Journal of Transactions in Systems Engineering
https://journals.tultech.eu/index.php/jtse.
ISSN: 2806-2973
Volume 2, Issue 2
DOI: https://doi.org/10.15157/jtse.2024.2.2.222-234
Received: 31.05.2024; Revised: 24.06.2024; Accepted: 04.07.2024

Research Article

Descriptive Analysis of Cybersecurity Awareness Among Smartphone Users in Higher Education

Enxhia Sala[1*]

[1]Department of Statistics and Applied Informatics, Faculty of Economy, University of Tirana, Tirana, Albania

***enxhia.sala@unitir.edu.al**

Abstract

In an era defined by technology evolution, cybersecurity awareness has emerged as a critical concern for smartphone users, especially within academic environments. This paper investigates the results of the survey "Assessing Cybersecurity Awareness Among Smartphone Users" conducted among students in Albanian Higher Education Institutions. The study evaluates dimensions such as Security Behavior, Security Intention, Influence of People and Media, Perceived Usefulness, and Perceived Ease of Use. Demographic analysis encompasses variables like age, gender, educational level, employment status, IT background, and smartphone operating system, providing vital context for understanding cybersecurity awareness. Using Likert-scale responses and established methodologies, the research identifies significant differences in cybersecurity practices between students with and without formal education in Information Security. It emphasizes the pivotal role of education in promoting informed cybersecurity behaviors and calls for targeted educational strategies to bolster digital resilience.

Keywords: Cybersecurity awareness; smartphone users; higher education; Information Security education

INTRODUCTION

Considering the rapid development in the digital world, it has become essential for smartphone users, particularly in academic context, to have a high level of knowledge about cybersecurity. The survey titled "Assessing Cybersecurity Awareness Among Smartphone Users" [1], conducted from March to April 2024, targets students in the Albanian Higher Education System, encompassing Bachelor, Master, and Doctorate programs. A random sampling of 1,982 students (completion rate of 82%) from various public and private higher education institutions in Albania was surveyed to assess their cybersecurity awareness and practices. The survey employed a comprehensive methodological approach, evaluating responses across five key components: Security Behavior, Security Intention, Influence of People and Media, Perceived Usefulness, and Perceived Ease of Use.

The demographic analysis of the survey provides a detailed understanding of the participants' backgrounds, covering multiple dimensions such as age, gender, educational

cycle, employment status, work experience, academic background in information technology, and the types of smartphone operating systems used by the respondents. These factors play an important role in contextualizing the findings of the survey and understanding the cybersecurity awareness levels among the respondents.

The survey's methodological approach involved assessing responses on a five-point Likert-type scale ranging from 1 (strongly disagree) to 5 (strongly agree), [2-4]. The questions were designed to assess several dimensions of cybersecurity awareness, including familiarity with typical risks, understanding of preventive actions, and perception of personal susceptibility to cyberattacks [5, 6]. Additionally, the survey examined the influence of social and psychological factors on cybersecurity behaviors, such as peer influence, and perceived self-efficacy [3].

By integrating demographic data, the study aims to assess the influence of variables such as age, education, and technological proficiency on cybersecurity awareness. This thorough exploration provides valuable insights into the cybersecurity practices and intentions of students, comparing those with formal education in Information Security to those without. It highlights the importance of targeted education in fostering a culture of cybersecurity awareness and proactive behaviors among the student population.

Evaluating the cybersecurity level of awareness is crucial for planning an ADR (Action Design Research) project aimed at increasing it [7]. This evaluation identifies knowledge gaps, informs tailored training programs, and establishes a baseline for measuring progress. By understanding current awareness levels, targeted interventions can be developed to enhance employee preparedness, foster a security-conscious culture, and ensure compliance with regulatory requirements, ultimately strengthening overall cybersecurity resilience.

DEMOGRAPHIC ANALYSIS

The demographic analysis of this survey provides a comprehensive and detailed understanding of the participants' backgrounds. The survey successfully captured data across multiple demographic dimensions, including age, gender, educational cycle, employment status, work experience, academic background in information technology, and the types of smartphone operating systems used by the respondents. This thorough demographic profiling is vital in contextualizing the findings related to cybersecurity awareness among smartphone users, particularly within the targeted population of students within the Albanian Higher Education System, spanning across Bachelor, Master, and Doctorate programs.

