International Journal of Innovative Technology and Interdisciplinary Sciences
https://journals.tultech.eu/index.php/ijitis
ISSN: 2613-7305
Volume 7, Issue 3
DOI: https://doi.org/10.15157/ijitis.2024.7.3.137-146
Received: 25.07.2024 ; Revised: 02.09.2024 ; Accepted: 11.10.2024

Research Article

Descriptive Analysis of Breach Experience Among Smartphone Users in the Albanian Higher Education Sector

Enxhia Sala *

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

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

Abstract

This paper investigates breach experiences among smartphone users in the Albanian Higher Education System. The survey examined the cybersecurity knowledge and breach incidents among students. The study focused on assessing cybersecurity awareness and experiences of unauthorized access, data loss, and malware infections. Results indicated that students with formal education in information security demonstrated higher self-assessed knowledge levels and reported fewer security incidents compared to their counterparts without such education. However, challenges such as smartphone loss and data breaches remain prevalent, even among educated users. These findings highlight the necessity for comprehensive and continuously updated cybersecurity education within academic curricula. By enhancing students' understanding and skills in digital security, educational institutions can better prepare individuals to safeguard their personal information and contribute to a more secure digital environment. This research underscores the importance of evolving cybersecurity education to address emerging threats and behaviors, eventually fostering a safer digital landscape for all users.

Keywords: Cybersecurity Awareness; Smartphone Users; Information Security Education; Breach Experience; Digital Security.

INTRODUCTION

The widespread usage of smartphones in a progressively networked global society has resulted in an evolutionary change in the process of how people get and share information [1]. Smartphones, although offering great convenience and connectivity, nevertheless present significant cybersecurity risks [3]. The rapid proliferation of smartphones has fundamentally transformed the digital landscape, hence demanding an in-depth understanding of the level to which smartphone users are aware of cybersecurity [9].

The survey "Assessing Cybersecurity Awareness Among Smartphone Users" [8], reveals a comprehensive analysis of cybersecurity awareness among students in the Albanian Higher Education System. Utilizing a random sampling method, the survey gathered data from a substantial number of students, achieving an impressive completion rate. The survey is divided into two primary sections: the first assessing the level of cybersecurity awareness and the second evaluating the breach experience of smartphone users. The demographic analysis of the survey, as detailed in the article "Descriptive Analysis of Cybersecurity Awareness Among Smartphone Users in Higher Education" [6], provides a detailed understanding of the participants' backgrounds.

This demographic profile highlights a young, female, highly educated, and largely unemployed population with limited work experience and a significant inclination towards iOS devices, providing essential context for understanding cybersecurity awareness among higher education students in Albania [6].

The second part of the survey focused on breach experience and also examined the computing experience, providing an in-depth overview of participants' technical skills and making the demographic analysis complete. This section included a range of questions that allowed respondents to rate their knowledge on a scale. The results distinguished between those educated in information security and those who are not. It also provides interesting insights into the perceived probability of various security risks, the perceived severity of security incidents, and actual breach experiences. Assessing the breach experience is also critical for planning an ADR (Action Design Research) project aimed at cybersecurity awareness of smartphone users [7]. These findings highlight the significant impact of formal education in information security, suggesting that such education enhances practical knowledge and boosts confidence in protecting digital assets. In general, the data underscores the value of integrating more information security content into curricula to improve cybersecurity awareness and competence among students.

METHODOLOGY

The survey titled "Assessing Cybersecurity Awareness Among Smartphone Users", conducted from March to April 2024, targets students across Bachelor, Master, and Doctorate programs within the Albanian Higher Education Sector. Using random sampling, data was collected from 1,982 students, achieving a completion rate of 82%. The survey was divided into two sections: the first focused on evaluating cybersecurity awareness, and the second explored students' breach experiences with smartphone security [8]. This research addresses the increasing cybersecurity risks posed by the widespread use of smartphones [1]. The survey assesses key aspects such as knowledge of risks, perception of threats, adherence to best practices, and adoption of protective behaviors [9]. Input from experts in fields such as statistics, IT, cybersecurity, psychology, and sociology was used to ensure the survey's accuracy and depth [2, 10]. Likert-scale questions measure participants' attitudes towards cybersecurity, including their

familiarity with common risks, understanding of preventive actions, and perceived vulnerability to attacks [5].

