Cybersecurity From the User's Perspective

IGOR BERNIK
Faculty of criminal justice and security
University of Maribor
Kotnikova 8, SI-1000 Ljubljana
SLOVENIA
igor.bernik@fvv.uni-mb.si

Abstract: With the goal of raising general cybersecurity, we investigated the user's perception of cyberspace and used measures to protect information assets and threats. Using the descriptive method, the analysis of questionnaire data and the synthesis of findings, we present a view of the cybersecurity of users in Slovenia. Knowing the perception of the cyberspace and awareness of its usefulness and the perceived threats, we present guidelines for ensuring the safety of users who connect from the local environment to the global cyberspace. The research is partially limited and can only be partially generalized to the entire population. With in-depth further research, we want to collect data that can be generalized. The presented results are the upgrade of the state of affairs in the field of Slovenia, and at the same time they open the possibility of preparing appropriate measures for improving current status of user's cybersecurity.

Key-Words: cyberspace, security, user, privacy, cybercrime, awareness, protection

1 Introduction

According to international professional organisations and cybercrime researchers, the number of cybercrime cases exceeds the number of violent and financial crimes, and the economic consequences of organised drug and human trafficking. Its prevalence can be attributed to the optimistic bias and poor awareness of cyberspace users. . Cybercrime is one of the most significant security challenges of the 21st century and, therefore, a priority of numerous international organisations ([1], [2], [3]). "Researchers examining the fear of crime have found that fear usually exceeds the actual level of criminality in society and that many people are afraid of criminality"[4].

Many people are afraid to use their credit card to shop online, even though very few misuses have been reported, while in reality they readily let it out of their sight for minutes at a time; users are afraid that their personal data will be mishandled, even though there has been a relatively small number of identity thefts in Slovenia, etc. It is quite obvious that individual offences are overexposed by the media, thus causing more fear than is appropriate considering the actual threat. Young [5] ascertained that, "the mass media is a spectacular notice-board of exclusion … it stresses order, justice and inclusion (the backcloth of the news), yet it highlights disorder, injustice and exclusion (the foreground)". We believe that you same can be said for the user awareness of cybercrime and cybersecurity understanding.

Cyberspace users are not aware of the threats and risks lurking in cyberspace and they usually do not possess sufficient technical capabilities to efficiently protect themselves against them. Users, who are aware of threats and risks posed by cybercrime and possess the necessary knowledge with respect to self-protective measures, often fail to protect themselves, however, the motivational factors leading to the use/or failure to use self-protective measures against cybercrime are not explained in a comprehensive manner.

Existing studies focus on the reasons why users choose not to protect themselves against general and technological threats (e.g. protection motivation theory ([6], [7]), avoidance of information technology threats theory [8]), however, these do not present a comprehensive explanation of socio-psychological factors [9]. D'Arcy et al. [10] suggest the use of three safeguards to minimize endangerment and fear: users must be aware of potential threats, they must be educated about information security, and they must be introduced to various safety programs. How users conduct themselves in cyberspace depends on how well they are informed about its dangers [11]. One of such programs is provided by ENISA – the European Network and Information Security [12].

Awareness of cybercrime is related to the user's knowledge about cyber threats lurking in cyberspace. A particular problem is the limited awareness and technical knowledge of users; most users follow technological development but not the development of cyber threats. Hereinafter we present the results of our research which shed light on how cybersecurity is perceived in Slovenia.

2 Method

For the purposes of determining the actual situation among users of cyberspace in Slovenia in terms of safety, a pilot study on the performance of citizens was carried out. We researched how users use cyberspace; how they protect content against unauthorized use and what is their privacy concern and standpoint. In order to determine the actual level of awareness it is crucial to have a good understanding of the users' knowledge and level of awareness of the threats they face. The aim of the study was to check among the respondents if they use protective measures and which ones and what type of security programs follows to safely use cyberspace and how protects their data.

Survey was published online. The link to the survey was distributed via Slovenian websites for literacy of users of cyberspace. (Safe.si, Online Eye and Safe on the Internet). The questionnaire was accessible on the Internet for 15 days. The two-part questionnaire also covered general data pertaining to the statistical population. The part of the questionnaire covered awareness and knowledge of cybercrime, the second fear of cybercrime. The questionnaire comprised 28 closed-ended questions (1 Likert-scale, 1 numerical, 4 categorical and 22 multiple choice). Respondents were aged between 18 and 51 years (average age was 27.4 years). There were 179 respondents in total; The survey was fully completed by 179 respondents 78.4% of men and 21.6% of women. Most of the respondents (69.4%) finished middle school, 19.5% were university graduates, 7.2% had postgraduate education, and 3.9% had elementary level education. The statistical population was evenly dispersed across all Slovenian geographical regions, considering the population density.