The survey commenced by addressing the age distribution of the respondents. With an average age of 21 years, the survey targets a young demographic, composed mainly of students and young professionals. The relatively young average age suggests that the respondents are likely to be digital natives, growing up in an era where smartphones and digital technology are ubiquitous. This factor is important as it may influence their familiarity and interaction with cybersecurity concepts and practices.

Gender distribution was another critical demographic factor explored in the survey. The results indicate a significant gender disparity among the participants, with females constituting 79% of the respondents, while males comprised only 21%, see Figure 1. This notable skew towards female respondents could have various implications for the study's findings, as gender differences can influence cybersecurity awareness and behaviours.

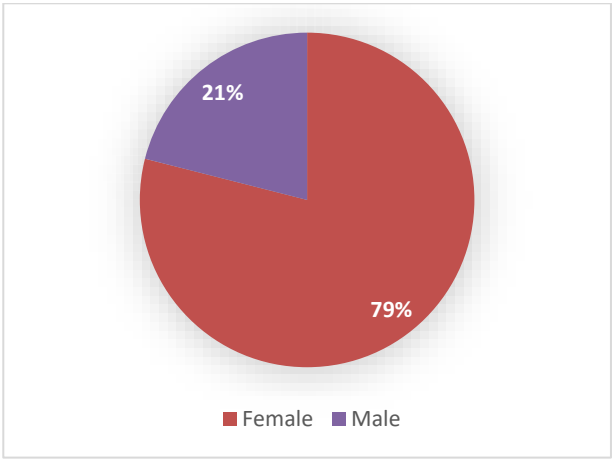


Figure 1. Gender (Pie Chart)

Educational cycle was thoroughly examined. Specifically, 82% of the participants reported attending a bachelor's program, while 14% indicated they were attending a master's program. Additionally, 4% of respondents were pursuing a doctorate, see Figure 2. This data suggests that the surveyed population is predominantly well-educated, which may correlate with higher levels of cybersecurity awareness. Participants' high educational cycle may also reflect their ability to comprehend and respond effectively to cybersecurity threats. It is important to note that higher education levels often correlate with increased access to information and resources, potentially leading to better cybersecurity practices.

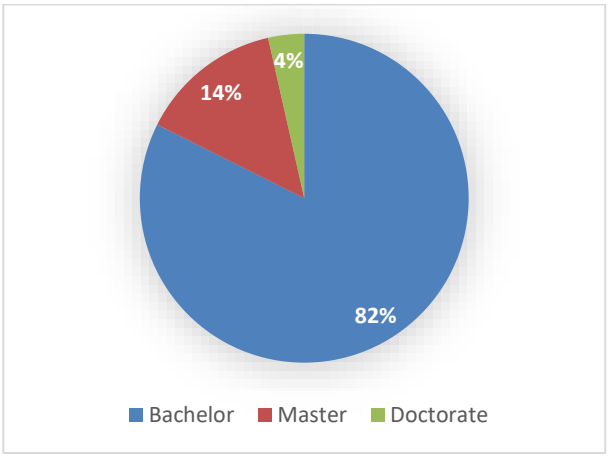


Figure 2. Educational cycle (Pie Chart)

The survey further investigated the employment status of the respondents, with a question on whether they were employed full-time or part-time. The results showed a

significant majority, 83%, of the participants were not currently employed, while only 17% reported being employed, see Figure 3. This large proportion of unemployed respondents might influence their cybersecurity practices, as employment status can impact both the necessity and the means to invest in cybersecurity measures. The clear distinction in employment status also provides an avenue to explore how varying levels of employment influence cybersecurity awareness.

