photo: Monika Tomajová

Lamija Silajdžić, Anida Dudić-Sijamija

The Importance of Cyber Security – Self-Assessment of Students from Bosnia and Herzegovina, Serbia and Montenegro

DOI: https://doi.org/10.34135/mlar-24-02-07

ABSTRACT

This study aims to identify the cybersecurity awareness of university students from Bosnia and Herzegovina, Serbia, and Montenegro in the following aspects: a) Malware, b) Password usage, c) Phishing, d) Social engineering, and e) Online scams. A quantitative-qualitative research approach was used. Data for the quantitative section were collected using the Cyber Security Behaviour Instrument questionnaire (Muniandy et al., 2017). In the qualitative section, five semi-structured interviews were conducted with students about their behaviour and protection on the internet. Research has shown that respondents apply some good, but still also some weak or dangerous cybersecurity practices in above mentioned aspects. That confirms that the human element remains a critical vulnerability for individuals, businesses, and societies facing rapidly evolving online threats, and that we urgently need the improvement of personal cyber hygiene. The findings highlight strengths and weaknesses in respondents' knowledge and behaviours related to cybersecurity, underscoring the need for continuous education and awareness-raising to improve internet security practices.

KEY WORDS

Bosnia and Herzegovina. Cybersecurity. Montenegro. Serbia. Students.

1 Introduction

More than 66% of the global population now uses the internet, and year 2024 is already marked as a bumper year for digital milestones (Kemp, 2024). The same data shows the increase in the time we spend online, which gives us a clear picture of the dominance of digital technologies in our daily lives. Internet users are fast approaching the status of a "supermajority", and the number of people who remain offline is decreasing.

As for the region, there were 2.67 million internet users in Bosnia and Herzegovina, with an internet penetration of 83.4%. About 16% of the population remained offline at the beginning of the year (Kepios, n.d.). Internet penetration in Serbia is 90% and 89.4% in Montenegro (Kemp, 2024). These high percentages show that, even though these are countries that are not EU members and are still considered countries in transition, they are very much immersed digitally. The digital transformation has occurred not only at the level of technology but also in society. In fact, the core of our societies has changed under the influence of digital technologies, as more and more of our daily activities have shifted into the digital space.

Considering the facts mentioned, we are aware that such extensive exposure to the digital realm carries certain risks. As the number of internet users and the amount of time spent online increase, so does the number of risks and threats which we should pay attention to, and we must learn how to protect ourselves and our societies as well. Just as society has transformed under the influence of ubiquitous digital information and communication technologies, so too have security threats and challenges transcended traditional understandings.

1.1 The Importance of Cyber Security Nowadays

Almost every aspect of our lives today can be prefixed with 'cyber' (related to or involving computers or computer networks – such as the Internet), thus words like cyber-space, cyber-sport, cyber-punk, cyber-activism, cyber-diplomacy, cyber-insurance, cyber-ethics, and many others, have become commonplace in everyday language. Among them is the concept of cyber-security, which encompasses

> the state and practice of protecting infrastructure, information and communication systems, networks, devices, and information from compromise, with the aim of protecting people, material and cultural assets in personal and social property, protecting society and its values, providing comprehensive protection to the people, nation, state, and international relations. (Vajzović, 2019, p. 533)

Cyber-security is based on a holistic approach, that is, learning how to ensure and manage the uninterrupted functioning of the modern information environment (Prskalo, 2022). The primary goal of cyber-security is the security and protection of information, devices, and equipment of companies, institutions, organizations, families, and individuals. However, we can increasingly speak of it in the context of protecting human lives.

Due to the increasing dependence on information and communication technologies in all aspects of our lives, there is an undeniable need to raise awareness and enhance knowledge and skills in cyber security. The first realization that computers could leak sensitive data and that there was a possibility of cybercrime is mentioned in the 1960s, and by the end of the century, we became aware that all computer and internet users were vulnerable, and very likely already exposed to cyberattacks. The growing number of users, devices, software applications and applications in the digital space results in an increasing volume of data circulating, much of which is sensitive or confidential. At the same time, the number and sophistication of cyber attackers and attack techniques are also increasing.

The main cyber threats encompass cybercrime, cyber espionage, cyber warfare, and cyber terrorism (Mataić, 2022; Li & Liu, 2021), and those attacks can be structured or unstructured. There are numerous types of cyber-attacks and methods used by cybercriminals to compromise individuals or institutions, and some of the most used methods include denial of service, malware, phishing, man-in-the-middle, and social engineering (Li & Liu, 2021; Končarević, 2023).

Denial of service implies that a hacker consumes all server resources, so access to the service is not possible for system users (Alghamdie, 2021). There also exists a Distributed-Denial-of-Service (DDoS) attack which represents a type of coordinated attack in which multiple computers, sometimes even botnets, are utilized to disrupt the functioning of a system (Spremić, 2017). These two kinds of attacks are those that do not aim to steal the victim's money or sensitive data but rather to cause damage. The techniques of these attacks can be different, and the most common are flooding (flooding the network or server with false requests which leads to congestion) and exploitation of vulnerabilities (exploiting specific vulnerabilities of software systems which may include targeting code errors that can cause service interruption) (Mirković & Reiher, 2004; Gu & Liu, 2007).

Malware are malicious computer programs designed to compromise the integrity, confidentiality, or availability of data, applications, operating systems, or other parts of a computer or information system, meaning, that it is in this way in which victims meet worms or viruses and their devices become infected (Pande, 2017; Edgar & Manz, 2017). Malware refers to viruses, worms, Trojans, ransomware, scareware, spyware, cryptocurrency miners, adware, and other programs designed to exploit computer resources for malicious purposes (Steinberg, 2019). Malware infections can lead to data loss, identity theft, financial losses and reputational damage to organizations.

