CYBERSECURITY IN BOSNIA AND HERZEGOVINA: A PILOT STUDY ON STUDENTS' AWARENESS, KNOWLEDGE, ATTITUDES, AND BEHAVIORS

Inda Kreso
Faculty of Criminal Justice, Criminology and Security Studies, University of Sarajevo, Bosnia and Herzegovina, indakreso@fkn.unsa.ba
Bernisa Šabaredžović Krsmanović
Faculty of Teacher Education, University of Džemal Bijedić in Mostar, Bosnia and Herzegovina
bernisash@gmail.com

Abstract: Cybersecurity is a constantly growing concern worldwide and Bosnia and Herzegovina is no exception. Younger generations and students are constantly exposed to different online threats (phishing, malware, data breaches, privacy violations and many others). It is very important to address cybersecurity phenomenon properly amongst students in order to build effective resilience techniques and to raise awareness about this topic. This study is quantitative, descriptive, and exploratory pilot study that provides an empirical insight into the level of cybersecurity awareness, knowledge, attitudes, and behavioral practices among university students in Bosnia and Herzegovina. This research addresses an evident research gap in this field, since there are no enough publications and research on the topic of cybersecurity awareness, knowledge, attitudes, and behavioral practices amongst students in general. In this study an online survey is used as methodological framework. The survey was divided into four sections: demographic data, knowledge-based questions, attitudinal statements, and behavioral indicators related to cybersecurity practices and total of 105 students participated in the study and completed the survey. Analysis of the collected data was conducted using the R programming language and R Studio environment and statistical methods included descriptive statistics (mean, standard deviation, minimum, maximum), internal consistency (Cronbach's α), and basic inferential tests (chi-square and ANOVA). The results suggests that there is a high level of awareness of cybersecurity risks amongst students and limited trust in institutions. Also, there is no statistically significant differences between level of knowledge in different disciplines and study programs amongst students. Cybersecurity vulnerabilities are systemically distributed and there is an evident need for interdisciplinary education, continuous awareness programs, and institutional capacity building. Furthermore, this pilot study provides the first empirical datasets from Bosnia and Herzegovina regarding awareness, knowledge, attitudes, and behavioral practices among university students in Bosnia and Herzegovina. Cybersecurity awareness, knowledge, attitudes, and behavioral practices have to considered an issue of national interest and it is not merely a technical issue, but an educational as well.
Keywords: cybersecurity, awareness, knowledge, attitudes, behavior, students, Bosnia and Herzegovina

1. INTRODUCTION

Studies addressing cybersecurity in Bosnia and Herzegovina underline that cybersecurity is not among national priorities, and there is an evident lack of unified and comprehensive national strategy and effective mechanisms for coordination and incident reporting (Baraković & Husić, 2015; Eva Nagyfejeo & Sarah Puello Alfonso, 2019)**.** Most of the registered cyberattacks and incidents include phishing attacks, wireless network abuse, credit card fraud, and various forms of social media misuse (Baraković & Husić, 2015). Previous research highlighted that raising awareness alone is not sufficient to ensure secure online behavior. For instance, (Bada & Sasse, 2014) points that changing security practices does not require only knowledge of risks and correct procedures, but it requires motivation, attitudes, and intentions of applying such behaviors consistently. This is consistent with psychological models such as the Theory of Planned Behavior (Ajzen, 1991) and Protection Motivation Theory (Rogers, 1975) both of which stress that intentions and motivational factors are crucial predictors of behavior. University students represent a critical group, as they are both among the most active Internet users and the future workforce in sectors increasingly dependent on cybersecurity resilience. When it comes to students, studies indicate that there is a relatively high of awareness amongst students, but knowledge component and behaviors suggest that here is a need for educational and institutional measures (Eva Nagyfejeo & Sarah Puello Alfonso, 2019; Silajdžić & Dudić-Sijamija, 2024)**.** Most of the previous studies focused on the institutional and legislative capacities (Baraković and Husić, 2015; Eva Nagyfejeo and Sarah L Puello Alfonso, 2019), or regional comparisons of the self-assessment of student awareness (Silajdžić & Dudić-Sijamija, 2024). However, this study focuses solely on students in Bosnia and Herzegovina aiming to provide data on awareness, knowledge, attitudes, and behaviors related to cybersecurity amongst students. This research provides an empirical insight into the cybersecurity awareness, knowledge,

attitudes, and behaviors of university students in Bosnia and Herzegovina and it helps in understanding of factors as critical vulnerabilities within the national cybersecurity landscape.