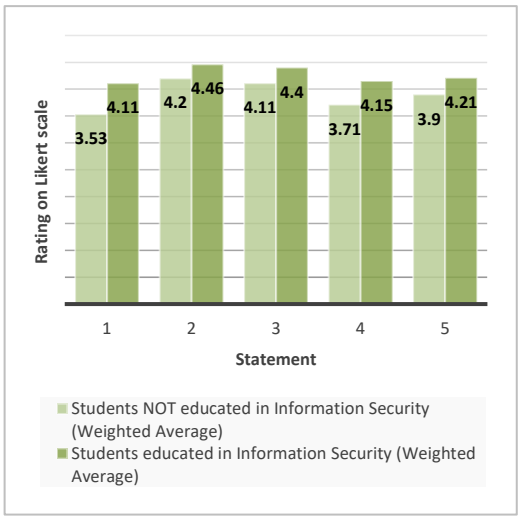
The second section captures data on breach experiences, allowing for insights into how these incidents influence security behaviors [4]. The study compares two subgroups: students from ICT-related programs and those from other disciplines, aiming to identify the impact of specialized education on cybersecurity practices. Demographic data such as age, education level, and technological proficiency is also collected to understand how these variables affect awareness [4]. A pilot test conducted with 100 students from the University of Tirana ensured the survey's reliability and clarity before full implementation, further enhancing the quality and relevance of the findings.

Demographic Analysis

The demographic analysis of the survey, published in the article "Descriptive Analysis of Cybersecurity Awareness Among Smartphone Users in Higher Education" [6], provides a comprehensive understanding of the participants' backgrounds. To summarize: the survey targeted a predominantly young demographic with an average age of 21 years, comprising mainly digital natives. There was a significant gender disparity, with females constituting 79% of the respondents. Most participants were pursuing a Bachelor's degree (82%), followed by Master's (14%) and Doctorate (4%) students. A majority (83%) were not employed, while only 17% were employed, and the average work experience was 1.4 years. Additionally, 64% of respondents had an academic background in information technology, though only 20% had studied information security. The analysis also revealed a strong preference for iOS devices, used by 68% of respondents, compared to 31% using Android and 1% using other operating systems.

The second part of the survey focused on breach experience also examined the computing experience, providing a detailed overview of participants' technical skills and making the demographic analysis complete. This section included five-scale Likert questions ranging from "very low" to "very high." The results distinguished between those educated in information security and those who are not.

When comparing students educated in information security with those who are not, it is evident that the educated group consistently rated their knowledge higher. For example, educated students rated their computer knowledge at 4.11 compared to 3.53 for non-educated students, smartphone usage knowledge at 4.46 versus 4.2, internet usage knowledge at 4.4 versus 4.11, information security knowledge at 4.15 versus 3.71, and knowledge about protecting smartphones at 4.21 compared to 3.9. These findings highlight the significant impact of formal education in information security, suggesting that such education enhances practical knowledge and boosts confidence in protecting digital assets. (Figure 1)



No.	Statement
1	Level of computer knowledge
2	Level of knowledge about using smartphone
3	Level of knowledge about using the Internet
4	Level of information Security knowledge
5	Level of knowledge about protecting smartphone

Figure 1. Computing Experience (Bar Chart)