Phishing involves an attack aimed at stealing identities or confidential data. It is a method in which a hacker sends a seemingly legitimate email asking users to disclose confidential information (Saxena & Gayathri, 2022). For example, an attacker might send an email that appears to be a legitimate message from a bank, asking the victim to click on a link within the email. When the victim clicks on the link, they are redirected to a fake website that looks legitimate, where they are prompted to log in with their account details. In this way, the attacker gains access to the user's information, including their password. Phishing attacks are one of the most common types of attacks. To illustrate, we can refer to the Valimail study from 2019, which states that nearly 3.5 billion phishing emails were sent globally every day during that year. Aside from email communication, phishing attacks can also be carried out through SMS or voice communication.

Man-in-the-middle attacks are a form of eavesdropping attack, where hacker puts himself between the victim device and the router, exploiting vulnerabilities in the network to bypass communication protocols (Končarević, 2023). More precisely, a malicious agent inserts themselves into a communication session between people or systems, falsely representing both sides, and gains access to the confidential data exchanged through that communication channel. Both victims are usually unaware of such a breach, as from their perspective, the communication appears to proceed normally, in the same manner as it did before the attack (Šimić, 2023).

Finally, social engineering represents a type of attack that exploits human error and induces an individual to open malicious documents, files, or e-mails to gain access to personal data or the system (Wang et al., 2021). Mashtalyar et al. (2021) emphasize that social engineering is often of predominant concern for industries, governments and institutions due to the exploitation of their most valuable resource – their people. Thus, social engineering is a process that relies on psychological manipulation to persuade people to take actions they would otherwise not take. This may include misrepresentation, urgency and pressure, and emotional manipulation.

The statistics shows that the landscape of cyber threats is evolving. A critical reality is: cybercriminals are diversifying their tactics, and no sector remains unscathed (Fox, 2023). Global cybercrime damage costs are expected to grow by 15%, reaching $10.5 trillion USD annually by 2025 (Ene, 2023). Phishing remains the most common form of cybercrime with nearly 2 billion emails being exposed in a single year, affecting 1 in 5 internet users. Considering the information that the human element remains a critical vulnerability for both individuals and businesses, where 82% of breaches against businesses involved a human element through issues like error and social engineering, it is crucial for every individual to pay attention to their own "cyber-hygiene" (AAG IT Services, 2024).

The number of cyber-attacks is on the rise in the countries of the research region too. According to the Report on Cyber Security Threats in Bosnia and Herzegovina, in just one month in 2022, Bosnia and Herzegovina recorded over 9.2 million cybersecurity threats, with DDoS attacks being the most reported (Mahmutović & Hodžić, 2022). Data from Serbia shows that approximately 26 million cyber-attacks on information and communication technology systems occurred in the country in 2020, with the most common being attempts to breach ICT systems and unauthorized data collection (Bjeloš & Pavlović, 2022). In the last few years, Montenegro has also faced an increase in cyber-attacks and crimes in the field of high-tech crime (Mujević, 2022).

Since young people, especially students, are predominantly online for both academic and leisure purposes, it is crucial to pay attention to this group when it comes to awareness of cybersecurity threats. According to the self-assessments of students in the study conducted by Verma and Pawar (2024), 27% of respondents feel extremely aware of cybersecurity threats, while approximately 37% have been victims of some form of cyber-attack. Another study among students (Kamaruddin et al., 2023) showed that 73% of students know about cybersecurity, while the rest have little to no knowledge about cybersecurity. Research by Pawlowski and Jung (2015) showed a relatively modest level of concern about different types of cyber-attacks among students, with the highest level of concern being about attacks targeting their personal computing/mobile devices.

On the other hand, the study by Du and Chintakovid (2023) addressed that even though the overall findings explained that the level of student's awareness about cybersecurity was good, people's behaviour still is the main obstacle to deal with cybersecurity threats and challenges.

Given the fact that societies have transformed under the influence of ubiquitous digital information and communication technologies, and that such extensive exposure to the digital realm carries certain risks, it is undoubtedly necessary to research the current state of cybersecurity awareness.

2 Methodology

This study aims to identify the cybersecurity awareness of university students from Bosnia and Herzegovina, Serbia, and Montenegro in the following aspects: a) Malware, b) Password usage, c) Phishing, d) Social engineering, and e) Online scams.

The research question we began with was: "What is the current state of cybersecurity awareness concerning malware, password usage, phishing, social engineering, and online scams among university students in Bosnia and Herzegovina, Serbia, and Montenegro?"

The hypothesis of this research is: "Although the respondents apply some good practices regarding their cybersecurity, yet their low awareness level in some aspects of malware, password usage, phishing, social engineering and online scams, could still expose them to security threats".

A quantitative-qualitative research approach was used. Data for the quantitative section were collected using the Cyber Security Behavior Instrument questionnaire (Muniandy et al., 2017), which has been piloted, validated and used in other research as well. It consists of two sections: A) sociodemographic data and online activities (2 items), and B) cyber security behaviour (50 items). The questionnaire was distributed online via e-mails of students who participated in the youth projects Regional FutuRise Media Forum and Regional Youth Academy on Constructive Narrative. The Statistical Package for the Social Sciences (SPSS) was used for data analysis, and the findings are presented using descriptive statistics to identify patterns in behaviour and cybersecurity awareness.

In the qualitative section, five semi-structured interviews were conducted with students about their behaviour and online protection. The aim was to identify behaviour patterns and sources of knowledge, the need for additional education, risk perception and an analysis of their online security practices. The obtained data were analysed using thematic analysis (Braun & Clarke, 2006), which includes collection and transcription of the data, then coding, i.e. the first level of data abstraction, after which topics describing the basic characteristics of the collected data are developed. The presented results in the thematic analysis are supported by statements from the participants, which are marked with a label and number (P:1, P:2, P:3, P:4 and P:5). This ensures the anonymity of the respondents, which is the professional and ethical obligation of the researcher. The Table 1 presents topics and codes that were obtained from the interviews:

Topics	Codes
General cyber security awareness	- Examples of online security threats
Specific threats awareness: malware, phishing, social engineering, online scams	- Malware recognition - Antivirus software status and updates - Password usage and update - Phishing attacks - Social engineering: personal information and online identities
Personal practices and self-improvement	- Good cyber security practices and behaviours - Areas for cyber security improvement
Education and training	- Cyber security education as part of formal and informal curricula - Additional resources and training

TABLE 1: *Qualitative research (topics and codes)*

Source: own processing, 2024

3 Results

3.1 Quantitative Research

The study involved 93 participants in the quantitative section through a survey questionnaire: 75 female (80.6%) and 17 male (18.3%). One didn't want to answer the question about gender. 73% of respondents were from Bosnia and Herzegovina, 19.4% from Serbia, and 8.6% from Montenegro. The data shows that 52% participants have completed secondary school, followed by 33% who have completed undergraduate studies. The data also shows that a smaller percentage have pursued higher education, with 9% having completed master's studies and 2% holding doctoral degrees. The presence of 3% in the "Other" category suggests some unique educational paths, while the 1% of respondents with no formal education reflects a minority.

