Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus - A Case Study of Higher Education Institutions in Portugal and Poland

Luís Oliveira[1][a], Andrzej Chmielewski[2][b], Paulina Rutecka[3][c], Karina Cicha[4][d], Mariia Rizun[3][e], Pedro Pinto[1,5][f]

[1]*Instituto Politécnico de Viana do Castelo, 4900-347 Viana do Castelo, Portugal*

[2]*Faculty of Computer Science, Bialystok University of Technology, 15-351 Bialystok, Poland*

[3]*Department of Informatics, University of Economics in Katowice, 40-287 Katowice, Poland*

[4]*Department of Communication Design and Analysis, University of Economics in Katowice, 40-287 Katowice, Poland*

[5]*INESC TEC, 4200-465 Porto and Universidade da Maia, 4475-690 Maia, Portugal*

l.oliveira@ipvc.pt, a.chmielewski@pb.edu.pl, {paulina.rutecka, karina.cicha, mariia.rizun}@uekat.pl, pedropinto@estg.ipvc.pt

Keywords: Cyber, Cybersecurity, Hygiene, Awareness, Campus, Higher Education Institutions

Abstract: Cybersecurity-related concerns emerge with the evolution and the scale of devices and the data exchanged between them. From developers to end users, cybersecurity minimal skills are of utmost importance to prevent or mitigate the impact of cyberattacks targeting devices, networks, and information. In higher education, there are graduations related to Information Technology (IT), where students are expected to be motivated to develop technical skills, including cybersecurity. Thus, it is relevant to collect the level of students' cybersecurity awareness when they start their academic studies and check if this awareness level is different depending on the countries where they study. This paper presents the results of an assessment regarding the cybersecurity awareness level of first-year students from computer science graduations from two different countries, Poland and Portugal. The assessment was designed as a survey divided into the following two main groups of questions: (1) awareness regarding cybersecurity hygiene and (2) awareness regarding cyber threats considered in the European Union Agency for Cybersecurity (ENISA) 2021 cyber threat report. The results of this survey show that Polish and Portuguese students present different self-perceptions and knowledge regarding cybersecurity hygiene and knowledge of cybersecurity. In these areas, in general, Polish students are more confident than Portuguese students. Also, Polish students presented better scores around 70%, against the ones obtained by the Portuguese students, scoring around 58%.

1 INTRODUCTION

The presence and use of technological devices have grown considerably in the past few years. The Internet is widespread today and the rapid global spread of the Internet has underscored the growing importance of cybersecurity (de Almeida Alves, 2008). The development of new technologies influences changes in the attitude of people towards the usage of the internet and other IT systems. Due to the emerging technologies, rapid changes in almost every area of our life where those technologies are present, make it impossible to protect our private information in a very effective way. Hence, these days cyber threats are also gaining in force and complexity (Szumski, 2018). Therefore, and as depicted in (Silva, 2019), the level of awareness needs to be increased. Users work with the Internet quickly - they read, consent, and share their data - often without taking into perspective the risks it may imply. The issue of cybersecurity in education becomes all the more important as even young children and teenagers use the Internet (Adachi et al., 2018). Educating people who study today in this area may be the beginning of disseminating

[a] https://orcid.org/0000-0002-0388-4468
[b] https://orcid.org/0000-0002-9313-0685
[c] https://orcid.org/0000-0002-1609-9768
[d] https://orcid.org/0000-0003-4575-6381
[e] https://orcid.org/0000-0002-9646-7638
[f] https://orcid.org/0000-0003-1856-6101

knowledge about cybersecurity to other groups: children and the elderly.

Cybersecurity awareness plays a fundamental role in educating and training students about IT threats and their prevention. Knowing how to recognize such threats and what steps are required to be taken to protect themselves are crucial competencies for today's students. Cyberspace, with its particularities and accessibility to anyone, needs to be a safe place to make the best use of the potential it has to offer (Pereira, 2022).

In the context of Higher Education Institutions (HEIs), students from different study fields also present different levels of cybersecurity awareness. Thus, it is relevant to understand these levels to know which areas the students are more comfortable in and in which further education is required.

This paper presents the results of a survey carried out with first-year computer science students from two HEIs in different countries, namely Bialystok University of Technology (BUT) in Poland, and Polytechnic Institute of Viana do Castelo (IPVC) in Portugal. These countries are located at the eastern and western ends of the European Union respectively and thus, this study allows us to capture differences between the level of education in these edge European countries. The survey intends to assess the awareness regarding cybersecurity hygiene and the awareness regarding threats considered in the ENISA 2021 threat report.

The results of this survey are presented and analyzed, as this is an important assessment initiative to check the status of students' awareness regarding cybersecurity and to drive the design of specific actions to increase that awareness.

This paper is organized as follows. Section 2 presents the works related to cybersecurity studies and their brief overview. Section 3 presents the methodology for the conducted research. Section 4 presents the results of the research: the collected data and their analysis. Section 5 provides the discussion on the results of the study, describes observations, and addresses topics for future work. Section 6 draws the conclusions about this work.

