World Academy of Science, Engineering and Technology
International Journal of Educational and Pedagogical Sciences
Vol:17, No:1, 2023

# Cybersecurity Awareness among Applied Sciences Student Population

Nikolina Kasunic, Sanja Bracun



***Abstract*—**After graduation, student population of applied sciences will become the population of employees on IT experts' positions or "just" business users of certain IT technologies for which the level of awareness of existing cybersecurity risks is extremely important. This research results define the current cybersecurity awareness level of students at Zagreb University of Applied Sciences (TVZ), what can be useful not only for teaching staff to form a curriculum related to cybersecurity more accurately but also to employers to know what to expect from their future employees regarding cybersecurity awareness level. There is also a connection determined between the student's behaviour and their level of cybersecurity awareness.

***Keywords*—**Applied sciences students' population, cybersecurity, cybersecurity awareness, student population cybersecurity awareness.

## I. Introduction

SINCE digital technologies are deeply incorporated in our everyday personal and professional life, security awareness regarding those technologies should be on a secure enough level, especially among the population of technically oriented students such as applied sciences students.

Social engineering is considered as a method most used for execution of attacks or as a step towards system intrusion, and human element in breaches scales up to 85% [1], showing the importance of security awareness among general population, especially employees.

According to the RAND Europe report, there is a trend observed in all parts of the world, from the United Kingdom, where over 75% of job openings request digital skills, to sub-Saharan Africa, where almost 65% of job openings mandate at least basic level of digital skills. The study showed that 69% of job openings in New Zealand, Australia, Singapore, the United States and Canada were in digital occupations and similar trends have been reported in Europe with 85% of all EU jobs requiring at least a basic digital skills level [2].

Applied sciences student population is a population which will most likely work with digital technologies (not only IT oriented students) thus they should have good level of cybersecurity awareness.

## II. Related Work

There is a significant number of related works published worldwide. In [3], authors evaluate the level of cybersecurity awareness among undergraduate students, concluding the need for raising the level of cybersecurity awareness among students and recommend obtaining different datasets from different universities for comparison. In [4] authors are assessing the level of cybersecurity awareness among college students in Indonesia, concluding their good level of awareness with recommendations for improvement in specific areas. In [5] authors made research to assess the level of cybersecurity awareness among students at a private tertiary education in South Africa, determined possible vulnerabilities and recommend targeted cybersecurity awareness campaigns and further surveying.

In [6] authors surveyed ICT users in Croatia to determine the level of cybersecurity awareness, coming to alarming results where 28.8% users have revealed their password for professional e-mail system and concluding with the need for actions to raise the level of cybersecurity awareness. In [7] authors made research on internet users in Croatia regarding their knowledge on internet security, with special emphasis on social networks, concluding that respondents were well informed on internet safety topics and willing to learn further. In [8] author researched on the topic of college student's internet usage and security awareness, with a significant result of 68% of students with an interest for deeper knowledge on cybercrimes.

Authors in [9] conducted a survey on Saudi general population concluding that in order to defend against the rapidly increasing number of cyber-attacks, the level of cyber-security awareness of everyday people should be significantly raised since 51% used their personal information to create their passwords and 32.5% did not have any idea about phishing attacks.

## III. Methodology

The methodology for conducting this research was developed as a sum of various research from related work, based on a sample of students of undergraduate and graduate studies at TVZ. The sample included 163 students of undergraduate and 55 students of graduate studies. The share of female students (17%) in the total sample is representative with the total number of students on TVZ. The sample size and their distribution by level of study (undergraduate and graduate studies) as well as by individual studies on TVZ are not possible. What is also indicative and related with our topic, in our sample 53% of TVZ students are already employed (in part- or full-time job).

To accelerate data gathering and to make it as simple as possible, collection of data was conducted via CAWI method

Nikolina Kasunic is with the Zagreb University of Applied Sciences, Zagreb, Croatia (corresponding author, e-mail: nikolina.kasunic@tvz.hr).

Sanja Bracun is with the Zagreb University of Applied Sciences, Zagreb, Croatia (e-mail: sanja.bracun@tvz.hr).

