A Case Study on University Students for Cyber Security Awareness

*Dr. Ravi Bala Goyal
**Geetansh Goyal

Abstract

This article presents the first findings of a quantitative study aimed at determining students' knowledge of and interest in cybersecurity education at Indian universities. The survey's goals were to determine how students in this developing nation are aware of cyberattacks, how they can protect themselves from them, and if universities have cybersecurity awareness programmes. The first findings showed that while the students claimed to have a rudimentary understanding of cybersecurity, they were not well-versed in data protection strategies. Additionally, it seems that few universities actively promote cybersecurity awareness to help students become more knowledgeable about how to defend themselves from dangers. The students who responded to the poll indicate a desire to learn more about cybersecurity.

Keywords: Password management, Two-factor authentication, and cybersecurity awareness

Introduction

The Globalisation opens up limitless opportunities for business, social interaction, and other human endeavours, but it is also more vulnerable to cybercrime as the quantity, expense, and complexity of assaults are rising at an alarming pace across the board. Digital India will not be an exception to the global risks and difficulties that cyber security and crime pose. This research was conducted to determine the level of cyber security knowledge among Delhi college students.

Being a nation of cities and villages, India has a high rate of digital illiteracy. Cities and metropolises have embraced digitization, but only to a certain level. Complete digitalization, which would include everyday cashless transactions and the use of online services to get official documents, would call for significant administrative, taxation, and cultural changes. As a result of its diversity, each state in India has separate laws and internet protocols, making it difficult to connect to every hamlet, town, and metropolis. Software compatibility is a critical problem due to the diversification of languages and religions. The practise of protecting cyberspace from both known and unknown hazards is known as cyber security.

Review of Literature

An overview of recent research on cyber security awareness and relevant to this study is presented in the parts that follow. According to the International Telecommunication Union, "cyber security" is the integrated use of strategies, security measures, plans, threats administration tactics, engagements, training, paramount practises, assurance, and expertise that can be used to protect the information system, organisation, and related assets. Information and communication technology (ICT) is used maliciously by numerous bad actors, either as a target or as a means, in cyberattacks. It also refers to protecting electronic systems, computer networks, and other devices against cyberattacks (Olayemi, 2014). Business operations have been greatly impacted by cyber security. The extent of an organization's dependence on the internet has grown in the contemporary information era (Strassmann, 2009). Due to the disclosure of sensitive data and information, data and information hacking has a detrimental impact on an organization's ability to compete (Tarimo, 2006). The confidentiality, integrity, and availability of an organisation are compromised by a successful assault on an ICT system and its data (Bulgurcu et al., 2010). Cyber theft (cyber espionage) may expose financial, sensitive, or proprietary information, allowing the invader to profit while costing the legitimate organisation money or patent information.

In the setting of a developing nation, particularly the UAE, Rezgui, Y., & Marks, A. (2008) investigate variables that influence staff members' understanding of information security, especially information systems decision makers, in higher education.An interpretative case-study methodology is used, and several data collection techniques are used. The study finds that characteristics including conscientiousness, cultural presumptions and beliefs, and social circumstances have an impact on university staff members' conduct and attitude towards work in general, and information security awareness in particular. A number of suggestions are made in order to start and foster IS security awareness in the research setting.

Security personnel always face the problem of rising cyber-security. It also looks at the kind of information that individuals choose to post online and how culture influences these decisions. This research supports the notion of creating personality-based UI designs to improve users' online safety.

Methodology

Results and Findings

The link to the survey was issued, and it will take respondents one month to reply before the connection is deactivated. 408 students in all completed the questionnaires, and a filtering process was done to determine whether any questions were left unanswered or blank. Due to not answering any of the provided questions, a total of 41 people were found and eliminated from the results. A total of 367 samples have been determined to be legitimate, and we will use these samples for our study.