All respondents reported that they use the internet every day, with only one person that do not have an account on social media platforms such as Facebook, Instagram, or TikTok. Instagram is the most popular platform, followed by Facebook in second place and TikTok in third among our respondents. In terms of time spent online, the data reveals that 36% of respondents are online for more than 5 hours a day, while 40% reported spending between 3 to 5 hours daily, and 15% indicated that they are online for 1 to 3 hours. Notably, 9% of respondents claimed they are "always" online, and none reported being online for less than one hour. This significant level of daily internet engagement raises important questions about the impact of extensive online activity on various aspects of life, including mental health, academic performance, and social interactions. The dominance of social media, particularly Instagram, suggests that it plays an important or even central role in the daily routines of respondents, potentially influencing their perceptions and behaviours in the digital landscape. Overall, these findings highlight the pervasive nature of internet use among respondents and underscore the need for awareness regarding the implications of extensive online engagement.

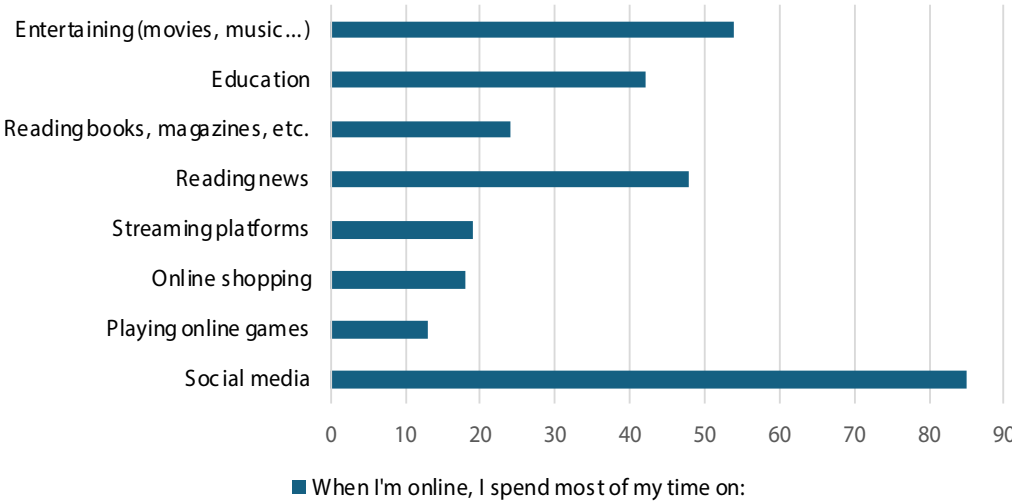

FIGURE 1: *Online activities of the respondents*

Source: own processing, 2024

Figure 1 shows a significant majority of respondents, specifically 85%, which spend most of their time on social media, indicating its dominant role in their daily digital interactions. Additionally, 54% of respondents engage in online entertainment, such as movies and music, suggesting that leisure activities are also an important component of their online experience. Notably, 48% of participants prioritize reading news, reflecting a strong inclination towards staying informed about current events. Education also plays a role in respondents' online activities, with 42% indicating that they utilize digital platforms for learning purposes. Conversely, engagement in activities such as reading books, magazines, and online shopping is comparatively lower, at 24% and 18%. The further data shows that only 19% of respondents use streaming platforms regularly, while a mere 13% engage in playing online games. These findings underscore the diverse ways in which respondents interact with online content, with a predominant focus on social media and information consumption.

No	Items	Agree (N)	Don't know (N)	Disagree (N)
M1	I open an email attachment from strangers.	23	14	55
M2	I open an email attachment if it has interesting subject line.	34	19	39
M3	I am very sure of the status of anti-virus software on my personal computer.	42	32	18
M4	I open attachments with multiple extensions.	16	34	41
M5	I have a sense something is wrong if computer runs extremely slowly.	57	12	22
M6	I download freeware on the Internet.	26	25	41
M7	I scan removable drives prior to using them on my personal computer.	33	29	30
M8	I installed anti-virus software, firewall and anti-spyware.	57	13	22
M9	I download materials from insecure sites.	28	8	56
M10	I apply security patches as soon as possible.	46	28	17

TABLE 2: *Student's cybersecurity behaviour on malware*

Source: own processing, 2024

The data in Table 2 reveals significant aspects of students' awareness and behaviour concerning cybersecurity. While 61% of participants report having installed antivirus software, firewalls, and antispyware, it is concerning that 34% are unaware of the status of this software on their computers, and 20% are unsure of its effectiveness (M8 and M3). This uncertainty may indicate a lack of training or awareness regarding the importance of regular maintenance and updates of security tools, which can leave computers vulnerable to attacks. Considering that more than 60% of respondents can recognize symptoms of a slow computer as a potential sign of problems (M5), it is important to notice that 24% do not identify this situation as a possible indication of malware. This data may suggest that while students are aware of symptoms, they lack knowledge about how to properly respond to these symptoms. The literature often emphasizes that recognizing threats and taking appropriate action are key components of effective protection (Bojanić et al., 2016). Furthermore, the finding that around 30% of respondents answer "I don't know" to questions related to basic security practices (M3, M4, M6, M7, and M10) highlights a serious problem regarding the lack of awareness of their own behaviour in the digital environment. This uncertainty may indicate that many students are not cognizant of the importance of implementing security measures, such as scanning removable devices or applying security patches. This raises serious questions about their preparedness to deal with potential threats, especially regarding risks such as opening email attachments from unknown senders or downloading files from insecure websites. In this context, the research findings underscore the urgent need for educational programs focused on raising cybersecurity awareness among students. Educational courses and workshops that address practical skills as well as theoretical understanding of threats could significantly enhance their ability to recognize and respond to risks.