2 RELATED WORKS

In the last few years, a number of studies about cybersecurity awareness have arisen. In (Alharbi and Tassaddiq, 2021), the authors investigate and evaluate the level of cybersecurity awareness among undergraduate students at Majmaah University using a scientific questionnaire based on several safety factors for Internet use. As a result, based on the collected data, they present recommendations on how to deal with carelessness and misinformation regarding cybersecurity on campus.

The research in (Chandarman and van Niekerk, 2017) was conducted to assess the levels of cybersecurity awareness among students at a private tertiary education institution in South Africa. The questionnaire tested students in terms of four variables: cybersecurity knowledge; self-perception of cybersecurity skills, actual cybersecurity skills and behaviour; and cybersecurity attitudes. The responses revealed several discrepancies, including the "cognitive dissonance" between variables, which makes the students potentially vulnerable to cyber-attacks. The findings demonstrate the need for targeted cybersecurity awareness campaigns that address the specific weaknesses of particular populations of users.

In (Garba et al., 2020), another research aimed to investigate the students' awareness of basic knowledge of cybersecurity. A quantitative approach was used for data collection using a set of designed questionnaires. The method was used to investigate the students' cybersecurity knowledge and observe their behaviour toward using the Internet. Collected data included a total of 201 responses from Computer Science students gathered in the Department of Computer Science at Yobe State University, Nigeria. The results obtained from the experiment were analyzed and show that University students have a satisfactory level of knowledge in cybersecurity, but at the same time, they still do not know how to protect their data. The research was crucial because there is no active cybersecurity awareness program in place. As the data showed, female students are more likely to be victims of cyber-attack. The survey also indicated a high enthusiasm for students to learn more about cybersecurity.

In (Al-Janabi and Al-Shourbaji, 2016) authors analyze the information security awareness among academic staff, researchers, undergraduate students, and employees within educational environments in the Middle East. The main focus of the study was to understand the level of awareness of information security, the associated risks, and the overall impact on the institutions. The results revealed that the participants did not have the required knowledge and understanding of the importance of information security principles for their daily work. Without training programs, negative consequences affect IT systems and their usage, as well as users' personal security. From the weaknesses identified in this survey, some essential recommendations were put forward to remedy the situation. One of the recommendations was to make reg-

ular backups so that there would be copies of all data and information, that can serve as restoration points in the case of data and information loss, corruption, or compromise.

Authors in (Moallem, 2019) report the preliminary outcomes of a quantitative survey intended to identify students' awareness and enthusiasm to learn cybersecurity in Nigerian universities. The authors surveyed how students in this developing country are mindful of cyberattacks and how they can mitigate the attacks. The researchers wanted to find out if there is cybersecurity awareness among the universities' programs. The preliminary results indicated that the students claimed to have basic cybersecurity knowledge, but were not well informed on how to protect their data. It was also revealed that most universities did not have an active cybersecurity awareness program to improve students' knowledge of how to protect themselves from any threats at that time. The surveyed students also showed interest in learning more about cybersecurity.

In (Peker et al., 2016), a study was conducted to understand the current level of cybersecurity awareness among college students and develop a module that could help raise their awareness. The main features of the module were interactivity and the presentation of shocking consequences of careless cyberhabits common among Internet users. The researchers designed a survey that included pre-and post-tests to fulfil the goals of the project and administered it to students on the campus. The results indicated that the module had been effective, particularly among the non-Computer Science majors.

In the study in (Maisikeli, 2020), the authors compared cyber activity and data perception in United Arab Emirates (UAE) with other nine developed nations. The results suggest a need for aggressive promotion of cybersecurity awareness programs in UAE. The authors also argue that the cyber risk behaviour is comparatively the same as in other developed nations. There are presented methodologies that can be used to develop cybersecurity assessments of cybersecurity risk behaviours, and a comparison of cyber-related risk behaviour among countries.

Based on the literature review of the works related to the topic of cybersecurity, it can be concluded that a set of previously conducted studies intended to capture the level of cybersecurity awareness among university students. One of the previous studies aimed at revealing academic staff's awareness as well. The researchers surveyed students of different academic communities from different countries such as Nigeria, South Africa, and the Middle East Region. The results show that students of IT-related graduate programs at universities are usually more knowledgeable about the risks in general. Also, students seem to be willing to learn about cybersecurity in order to expand their knowledge and empower their competencies. Although it can be considered that recent data is important for assessing the current cybersecurity awareness of the university communities, the main focus of the discussed studies was not on comparing different academic communities from different countries. This is the basis when designing the study presented in this paper, which aims to assess students with similar characteristics simultaneously in two different countries, Portugal and Poland.

3 METHODOLOGY

The presented study was designed for first-year computer science bachelor students in Portugal and Poland. The methodology for this research included the preparation, delivery of a survey, and the collection and analysis of its results.

The survey includes a set of 3 initial questions that were designed to characterize the population regarding their age, gender, and self-assess respondents' cybersecurity knowledge. The remaining questions were designed in two main groups: (1) awareness regarding cybersecurity hygiene, (2) awareness of threats recently pointed out by ENISA in its "ENISA Threat Landscape 2021" report in (ENISA, 2021).