Demography

Demographic information was gathered for the completed survey, including age and gender. Out of 367 respondents, 50 students are between the ages of 18 and 20; 200 students are between the ages of 21 and 25; and 117 respondents are between the ages of 26 and 30. Of the respondents, 308 are men; 53 are females; and 4 said they would rather not tell. According to this data, the majority of respondents are men between the ages of 21 and 25.

Basic Knowledge of Cybersecurity

To ascertain the general understanding of cybersecurity, the question "Do you consider yourself knowledgeable about the concept of cybersecurity" was posed.

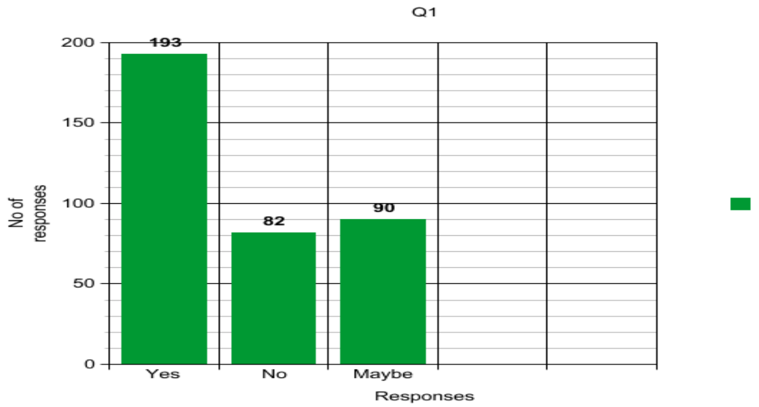

Figure 1: Cyber security Response

Figure 1 displays the responses to Question 1; according to this graph, there are 193 students who have fundamental understanding, 82 who responded "No," and 90 who are unsure and indicated "Maybe." This demonstrates that although the majority of students have a fundamental understanding of what cybersecurity is, half of them are unsure. However, when the percentages of no and maybe are added together, they reach 172, which is over half of the total. This demonstrates the need of introducing pupils to the idea of cybersecurity. Do you understand and use two-factor authentication (2FA)? Out of 367 people surveyed, 162 stated they were familiar with two-factor authentication, while 29 said they were unsure. This statistic demonstrates that even among the majority, the majority of students are not acquainted with this method. This calls into question the need to elevate one's degree of awareness about cybersecurity. Do you open emails from senders you are not acquainted with? Out of 367 respondents, 219 responded "yes" when asked to open an unknown email, 110 said "no," and 36 responded "maybe." This finding suggests that most students are unaware of phishing scams. Information about students is at risk, as are institutions. Before any catastrophe happens, there has to be an immediate awareness to dispel this mistrust. Q4: Your credentials information, such as your name, date of birth, age, and credit card number, may be requested in an email. Does it get sent? Below is a representation of the outcomes.