No	Items	Agree (N)	Don't know (N)	Disagree (N)
P1	My passwords don't follow keyboard patterns.	52	20	20
P2	I share passwords with other people.	6	2	83
P3	I use different passwords for different applications.	62	8	22
P4	My passwords consist of lowercase, uppercase, numbers, special characters	78	8	6
P5	I use passwords longer than 8 characters.	85	3	4

P6	My passwords are based on personal information.	28	12	51
P7	I never change passwords.	24	10	57
P8	I use “Remember my password” option.	53	12	27
P9	I used to write down my passwords.	58	10	23
P10	I never use “hint” to recover forgotten password.	31	23	37

TABLE 3: *Student’s cybersecurity behaviour on password usage*

Source: own processing, 2024

Table 3 shows interesting insights into the password security practices of respondents. While nearly 90% report that they do not share their passwords with others (P2), and a significant 91% use passwords that are longer than 8 characters (P5), there are still concerning trends. Notably, 84% create passwords that incorporate a mix of lowercase and uppercase letters, numbers, and special characters (P4), indicating a good understanding of complexity requirements. However, it is troubling that 55% of respondents use passwords based on personal information (P6). This practice can significantly weaken password security, as personal information is often easily accessible or guessable. Additionally, 63% of respondents admitted to writing down their passwords, which poses another risk, especially if these notes are not stored securely. The fact that 26% of them never change their passwords (P7) further emphasizes potential vulnerabilities, as stagnant passwords can become targets for attackers over time. On a positive note, 67% of respondents use different passwords for different applications (P3), which is a commendable security practice that can limit exposure in the case of a data breach. Moreover, 56% reported that their passwords do not follow predictable keyboard patterns, suggesting a level of awareness regarding common password vulnerabilities. Overall, while there are some positive aspects to the password practices of the respondents, the reliance on personal information and the tendency to write down passwords indicate areas where improvement is needed.

No	Items	Agree (N)	Don’t know (N)	Disagree (N)
Ph1	I am upgrading my phishing knowledge by reading phishing materials.	34	29	28
Ph2	I am not a target of phishing attacks because I am a student.	14	38	39
Ph3	I provide confidential information to any types of emails.	10	30	51
Ph4	I click hyperlinks in email messages.	20	19	52
Ph5	I trust any email messages announcing contests/prizes.	10	12	68
Ph6	URL must be “https” if I’m transmitting confidential information.	27	43	20
Ph7	Padlock symbol is a must to transmit sensitive information.	20	61	10
Ph8	I prefer to type URL in a new browser rather than clicking on hyperlinks.	20	39	32
Ph9	Receiving suspicious emails will prompt me to contact the relevant party for verification.	32	29	29
Ph10	I check URL spelling prior to any types of transactions.	33	33	25

TABLE 4: *Student’s cybersecurity behaviour on phishing issues*

Source: own processing, 2024

The data in Table 4 highlights critical gaps in respondents’ knowledge and awareness related to phishing and secure information transmission. Notably, 30% of respondents do not actively seek to upgrade their knowledge about phishing threats, while 31% answered

"I don't know" regarding their awareness of phishing (Ph1). This lack of proactive engagement with cybersecurity education raises concerns about their vulnerability to phishing attacks. A particularly alarming finding is that 46% of respondents are unaware that URLs must begin with "https" when transmitting confidential information, and 22% believe that this is not necessary (Ph6). This indicates a fundamental misunderstanding of secure online practices, which could lead to significant risks when handling sensitive data. Additionally, 66% of respondents do not recognize the necessity of a padlock symbol when transmitting sensitive information, and 11% incorrectly believe that it is not essential (Ph7). The absence of knowledge about these security indicators can expose users to threats, as they may unknowingly provide personal information over insecure channels. Moreover, 33% of respondents are unsure if they might provide confidential information in response to any type of email, and 11% admit to providing such information (Ph3). This uncertainty about the legitimacy of email requests can increase the risk of falling victim to phishing scams. On a more positive note, almost 35% of respondents indicated that they would contact the relevant party for verification upon receiving a suspicious email (Ph9), and 36% reported that they check the URL spelling prior to any transactions (Ph10). These behaviours demonstrate a degree of caution and awareness that is essential for protecting personal information online. Overall, while there are some encouraging signs of vigilance among respondents, the high percentages of uncertainty and misinformation surrounding key security practices emphasize the urgent need for targeted education and training on phishing and online safety. Enhanced awareness and proactive measures can significantly mitigate the risks associated with phishing attacks and secure the transmission of sensitive information.

No	Items	Agree (N)	Don't know (N)	Disagree (N)
S1	I am not interested in reading social engineering issues.	28	32	30
S2	I am willing to reveal username and password to anyone claiming to be system administrator.	12	16	63
S3	I am not a target of social engineering attacks because I am a student.	12	34	45
S4	I respond to calls, SMS, or email messages to friendly/non-threatening strangers.	23	15	53
S5	I follow instructions given by people who speak with authority.	27	26	38
S6	I provide passwords to a help desk.	11	29	51
S7	I check the authorization or identity of someone before talking on any issues.	59	16	14
S8	I don't feel intimidated with questions by someone.	35	34	21
S9	I wouldn't communicate with a stranger although his/her looks warrant sympathy.	35	31	25
S10	I wouldn't reveal any confidential information under any circumstances.	61	20	10