RESULTS

The results of this study align closely with previous research in the field of cybersecurity awareness and education. Studies have consistently shown that individuals with formal training in cybersecurity are more capable of identifying and responding to security threats, which leads to reduced vulnerability to issues such as malware, unauthorized access, and data breaches [1, 6]. This survey similarly found that students educated in information security (IS) had a lower perceived probability of security risks like unauthorized access and virus infections compared to those without such education. This supports the broader trend observed in earlier research, where cybersecurity education has been linked to increased confidence in managing digital threats [6]. In addition to perceived risks, the actual reduction in security breaches among IS students further validates the connection between education and practical breach mitigation. However, despite these positive effects, certain challenges persist. For example, the unexpected finding that IS students reported a higher incidence of smartphone loss suggests that behavioral factors may play a role in physical device security. This outcome indicates that education alone may not fully address all aspects of security behavior, and that there may be other influences at play, such as habits or lifestyle factors, which affect the physical management of devices. This highlights the need for a more comprehensive approach that combines both technical knowledge and behavioral interventions to fully mitigate risks.

Perceived Probability

The second part of the survey reveals interesting insights into the perceived probability of various security risks. The survey responses were also divided into two groups: students educated in Information Security (IS) and those not educated in IS, focusing on three key

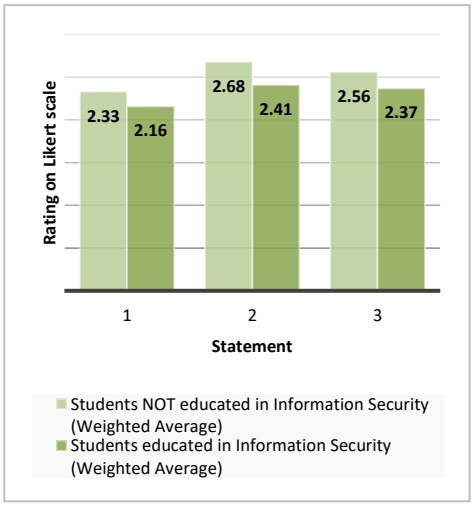
statements regarding unauthorized access, infection with viruses/spyware, and loss of smartphones and important data.

For the statement "It is possible for my smartphone to be accessed by unauthorized people", the general perception shows that a significant portion of respondents strongly disagree or disagree, with 40.68% and 18.88% respectively. The weighted averages indicate that students not educated in IS have a higher perceived probability (2.33) compared to those educated in IS (2.16), suggesting that education in information security might reduce concerns about unauthorized access.

Regarding the statement "It is possible that my smartphone is infected with viruses/spyware", the perception is more moderate, with responses distributed across neutral, agree, and strongly agree categories. The weighted averages again show a difference, with students not educated in IS at 2.68 and those educated in IS at 2.41, indicating that knowledge in information security reduces perceived vulnerability to malware.

For the statement "It is possible that my smartphone and important data will be lost", the responses are balanced across the spectrum, with a noticeable portion of respondents selecting neutral, agree, or strongly agree. The weighted averages are 2.56 for students not educated in IS and 2.37 for those educated in IS, suggesting a slightly lower concern among those with security knowledge.

Overall, the data indicates that education in information security generally lowers the perceived probability of security breaches among smartphone users. The consistent differences in weighted averages across all three statements suggest that increased awareness and knowledge in information security can positively influence individuals' confidence in managing smartphone security risks. To address these findings, enhancing information security education, implementing awareness campaigns, and developing targeted interventions for groups with higher perceived risks are recommended. (Figure 2)



No.	Statement
1	It is possible for my smartphone to be accessed by unauthorized people.
2	It is possible that my smartphone is infected with viruses/spyware.
3	It is possible that my smartphone and important data will be lost.

