SOCIETY. INTEGRATION. EDUCATION
Proceedings of the International Scientific Conference. Volume V, May 28th-29th, 2021. 426-435

CYBER VULNERABILITY IN LIGHT OF ONLINE LEARNING REALITY

Inga Piščikienė
Vilnius College of Technologies and design, Lithuania

Jūratė Romeikienė
Vilnius College of Technologies and design, Lithuania

Brigita Šustickienė
Vilnius College of Technologies and design, Lithuania

Abstract. *Presently, as Covid 19 has caused most of educational processes to move online, cybersecurity and data protection is rapidly gaining importance in all educational institutions, and most of the academia became more vulnerable to cyberattacks. This article sheds some light on how communities of higher education institutions perceive increased online threats, what measures they take to protect themselves against cybercrime, whether they practice good security hygiene. This paper presents and analyses results of a survey conducted at higher education institutions (universities, colleges) into perception of cybersecurity, online culture and hygiene during the present times of remote education.*
Keywords: *Cyber threats, Privacy, Security, Social engineering, Social Networking Websites.*

Introduction

Social media and social networks are a beneficial realm for contemporary society. Interacting with millions of other Internet users in real time, shopping without leaving home, searching for information, blogging, studying and training remotely during a pandemic is just a small part of the benefits that Internet users enjoy in their world. However, Internet, despite the many benefits humanity enjoy, has increasingly been proven to be a double-edged sword. In the age of digitalization, much of both personal and organizational data has been transferred to the internet space, and alongside the facilitation of everyday life, information technology created threats. News about identity theft, information leakage, and violation of personal privacy has become part of frequent, if not every day, news.

The dominance of digital technology, the convergence of computer and communication devices have altered the way we communicate, conduct other important work, and so on. Technological advances in the past meant greater connectivity for computers; however, over the past decade it has shifted to digital socialization of people. The main factor behind this change is the growing

https://doi.org/10.17770/sie2021vol5.6367

popularity of the Internet, and thus of social networking sites (Bialaszewski, 2015). It has especially been apparent since the beginning of 2020, when in majority areas, business, education, etc., the use of the Internet from being optional became compulsory. According to the official statistics portal (Statistics Lithuania, 2020), in 2020, 82% of households in Lithuania had Internet access, 82% of the population aged 16-74 used the Internet at least once a week, 79% used the Internet for communication. 74% of the population of the same age read the news, 71% used it in their free time (watching movies or TV shows, listening to music, playing or downloading recordings, games), and 68% used online banking services. Unfortunately, such a huge digital population also means access to a countless number of potential victims of interactive scams. Digital photography allows global distribution of child sexual abuse material on a large scale. Digital information may be copied and shared, allowing copyright and related rights to be infringed. Social networks can be used for intimidation and bullying. Mankind's growing dependence on computers and digital networks is turning technology itself into a target for crime (Clough, 2011). Presently, not a day goes by without a record of some type of cybercrime: hijacking and defacement of websites, identity theft, a devastating virus attack, diversion of money from bank accounts, ransomware and theft of sensitive data. Security professionals face a never-ending battle with criminals, programmers, terrorists, and foreign intelligence agencies who feel the satisfaction of running viruses, trojans, worms, and other malicious software (Peltsverger & Zheng, 2016). Clearly, both a cybersecurity culture and an understanding of what constitutes a cybersecurity threat at all are particularly important today.

The Law on Cybersecurity of the Republic of Lithuania and the National Cybersecurity Strategy (National Cybersecurity Strategy, 2017) define the threat of cybersecurity as a threat arising ("may arise") "... to the availability, authenticity, integrity and confidentiality of electronic information transmitted or processed by communication and information systems and /or possibility to interfere with the operation, management and provision of services by communication and information systems". In this context, in accordance with the logic of the Law on Cybersecurity of the Republic of Lithuania, "cyber" should be understood as related to the environment consisting of computers and other communication and information technology equipment and the creation and / or transmission of electronic information. Thus, a cybersecurity threat is a threat to the environment between computers and information technology equipment and the information it contains and transmits.

The aim of this study was to find out the level of cyber literacy and culture among students and lecturers (academic community), their opinion about the usefulness of applying virtual environment elements at present, and to compare

the results of the survey in different age groups. For this purpose, the methods of the questionnaire survey and comparative analysis of the obtained data were used.