In the first group, 6 questions were designed with answers rated from one to ten or short answers (e.g. "Yes", "No", and "I don't know"). In the second group, ENISA report divides threats into the following eight categories:

1. Malware
2. Ransomware
3. Cryptojacking
4. E-mail-related threats
5. Threats against data
6. Threats against availability and integrity
7. Disinformation - Misinformation
8. Non-Malicious Threats

For each of these threats, 2 questions were defined: an overview multiple-choice question, and a more advanced question.

Thus, the survey was designed with a total of 25 questions and it was delivered to the students from 21 February to 14 March 2022. In Portugal, the survey was applied at IPVC and, in Poland, the survey was applied at BUT.

4 RESULTS AND ANALYSIS

After delivering the survey, the respondents' answers were collected and analyzed. In total, 110 surveys were filled, where 56 were from students of Portugal and 54 from students of Poland.

Fig. 1 presents the ages of the respondents highlighting that there is a higher incidence of Polish students between 19 and 20 years old, while in Portugal, the age of students is more distributed across a wider age group.

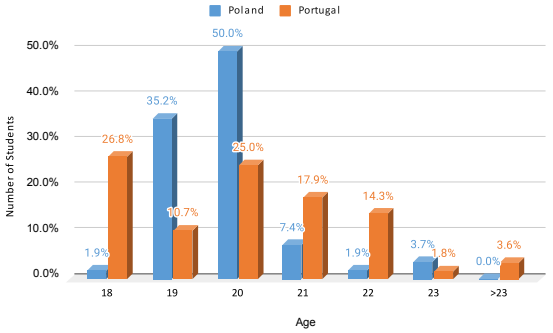

Figure 1: Age of the Respondents

Fig. 2 presents the gender of the respondents. The majority of the participants were male (101), and nine were female participants, numbers considering both countries.

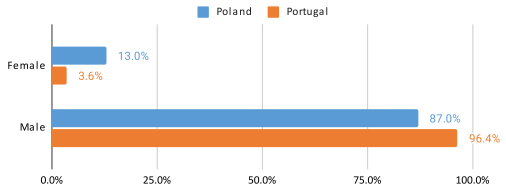

Figure 2: Gender of the Respondents

Fig. 3 presents the results of this self-assessment to capture respondents' perceptions of knowledge in cybersecurity. The answers were scaled from 1 to 10, where 1 meant "No knowledge", and 10 stood for "High/very high knowledge". It was verified that Portuguese students mainly evaluate themselves on levels between 1 and 6 (42 responses), while most Polish students (32) claimed their level was between 7 and 10.

4.1 Cybersecurity Hygiene

Fig. 4 presents shows that 89% of students from both countries chose the recommended option, i.e. "No", when asked whether it is safe to use an unsecured Wi-

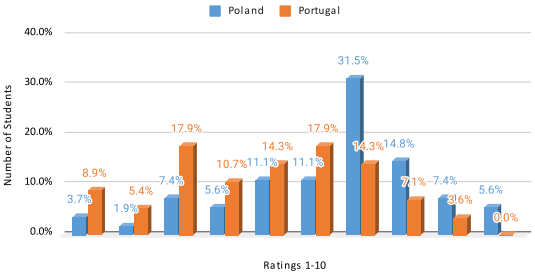

Figure 3: Answers to the question "How would you rate your knowledge about Cybersecurity?"

Fi network in public.

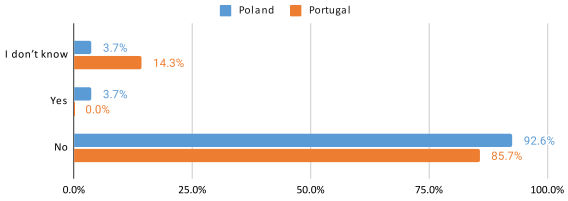

Figure 4: Answers to the question "Is it safe to use unsecured Wi-Fi networks in public places?"

Fig. 5 shows that in both countries, the majority of the students choose to use multi-factor authentication when possible. However, 37% of the students from Poland and 31% from Portugal chose the options "I don't know" and "No".

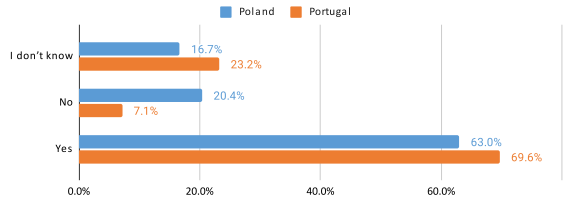

Figure 5: Answers to the question "Do you use multi-factor authentication when possible?"

Fig. 6 presents that most of the Portuguese students (71%) stated that they perform backups. In Poland 46% of the students said they do not do backups, and 52% stated that they do.