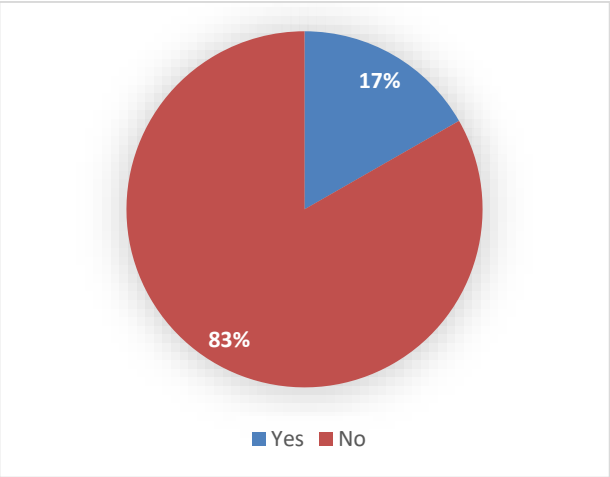


Figure 3. Employment status (Pie Chart)

Work experience was another demographic aspect addressed in the survey. The average number of years of work experience among respondents was calculated to be 1.4 years. This low average indicates that most participants are relatively new to the workforce, which could impact their cybersecurity awareness and behaviors. Less work experience might correlate with less exposure to formal cybersecurity training and policies typically encountered in professional settings. Understanding the work experience of the respondents is important as it can correlate with their familiarity and interaction with cybersecurity protocols, especially in professional environments. The combination of a young average age and limited work experience suggests that the respondents may rely more on personal knowledge and informal learning when it comes to cybersecurity practices.

The survey also inquired about the respondents' academic background in information technology. It revealed that 64% of participants have a study program background in information technology, while 36% do not, see Figure 4. This significant majority with an IT background suggests that a large portion of the respondents are likely to have a foundational understanding of technical concepts, which could positively influence their cybersecurity awareness and practices. This academic exposure to IT is an important factor as it likely contributes to the participants' familiarity with cybersecurity issues and preventive measures.

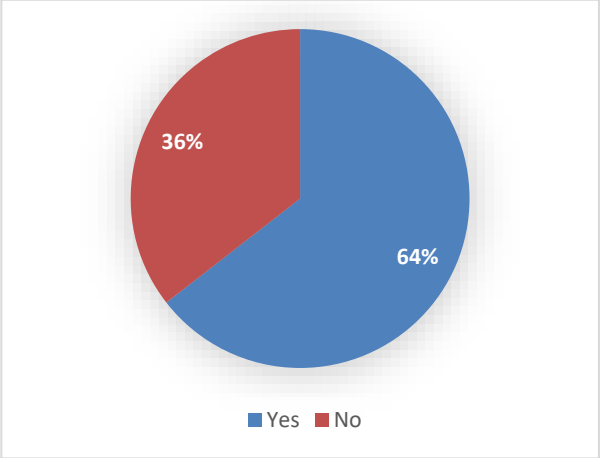


Figure 4. IT Background (Pie Chart)

Furthermore, the survey explored whether the respondents had specifically studied information security. It indicated that only 20% of the respondents had studied information security, while a substantial 80% had not, see Figure 5. This reveals a gap in specialized knowledge among the majority of participants, despite many having an IT background. The lack of formal education in information security among most respondents could highlight a potential area for improvement in educational curricula, aiming to better equip individuals with the necessary skills to navigate and mitigate cybersecurity threats.

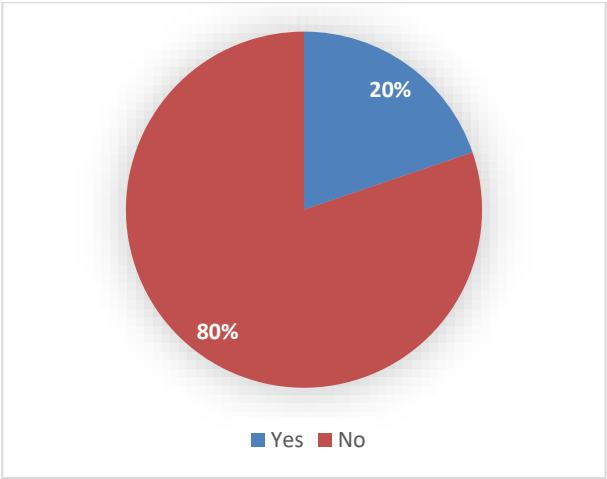


Figure 5. Information Security education (Pie Chart)

Lastly, the survey examined the types of smartphone operating systems used by the respondents, revealing a predominant preference for iOS. Specifically, 68% of participants reported using iOS while 31% used Android, and a marginal 1% indicated using other operating systems, see Figure 6. This strong inclination towards iOS could be indicative of the demographic's purchasing power, brand loyalty, or specific preferences that influence their cybersecurity practices. The preference for iOS over Android might also reflect perceived security features associated with these operating systems. This information is significant as different operating systems have varying security features and

vulnerabilities, which can influence the overall cybersecurity awareness and practices of the users.