(Computer-assisted web interviewing). The collected data were analysed using the computer statistical programme SPSS 20.0, which is appropriate for research in social and technical fields.

The basic analysis of the collected data is based on descriptive statistics, which describes the main characteristics of collected data in quantitative terms. In further statistical analysis Spearman's correlation coefficient was used to check the direction and strength between selected variables, while their statistical significance was tested by Chi-square. Through the research we tested a positive correlation between the level of cybersecurity awareness and students working status, how careful they are clicking on links in an email or social media posts and the habit of checking the legitimacy of a website before accessing it. Based on our experience, we expected a higher level of cybersecurity awareness among students who are already employed, who very carefully click on unknown links and those who regularly check the credibility of the site before accessing it.

*Research Method*

The data were collected via the web questionnaire available for student access over a 15-day period in March 2022. The questionnaire was prepared as a Google form and students were provided with a link for access. Call for participation was posted on University of Applied Sciences web site, e-mail with a call for participation was sent to teaching staff at Zagreb University of Applied Sciences to motivate students for participation on their classes.

The structure of the questionnaire is as follows:

- Part 1. Internet access: determining student's most used device type, internet access type and OS.
- Part 2. Actual knowledge: determining student's actual knowledge on cybersecurity topics.
- Part 3. Security practices: determining student's self-perception of cybersecurity practices.
- Part 4. Actual cybersecurity skills and behaviour: determining student's actual cybersecurity skills and behaviour.
- Part 5. Cybercrime experience: determining student's experience with cybercrimes.
- Part 6. Demography: determining student's demography information.

The questionnaire was pretested and adapted according to feedback prior to distribution to students. Testing was done with five lecturers at Zagreb University of Applied Sciences, later engaged in questionnaire distribution among students.

Each part of the questionnaire is designed to show different aspects of cybersecurity to enable us to define a comprehensive cybersecurity awareness (CSA) level. In CSA framework calculation we included only parts 2 to 4 which have a different weight. Answers from part 2 (Actual knowledge) and part 3 (Security Practices) are weighted at 30% and part 4 (Actual Behaviour) is weighted at 40 %, as shown in Fig. 1.

Preferred answers on questions from all three parts of the questionnaire could reach maximum of 100 points. After application of the specified weights on total number of points, each student is assigned to a specific level of CSA. Result was 3 different levels: not satisfactory or poor (0-55 points), good enough (56-80 points) and satisfactory or good (81-100) level of CSA.

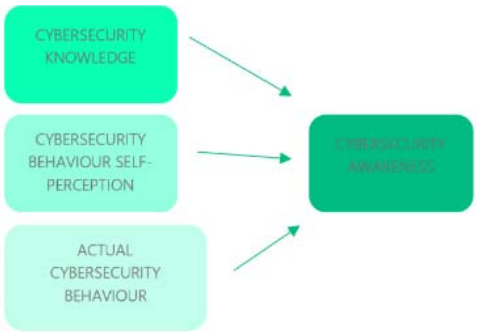


Fig. 1 CSA framework

## IV. Results

As expected, almost all students in our survey (96%) access the internet on daily basis, mostly from their smartphones (92%), but also from their laptops (56%) or desktop computers (38%). Most used type of internet access is via private Wi-Fi (79%) or direct internet access from their smartphone (72%). The use of public access to the internet is almost sporadic (3%).

Students are not particularly concerned about the possibility of being targeted by cyber-attacks. Only 16% of them think their digital devices (computer or smartphones) possess some value to potential hackers so they could be a reason to target them. The most common used operating systems are MS Windows (50%) and Android (35%). iOS, Linux, or Mac operating systems are each used less than 7%.

E-mail from fake bank account asking to provide information regarding credit card (95%) or encryption of all data with asking to make a payment for their decryption (94%) are most often expressed examples considered as cybercrime. Common examples considered as cybercrimes are also e-mail threatening to publish private data on visits on adult sites unless making a specific payment (85%), collecting and monitoring traffic on a public or a private network (85%) and mining cryptocurrency without necessary authorizations (83%). Only slightly fewer common examples recognized as cybercrime are Website with fake web shop (80%) and deliberate generation of high volume of traffic to cause a service unavailability (79%). In following, some of the forms of cybercrime are analysed.