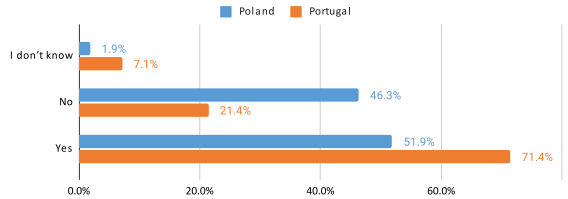

Figure 6: Answers to the question "Do you back up your files?"

Fig. 7 presents the answers to the question about using the same password on multiple websites. In Poland 67% of the students said they do not use it, and the same was stated by 54% of Portuguese students. However, 30% of the students from Poland and 36% from Portugal said that they do use the same password.

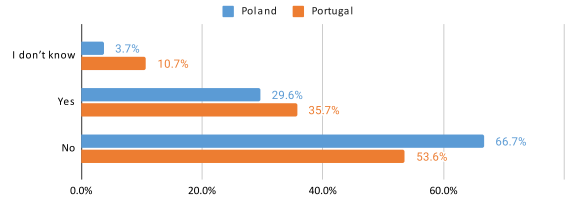

Figure 7: Answers to the question "Are you using the same password on multiple websites?"

Fig. 8 presents answers to the question of whether the incognito mode hides an IP address. The majority of students in both countries (77%), chose the correct answer - "No".

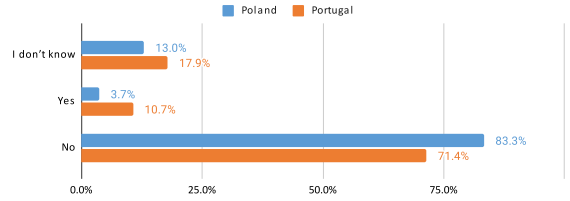

Figure 8: Answers to the question "Does incognito mode hide your IP address?"

Fig. 9 shows the result of the question about being a victim of a scam or a computer infection. The majority of Portuguese students (68%) said they had not been a victim, while the responses among the Polish students were more divided: 48% of the students said they had not been a victim, while 46% of the students admitted they had been.

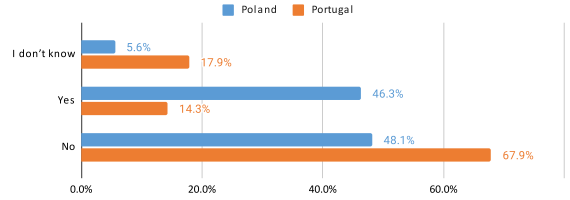

Figure 9: Answers to the question "Have you ever been a victim of a scam or infection on your computer?"

4.2 Awareness of Cyber Threats

This section presents the results regarding cyber threat awareness according to the ENISA Threat Landscape.

4.2.1 Malware

Fig. 10 presents the results for the question about the Trojan Horse. Here the students were to select which answer option they consider correct. Most of the students answered correctly, stating that a "Trojan horse is a malicious program that, when installed, pretends to be a useful application, but actually disrupts or steals information from your computer". The correct answer was given by 67% of Polish students and 41% of Portuguese students. As many as 25% of Portuguese students chose the answer "I don't know".

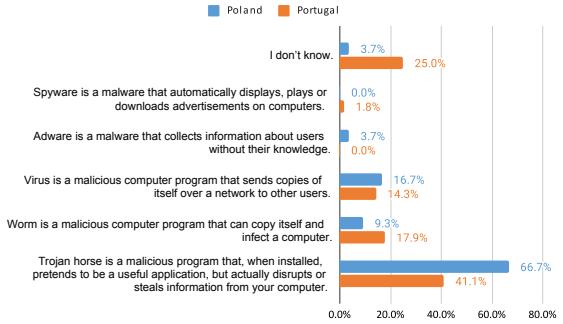

Figure 10: Answers to the question "What is the correct answer?"

Fig. 11 presents the responses regarding the Malware threat, in which the students were asked to complete the sentence "A rootkit is ...". Most of the Polish students gave the correct answer (74% of students). The correct answer was given by 45% of Portuguese students, and the same number chose the answer "I don't know".

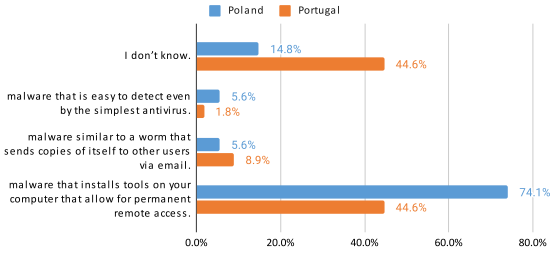

Figure 11: Answers to the question "A rootkit is ..."

4.2.2 Ransomware

Fig. 12 presents the results regarding the question on Ransomware threat. The correct option was "Ransomware is an attack where attackers encrypt an organization's data and demand payment to restore access", and it was selected by 57% of Polish students and by 46% of students from Portugal. However, a high share of students stated they did not know the answer to the question: around 24% in Poland and around 43% in Portugal.