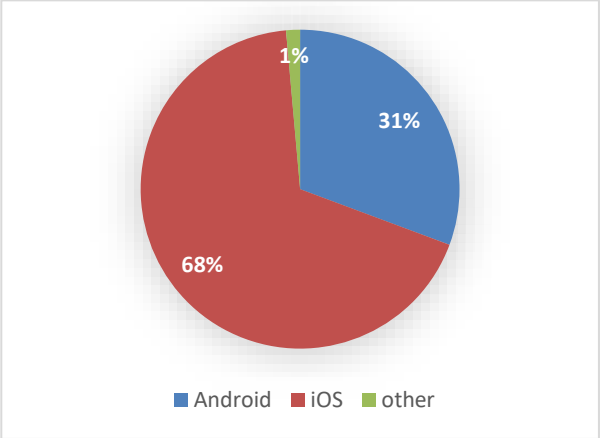


Figure 6. Operating System Information (Pie Chart)

Overall, the demographic analysis of this survey presents a well-rounded profile of the respondents. The survey attracted full participation in key demographic areas, ensuring the reliability of the data. The findings reveal a predominantly young, female, highly educated, and largely unemployed population with limited work experience and a strong preference for iOS devices. A significant portion of the respondents has an academic background in information technology, though few have studied information security specifically. These demographic characteristics are essential for understanding the cybersecurity awareness levels among smartphone users and provide valuable insights into how various factors such as age, gender, education, employment status, work experience, academic background, and smartphone OS preference influence cybersecurity behaviors and awareness. This comprehensive demographic profiling sets the foundation for deeper analysis and interpretation of the survey's findings on cybersecurity awareness within the context of the Albanian Higher Education System.

RESULTS

Security Behavior

The analysis of the survey "Assessing Cybersecurity Awareness Among Smartphone Users" provides a detailed examination of the security behaviors of students within the Albanian Higher Education System, specifically comparing those who have been educated in Information Security (IS) with those who have not. This comparative analysis highlights key differences and similarities in their cybersecurity practices and awareness, providing insights into how education in Information Security impacts these behaviors.

The survey question regarding the use of hard-to-guess passwords, PINs, patterns, or biometric recognition on smartphones shows a significant difference between the two groups. Among students not educated in Information Security, the weighted average was 4.29. In contrast, students educated in Information Security had a higher agreement level,

with a weighted average of 4.55. This indicates that IS-educated students are more likely to adopt strong security measures for smartphone access, reflecting their awareness and understanding of the importance of secure authentication.

When it comes to downloading software from known and safe sources, the discrepancy is also notable. Students without Information Security education have a weighted average of 3.95, while those with IS education score higher at 4.29. This suggests that IS-educated students are more cautious about the sources of their software downloads, likely due to their knowledge of the risks associated with downloading from untrusted sources. This behavior reduces the likelihood of malware infections and other security threats.

The practice of avoiding charging smartphones at public gates shows a smaller difference between the two groups, with non-IS students having a weighted average of 3.52 and IS students at 3.69. Although both groups exhibit caution, IS-educated students demonstrate slightly higher awareness, possibly due to their understanding of potential security risks like data theft through public charging stations, known as "juice jacking."

Regularly updating smartphone software is another area where IS-educated students show higher compliance. The weighted average for students without IS education is 4.07, compared to 4.25 for those with IS education. Regular updates are vital for patching security vulnerabilities, and the higher adherence among IS-educated students highlights their proactive approach to maintaining smartphone security.

The behavior regarding the use of free public Wi-Fi reveals a more significant difference. Students without IS education have a weighted average of 3.01, whereas IS-educated students score 3.39. This indicates that IS-educated students are more diligent in ensuring that public Wi-Fi is protected before connecting, reducing the risk of exposure to unsecured networks and potential cyber-attacks.