Phishing is correctly recognized as a spam to fool receivers to disclose their personal information (81%). For our survey participants' Website spoofing is even less recognized. 69% of them recognize it as presenting false information to deceive visitor to disclose his private information. For 11% of them website spoofing is representing spying their device, while 19% of participants can not clearly express their definition of website spoofing. Definition for man in the middle attack for 77% of our survey participants is situation when attacker intercepts communication between two users, 6% think it is a situation when attacker misleads its victims in disclosing sensitive information and 17% of them cannot express what is behind this situation.

There is an even more different view of what is implied by social engineering. Majority of survey participants consider social engineering as a situation when attacker misleads its victims in disclosing sensitive information (50%), following with abuse of social network usage or attacker using information from social media (each by 18%). 14% of this survey participants cannot clearly express their attitude regarding social engineering.

Majority of our sample participants (67%) often or sometimes check the legitimacy of a website before accessing it (check the domain name, the protocol in use or explore the domain with search tool etc.). Only 13% of our survey participants do that always, while 20% of them check the legitimacy of websites seldom or never (7%) as it may be seen in Fig. 2. 67% of them are aware of potential danger when clicking on banners, advertisements or pop-up screens that appear when surfing the internet. Only 3% are not aware some of this potential danger.

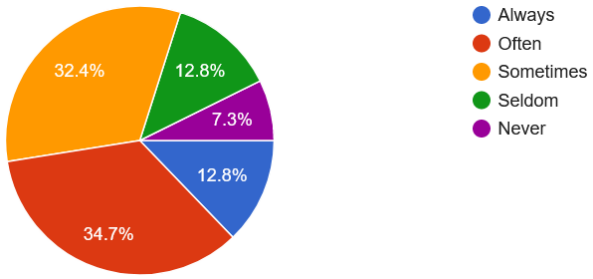


Fig. 2 Results on checking the legitimacy of a website

When they are on social media (e.g., Facebook, Instagram, etc.) 70% of the participants give always or often due attention to privacy settings, the rest of them do it sometimes or seldom. That is because majority of them do not believe that social media services have task to protect any personal information. Before using any website only 3% of the participants carefully read the terms and conditions of their usage but 83% of them regularly install available software updates and 71% of them think they are very careful about clicking on links in an email or social media posts, as seen in Fig. 3.

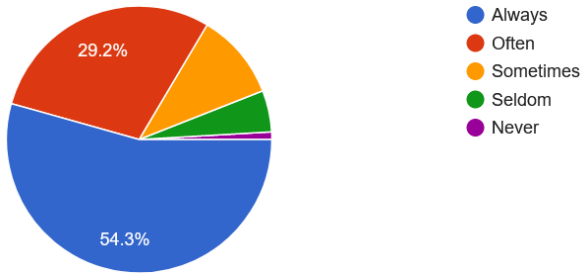


Fig. 3 Results on careful clicking on links in e-mails and social media posts

The following set of questions were crucial for definition of student's CSA level which depends on their knowledge, security practices and actual behaviour regarding cybersecurity. Students should have chosen the correct procedure in case of the following situations:

- When they receive an e-mail with a message “Hey, check this paper and click on the link below!”, and they are not writing a seminar with certain professor 90% will ignore or delete his email.
- When they see an advertisement for a new web shop offering number of trendy brands with great acceptable prices and find cool sneakers want to buy, 99% will firstly check web shop credibility and after that proceed only if they offer payment on delivery.
- When college IT administrator mandates all users to create strong passwords 81% will create a password like: S4dm3v1d1Ss4d$n3& or use password generator.
- When they are on a trip which they planned for months, 55% will share photos of all the great scenes directly with friends or family (on Telegram, WhatsApp, etc.) and 33% of them will not share at all their photos before returning home. With ignoring security 12% of them will immediately put all photos on favourite social media accounts (Instagram, Facebook, etc.).
- When they are in a coffee shop with open Wi-Fi network and need to make a payment over bank account, 59% will make the payment with usage of own mobile network connection (mobile data) or 33% who will also correctly make the payment subsequently when they will be on their home network (secure Wi-Fi). Again, with ignoring security, 7% of this survey participant will log into their banking application and make the payment on available open Wi-Fi network.