Identification of the Problem

Cybersecurity threats and the consequences of cyber incidents have been in the focus of the scholarly world for quite a while. The issues have been analyzed by Bellovin et al. (2017), Cullen & Armitage (2016), Heitzenrater & Simpson (2016) and Renaud & Zimmermann (2020). The authors highlight a variety of cybersecurity threats, e.g., malicious code, ransomware, spam, phishing scams, etc. Cyber-attacks in Lithuania usually happen using various social engineering methods, such as phishing, smishing, vishing (Kapsevičius, 2019). The concept of social engineering in information and computer systems is generally defined as a way to obtain information by technical and / or non-technical means (Manske, 2000).

Social engineering encompasses a broad spectrum of malicious activity. As the purpose of this article is cybersecurity perception and online culture, the focus here will only be on social engineering in the IT context. In terms of information security, social engineering is often used solely for the attacker's benefit. In these cases, social engineering involves manipulation to obtain sensitive information, such as personal or financial information. Computer users are tricked into voluntarily taking action to help break into and take over computer networks. It is observed that more and more social engineering methods are used to persuade the user to reveal confidential information (passwords, credit card numbers, etc.), to infect the computer with malicious code. This method manipulates users' emotions and psychology, lack of attention, ignorance of technology. For example, phishing is a form of attack primarily aimed at the human factor rather than the system. The consumer usually receives an email that mimics a request sent from a government agency or, say, a bank. The letter identifies the problem and asks for personal details. Because such a letter is very similar to that sent by a real institution, the consumer enters the required information, and this way, scammers achieve their purpose. Such emails can also contain viruses. Whaling works in a similar way, except that it is usually aimed at high-ranking employees and officials.

There are numerous forms of cyber-attacks, and while they are being prevented by various institutions at the national level, as well as by countless IT professionals, the real fight against them begins with the awareness of every Internet user. Cyber literacy and culture should be part of school curriculum, and knowledge about cyberspace and its protection should be constantly refreshed. In 2020, a survey was conducted in Vilnius higher education institutions to

determine the level of knowledge academic community has about cybersecurity, cyber threats, social networks security.

Research Methodology and Purpose

The aim of this study was to find out the level of cyber literacy and culture among students and lecturers (academic community), their opinion about the usefulness of applying virtual environment elements at present, and to compare the results of the survey in different age groups. For this purpose, the methods of the questionnaire survey and comparative analysis of the obtained data were used.

A quantitative survey was conducted in 2020, and 308 questionnaires were completed. The study involved staff and students from higher education institutions. Respondents were provided with questionnaires consisting of 20 questions. The questions were both closed and open, and this allowed for more detailed answers and more reliable information.

The questionnaire included general questions regarding information about the respondent, and more specific ones that were focused on the issues related to perception of security in cyberspace and preparation for it.

The survey involved 195 women and 113 men. For the most part, the respondents were students, so the 18-30 age group was the largest (83 %). The distribution of other respondents, who were academic staff, was as follows: 30-40 age group - 4 %. 40-50 age group - 8 %. and 50 years and more - 5 %. Students and lecturers of social and technological sciences were interviewed.

Research Results

The first set of questions was aimed at finding out the level of self-confidence and psychological characteristics of the respondents, and the very first question was *Do you trust other people*? Slightly more than half of all respondents (54.5%), said they tended to consider themselves distrustful, but almost the same number of the surveyed (30 %) thought themselves to be trusting, and 16.5% assigned themselves to neither of the categories. Comparing the results obtained in different age groups, it turned out that the older respondents were, the less trusting they thought themselves to be. Another question of that group - *Did you have to deal with scammers or manipulators* – received diverse answers. Almost a fifth (17,4%) respondents answered that they had not experienced such encounter. The majority of respondents (39.1%) had encountered telephone scammers, 26.1%. – had been faced with physical fraudsters and 17.4% with online scammers. The distribution of responses across age groups appeared to be very similar.

The next question *What information did the scammers want to obtain* received various replies. Some respondents reported that phone scammers tried to manipulate *a disastrous accident of a loved one*, to find out *bank account numbers*, to offer a *panacea for all diseases*, to ask for *financial support for an ill person*; internet fraudsters *hacked email and stole game data*, *stole money from the account*, infected the computer with a virus.

When asked how survey participants evaluated their learning/working environment in terms of security and confidentiality, two-thirds (68.8%) stated they felt safe, almost a fifth (18.8%) said that they did not feel safe, and the rest (12.5 %) did not have an opinion.

The next set of questions addressed the perception of cybersecurity among academia. To achieve this end, questions of practical nature were asked. For example, a question regarding knowledge of the concepts of social engineering, phishing, firewall revealed that more than a fifth (21%) respondents have not heard any of these concepts, one third (33%) of respondents have heard the concept of a firewall, more than one fifth were familiar with the concepts of social engineering and phishing (21% and 25% respectively). The finding emphasizes the general lack of cyberliteracy among some academic community. The analysis of the results across different age groups revealed that the majority participants of the youngest group were well aware of the meaning of the concepts, while a significant number of older respondents admitted not knowing the terms.