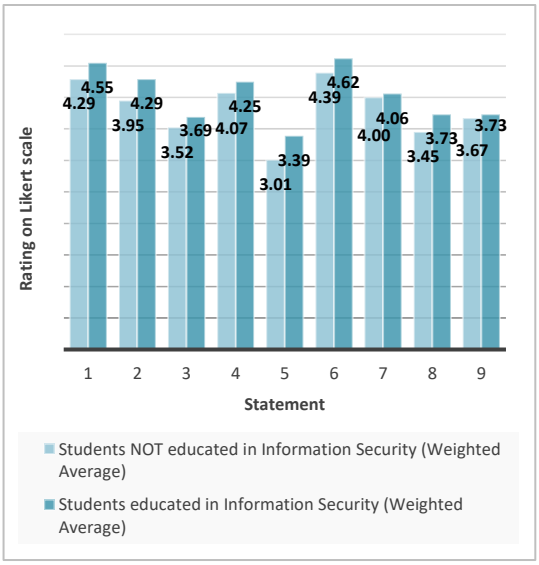
Avoiding clicking links from unknown senders is an essential cybersecurity practice where IS-educated students again demonstrate higher caution. The weighted average for non-IS students is 4.39, while for IS students it is 4.62. This behavior is important for preventing phishing attacks and malware infections, and the higher scores among IS-educated students reflect their heightened awareness of these risks.

Managing app permissions carefully is another area where the two groups show a smaller but notable difference. Students without IS education have a weighted average of 4.00, while those with IS education score 4.06. This slight difference suggests that IS-educated students are marginally more meticulous in reviewing and managing app permissions, which can prevent unauthorized access to personal data and device functionalities.

The use of recovery apps to locate lost smartphones shows a more significant gap. Non-IS students have a weighted average of 3.45, compared to 3.73 for IS students. This behavior highlights the preparedness of IS-educated students in mitigating the impact of losing their smartphones by utilizing recovery tools.

When it comes to storing sensitive personal data on smartphones, both groups exhibit similar behaviors, with non-IS students having a weighted average of 3.67 and IS students slightly higher at 3.73. This indicates that despite their education, a significant portion of

IS-educated student's still store sensitive data on their devices, suggesting a potential area for further education and improvement, see Figure 7.



No.	Statement
1	I use hard-to-guess password/pin/pattern or biometric recognition (face, fingerprint) on my smartphone.
2	I download software from known and safe sources on my smartphone.
3	I avoid charging my smartphone at public gates.
4	I regularly update my smartphone software.
5	I make sure that free public Wi-Fi is protected before connecting my smartphone.
6	I do not click links from unknown senders on my smartphone.
7	I carefully manage app permissions on my smartphone.
8	I use the recovery app, which allows me to locate my smartphone in case I lose it.
9	I store sensitive personal data on my smartphone.

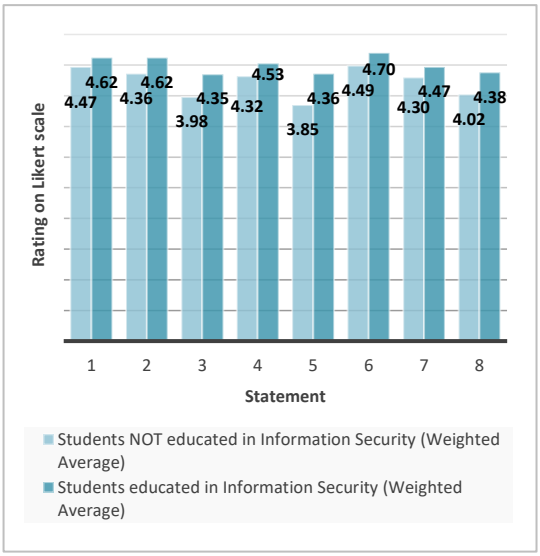
Figure 7. Security Behavior (Bar Chart)

Overall, the demographic analysis indicates that students educated in Information Security demonstrate higher cybersecurity awareness and better security practices compared to their non-IS educated peers. The differences in weighted averages across various security behaviors suggest that Information Security education plays a significant role in shaping students' attitudes and practices towards smartphone security. These findings underscore the importance of integrating cybersecurity education into academic curricula to enhance overall cybersecurity awareness and practices among population. As the surveyed population is predominantly young, highly educated, and composed of students within the Albanian Higher Education System, these insights are essential for developing targeted educational programs and policies aimed at improving cybersecurity awareness and behavior among this demographic.