Based on all those results and applied CSA framework on our survey participants sample, we defined 56% students with satisfactory, 28% with good enough and 16% with poor level of CSA. Obtained results are little bit disappointing bearing in mind the sample consists of students of Informatics and Computing who should have a significantly higher level of CSA.

Positive correlation between established level of CSA and students careful clicking on links in an email or social media posts and checking the legitimacy of a website before accessing it is confirmed. The greater CSA of students also implies their greater attentiveness when clicking on links in an email or social media posts, as seen in Fig. 4. Between these two variables there is a proven positive, although relatively weak correlation ($\rho = 0.37940885$) which is statistically significant ($p = 0.004454543$). The greater cyber security awareness of students also implies and their greater attentiveness checking the legitimacy of a website before accessing it, as seen in Fig. 5. Between these two variables there is also proven positive and relatively weak correlation ($\rho = 0{,}314083938$) which is statistically significant ($p = 0{,}002073515$).

Although we expected that students who are full-time or at least occasionally employed have a more pronounced CSA, the results of this research did not support our expectations. All levels of CSA are almost equally represented among working and non-working students. With a risk level less than 5%, we can conclude that there is no statistically significant difference ($p = 0.020656863$) between the level of CSA and the working

status of students.

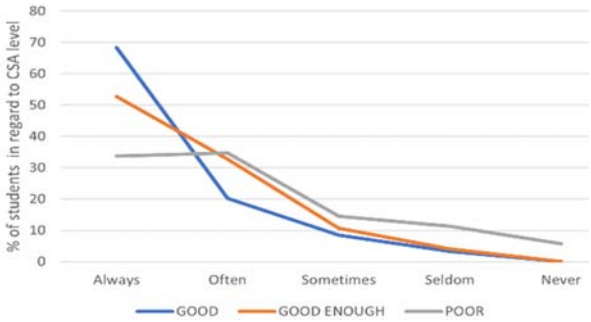


Fig. 4 Correlation of CSA and caution while clicking links

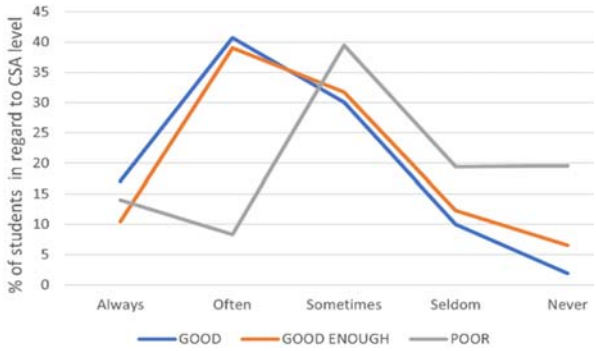


Fig. 5 Correlation of CSA and caution while visiting websites

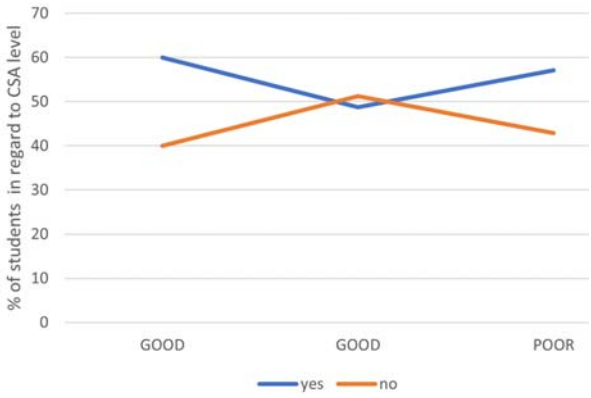


Fig. 6 Correlation of CSA and work status

## V. Conclusion

Positive connections with cautious clicking on links in e-mails and social media posts as well as checking the legitimacy of a website before accessing it, and the level of CSA were found. These questions can be used as a pointer of CSA level.