3 Results

If we consider how respondents appraise threats to cybersecurity it becomes evident that many of them have knowledge of certain threats.

On the basis of the time spent in cyberspace of the respondents we conclude the intensity of the technologies and services use – Fig. 1.

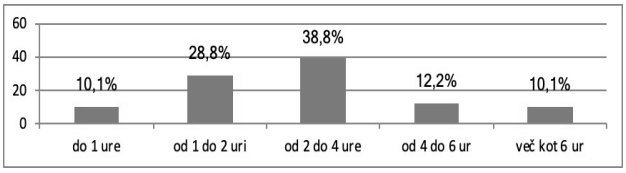

Fig. 1: Average daily use of cyberspace

The location and purpose of the primary use of the cyber space without interaction in the online social networks is shown in Fig. 2.

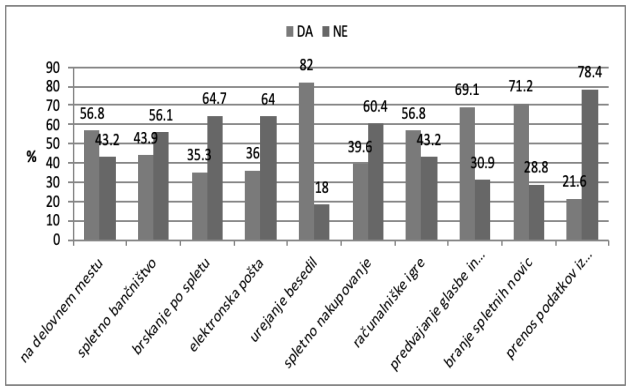

Fig. 2: Are the electronic devices in the cyberspace use safe?

Interesting is the deviation where as many as 82% of respondents feel that when using text editors (which can be extended to office programs), they are safe from abuse when working. On the contrary, in the transmission of data from the cyberspace where 78.4% of respondents consider their data to be more exposed to the dangers of abuse, even though the use of cryptography would eliminate the risks to a greater extent. Online social networking is intensively used by all respondents but they do not feel threatened at using it.

The use of security features for the protection of electronic devices is shown in Fig. 3. The image does not show the use of fingerprint protection, which is a fantastic option to protect modern devices (especially with the iOS and Android operating system). It is used by about ½ of all users.

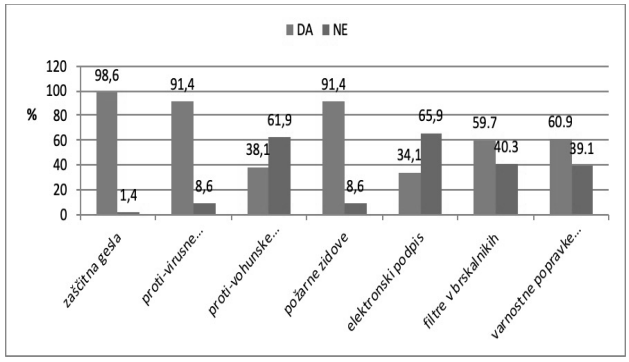

Fig. 3: Use of basic safety features

On the basis of the presented and other research results, obtained from survey responses and comparative analysis, wider starting points and comparative research, we conclude on the operation of citizens in the cyber space. Our research showed that users are relatively well informed about the various types of cybercrime and protections available for safe use of cyberspace.

4 Discussion and Conclusion

Using electronic devices, connecting to cyberspace and constantly exchanging data have become the constant of our everyday life. Access to information and linking users has changed completely with the emergence of the cyberspace, which has a significant impact on our work, communication and behaviour in society.

The results show (Fig. 1) that the average time used for cyberspace among the majority of users is about 2 hours a day, which is, in addition to the use of ICT for work / studies / school, approximately ¼ of you daily individual's free time. It is also due to this fact that it is clear that the way in which the principles of safety are respected and that the principles are respected is of the utmost importance.

