; Kumar, H.; Singla, R. K.; Ketti, R. R. Internet attacks and intrusion detection system. // Online Information Review 41 (2017), 171-184.

Sherr, Ian. WannaCry ransomware: Everything you need to know. 18.5.2017. https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/ (19.5.2017.)

Sveučilišni računski centar. http://www.srce.unizg.hr/osnovni-tecajevi/popis-tecajeva (13.5.2017.)

The 11 most common computer security threats. http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx (18.5.2017.)

Threat. http://www.businessdictionary.com/definition/threat.html (13.5.2017.)

van den Berg, B.; Keymolen, E. Regulating security on the Internet: control versus trust. // International Review of Law, Computers & Technology. 31 (2017), 188-205.

Vrana, R. Making the Internet a safer place: students' perceptions about Internet security threats // Proceedings of the 23rd Central European Conference on Information and Intelligent Systems, University of Zagreb Faculty of Organization and Informatics, 2012, 91-98.

Vrana, R. Online social networks and security of their users: an exploratory study of students at the Faculty of humanities and social sciences Zagreb // Central European Conference on Information and Intelligent Systems, University of Zagreb Faculty of Organization and Informatics, 2013, 214-221.