TABLE 5: *Student's cybersecurity behaviour on social engineering*

Source: own processing, 2024

Table 5 presents important insights into respondents' awareness of social engineering attacks. Notably, 37% of respondents are uncertain about whether they are targets of social engineering attacks due to their status as students, while 13% believe they are not targeted for this reason (S3). This uncertainty suggests a lack of awareness regarding the risks associated with being a student in a potentially vulnerable position. Encouragingly, about 66% of respondents indicated that they would not reveal any confidential information under any circumstances, reflecting a commendable level of awareness about social engineering tactics (S10). However, there are concerning trends: 30% of respondents express no interest in reading about social

engineering issues, and 35% answered "I don't know" when asked about their knowledge on the topic (S1). This lack of interest and knowledge can leave them more susceptible to manipulation by malicious actors. Additionally, 32% of respondents are unsure whether they would provide their passwords to a help desk, and 12% admit that they would (S6). This ambiguity can pose serious risks, as it highlights a potential vulnerability in trusting unverified sources. Furthermore, 29% of respondents indicated that they would follow instructions from individuals who present themselves with authority (S5), which can lead to dangerous situations if those individuals are not legitimate. On a positive note, 64% of respondents reported that they check the authorization or identity of someone before discussing any issues (S7). This behaviour reflects a proactive approach to safeguarding their information and demonstrates an understanding of the importance of verifying identity in interactions. Overall, while there are some positive indicators of awareness and caution among respondents regarding social engineering, the significant percentages of uncertainty and disinterest highlight critical areas that need to be addressed. Both formal and informal educational initiatives aimed at increasing awareness and knowledge about social engineering tactics could greatly enhance students' ability to protect themselves from such attacks.

No	Items	Agree (N)	Don't know (N)	Disagree (N)
O1	I established trusted online relationships with strangers.	23	14	55
O2	I ignored emails from well-known organizations regarding announcements on something unusual or too good.	44	24	24
O3	I respond to SMS announcing contests involving huge sums of money.	9	10	73
O4	I never trust strangers identity information given on the Internet.	57	23	12
O5	I never consider any amount of money for services offered by an online site.	57	24	11
O6	I am willing to deposit money requested by online friends.	5	12	75
O7	I am aware of and able to identify the latest online scams.	50	24	18
O8	I trust strangers' pictures posted on the Internet.	5	17	70
O9	I never receive parcels and gifts from Internet friends.	54	19	17
O10	I wouldn't hesitate to meet face-to-face with Internet friends.	23	24	45

TABLE 6: *Student's cybersecurity behaviour on online scam issues*

Source: own processing, 2024

Data from Table 6 indicates that respondents demonstrate a relatively high awareness of issues related to online scams. Approximately 61% of them reported that they never trust identity information provided by strangers on the Internet (O4), and a corresponding 61% stated they would never consider any amount of money for services offered by an online site (O5). These findings suggest a cautious approach toward online interactions, which is crucial in an era where online scams are increasingly prevalent. However, there are concerning gaps in knowledge. About 26% of respondents are unsure whether they can identify the latest online scams, and 20% believe they are not capable of doing so (O7). This uncertainty highlights the need for improved education and awareness regarding the evolving tactics used by scammers. In terms of financial transactions, a notable 81% of respondents expressed that they are unwilling to deposit money requested by online friends, while 13% were unsure, and only 5% indicated that they would comply (O6). This suggests a strong sense of scepticism when it comes to

financial requests from online acquaintances, which is a positive sign for potential vulnerability to scams. Conversely, around 25% of respondents reported having established trusted online relationships with strangers (O1), and the same percentage expressed a willingness to meet face-to-face with internet friends (O10). This indicates a level of comfort and trust that could be risky if not approached with caution. Furthermore, our research underscores the importance of collaboration between educational institutions and industry stakeholders to ensure that educational initiatives address current needs and challenges in the field of cybersecurity. By fostering partnerships, we can enhance the effectiveness of training programs and better equip individuals to navigate the complexities of online environments securely. In conclusion, while there are positive indicators of awareness among respondents regarding online scams, there remain significant areas for improvement, particularly in knowledge about identifying scams. Targeted educational efforts that address these gaps can greatly enhance overall cybersecurity awareness and protect individuals from potential online threats.

3.2 Qualitative Research

All respondents stated that they had experienced a situation where they felt their online security was compromised or at risk. The most common challenges were related to social media profiles (Facebook and Instagram), specifically hacking or deletion of profiles. This highlights a growing concern among users regarding the vulnerabilities associated with widely used platforms. Additionally, respondents received emails from seemingly relevant addresses, which were phishing messages: (P:5) “Facebook once sent me a notification that I could file a lawsuit against them because my data were stolen while I was visiting the USA. To this day, I don’t know where that data was used or for what purpose”. This statement reflects the anxiety individuals feel when their personal information is at risk, emphasizing the need for clearer communication from companies regarding data breaches.

As for specific security threats, such as malware, phishing, social engineering, and online scams, respondents say that they regularly update their antivirus software to ensure system stability and its improved ability to detect issues. This proactive behaviour indicates an awareness of the importance of maintaining robust security measures. Additionally, they are aware that they need to react if their computer is running unusually slowly. This self-monitoring is a key aspect of digital literacy, demonstrating an understanding that system performance can signal underlying security issues. They first try to determine the cause themselves, and if they fail, they consult with experts. Only one respondent is not sure that she can recognize malware, while the others claim that they are successful in this. (P:1): “I’m confident in my ability to identify malware. For example, if I notice that the computer is running unusually slowly or unexpected pop-up windows appear, I immediately suspect the presence of malware and run an antivirus scan”. Such confidence suggests a level of education and familiarity with technology that may not be universally shared by all users.

Three respondents say they do not use the same passwords for different accounts, two of them use similar ones (and are aware that this is risky), while one respondent says she uses identical passwords for several different accounts. This variance in password management reflects differing levels of risk tolerance and awareness among respondents. Two respondents admit that they very rarely (or almost never?) change their passwords, while two respondents show an extremely high awareness of the necessity of regular password changes and do so every two months. This contrast underscores the need for ongoing education about password security and the risks associated with complacency. One respondent stated that she does not check security indicators such as “https” before entering sensitive information online, while other respondents do so regularly. This highlights a critical gap in knowledge that could potentially expose individuals to significant security threats. Three respondents stated that they have

encountered attempts at online scams (abuse in online shopping and fake job offers) and that they regularly check the identity of email and message senders. Only one respondent mentioned that if the message/email came from a sender known to be in an authoritative position, she does not check the sender's identity. This illustrates the complexities of trust in digital communications and the need for a more nuanced understanding of online interactions. Three respondents have not been in a situation where someone asked for their personal information, while two have, and they felt quite uncomfortable about it. This discomfort signals an awareness of personal boundaries in digital contexts, which is crucial for maintaining online safety.