Another interesting fact is the perception of security in the cyber space (Fig. 2), where a relatively small understanding of cybernetic threats from the public is observed, and therefore, when interacting with cyberspace, the basic security principles often fail to meet the requirements because they do not feel the need for it. This is reflected in the use of security solutions (Fig. 3), since they use the basic protection for private operation, which in the present complexity of the cyber space provides only partial and basic protection, they do not protect against the most frequently encountered threats. The year 2016, for example, in cybersecurity is also called Crypto virus year [13]and Ransomware, because they are one of the most pressing threats that can be avoided primarily by understanding and awareness of their presence (opening attachments, linking to web addresses). While comparing results we noted that more educated and/or older respondents were less afraid of cybercrime. This is obviously a consequence of the fact that these respondents know more, are more aware of the threats and likelier to protect their computer with at least the most elementary security software. Users who spend more time doing serious work on their computer are more aware how important it is to secure their equipment and save data, so they take more time to do so. Therefore even though these users are more exposed – business data is valuable, so it is more often the target of cyber criminals – they feel less threatened.

Working with computers, making use of mobile devices to connect to the Internet and exchange data, are now daily occurrences. Cyberspace has changed how users access information and establish connections, and this has greatly influenced our work, communications and social interactions. Of course, at the same time that data and other contents are transferred into cyberspace, so are various forms of cybercrime. New cybercrimes are emerging, for example those connected with social networks, because "the extent of personal information individuals exchange and publish on the Internet is increasing rapidly, particularly with the increasing popularity of social networks" [14]. Processes at the work place are so simplified that users don't need any knowledge about computer equipment and communication systems, and therefore also have no understanding of what really transpires in cyberspace.

There is a widespread lack of awareness regarding cybercrimes and cyber laws among the people who are constantly using information technology infrastructure for official and personal purposes. To raise awareness of this problem, users should be informed about all its various types, e.g.: web defacement, unauthorized network access, cyber-stalking, Internet fraud, identity theft, child pornography, interception and fabrication of e-mails and theft of passwords, to name just a few. To ensure protection against cyber criminals, to reduce endangerment and avoid possible consequences, it is important to follow basic guidelines.

Informing and educating about the dangers of cybercrime must become widespread, common and continuous at all level of society, so that cyberspace users will know how to use this technology rationally and responsible, and will not be afraid of it.

Disclaimer

This paper is based on a research programme Security and safety in local communities (P5-0397, 2015-2018, financed by the Slovenian Research Agency) carried out by the Faculty of Criminal Justice and Security, University of Maribor, Slovenia.

References:

[1] UNODC. (2015). *Doha Declaration on integrating crime prevention and criminal justice into the wider united nations agenda to address social and economic challenges and to promote the rule of law at the national and international levels, and public participation*. 13th United Nations Congress on Crime Prevention and Criminal Justice, Doha. Retrieved from https://www.unodc.org/documents/congress/Declaration/V1504151_English.pdf

[2] European Commission. (2015). *The European agenda on security*. Strasbourg: European Commission. Retrieved from http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[3] World Economic Forum. (2015). *Global risks 2015*. Retrieved from http://reports.weforum.org/global-risks-2015

[4] Meško, G. and Šifrer, J. (2008). Fear of crime in urban settings - an inquiry, *Journal of Criminal Justice and Security*, vol. 4, 2008, pp. 550-560.
[5] J. Young, J. (2007). *The vertigo of late modernity*, London, Sage.
[6] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, (91), 93-114.
[7] Rogers, R. W. (1983). Cognitive and physiological process in fear appeals and attitude change: a revised theory of protection motivation. In J. Cacioppo, & R. Petty (eds.), *Social Psychophysiology: a source book* (pp. 153-176). New York, NY: Guilford Press.
[8] Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), 71-90.
[9] Mihelič, A., & Vrhovec, S. (2017). Explaining the employment of information security measures by individuals in organizations: The self-protection model. In I. Bernik, B. Markelj, & S. Vrhovec (eds.), *Advances in cybersecurity 2017* (pp. 23-34). Maribor: University of Maribor Press.
[10] D'Arcy, J., Hovan, A., and Galletta, D. (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, vol. 20, pp. 79-98.
[11] Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information security policy compliance: an numerical study of rational-based beliefs and information security awereness. *MIS Quarterly, vol. 34*, pp. 523-A7.
[12] *ENISA*, (2016). Retrieved from http://www.enisa.europa.eu/
[13] Heater, B. (2106). *The Growing Threat of Ransomware*. Retrieved from http://www.pcmag.com/news/343547/the-growing-threat-of-ransomware
[14] Dimc, M. and Dobovšek, B. (2010). Perception of cybercrime in Slovenia, *Journal of Criminal Justice and Security*, no.4, pp. 378-396.