2. MATERIALS AND METHODS

This research conducted a quantitative, descriptive, and exploratory research design in the form of a pilot survey. The sample consisted of 105 university students in Bosnia and Herzegovina, representing diverse age groups, years of study, and academic programs. The aim of this research was to obtain an initial empirical insight into prevailing levels of awareness, knowledge, attitudes, and behaviors related to cybersecurity amongst students in Bosnia and Herzegovina. Respondents participated in the survey voluntarily and anonymously in a form of online questionnaire distributed through academic networks and social media platforms. Survey was structured and designed into four main sections. The first section of the conducted survey collected demographic data (gender, age, year of study, and study program). The second section of the survey was designed to specifically measure cybersecurity knowledge using questions with correct and incorrect answers (regarding following cybersecurity topics: phishing, password practices, HTTPS, Wi-Fi security, and password managers). The third section of the survey was designed to collect data about attitudes and behaviors through Likert-scale, covering topics such as privacy, incident reporting, data backup, and institutional trust. The fourth section measured personal experience with cyberattacks and preferred incident-reporting channels. All the collected data were using R programming language, R Studio environment, employing descriptive statistics (mean, standard deviation, minimum, maximum), internal consistency (Cronbach's α), and basic inferential tests (chi-square and ANOVA) to examine potential demographic differences. The analyzed results were used to answer on 3 research questions defined in this study.

Research questions are:

RQ1: What are the prevailing levels of awareness, knowledge, attitudes, and behaviors related to cybersecurity among students in Bosnia and Herzegovina?

RQ2: To what extent do study programs and prior educational background shape students' interest in and readiness to engage in additional training on digital security?

RQ3: What vulnerabilities detected among students pose potential risks to cybersecurity in Bosnia and Herzegovina, and how these potential risks can be mitigated through educational and institutional measures?

3. RESULTS

Authors continuously highlight that interconnection between psychological, behavioral, and emotional factors within cybersecurity phenomenon shape the digital resilience of individuals and organizations (Moustafa et al., 2021). Moreover, (Moustafa et al., 2021) argue that personality traits, cognitive abilities, and individual differences are crucial for understanding users' vulnerability to attacks such as social engineering and phishing, and psychological approaches can contribute to better compliance with security policies. (Zwilling et al., 2022) underlines that cybersecurity threat awareness among users is generally consistently high, but users are applying only basic protection methods, whereas more advanced ones are not used enough. (Singh & Cheema, 2024) argue that specific human emotional reactions and understanding cognitive biases can help in designing modern security systems. On the other hand, authors (Budimir et al., 2021) suggest that victims of the cyberattacks tend to react emotionally and usually go through different extreme emotions such as anxiety and anger. Psychological aspects are equally important as technical mechanisms in the prevention and recovery from cyber incidents. Based on the previous research, this study addresses a clear gap in the literature by focusing on the specific context of Bosnia and Herzegovina. Results of the statistical analysis conducted in R programming language for statistical calculations are presented in the Results section of this research. All three research questions are answered, addressed and explained in this section.

RQ1: What are the prevailing levels of awareness, knowledge, attitudes, and behaviors related to cybersecurity among students in Bosnia and Herzegovina?

Results of the statistical analysis are presented in the Tabele 1. When it comes to awareness, students reported a high level of awareness regarding cybersecurity risks (M = 4.14, SD = 0.76, Min = 1.8, Max = 5). Students are well informed regarding potential threats of cyberattacks, understand the importance of cybersecurity and they recognize the importance of protective measures. It is important to underline that the awareness is the strongest domain across the sample. Knowledge domain demonstrated a moderate average level (M = 3.05, SD = 1.53, Min = 0, Max = 5). Results regarding knowledge dimension significant variability among respondents, meaning that some of the respondents achieved perfect score with all correct answers, and others provided no correct answers. Described variability stresses gap in fundamental cybersecurity competencies that require targeted educational interventions that has to be addressed.