Security Intention

Security intentions provide insight into the future behaviors of students regarding cybersecurity practices. Students educated in Information Security exhibit stronger intentions to adopt secure behaviors, as reflected in their higher weighted averages. For example, the intention to use hard-to-guess passwords or biometric recognition has a higher weighted average among students educated in Information Security (4.62) compared to those not educated in Information Security (4.47). This indicates that formal education in Information Security not only impacts current behaviors but also shapes future intentions towards maintaining high cybersecurity standards. The intention to download software from known and safe sources also shows a higher weighted average among Information Security-educated students (4.62) compared to those not educated in Information Security (4.36), further emphasizing the long-term impact of Information

Security education on secure behaviors. Avoiding public charging stations, which can be potential security risks, is another behavior where students educated in Information Security exhibit stronger intentions (4.35) compared to those not educated in Information Security (3.98). This reflects a deeper understanding of the risks associated with public charging stations, such as juice jacking, among those with Information Security education. The intention to regularly update smartphone software also shows a higher weighted average among students educated in Information Security (4.53) compared to their counterparts (4.32), etc. This demonstrates a recognition of the importance of keeping software up to date to protect against vulnerabilities, see Figure 8.

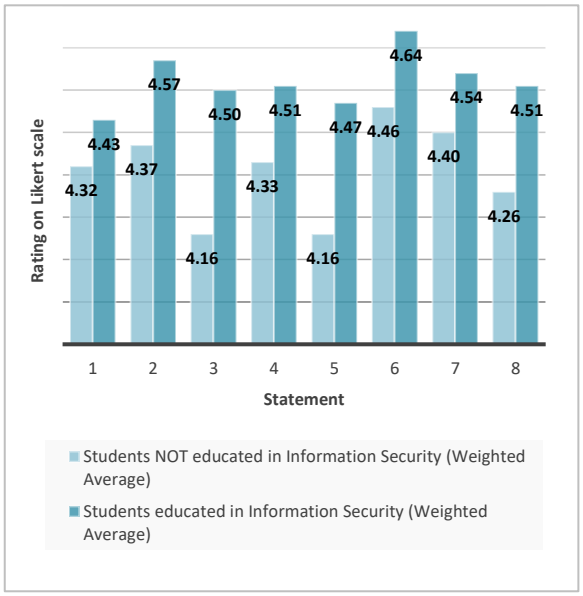


No.	Statement
1	I intend to use hard-to-guess password/pin/pattern or biometric recognition (face, fingerprint) on my smartphone.
2	I intend to download software from known and safe sources to my smartphone.
3	I intend to avoid charging my smartphone at public gates.
4	I intend to update the software of my smartphone.
5	I intend to make sure that free public Wi-Fi is protected before connecting my smartphone.
6	I intend not to click on links from unknown senders on my smartphone.
7	I intend to carefully manage app permissions on my smartphone.
8	I intend to use the recovery app on my smartphone.

Figure 8. Security Intention (Bar Chart)

Influence of People and Media

The influence of people and media plays a significant role in shaping cybersecurity practices. Students educated in Information Security show a greater propensity to follow recommendations from trusted sources, such as friends, family, professors, and media. For example, the weighted average for using hard-to-guess passwords or biometric recognition based on recommendations is higher among students educated in Information Security (4.43) compared to those not educated in Information Security (4.32). This trend is evident in other behaviors, such as downloading software from known sources (4.57 vs. 4.37), avoiding public charging stations (4.50 vs. 4.16), and updating smartphone software regularly (4.51 vs. 4.33), etc. These findings underscore the importance of credible sources in promoting secure practices, especially among those with formal education in Information Security, see Figure 9.