Even though this survey participants show majorly good enough and good level of CSA, more intake should be on a good level. Many of them will work on network, application, software or information system design, implementation and/or upgrade and they should be aware of potential cybersecurity issues when planning any of previously listed activities. The rest of them represent a population which will most likely work with digital technologies, and they should be aware of the dangers their online and offline behaviour could bring. As mentioned in introduction, human factor is the weakest link in every cyber defence procedure.

To ensure a higher level of CSA among student population, TVZ should ensure a cybersecurity topic on all departments, in a form of designated lectures as part of currently active courses or as new courses with focus on cybersecurity topics. Topics should be adapted to each department and study learning outcomes. Before these lectures will be launched, TVZ will, as a continuation of this research, additionally test the interest of its students for participation in lectures related to cybersecurity.

## References

[1] Verizon Communications. Data breach investigations report, 2021. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf Accessed 13 July 2021

[2] C. Feijao, I. Flanagan, C. van Stolk and S. Gunashekar, “The global digital skills gap, Current trends and future directions”, RAND Corporation, Santa Monica, Calif., and Cambridge, UK, 2021

[3] T. Alharbi, A. Tassaddiq, “Assessment of Cybersecurity Awareness among Students of Majmaah University”, Big Data Cogn. Comput. 2021, 5(2), 23

[4] Chasanah, B. R., & Candiwan, C. (2020). Analysis of College Students’ Cybersecurity Awareness in Indonesia. SISFORMA, 7(2), 49. https://doi.org/10.24167/sisforma.v7i2.2706

[5] Chandarman, R., & Van Niekerk, B. (2017). Students’ Cybersecurity Awareness at a Private Tertiary Educational Institution. *AJIC Issue*, *20*. https://doi.org/10.23962/10539/23572

[6] K. Solic, T. Velki and T. Galba, "Empirical study on ICT system's users' risky behavior and security awareness," *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2015, pp. 1356-1359, doi: 10.1109/MIPRO.2015.7160485.

[7] Božić, S., & Jakšić, D. (2020). Users’ Perception of Online Privacy and Security in Croatia–A Survey. *Communication Management Review*, *5*(02), 6-29.

[8] M. Bošnjak, (2021). A cybercrime awareness among young adults with special reference to Croatian college students. University of Zagreb, Faculty of Economics and Business, Master’s thesis, https://gs.statcounter.com/social-media-stats/mobile/croatia/2018

[9] A. Alzubaidi, “Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia”, Heliyon 7, e06016, 2021

**Nikolina Kasunic** is a lecturer at Zagreb University of Applied Sciences, with course portfolio in Computer Networks and Cybersecurity area. Majority of formal and informal education has been focused on Computer Networks area: undergraduate study programme in Electrical Engineering (Communication and Computer Engineering), graduate study programme in Information Technologies Engineering (Design and Development of Computer Networks), various Cisco programmes and certifications: CCNA, CCNP, CCNA Cybersecurity Operations, CCAI.

She has been a Cisco Networking Academy manager at Zagreb University of Applied Sciences for more than 10 years, the only Cisco academy in Croatia with Academy Support Center – ASC and Instructor Training Center – ITC status and academy with numerous awards for excellence in programme deployment.

**Sanja Bracun** born 1965 in Zagreb, where she graduated in 1989 and in 1992 received her master's degree from the Faculty of Economics, University of Zagreb. After 26 years of work in the real sector and active participation in numerous projects, since 2013 she has been working at the Zagreb University of Applied Sciences as a lecturer in Electronic Business in Economics, Market Communications, Asset Management, Technology and Business Management Systems and Innovations in Digital Economy. As a continuation of her scientific research work, in 2020 she defended her doctoral dissertation entitled as "Entrepreneurial competencies in creative and cultural industries" at the International Interuniversity Postgraduate Interdisciplinary Doctoral Study "Entrepreneurship and Innovation" at the Faculty of Economics in Osijek.

For the last two years, together with other teachers in her institution, she mainly teaches online, trying to transfer her knowledge and experience to

students in these different conditions to enable their easier integration into the labour market after graduation.