Table 2: Descriptive statistics for cybersecurity awareness, knowledge, attitudes, and behavior

Domain	Mean	SD	Min	Max	Interpretation
Awareness	4.14	0.76	1.8	5	High awareness of cybersecurity threats and risks.
Knowledge	3.05	1.53	0	5	Moderate knowledge, with wide variability (ranging from 0 correct answers to all correct answers).
Attitudes	3.18	0.56	1.56	5	Attitudes are moderate positive and trust in institutions limited.
Behaviors	3.79	0.90	1	5	Moderate engagement in protective practices.

Source: Author's research

Attitudes towards cybersecurity are moderately positive (M = 3.18, SD = 0.56, Min = 1.56, Max = 5), and results of the survey also suggest limited trust in relevant institutions and moderate perceptions of safety when engaging online. Attitudes of the students are not negative, but there is a need for continuous improvement of confidence in institutional support mechanisms. The assessed behavioral domain among students expressed moderate engagement in protective practices (M = 3.79, SD = 0.90, Min = 1, Max = 5). Students responded that they are taking some proactive actions such as using strong passwords, updating systems, and creating backups, which is positive. Nevertheless, there is evident variations in responses and this inconsistency highlights that there has to be further improvement and awareness campaigns.

RQ2: To what extent do study programs and prior educational background shape students' interest in and readiness to engage in additional training on digital security?

In order to identify if study programs had influence on the students' cybersecurity knowledge and their readiness for additional training, two one-way ANOVAs were conducted. The first ANOVA analysis tested differences in the perceived knowledge among students gained from formal education across study programs. The results are presented in the Table 2. The results underline that there are no significant education-level differences ($F(10,84) = 0.70$, $p = .726$, $\eta^2 = 0.063$), which means that study program, department or interest or prior academic educational background do not substantially shape either their perceived knowledge or their willingness to participate in future cybersecurity educational programs or trainings. Also, in comparing training readiness across study programs, there is no significant deviation ($F(10,84) = 0.52$, $p = .869$, $\eta^2 = 0.112$). The results are similar and only verify that students' study programs and prior educational background do not substantially shape either their perceived knowledge or their willingness to engage in further cybersecurity training.

Table 3: Effects of study program on cybersecurity knowledge and training readiness (ANOVA results)

Outcome variable	Test	Result	Effect size	Interpretation
Knowledge from formal education × Program	ANOVA	$F(10,84) = 0.70$, $p = .726$	$\eta^2 = 0.063$	No significant program differences
Training readiness × Program	ANOVA	$F(10,84) = 0.52$, $p = .869$	$\eta^2 = 0.112$	No significant program differences

Source: Author's research

The results of the analysis indicate that students studying technical, social or medical sciences have similar levels of knowledge and willingness to take part in additional cybersecurity training. This is also expected, because younger generations are exposed to the Internet from the young age, so they are familiar with most of the online threats, possibilities and challenges. Demographic and field of study do not play a crucial or decisive role in shaping students' cybersecurity preparedness. Described specificity only uncovers a systemic gap rather than discipline-specific weaknesses, since vulnerabilities appear to be widespread across all disciplines and study fields. Consequently, strengthening students' cybersecurity knowledge should not focus on isolated study fields, but should instead target the entire academic spectrum through comprehensive, cross-disciplinary initiatives.

RQ3: What vulnerabilities detected among students pose potential risks to cybersecurity in Bosnia and Herzegovina, and how these potential risks can be mitigated through educational and institutional measures?