One more question of the same set addressed the ability to recognize cyber-attacks. The survey participants were presented with a few examples of cyberactivity and were asked to decide whether these were criminal or not. The majority of the respondents (86%) knew that a cyber-attack could be an email that contains a malicious link which is disguised to look like a familiar link or a link to an announcement about a bogus award, a fake website that looks almost identical to real, where internet users are tricked into revealing their personal/login information.

The answers to the question *Do you know how to distinguish dangerous from non-dangerous sites?* are visualized in fig. 1. The chart shows that respondents aged 18-30 believe they distinguish dangerous from non-dangerous sites, while the older age groups provided completely opposite answers.

When asked a more detailed question *What do http: // and https: // mean in a website address?* respondents of the youngest age group again demonstrated much better knowledge than older ones, as three-quarters of 18-30 age group knew that HTTPS encryption protects the channel between the browser and the website being visited, while in the older groups only up to one third knew the meaning.

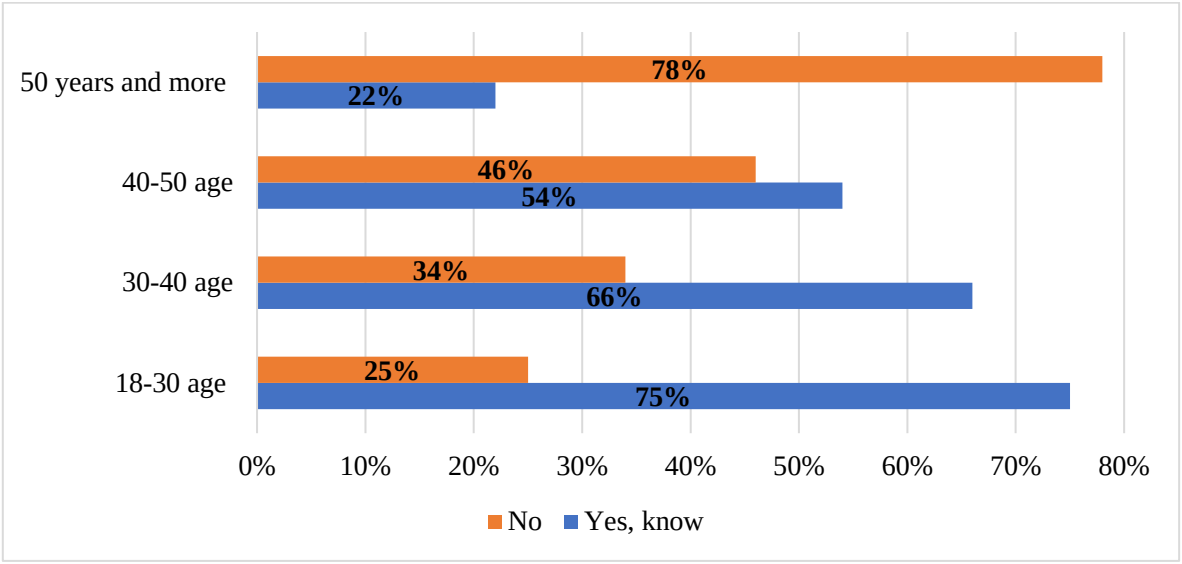

Figure 1 ***Respondents' Ability to Recognize Dangerous Websites***

Responses to a question about searching ("browsing") the Internet *Does your computer / phone have a filter (ban on unwanted and dangerous websites)?* again pinpointed to a lack of cyber-education among academia. Only one quarter of all respondents indicated that their devices were equipped with a filter that prevented visiting unwanted and dangerous websites; as many as three-quarters answered "I don't know." Responses did not differ between age groups.

When asked whether respondents *agree with all the statements/cookies/pop ups* when they open the file or download the program, more than half of the respondents in all age groups admitted that they do not if they do not understand all information provided, one tenth stated that they always agreed even without reading, and a quarter of survey participants read the information carefully before agreeing.

Respondents were asked to specify arguments for their answers. The most common motives were as follows: too many rules to read, time-consuming activity, unknown terminology, some participants indicated language barrier.

To find out how aware respondents were of the safety of the public internet use, a practical question *If you want to access a public Wi-Fi network and need a password, is it safe to use that network for sensitive activities such as online banking?* was asked. Although the majority (56.3%) believe that such a network is not safe to use for the transmission of "sensitive" information, many respondents (37.5%) still admitted not knowing whether the public Internet network is secure, and 6.3% believe that it is secure.