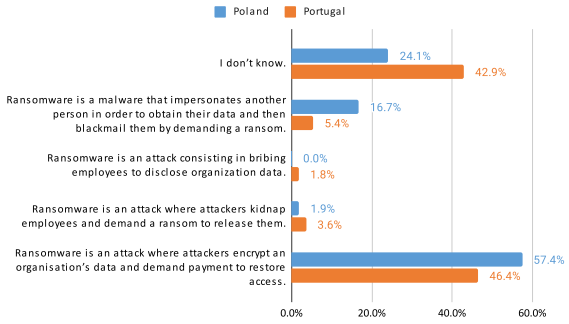

Figure 12: Answers to the question "What is the correct answer?"

Fig. 13 presents the distribution of answers to the question "What does a disk encryptor (such as Petya) do?". The option "Encrypts the victim's entire disk and prevents the operating system from booting.", being the correct one, was selected by 57% of Polish and 36% of Portuguese students. As many as 30% of all respondents stated that they did not know how to answer this question.

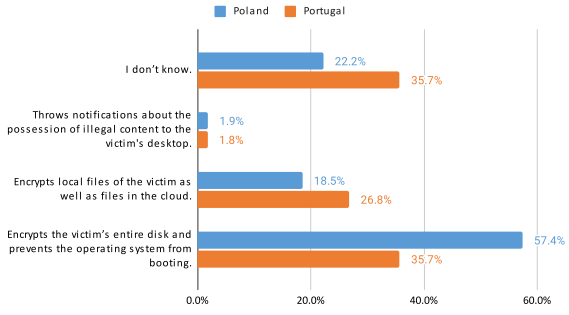

Figure 13: Answers to the question "What does a disk encryptor (such as Petya) do?"

4.2.3 Cryptojacking

Fig. 14 presents the results to the question about the cryptojacking definition. The option "Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency" was correct and was given by 81% of the Polish students and 50% by Portuguese students.

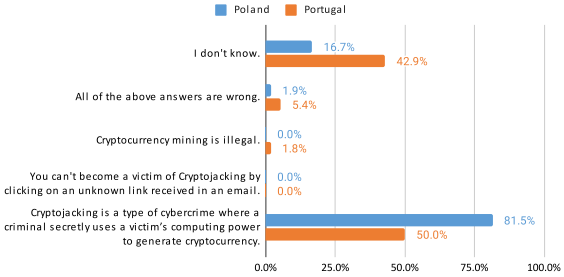

Figure 14: Answers to the question "What's the correct answer?"

Fig. 15 shows the results to the question "How can I check if I am a victim of Cryptojacking?". The correct option was "Computer runs slower. Web pages take longer to load. You can see a greater load on the CPU and GPU", and it was selected by 81% of Polish students and by 52% of students from Portugal. There were also 41% of Portuguese students who answered "I don't know.".

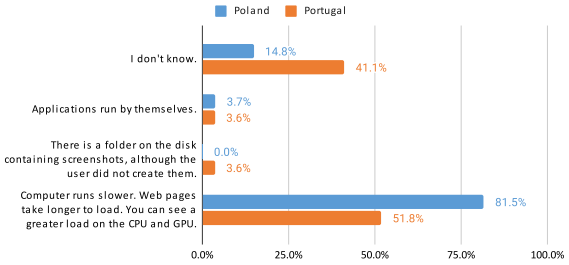

Figure 15: Answers to the question "How can I check if I am a victim of Cryptojacking?"

4.2.4 E-mail-related threats

Fig. 16, shows the results of the question about E-email-related threats. The overwhelming majority of students in both countries chose the correct option which is "It is wise to use different email addresses, e.g. one for work and another for communication with friends", chosen by 83% of Polish students and 88% of Portuguese students.

Fig. 17 shows the results of the question about the meaning of the term "phishing". The option selected by 70% of the students from Poland and by 57% of Portuguese students was "Manipulating users to obtain confidential information", which shows that more than half of the students in both countries answer correctly.

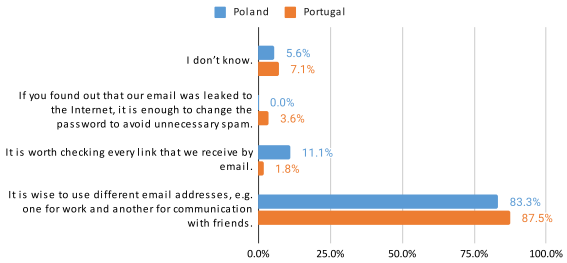

Figure 16: Answers to the question ”What is the correct answer?”

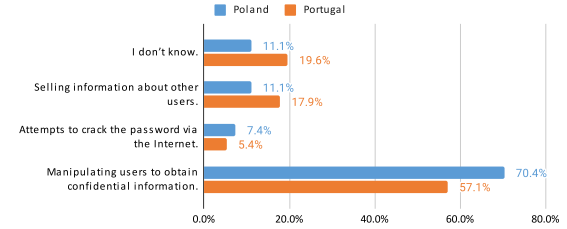

Figure 17: Answers to the question ”What does phishing mean?”

4.2.5 Threats against data

Fig. 18 shows the results of the question about password difficulty. The correct option ”If you want your password to be hard to crack, use a random password with a minimum of 15 characters” was the most chosen by 92% of the students from both countries.