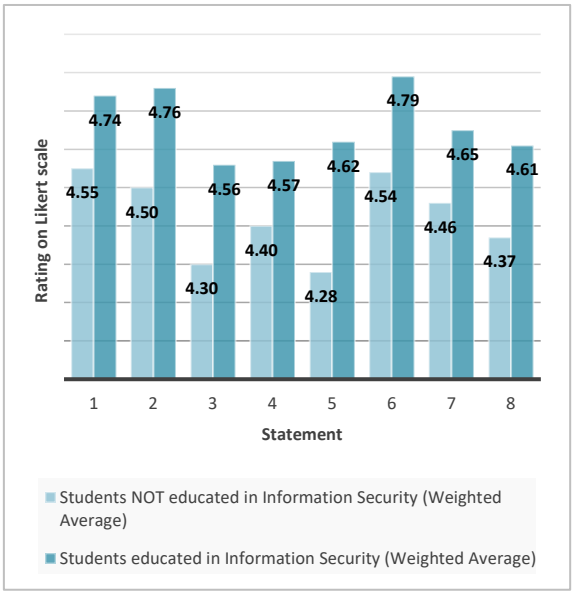


No.	Statement
1	If recommended by people (friends, family, professors, managers, etc.), or media (TV, Internet, etc.) that are important to me, I would use hard-to-guess password/pin/pattern or biometric recognition (face, fingerprint) on my smartphone.
2	If recommended by people (friends, family, professors, managers, etc.), or media (TV, Internet, etc.) that are important to me, I would download software from known and safe sources to my smartphone.
3	If recommended by people (friends, family, professors, managers, etc.), or media (TV, Internet, etc.) that are important to me, I would avoid charging my smartphone at public gates.
4	If recommended by people (friends, family, professors, managers, etc.), or media (TV, Internet, etc.) that are important to me, I would update my smartphone software regularly.
5	If recommended by people (friends, family, professors, managers, etc.), or media (TV, Internet, etc.) that are important to me, I would make sure that free public Wi-Fi is protected before using it. connect my smartphone.
6	If recommended by people (friends, family, professors, managers, etc.), or media (TV, Internet, etc.) that are important to me, I would not click on links from unknown senders on my smartphone.
7	If recommended by people (friends, family, professors, managers, etc.), or media (TV, Internet, etc.) that are important to me, I would carefully manage the app permissions on my smartphone.
8	If recommended by people (friends, family, professors, managers, etc.), or media (TV, Internet, etc.) that are important to me, I would use the recovery app on my smartphone.

Figure 9. Influence of People and Media (Bar Chart)

Perceived Usefulness

Perceived usefulness of security measures is another important aspect analyzed in the survey. Students educated in Information Security consistently rate the usefulness of various security practices higher than their counterparts. For instance, the weighted average for the perceived usefulness of using hard-to-guess passwords or biometric recognition is higher among students educated in Information Security (4.74) compared to those not educated in Information Security (4.55). This pattern holds for other security measures, such as downloading software from known sources (4.76 vs. 4.50), avoiding public charging stations (4.56 vs. 4.30), and ensuring public Wi-Fi is protected (4.62 vs. 4.28), etc. These results indicate that education in Information Security enhances students' recognition of the importance and effectiveness of these practices, see Figure 10.