A vast majority of the survey participants (87.5%) appeared to realise the importance of a strong password and claimed to know how to create one. However, if the webpage does not provide a set of requirements for password

development, many admit still choosing their own or their children's names and birth dates, or using the same password for many web addresses. It is well known that such passwords are easy to crack and they do not protect against data breaches.

To find out opinion of the survey participants about the risks online, the following question was asked: *What internet threats do you find most dangerous?* The replies according to the age groups are presented in Table 1.

Table 1 ***Threats Named by Respondents***

	18-30 age group	30-40 age group	40-50 age group	50 year old and above group
Bullying on the internet	9.7%	18.1%	21.4%	33.1%
Internet fraud	19.2%	21.2%	19.9%	19.2%
Pirating	5.3%	5.3%	5.3%	3.2%
Viruses	21.3%	16.3%	12.3%	9.3%
Spam	4.6%	3.2%	3.2%	2.7%
False information	15.4%	11.5%	4.8%	11.4%
Data theft	24.5%	24.4%	33.1%	21.1%

A question *Which source of information do you trust the most?* addressed the level of trust people have in various sources of information. The majority of respondents aged 18-30 admitted that they equally trusted the information received on internet news portals (Delfi, 15min.lt, lrytas.lt, etc.) and the information received from friends. The groups of older respondents, however, expressed more faith in the information obtained from the news portals. In light of the previous question *Do you trust other people?* to which more than a half of responses were negative, it can be concluded that members of the educational community look for "reliable", "verified" information, sometimes using "information provided by friends" as a reliable source. Some respondents mentioned that "obtaining news is only getting information and does not create trust", a few admitted "checking several sources of information" and "using the knowledge of specialists".

The next set of questions was designed to find out how much knowledge the academic community had about cybersecurity.

The survey revealed that in all age groups only less than a fifth (18.6%) of respondents were educated about internet / cybersecurity in educational institutions, two thirds (62.1%) of respondents were interested in this issue and sought information themselves, but did not take part in any formal training or

lectures on the topic. A fifth of respondents (19.3%) stated that they had no interest in online safety at all.

The question *What would you do in the event of a cyber-attack?* (Figure 2), received diverse answers. This diversity proves that no uniform norms of behavior have been formed in the event of a cyber-attack. In such an event, everyone would behave spontaneously.

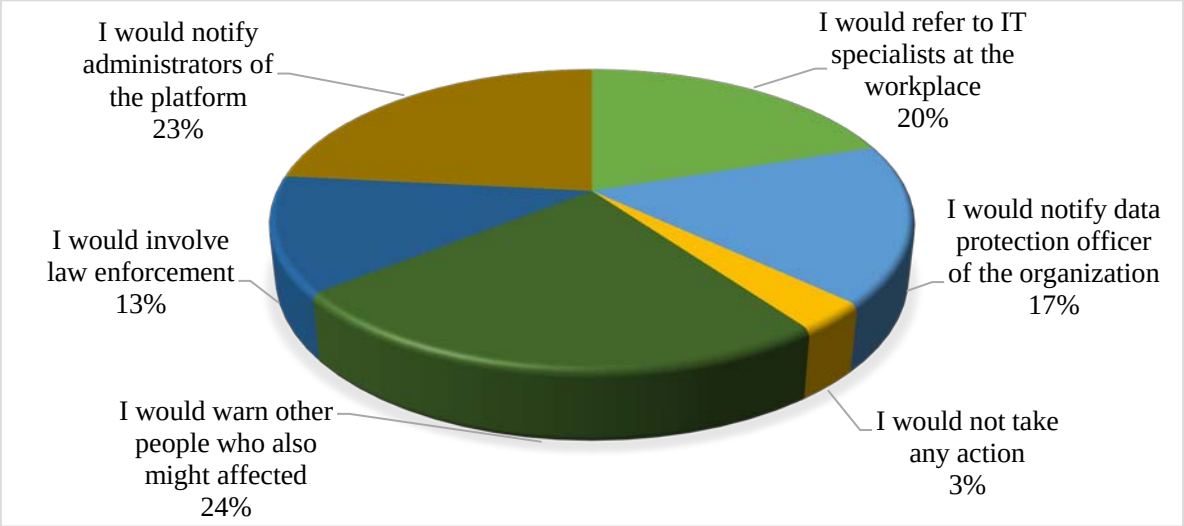

Figure 2 ***Actions of Respondents in the Event of a Cyber-attack***

The majority (90%) of respondents answered the question *Have you had to contact the relevant authority about a cyber-attack organized against you?* negatively. Survey participants claimed they had not experienced or been unaware of cyber-attacks because these did not cause any appreciable damage, and only 2% said they had to apply.