When it comes to meeting in person with people they meet online, respondents say they have had such experiences. They either schedule meetings in a public place in the city centre or take another person with them for greater security. This careful approach shows a commendable level of caution and understanding of the potential risks associated with offline interactions stemming from online relationships. Of course, these meetings were preceded by longer-term online contact and acquaintance.

In the qualitative research, there was a special emphasis on respondents' personal good cyber security practices and behaviours, as well as areas for cyber security improvement. When asked what good cyber security practices they currently follow, the respondents answered: (P:4) "Checking websites and using different and strong passwords. I am aware that I can be a victim of phishing and catfishing at any moment"; (P:5) "Keeping my information private and maintaining an antivirus"; (P:1) "I currently follow practices such as regular software updates and regular computer virus scans". These responses reflect a range of effective strategies that individuals employ, yet they also reveal a disparity in knowledge and practices among different users. One respondent admitted that she does not have enough knowledge about good cyber security practices, and one respondent stated that he attends cyber security training. This suggests that while some individuals actively seek to enhance their knowledge, others may not have the same opportunities or motivation. Areas of cyber security in which respondents feel they need more knowledge or improvement are recognition of AI-created content, advanced protection techniques against various frauds, protection of personal data, multiple authentication, and legal protection against attempted online harassment.

The last topic we discussed in the interviews is whether respondents believe that education has adequately prepared them to deal with cyber security threats, what additional resources or training would help them improve their awareness and practices, and whether it is important to include cyber security education into the formal curriculum of their studies. The respondents agree that their previous education (from elementary school to university level) did not prepare them enough to deal with online threats and that they learned most things about cyber security independently thanks to their own interest and research. This finding underscores a critical gap in the educational system regarding cyber security training. Therefore, additional resources and training would certainly be valuable. (P:1) "Additional resources such as online courses, seminars, and webinars on cybersecurity would help improve my knowledge and practices"; (P:4) "I think that every faculty and university should hold a seminar about cyber security once a year, which would be mandatory, or that certain professors include a section on cyber security in their lectures and within their subject". These suggestions reflect a proactive desire for institutional support in enhancing cyber security education. Also, all respondents agree that cyber security topics should be incorporated into the curricula of their studies. This consensus suggests a recognition of the importance of equipping future generations with the necessary skills to navigate an increasingly complex digital landscape. This, they believe, would prepare students better for facing modern threats and to develop awareness of the importance of protecting their digital data.

The results of the qualitative research indicate significant challenges and gaps in awareness of cybersecurity among students. While most respondents demonstrate a certain level of confidence in recognizing and managing security threats, there is a clear need for additional

education and resources to enable them to better understand and implement good practices. Empowering students through systematic education on cybersecurity can significantly reduce the risks associated with online interactions. Ultimately, it is evident that education is crucial for developing awareness of the importance of protecting digital data, which will help shape a safer online environment for all users.

4 Discussion

The combined insights from both quantitative and qualitative research underscore a critical picture of cybersecurity awareness and practices among students from Bosnia and Herzegovina, Serbia, and Montenegro. Our findings indicate that while a significant number of participants exhibit some awareness and engage in positive cybersecurity practices, a troubling percentage remain uninformed about essential security measures, thus exposing themselves to various risks.

Quantitatively, the data revealed that while 61% of respondents utilize antivirus software and 85% are active on social media platforms, still considerable number remain unaware of fundamental cybersecurity concepts, such as the importance of checking for “https” in URLs or recognizing phishing attempts. This aligns with Muniandy et al. (2017), whose research highlighted the vulnerabilities in user behaviour that could lead to security threats. Similarly, Huraj et al. (2023) observed that despite a recognition of cybersecurity’s significance among students in differing disciplines, actual behaviours often do not reflect this awareness, indicating a gap between knowledge and practice.

Qualitatively, interviews with participants revealed a range of self-reported cybersecurity practices. While many acknowledged the importance of using strong, unique passwords, a notable proportion admitted to using easily guessable passwords based on personal information or neglecting to change their passwords regularly. This inconsistency mirrors findings from Ahamed et al. (2024), which demonstrated a positive correlation between cybersecurity knowledge and password management practices. Our research further emphasizes the necessity for educational interventions targeting password security and overall cybersecurity awareness.

Respondents also expressed a common sentiment that their formal education has not sufficiently prepared them for the complexities of modern cyber threats. This aligns with findings from López Mendoza et al. (2023), which advocate for enhanced curricular and extracurricular training in cybersecurity. Participants in our study specifically requested additional resources, such as online courses and seminars, to bolster their understanding and application of cybersecurity practices.

Finally, aligning with the perspective of Yan et al. (2018), our research reinforces the notion that ordinary users, rather than technological systems, represent the weakest link in cybersecurity. The average cybersecurity judgment among students was notably low, suggesting a pressing need for targeted educational initiatives. By focusing on enhancing students’ cybersecurity literacy and practical skills, educational institutions can empower individuals to navigate the digital landscape more safely, ultimately fostering a more secure online environment.

In conclusion, our findings reveal both positive behaviours and significant gaps in cybersecurity awareness among students. The need for ongoing education and proactive measures is clear, as it is essential to equip the younger generation with the tools necessary to mitigate risks associated with their online activities. Future research should continue to explore these dynamics and evaluate the effectiveness of educational interventions aimed at improving cybersecurity practices among students.

5 Conclusion

The triangulation of research methods, in the form of a quantitative questionnaire survey and qualitative research through semi-structured interviews conducted among students from Bosnia and Herzegovina, Serbia, and Montenegro provided significant insights into their behaviours and awareness of cybersecurity, as it allowed for both statistical analysis and in-depth exploration of their experiences and perspectives. The research results show a diversity of practices among respondents, with some demonstrating commendable cybersecurity habits while others are exposed to significant risks. These findings underscore the vulnerability of young internet users and the critical need for enhancing cybersecurity education and awareness programs.