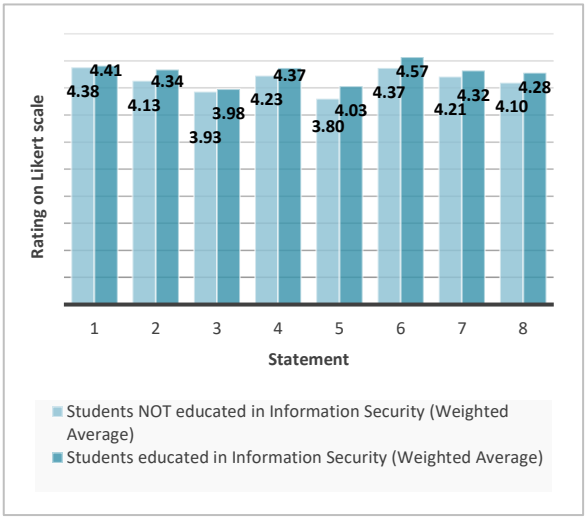


No.	Statement
1	I think it is useful and effective to secure my smartphone from security threats using hard-to-guess password/pint/pattern or biometric recognition (face, fingerprint) on my smartphone.
2	I think it is useful and effective to secure my smartphone from security threats to download software from known and safe sources on my smartphone.
3	I think it is useful and effective to secure my smartphone from security threats to avoid charging my smartphone at public gates.
4	I think it is useful and effective to secure my smartphone from security threats to update my smartphone software regularly.
5	I think it is useful and effective to secure my smartphone from security threats to ensure that free public Wi-Fi is protected before I connect my smartphone.
6	I think it is useful and effective to secure my smartphone from security threats not to click the links coming from unknown senders on my smartphone.
7	I think it is useful and effective to secure my smartphone from security threats to carefully manage app permissions on my smartphone.
8	I think it is useful and effective to secure my smartphone from security threats using the recovery app on my smartphone.

Figure 10. Perceived Usefulness (Bar Chart)

Perceived Ease of Use

Lastly, perceived ease of use of security measures reveals that students educated in Information Security find these practices slightly easier to implement. For example, the weighted average for the ease of using hard-to-guess passwords or biometric recognition is marginally higher among students educated in Information Security (4.41) compared to those not educated in Information Security (4.38). Similar trends are observed for other practices, such as downloading software from known sources (4.34 vs. 4.13), avoiding public charging stations (3.98 vs. 3.93), and updating smartphone software regularly (4.37 vs. 4.23), etc. This suggests that education in Information Security may reduce perceived barriers to implementing secure practices, see Figure 11.



No.	Statement
1	It's easy to use hard-to-guess password/pin/pattern or biometric recognition (face, fingerprint) on my smartphone.
2	It's easy to download software from known and safe sources to my smartphone.
3	It's easy to avoid charging my smartphone at public gates.
4	It's easy to update my smartphone software regularly.
5	It's easy to make sure free public Wi-Fi is protected before I connect my smartphone.
6	It's easy not to click on links from unknown senders on my smartphone.
7	It's easy to carefully manage app permissions on my smartphone.
8	It's easy to use the recovery app on my smartphone.

Figure 11. Perceived Ease of Use (Bar Chart)

CONCLUSION

In conclusion, the survey results highlight significant differences in cybersecurity awareness and practices between students educated in Information Security and those who are not. Students with formal education in Information Security demonstrate higher levels of secure behaviors, stronger intentions to adopt secure practices, greater influence from trusted sources, and higher perceived usefulness and ease of use of security measures. These findings emphasize the key role of Information Security education in enhancing cybersecurity awareness and practices among smartphone users in the Albanian Higher Education System. This analysis underscores the importance of integrating comprehensive cybersecurity education into academic curricula to equip students with the necessary knowledge and skills to protect themselves in an increasingly digital world. By comparing the weighted averages of these two groups across various dimensions, it is clear that Information Security education significantly contributes to fostering a culture of cybersecurity awareness and proactive security behaviors.

CONFLICT OF INTERESTS

The author would like to confirm that there is no conflict of interests associated with this publication and there is no financial fund for this work that can affect the research outcomes.

REFERENCES

1. Sala, E. and Martiri, E. Assessing Cybersecurity Awareness Among Smartphone Users: Designing a Comprehensive Survey, *Proceedings of the 2nd International Conference Creativity and Innovation in Digital Economy*, **2023**; pp. 46-52.

2. Fishbein, M. and Ajzen, I. Predicting and Changing Behavior: The Reasoned Action Approach, *Psychology Press*, **2010**.
3. Dinev, T. and Hart, P. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, **2006**; 17; pp. 61-80.
4. Taylor, S. and Todd, P.A. Understanding Information Technology Usage: A Test of Competing *Information Systems Research*, **1995**; 6; pp. 144-176.
5. Rook, D.W. and Fisher, R.J. Normative Influences on Impulsive Buying Behavior. *Journal of Consumer Research,* **1995**; 22; pp. 305-313.
6. Slovic, P. The Perception of Risk, *Earthscan*, **2000**.
7. Sala, E. and Martiri, E. ADR Project Planning to increase Cyber Security Awareness of Mobile Device Users. *International Journal on Technical and Physical Problems of Engineering (IJTPE)*, **2023**; 15; pp. 327-333.