Respondents were also asked to identify knowledge they lack to protect themselves from social engineering attacks. The survey participants said they would benefit from acquiring technical knowledge about equipment security, safe internet browsing, they also expressed a desire to get some psychological knowledge enabling them to recognize aspects of manipulating.

Conclusions and Recommendations

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security. The purpose of cyber-attacks is usually to gain access to, modify or destroy confidential information, cheat out users of their money, or disrupt normal business processes.

Implementing effective cybersecurity measures today is particularly challenging, as devices outnumber people and hackers are using increasingly sophisticated attack techniques.

Manipulators frequently know the weaknesses of the IT users better than the users themselves, and people become easy prey for cybercrime.

The analysis of the survey revealed that the academic community is acquainted with cyber threats; however, in most cases, majority do not know what actions should be taken when faced with cyber-criminal activities. However, some responses clearly identified a lack of consensus on certain issues.

Although the scope of the research was not really large, the results of the survey still permit to conclude that younger members of the academic community have more experience using information technology, more flexibly seek information, trust information based on friends' experiences, have heard more about social engineering and manipulation terms, but do not dramatize cyber-attack threats. The older users of information technologies, on the contrary, collect information, verify it, trust major "verified" news portals.

Insufficient knowledge of academia about cybersecurity and accidental attacks by online manipulators can result in higher education institutions becoming a target for large-scale cyber-attacks that would disrupt the institution's work and leak "sensitive information".

The purpose of the survey was to shed some light on cyber-security awareness among members of higher education community. As a result, this study uncovered clear gaps in cyber literacy and a lack of in-house cyber-training. The situation could be changed if regular seminars on cybersecurity for the first-year students of a college or a university, as well as for academic and administrative staff were organized. The content of these trainings should cover information about secure passwords, secure use of personal data, social engineering threats, managing and banning access to different accounts (e.g., social networks), e-banking and other systems, law enforcement authorities that manage cyber-issues, and so on.

Cybersecurity is first and foremost a set of protective layers for computers, networks, applications, and data. It is important that all organizations, including educational, understand the importance of taking care of their cybersecurity and the cyber-literacy of their community. Effective protection against cyber-attacks is only possible with the right coordination of people, processes and technologies.

References

Bellovin, S.M., Landau, S, &Lin, H.S. (2017). Limiting the undesired impact of cyber weapons: technical requirements and policy implications, *Journal of Cybersecurity, 3*(1), 59–68.

Bialaszewski, D. (2015). Information security in education: Are we continually improving? *Issues in Informing Science and Information Technology, 12*, 45-54. Retrieved from http://iisit.org/Vol12/IISITv12p045-054Bialaszewski1770.pdf

Clough, J. (2011). Cybercrime. *Commonwealth law bulletin, 37*(4), 671–680.

Cullen, A., & Armitage, L. (2016). The social engineering attack spiral. *In Proceedings of the IEEE International Conference on Cybersecurity and Protection of Digital Services*, 1-6. Retrieved from https://ieeexplore.ieee.org/document/7502347

Heitzenrater, C.D., & Simpson, A.C. (2016). Policy statistics and questions: reflections on UK cyber security disclosures. *Cybersecur*. *2*(1), 43.

Kapsevičius, G. (2019). *Verslui vis labiau skaitmenizuojantis, kibernetinių įsilaužimų nuostoliai auga*. Retrieved from https://www.alfa.lt/straipsnis/50407155/verslui-vis-labiau-skaitmenizuojantis-kibernetiniu-isilauzimu-nuostoliai-auga

National Cybersecurity Strategy. (2017). January 28. Nr. XIII-202. Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.167925/asr

The Law on Cybersecurity of the Republic of Lithuania. (2018). June 27. Nr. XIII-1299. Retrieved from https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/15e540727ac211e89188e16a6495e98c

Manske, K. (2000). An introduction to social engineering, *Security Management Practices*, *6*, 53-59.

Peltsverger, S., & Zheng, G. (2016). Enhancing Privacy Education with a Technical Emphasis in IT Curriculum, *Journal of Information Technology Education: Innovations in Practice*, (15). Retrieved from http://www.jite.org/documents/Vol15/JITEv15IIPp001-017Peltsverger1873.pdf

Renaud, K., & Zimmermann, V. (2020). How to Nudge in Cybersecurity, *Network Security*, 2020(11).

Statistics Lithuania. (2020). *Informacinių technologijų naudojimas namų ūkiuose*. Retrieved from https://osp.stat.gov.lt/informaciniai-pranesimai?articleId=8028975