Analysis of the results of knowledge, attitudes, and behaviors amongst student in Bosnia and Herzegovina reveals several vulnerabilities. Results regarding attitudinal and behavioral domains stress further weak spots, such as low consistency in data backup, limited incident reporting, and low trust in institutions. Tables 3 and 4 present three items with highest scores and three items with the lowest scores. Descriptive analysis of the respondents' attitudes presents the highest mean for willingness to attend additional training (M = 3.76, SD = 1.38), concern for online

privacy (M = 3.60, SD = 1.27), and readiness to report incidents (M = 3.36, SD = 1.19). These results are indicating that students in Bosnia and Herzegovina are overall open for further cybersecurity education, aware of the significance of protecting their privacy and personal information, and moderately willing to engage in reporting mechanisms when they experience cyberattack

Table 4: Attitudes – Top 3 items

Item (shortened)	**M**	**SD**
Willing to attend training (Q20)	3.76	1.38
Concerned about privacy (Q22)	3.60	1.27
Ready to report incidents (Q16)	3.36	1.19

Source: Author's research

On the other hand, the lowest scores are found in the perceived contribution of formal education to cybersecurity knowledge (M = 3.04, SD = 1.30), clarity about whom to contact in case of a cyber incident (M = 2.65, SD = 1.34), and trust in relevant institutions (M = 2.54, SD = 1.21). According to the results, we can say that there are following vulnerabilities: current educational system and program do not efficiently and successfully prepare student with the satisfactory level of practical cybersecurity skills, students do not clearly know to whom to report cyberattacks and trust in the institution when it comes to punishing cyberattacks is relatively weak. Generally speaking, students are willing to learn and educate themselves in the cybersecurity topics, and they recognized the importance of cybersecurity.

Table 5:Attitudes – Top 3 items

Item (shortened)	**M**	**SD**
Formal education knowledge (Q18)	3.04	1.30
Knowing who to contact (Q13)	2.65	1.34
Trust in institutions (Q15)	2.54	1.21