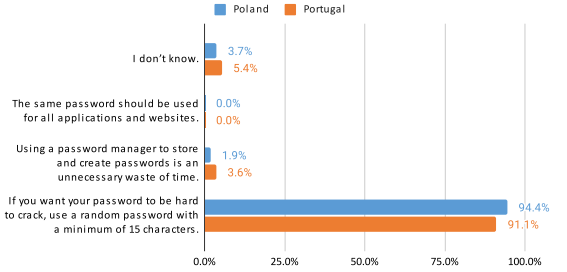

Figure 18: Answers to the question ”What is the correct answer?”

In Fig. 19 students were asked to complete the sentence ”A dictionary attack ...”. There was a great disparity in the answers obtained. The correct option is ”Will use words that appear frequently in everyday speech to crack the password” and got chosen by 54% of students from Poland and 30% by Portuguese students. Also, 39% of Portuguese students selected the option ”I don't know.”.

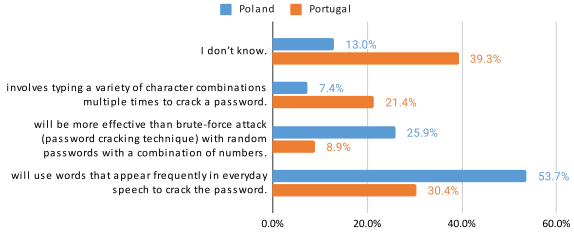

Figure 19: Answers to the question ”A Dictionary attack...”

4.2.6 Threats against availability and integrity

Fig. 20 presents the results for the question about the effects the DDos attack causes. The item ”I do not know” was chosen by 36% of Portuguese students, while the correct option ”A DDoS attack causes an Operative System to slow down. The attacker of the DDoS attack uses other people's devices, they are not aware of it” was chosen by 72% of Polish students.

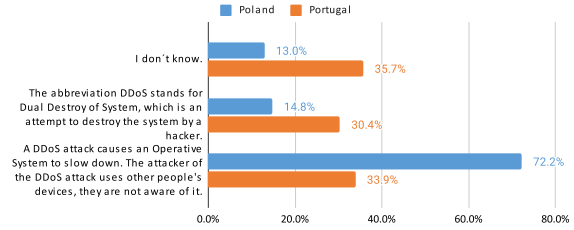

Figure 20: Answers to the question ”What is the correct answer?”

In Fig. 21 the answers to the question about the meaning of a Ransom Distributed DoS (RDDoS) attack are presented. The option ”I don't know” received 54% of the responses from Portuguese students, while the correct option ”Rush DDoS - (Rush Distributed Denial of Service) attacks in a short time on many instances of the same organization” received 43% of the responses from Polish students.

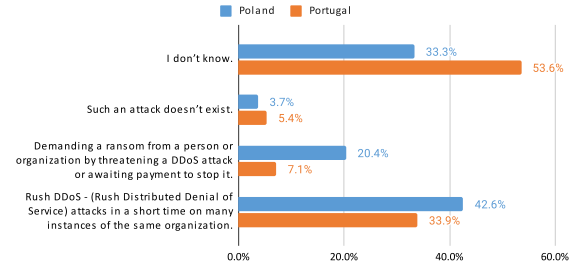

Figure 21: Answers to the question ”What does an RDDoS attack mean?”

4.2.7 Disinformation - Misinformation

Fig. 22 shows the results of the question about the credibility and security of information. Several options were presented, with the majority of students (88%) in both countries choosing the right answer "Always check that there is a padlock next to the link on the page where you enter your login details, which means that the page is encrypted". The options "You can always trust articles published on the internet with the author's signature" and "I don't know", were chosen by 12% of the students from both countries.

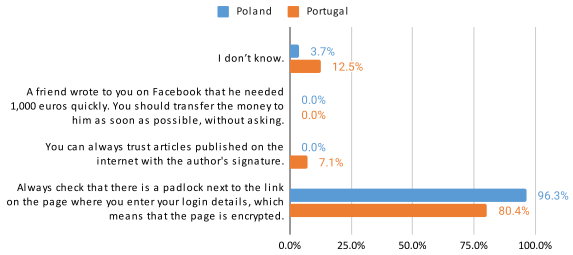

Figure 22: Answers to the question "From the following sentences, which one is correct?"

Fig. 23 presents the results of the question about HTTPS. It can be highlighted that the majority of Polish students (80%) chose the right option "HTTPS is an extension of HTTP with the use of SSL or TLS protocols to encrypt requests and responses.", while only 43% of the Portuguese students chose the right option. Furthermore, a high share of Portuguese students stated they did not know the answer to the question (32%).

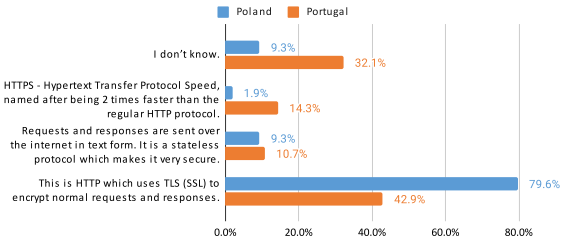

Figure 23: Answers to the question "What is HTTPS?"