From the quantitative data, while most respondents use internet and social media intensively, their awareness and practices in managing cybersecurity measures vary widely. Qualitative interviews further highlighted students' personal experiences and perspectives on cybersecurity. Respondents expressed shortcomings in formal education on cybersecurity, indicating their need for self-learning to fill these knowledge gaps. They identified specific areas for improvement, such as recognizing advanced online threats and implementing multi-factor authentication. So, it is not enough to know how to use (technically) modern digital devices, software, and applications; it is necessary to take care to protect both your own and others' data. Students are the ones who will enter the job market after completing their studies, become employees of companies and institutions, and have access to a wider range of data, many of which can be vulnerable, confidential, and significant both for the company and the wider community. It is crucial for them to be aware of the above-mentioned aspects of cybersecurity.

Although there are examples of good cybersecurity practices among students, there is a clear imperative to raise awareness and readiness against evolving cyber threats. Enhancing cybersecurity literacy and promoting safer online behaviour will not only protect students but also contribute to a safer digital environment overall. Future initiatives should focus on empowering students to manage the digital space safely and responsibly.

Cybersecurity hygiene can be improved through personal commitment – lifelong learning and self-improvement through training and informal education, as well as by incorporating cybersecurity topics into all segments of formal education. It is not necessary to introduce new subjects of course, rather, cybersecurity topics can be incorporated into existing curricula, because every aspect of our lives today can face online security threats. The foundation for further development and enhancement of cybersecurity through educational initiatives may lie in improving media and information literacy as a strategic commitment to the overall advancement of the cybersecurity domain (Vajzović, 2019). In this context, a hybrid model of the multi-component integration of media and information literacy into the educational system could serve as an educational initiative, which implies a method of integrating media and information literacy into educational systems, both horizontal and vertical integration are included. Vertical integration involves the development of science, research, and lifelong education for future teachers, which will, through science and research, support decision-makers, ensure professional development, and facilitate work with teachers, librarians, and other stakeholders at all levels of the educational system. Horizontal integration entails cross-curricular collaboration between teachers and librarians within curricula and teaching plans, as well as learning outcomes. In this context, the focus is on the principles and content for developing media and information literacy as a foundational competency within the educational system and society (Vajzović et al., 2021).

The strength of this study lies in selection of students from three Balkan countries (Bosnia and Herzegovina, Serbia, and Montenegro), which provides valuable data and expands the discussion on cybersecurity in regions where research activity in this area is comparatively lower. However, future research could focus on identifying cultural and contextual factors influencing the attitudes and behaviours of youth in cybersecurity. Investigating the impact of educational background, field of study, and socioeconomic status on cybersecurity behaviours could provide detailed insights.

Bibliography

AAG It Services. (2024, July 1). *The latest 2024 cyber crime statistics*. https://aag-it.com/the-latest-cyber-crime-statistics/

Ahamed, B., Polas, M. R. H., Kabir, A. I., Sohel-Uz-Zaman, A. S. Md., Fahad, A. A., Chowdhury, S., & Dey, M. R. (2024). Empowering students for cybersecurity awareness management in the emerging digital era: The role of cybersecurity attitude in the 4.0 industrial revolution era. *SAGE Open*, *14*(1). https://doi.org/10.1177/21582440241228920

Alghamdie, A. (2021). Denial of service attacks: An overview and mitigation strategies. *Journal of Cybersecurity and Information Systems*, *45*(3), 112-124.

Bjeloš, M., & Pavlović, M. (2022). *Sajber bezbednost i ljudska prava na zapadnom Balkanu: slučaj Srbije.* Beogradski centar za bezbednosnu politiku. https://bezbednost.org/wp-content/uploads/2022/10/cyber-security-srb-03-1.pdf

Bojanić, D., Gorski, I., & Razum, M. (2016). Zašto studenti ne traže pomoć? Barijere u traženju stručne pomoći kod studenata s psihičkim smetnjama. *Socijalna psihijatrija, 44*(4), 330-342.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Du, X., & Chintakovid, T. (2023). A survey of cybersecurity awareness among undergraduate students at Yunnan University of Finance and Economics in China. In X. Yuan, Y. Kurniawan, & Z. Ji (Eds.), *Proceedings of the 2023 4th international conference on education, knowledge and information management (ICEKIM 2023)* (pp. 740-753). Atlantis Press. https://doi.org/10.2991/978-94-6463-172-2_78

Edgar, T. W., & Manz, D. O. (2017). Chapter 2 – Science and cyber security. In T. W. Edgar, & D. O. Manz (Eds.), *Research methods for cyber security* (pp. 33-62). Syngress. https://doi.org/10.1016/B978-0-12-805349-2.00002-9

Ene, C. (2023, February 22). 10.5 trillion reasons why we need a united response to cyber risk. *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2023/02/22/105-trillion-reasons-why-we-need-a-united-response-to-cyber-risk/?sh=8ed0f773b0c4

Fox, J. (2023, December 8). *Top cybersecurity statistics for 2024*. https://www.cobalt.io/blog/cybersecurity-statistics-2024

Gu, Q., & Liu, P. (2007). Denial of service attacks. In H. Bidgoli (Ed.), *Handbook of computer networks: Distributed networks, network planning, control, management, and new trends and applications* (pp. 454-468). John Wiley and Sons. https://doi.org/10.1002/9781118256107.ch29

Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring cyber security awareness: A comparison between computer science and media science students. *TEM Journal*, *12*(2), 623-633. https://doi.org/10.18421/TEM122-05

Kamaruddin, M. D., Khuzairi, I. S. M., Rasid, A. F. D., Mohd, S. M., Kamarudin, S., Jan, M. N., & Idris, F. M. (2023). Assessing student awareness of cybersecurity: A mini survey. In A. F. Mohamad Amin, N. M. J. Mohamad Jan, N. A. Mohamed, & N. F. F. M. Mazlan (Eds.), *Proceedings of iJURECON 2023 Stream for the better future* (pp. 454-468). Kolej PERMATA Insan. https://oarep.usim.edu.my/server/api/core/bitstreams/5c37c99e-8d7f-4cd8-9255-fef49baa5f80/content