Figure 2. Perceived Probability (Bar Chart)

Perceived Severity

The second part of the survey also provides valuable information into the perceived severity of security incidents, with responses from both students educated in Information Security (IS) and those not educated in IS. For the statement, "If my smartphone was accessed by unauthorized people, it would be a serious problem for me", 60.86% of respondents strongly agreed, highlighting a substantial concern. The weighted averages were 4.25 for students not educated in IS and 4.23 for those educated in IS, indicating that education in information security slightly reduces the perceived severity but the concern remains high overall. In the case of the statement, "If my smartphone was infected by viruses/spyware, it would be a serious problem for me", 60.94% of respondents strongly agreed. Here, the weighted average was slightly higher for students educated in IS at 4.37 compared to 4.35 for those not educated in IS, suggesting that awareness of the risks associated with malware might be greater among those with security education, leading to a marginally higher perception of severity. The statement, "If I lose my smartphone or my important data on it, it would be a serious problem for me", had the highest perceived severity, with 70.68% of respondents strongly agreeing. The weighted averages were 4.5 for students not educated in IS and 4.46 for those educated in IS, indicating that while both groups view this scenario as highly severe, those without security education perceive it to be slightly more severe.

To sum up, the data demonstrates a high perceived severity of smartphone security breaches among users, irrespective of their education in information security. The slight differences in weighted averages suggest that while security education can slightly mitigate perceived severity, the overarching concern remains significant. These findings highlight the need for comprehensive measures to address smartphone security risks, including enhanced information security education, regular updates on best practices, and robust support for data backup and recovery. By fostering a proactive approach to smartphone security, organizations and educators can help users better manage and mitigate the risks associated with unauthorized access, malware infections, and data loss, eventually reducing the potential impact of these security breaches. (Figure 3)

No.	Statement
1	If my smartphone was accessed by unauthorized people, it would be a serious problem for me.
2	If my smartphone was infected by viruses/spyware, it would be a serious problem for me.
3	If I lose my smartphone or my important data on it, it would be a serious problem for me.

Figure 3. Perceived Severity (Bar Chart)

Breach Experience

The survey section on breach experience provides interesting data on various security incidents experienced by smartphone users, segmented by educational background in information security (IS). This analysis examines the results of four key questions, highlighting the impact of cybersecurity education on breach incidents.

The first question addressed whether users had experienced unauthorized access to their smartphones. Among students not educated in information security, 17.99% reported such incidents, whereas only 16.96% of IS students had experienced unauthorized access. This slight reduction among IS students suggests that cybersecurity education has a marginal but positive effect on preventing unauthorized access. This discrepancy might be due to IS students being more aware of and proactive in implementing security measures such as strong passwords, multi-factor authentication, and regular monitoring of their devices. While the difference is not vast, it underscores the importance of even basic cybersecurity awareness in reducing the likelihood of unauthorized access. (Figure 4)

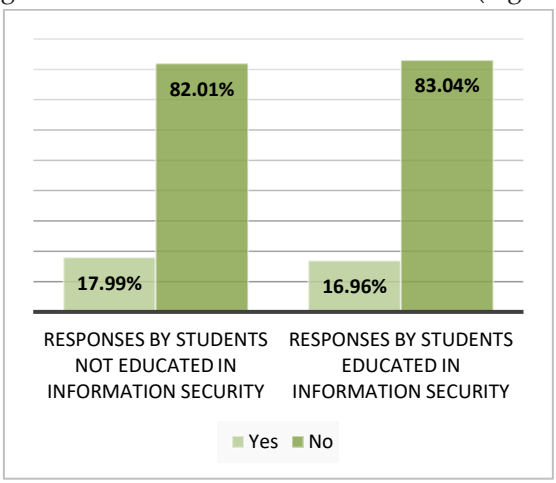


Figure 4. Responses of the question "Has your smartphone ever been accessed by unauthorized people (to your knowledge)?" (Bar Chart)

The second question investigated the incidence of smartphone loss. Here, 14.41% of non-IS students reported losing their smartphones, compared to a slightly higher 15.77% among IS students. This unexpected result could be due to various factors. IS students, often more engaged in tech activities and more mobile, might be at a higher risk of losing their devices despite their knowledge of security. This finding indicates that while cybersecurity education improves knowledge and practices related to data and software security, it might not significantly impact the physical security of devices. Therefore, it emphasizes the need for better personal management strategies and the utilization of technology such as tracking apps and secure backups to mitigate the risks of physical loss. (Figure 5)