4.2.8 Non-Malicious Threats

Fig. 24 presents the results of the question "From the following sentences, which one is correct?". The majority of the students from both countries (82%) choose the right answer "If you want to open unknown files or programs, you should do it in the sandbox".

Fig. 25 presents the results to the question regarding the protection of a home Wi-Fi network. In both countries, the students chose the correct answer "Set up the WPA2 protocol and set a strong password", with 92% of the votes.

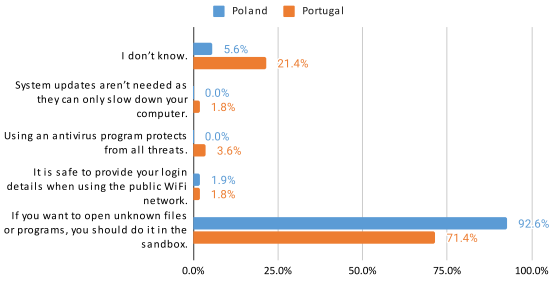

Figure 24: Answers to the question "From the following sentences, which one is correct?"

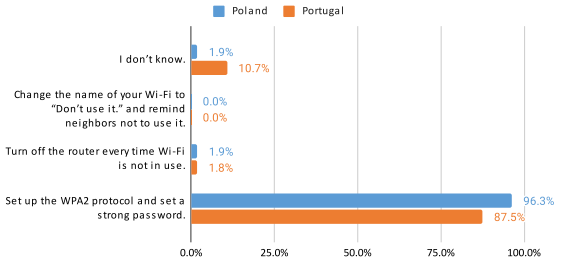

Figure 25: Answers to the question "How can you protect your home Wi-Fi?"

5 DISCUSSION

This paper explores cybersecurity awareness among students of higher education institutions. A survey was conducted at two universities - in Poland and Portugal since they represent two countries of the European Union, and thus may serve to check differences in first-year computer science students regarding their cybersecurity hygiene and cyber threats awareness.

The review of the research papers dedicated to the issue of students' cybersecurity awareness has allowed obtaining an understanding of how well cybersecurity hygiene and cyber threats awareness is currently researched in a campus environment. It can be seen that no similar studies have been conducted so far; the ones that exist are dedicated to one or a few educational institutions within one country. Thus, the necessity of studying the level of students' knowledge, as well as their will to learn is high and is caused by the urgency of making sure the youth knows how to protect their data when they work online.

The survey was conducted and from the analysis of the questions about the awareness regarding cyber-

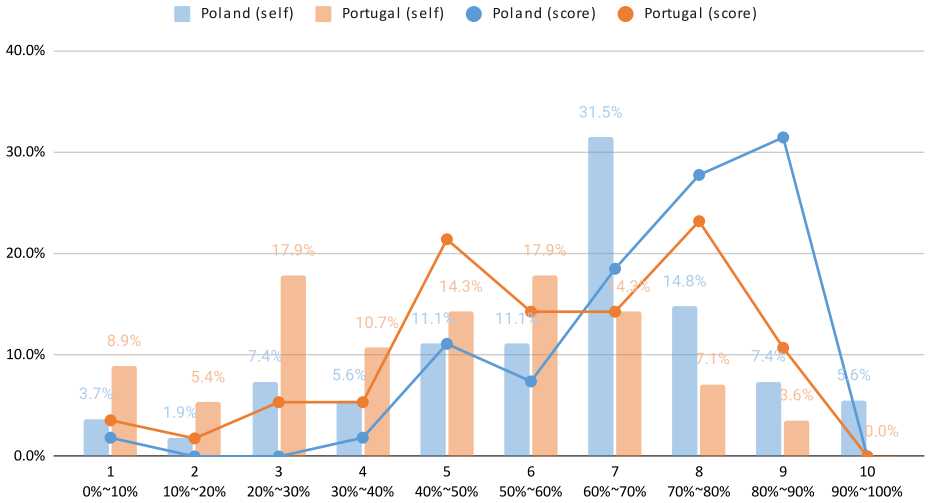

Figure 26: Results of self-assessment knowledge and results of the survey

security hygiene showed that despite their knowledge, students from both countries relatively seldom use the option of multi-factor authentication. However, they are aware that using WIFI in public places is unsafe, and that using the Incognito mode they do not mask their IP number. Despite the Polish students' greater knowledge, they used the available security options less frequently. The majority of Portuguese students declare that they back up their files and use different passwords on different websites. In contrast, the majority of Polish students do not implement these solutions for their security. More students from Poland declared that they had fallen victim to an attack (victim of a scam or infection on their computer).