Kemp, S. (2024, January 31). *Digital 2024: Global overview report*. https://datareportal.com/reports/digital-2024-global-overview-report

Kepios. (n.d.). *Make sense of digital trends*. https://kepios.com/?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2024&utm_term=Bosnia_And_Herzegovina&utm_content=Kepios_Home_Link

Končarević, M. (2023). *Znanje i osviještenost opće populacije o kibernetičkoj sigurnosti* [Master's thesis]. University of Zagreb. https://urn.nsk.hr/urn:nbn:hr:148:430380

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

López Mendoza, A., Roque Hernández, R. V., Prieto Quezada, M. T., & Salazar Hernández, R. (2023). Cybersecurity among university students from Generation Z: A comparative study of the undergraduate programs in administration and public accounting in two Mexican universities. *TEM Journal*, *12*(1), 503-511. https://doi.org/10.18421/TEM121-60

Mahmutović, A., & Hodžić, E. (2022). *Izvještaj o cyber sigurnosnim prijetnjama u Bosni i Hercegovini.* CSEC; BIRN BiH.

Mashtalyar, N., Ntaganzwa, U. N., Santos, T., Hakak, S., & Ray, S. (2021). Social engineering attacks: Recent advances and challenges. In A. Moallem (Ed.), *HCI for cybersecurity, privacy and trust* (pp. 318-335). Springer. https://doi.org/10.1007/978-3-030-77392-2_27

Matаić, I. (2022). *Cyber security-zaštita kritičnih infrastruktura* [Master's thesis]. University of the North.

Mirković, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communications Review*, *34*(2), 39-53. https://doi.org/10.1145/997150.997156

Mujević, M. (2022). Synthesis of threats and risks of cyber security of Montenegro – the vulnerability aspect of information communication infrastructure. *SCIENCE International Journal*, *1*(1), 9-20. https://doi.org/10.35120/sciencej010101m

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cyber Security*, *2017*, 1-13. https://doi.org/10.5171/2017.800299

Pande, J. (2017). *Introduction to cyber security*. Uttarakhand Open University.

Pawlowski, S. D., & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education*, *26*(4), 281-294.

Prskalo, D. (2022). Kibernetička sigurnost kao ključna determinanta nacionalne sigurnosti Republike Hrvatske. *Zbornik Sveučilišta Libertas*, *7*(8), 185-199. https://hrcak.srce.hr/294123

Saxena, R., & Gayathri, E. (2022). Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solutions. *Materials Today: Proceedings*, *51*(1), 682-689. https://doi.org/10.1016/j.matpr.2021.06.204

Spremić, M. (2017). *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije.* Ekonomski fakultet.

Steinberg, J. (2019). *Cybersecurity for dummies.* For Dummies.

Šimić, Z. (2023). *Analiza prijetnji i rizika kibernetičke sigurnosti te njihov utjecaj na poslovanje poduzeća* [Master's thesis]. Sveučilište Josipa Jurja Strossmayera u Osijeku.

Vajzović, E. (2019). Medijska i informacijska pismenost u sistemu cyber sigurnosti. *Posebno izdanje časopisa Kriminalističke teme, 19*(5), 529-542.

Vajzović, E., Hibert, M., Turčilo, L., Vučetić, V., & Silajdžić, L. (2021). *Medijska i informacijska pismenost: dizajn učenja za digitalno doba*. Fakultet političkih nauka.

Verma, V., & Pawar, J. (2024). Assessment of students cybersecurity awareness and strategies to safeguard against cyber threats. *Journal of Advanced Zoology, 45*(4), 82-89. https://doi.org/10.53555/jaz.v45iS4.4156

Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: A domain ontology and knowledge graph application examples. *Cybersecurity*, *4,* Article 31. https://doi.org/10.1186/s42400-021-00094-6

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior, 84*, 375-382. https://doi.org/10.1016/j.chb.2018.02.019

Authors

Dr. sc. Lamija Silajdžić
University of Sarajevo
Faculty of Political Sciences
Skenderija 72,
71 000 Sarajevo
BOSNIA AND HERZEGOVINA
lamija.silajdzic@fpn.unsa.ba
ORCID ID: 0000-0002-9248-1440

Lamija Silajdžić has been an assistant professor at the Department of Journalism at the Faculty of Political Sciences University of Sarajevo (Bosnia and Herzegovina) since June 2023. She received two Golden Badges of University of Sarajevo as the best student of her faculty during BA and MA studies. She has participated in domestic and international conferences and seminars and has published a respectable number of professional and scientific papers. She is the co-author of the book *Media and Information Literacy: Learning Design for the Digital Age* (2021). She is interested in the field of TV journalism, as well as in the impact of digital technologies on journalism, and media and information literacy. She has worked as a project manager, assistant, and researcher in several domestic and international scientific research projects. Prior to her academic career, she worked as a TV journalist for the Bosnian and Herzegovinian public broadcasting service.

Dr. sc. Anida Dudić-Sijamija
University of Sarajevo
Faculty of Political Sciences
Skenderija 72,
71 000 Sarajevo
BOSNIA AND HERZEGOVINA
anida.dudic@fpn.unsa.ba
ORCID ID: 0000-0002-2814-5661

Anida Dudić-Sijamija is an Assistant Professor at the Department of Social Work, Faculty of Political Sciences, University of Sarajevo. She has published scientific and professional papers in reputable international and domestic journals, and has been involved in domestic and international research projects. She has participated in numerous domestic and international scientific conferences, seminars, trainings, and workshops. She is a co-author of the following books: *Youth Study 2018/19, Scientific Research Study Social Work in Education* (2019). She is also the editor of the Proceedings: *Field Practice and Social Work in the Era of COVID-19 Pandemic: Experiences from Bosnia and Herzegovina and Croatia* (2023).