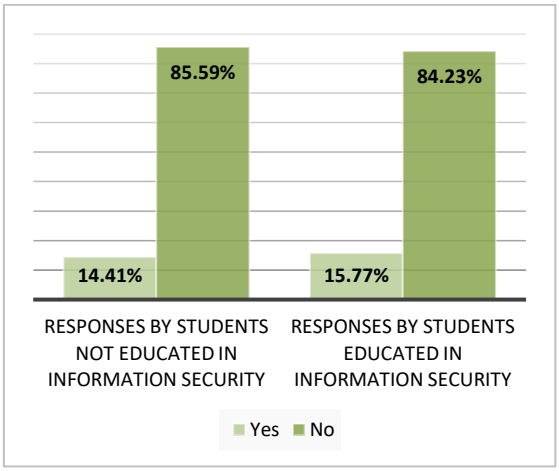


Figure 5. Responses of the question "Have you ever lost your smartphone?" (Bar Chart)

The third question explored the loss of important information or access to accounts on smartphones. A significant 38.63% of non-IS students reported losing data or access, compared to 35.42% of IS students. The lower rate among IS students suggests that their education helps reduce the likelihood of data loss. This can be attributed to better practices such as regular backups, secure storage methods, and vigilance against phishing attacks. However, the relatively high percentage of data loss incidents even among IS students indicates that there is still a substantial risk that needs to be addressed. It highlights the necessity for continuous education and improvement in data management practices, reinforcing the idea that cybersecurity education must evolve to keep pace with emerging threats and user behaviors. (Figure 6)

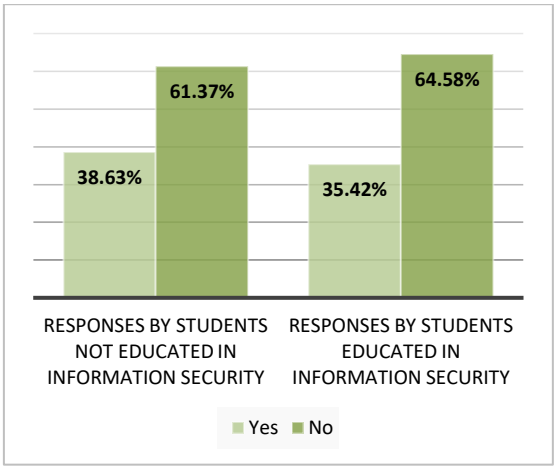


Figure 6. Responses of the question "Have you ever lost important information (documents, photos, videos, etc.) or access on different accounts (social networks, e-mail, etc.) on your smartphone (to your knowledge)?" (Bar Chart)

The fourth question focused on the prevalence of malware and spyware infections on smartphones. Among non-IS students, 23.29% had experienced such infections, while only 19.64% of IS students reported similar issues. The reduced incidence among IS students

underscores the effectiveness of cybersecurity education in mitigating the risk of such infections. IS students are likely more aware of the dangers posed by malicious software and thus more diligent in practices like installing antivirus programs, avoiding suspicious downloads, and keeping their operating systems up to date. This proactive approach significantly contributes to the lower infection rates observed in this group. (Figure 7)

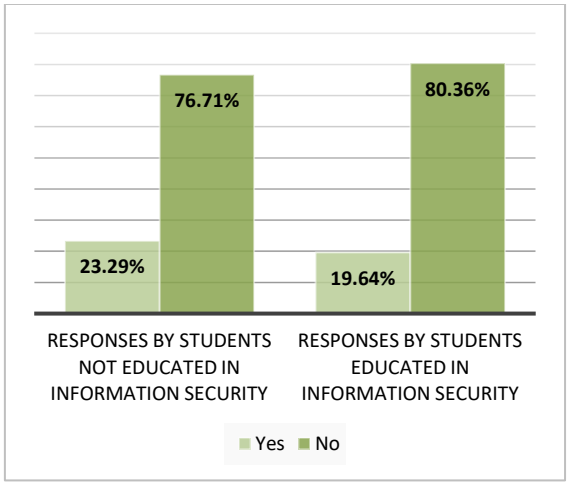


Figure 7. Responses of the question "Have you ever had a virus/spyware on your smartphone?" (Bar Chart)