There was an initial question of the survey capturing the self-assessment regarding students' knowledge perception and the remaining questions were designed to have only one correct answer, thus, it was possible to compare students' self-assessments to the real score obtained. Fig. 26 presents these results. From these results, it can be depicted that, in general, Polish students are more confident about their knowledge of cybersecurity, showing a top number around level 7 out of 10, while the Portuguese students are more distributed from all ranges of percentages. Also, regarding the overall score, Polish students presented better scores, with the top between 80% and 90% and with an overall average of about 69.7%, than the Portuguese students, which scores are more distributed between 40% to 90%, and with an overall average of about 57.8%.

In this work, it is possible to point out the following limitations. First, the study was performed only in two countries of the European Union; the education system in these countries might have differences important for this research. A survey covering more countries would definitely provide the authors with another view of the awareness of students in the whole of Europe. Second, the study included only two HEIs in Poland and Portugal. Engaging more institutions in both countries could provide the authors with a clear understanding of the government policies regarding cybersecurity education for youth. Third, both institutions engaged in the survey (BUT in Poland, and IPVC in Portugal) are technical universities. That allows assuming that study programs for students of computer science may include more specific technical subjects that non-technical universities may offer. If this assumption is true, it may be stated that students at these universities know more about cybersecurity from their education programs. Fourth, the authors consider that students in the first year possess their knowledge on cybersecurity not primarily because of their education, but because of their personal interests - since they, as freshmen, had not yet studied all the important topics connected with security.

These limitations open avenues for future research. This study can be expanded to include more other HEIs in Poland and Portugal, and in a second stage, to include other partner universities in other European countries to expand the understanding of cybersecurity awareness on European campuses.

Also, an interesting direction of research can be using these results to design measures to increase students' awareness of cyber threats and their will to learn more about how to protect themselves, such as to prepare specific training or using gamification as a way to learn cybersecurity-related topics.

6 CONCLUSIONS

This study aimed to assess the awareness of students of HEIs in Poland and Portugal, regarding their cybersecurity hygiene and knowledge regarding top cyber threats. The review of the related work on students' cybersecurity awareness has allowed the understanding of how well cybersecurity hygiene and cyber threats awareness is currently researched in a campus environment and allowed the conclusion that the main focus of the related works was not on comparing different academic communities from different countries.

The current assessment was based on a survey distributed among students of two universities in these two countries. In this survey, the respondents had to evaluate their knowledge of cybersecurity, and their cybersecurity hygiene, and then answer questions about top cyber threats highlighted by ENISA. The study has allowed comparing the levels of students' awareness, and the levels of their confidence in their knowledge, and also to assess whether the estimated level of knowledge corresponds to the level actually presented (when answering questions about particular threats).

From the results obtained it was possible to conclude that Polish and Portuguese students present different self-perceptions and knowledge regarding the cybersecurity area. In general, Polish students are more confident than Portuguese students about their knowledge of cybersecurity and Polish students presented better scores, which scored an overall average of around 70%, than the Portuguese students, which scored an overall average of around 58%.

Future work may expand the current study to other HEIs in Poland and Portugal, and expand also to other partner universities in other European countries to assess cybersecurity awareness on a wide range of European campuses. The results may also be used to design measures to prepare specific training or use gamification as a way to learn cybersecurity-related topics.

ACKNOWLEDGEMENTS

This study had the contribution of the students Błażej Kobeszko and Filip Roszkowski, which supported the collection of data from the Faculty of Computer Science, Bialystok University of Technology Bialystok, Poland.

REFERENCES

Adachi, C., Blake, D., and Riisla, K. (2018). Exploring digital literacy as a graduate learning outcome in higher education–an analysis of online survey. *Open Oceans: Learning Without Borders*, 292:292–297.

Al-Janabi, S. and Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the middle east. *Journal of Information & Knowledge Management*, 15(01):1650007.

Alharbi, T. and Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of majmaah university. *Big Data and Cognitive Computing*, 5(2):23.

Chandarman, R. and van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, 20:133 – 155.

de Almeida Alves, N. (2008). Perfis dos utilizadores da internet em portugal. *Análise Social*, pages 603–625.

ENISA (2021). ENISA Threat Landscape 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

Garba, A. A., Siraj, M. M., Othman, S. H., and Musa, M. (2020). A study on cybersecurity awareness among students in yobe state university, nigeria: A quantitative approach. *International Journal on Emerging Technologies*, 11(5):41–49.

Maisikeli, S. (2020). UAE Cybersecurity Perception and Risk Assessments Compared to Other Developed Nations. In *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, pages 432–439.

Moallem, A. (2019). Cyber security awareness among college students. In Ahram, T. Z. and Nicholson, D., editors, *Advances in Human Factors in Cybersecurity*, pages 79–87, Cham. Springer International Publishing.

Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., and Lamberson, C. (2016). Raising cybersecurity awareness among college students. In *Journal of The Colloquium for Information Systems Security Education*, volume 4, pages 17–17.

Pereira, S. M. T. (2022). *Cibersegurança: o papel da polícia de segurança pública na prevenção do cibercrime*. PhD thesis.

Silva, J. (2019). Cybersecurity and cybercrimes in portugal. In *Digital Privacy and Security Conference 2019*, page 39.

Szumski, O. (2018). Cybersecurity best practices among polish students. *Procedia Computer Science*, 126:1271–1280.