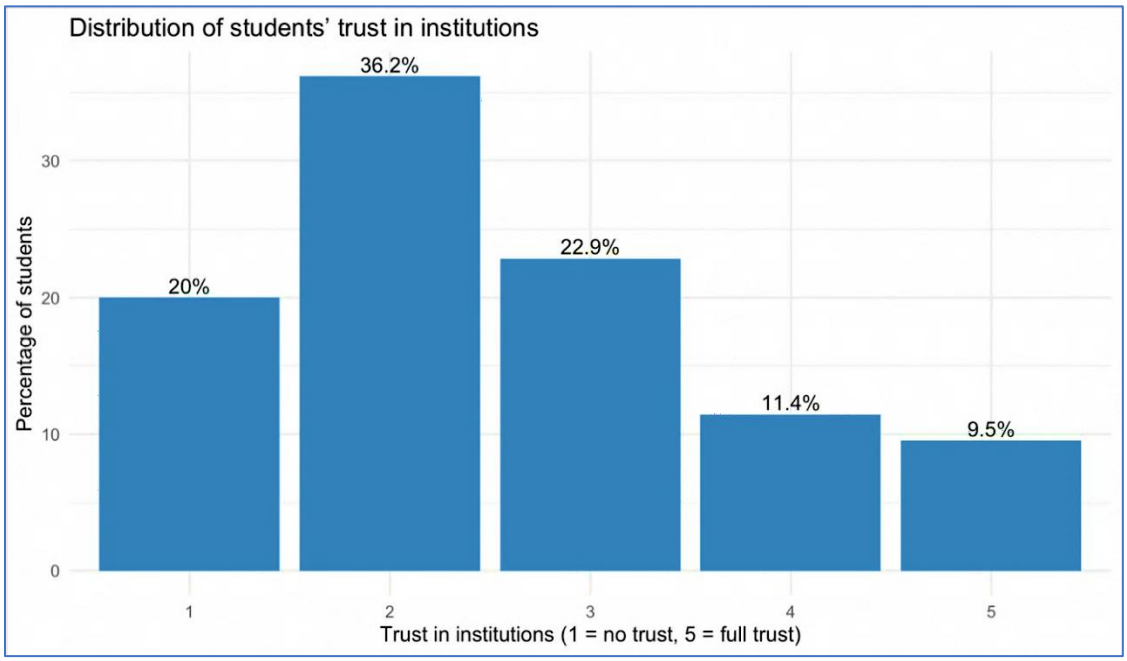
Source: Author's research

4. DISCUSSIONS

The findings of this study are consistent with the psychological and behavioral frameworks outlined by (Moustafa et al., 2021) and (Zwilling et al., 2022), confirming that awareness alone does not necessarily translate into secure behavior. Although students in Bosnia and Herzegovina have high awareness of cybersecurity threats, their inconsistent use of protective practices and limited institutional trust indicate that emotional and motivational factors continue to play important role in shaping cybersecurity behavior. These results support the argument that cybersecurity is not merely a technical issue but also a psychological and educational challenge. The results of this study underline several present vulnerabilities among university students in Bosnia and Herzegovina. Respondents of the survey do have awareness of cybersecurity threats and a willingness to attend additional training, but there are noticeable gaps found in behavior dimension.

Results also revealed limited trust in institutions (M = 2.54). Even though, moderate readiness to report incidents is present, students have expressed lack of trust in competence of the institution responsible for sanctioning cyberattacks. It is important to emphasize that these results in no way imply that institutions are inherently incompetent or unable to respond adequately to cyberattacks. Assessing institutional capacity was not within the scope of this study. Rather, the findings only reflect students' perceptions and their reported lack of trust in institutions, which should be interpreted as an attitudinal pattern rather than an evaluation of institutional performance. It is important to build confidence and trust in official structures and that way to shift students' attitude thereby enhancing overall cyber resilience. Figure 1 represents the distribution of students' trust in institutions (1= no trust and 5=full trust). Form the Figure 1 it can be seen that 36,2% of the respondents marked trust in the institutions with 2, which is particularly low.

Figure 1: Distribution of students' trust in institutions



Source: Author's research

5. CONCLUSIONS

The results of this study provide empirical evidence of the awareness, knowledge, attitudes, and behaviors amongst students regarding on cybersecurity in Bosnia and Herzegovina. Since, there is a limited number of publications in this field, this pilot study enriches the academic field of cybersecurity by providing a concrete result. The results underline noticeable gap in knowledge, trust in institutions and consistency of using protective measure while being online. It is interesting to stress that there are no significant differences between level of knowledge and study programs. Cybersecurity vulnerabilities are systemically spread among students, without stressing specific disciplines. These findings underline the importance of providing developing comprehensive, cross-disciplinary educational programs and institutional mechanisms that will aim to gain trust of students in Bosnia and Herzegovina. Finally, this pilot study highlights a fact that cybersecurity is not only a technical problem but also incorporates factors of awareness, education, and collective responsibility.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Bada, M., & Sasse, A. (2014). Global Cyber Security Capacity Centre: Draft Working Paper Cyber Security Awareness Campaigns Why do they fail to change behaviour?

Baraković, S., & Husić, J. B. (2015). "We Have Problems for Solutions": The State of Cybersecurity in Bosnia and Herzegovina. Information & Security: An International Journal, 32, 131–154. https://doi.org/10.11610/isij.3205

Budimir, S., Fontaine, J. R. J., & Roesch, E. B. (2021). Emotional Experiences of Cybersecurity Breach Victims. Cyberpsychology, Behavior, and Social Networking, 24(9), 612–616. https://doi.org/10.1089/cyber.2020.0525

Eva Nagyfejeo, & Sarah Puello Alfonso. (2019). Cybersecurity Capacity Review Bosnia and Herzegovina 2019. https://ssrn.com/abstract=3658404

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. In Frontiers in Psychology (Vol. 12). Frontiers Media S.A. https://doi.org/10.3389/fpsyg.2021.561011

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Silajdžić, L., & Dudić-Sijamija, A. (2024). The Importance of Cyber Security – Self-Assessment of Students from Bosnia and Herzegovina, Serbia and Montenegro. Media Literacy and Academic Research, 7(2), 96–112. https://doi.org/10.34135/mlar-24-02-07

Singh, B., & Cheema, Dr. S. S. (2024). Psychology in Cybersecurity: Unveiling the Human Dimensions of Digital Resilience. International Journal of Advanced Networking and Applications, 16(01), 6281–6290. https://doi.org/10.35444/ijana.2024.16107

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269