CONCLUSION

The findings of this study align with prior research, which has consistently highlighted the importance of cybersecurity education in reducing security breaches. Studies, such as those by Anderson [1] and Sala [6] have shown that individuals with formal education in information security are better equipped to handle cybersecurity risks, reporting lower rates of unauthorized access, data loss, and malware infections. This study reinforces that cybersecurity awareness and behavior are strongly influenced by educational background and training [2]. The implications of these findings are significant: they suggest that cybersecurity education must be integrated across all academic disciplines, not just in specialized programs. While education clearly helps, the ongoing issues of smartphone loss and account breaches, even among IS students, indicate that education alone is insufficient. This gap points to the need for more practical training and a focus on physical security measures alongside theoretical learning. Future research can extend this work by focusing on hands-on cybersecurity training programs that provide more practical, real-world applications. Additionally, expanding the scope to include broader demographic groups, such as professionals or users in different sectors, can help build a more comprehensive understanding of cybersecurity awareness across various populations. Future studies could also explore how educational methods and materials can be updated more frequently to address the evolving nature of cybersecurity threats. Finally, assessing the impact of specific cybersecurity interventions could help refine and enhance current education strategies to better equip users for modern digital threats. In conclusion, the breach experience survey provides clear evidence that cybersecurity education positively

impacts smartphone security. By expanding and enhancing such educational programs, we can better prepare individuals to safeguard their devices and data. This proactive approach to cybersecurity not only equips individuals with the tools to protect their personal information but also fosters a more secure digital environment overall. As threats continue to evolve, so must our educational strategies, ensuring that all users are prepared to face and mitigate potential risks effectively. This ongoing commitment to cybersecurity education will play an important role in reducing the prevalence of security breaches and enhancing the overall security posture of smartphone users.

CONFLICT OF INTERESTS

There are no conflicts of interest associated with this publication.

REFERENCES

1. Anderson JR. **2014**. Cognitive psychology and its implications. *Macmillan*.
2. Fishbein M., A*jzen I. **2010**. Predicting and changing behavior: The reasoned action approach. Psychology Press*.
3. Gartner. **2021**. Forecast: Information Security and Risk Management, Worldwide, 2021. *Gartner, Inc*.
4. Kim Y., Peterson R. A. **2017**. A meta-analysis of online trust relationships in e-commerce. *Journal of Interactive Marketing*, 38, pp. 44-54.
5. Rook D. W., Fisher R. J. **1995**. Normative influences on impulsive buying behavior. *Journal of Consumer Research*, 22(3), pp. 305-313.
6. Sala E. **2024**. Descriptive Analysis of Cybersecurity Awareness Among Smartphone Users in Higher Education. *Journal of Transactions in Systems Engineering (JTSE)*. 2: pp. 222-234.
7. Sala E, Martiri E. **2023**. ADR Project Planning to increase Cyber Security Awareness of Mobile Device Users. *International Journal on Technical and Physical Problems of Engineering (IJTPE)*. Sep;15: pp. 327-333.
8. Sala E, Martiri E. **2023**. Assessing Cybersecurity Awareness Among Smartphone Users: Designing a Comprehensive Survey. *Proceedings of the 2nd International Conference Creativity and Innovation in Digital Economy*. pp. 46-52.
9. Slovic P. **2000**. The perception of risk. *Earthscan*.
10. Taylor S, Todd PA. 1995. Understanding information technology usage: A test of competing models. *Information Systems Research*. 6(2): pp. 144-176.