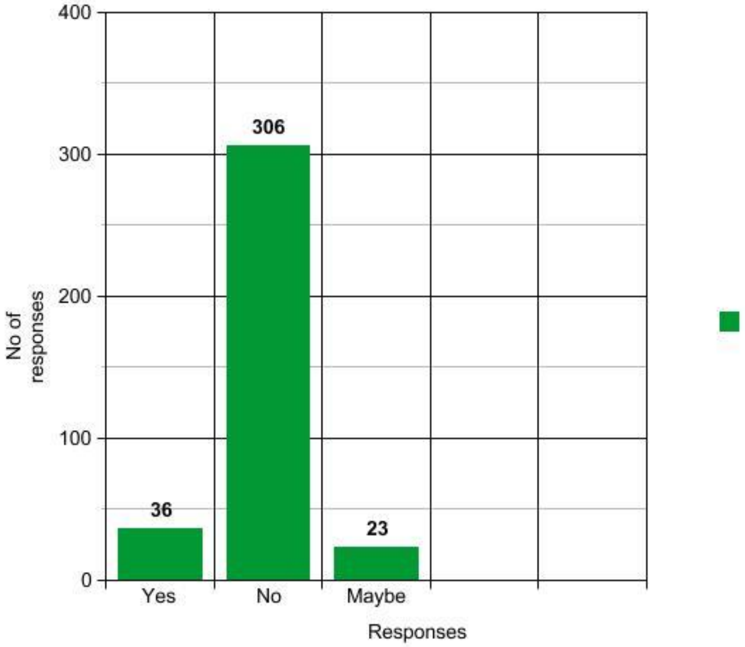

Figure 2: Reaction to Transmitting Credit Card Data

Figure 2 demonstrates that almost all students are aware of the 419 tactics, and 306 out of 367 respondents indicated they would not provide their names, dates of birth, or credit card information to an unknown recipient.

This demonstrates that kids are more aware of important problems, particularly those that involve money. Do you ever refuse an app's permission? Out of 367 respondents, 210 students said that they deny app permission, 126 indicated that they do not, and 29 indicated that they may do so, demonstrating the students' cybersecurity expertise. These findings show that the majority of users do not consent to apps accessing their location or contact information. This demonstrates that kids are aware of the risk. Do you understand the difference between HTTP and HTTPS? According to the findings, 197 people answered "yes," 155 said "no," and 13 stated they were unsure. The majority of respondents grasped the distinction, but the analysis of the results reveals that 170 do not. This suggests that knowledge is required to explain the differences.

Privacy

What makes you feel safe while using a computer and the Internet, was the question posed. Figure 3 displays the outcomes.

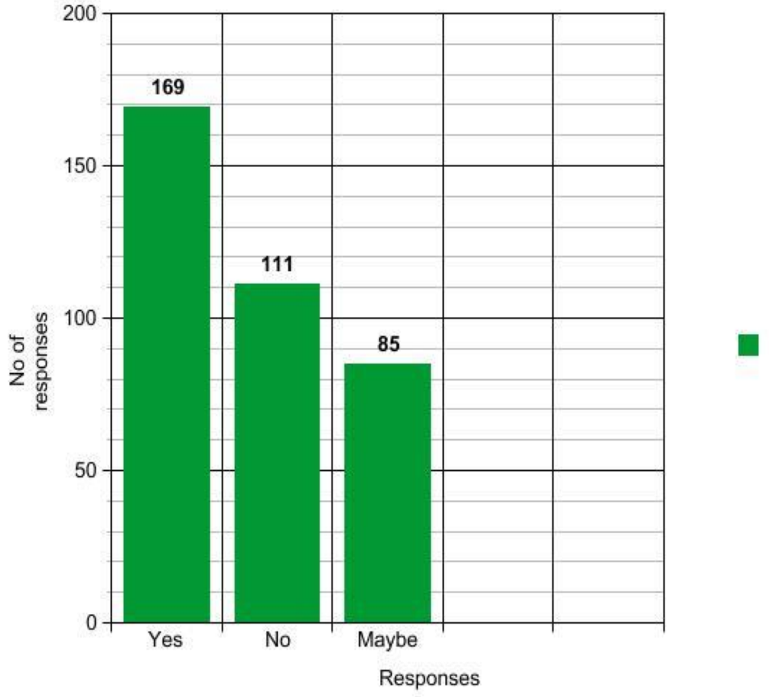

Figure 3: Privacy Response

Figure 3 displays the responses to the privacy question mentioned above. Out of 367 respondents, 169 replied "yes," 111 said "no," and 85 said "maybe." If the entire number of No and Maybe responses are added, 199 people are unsure about their security. This demonstrates that children feel uncomfortable accessing the internet, which highlights the necessity to teach them how to do so safely. Question 2: Have you ever declined a request from a mobile app to access your contacts, camera, or location?

The outcome reveals that 195 students agreed to provide the app access to their contacts, cameras, and locations, 153 students disagreed, and 17 students suggested they may. The majority of students responded in the affirmative, but the findings reveal that over half did not, which indicates that they lack even the most fundamental understanding of privacy.

Trust

Do you have cause to suspect that someone is watching you online without your knowledge? was the question posed. To learn more, see Figure 4.

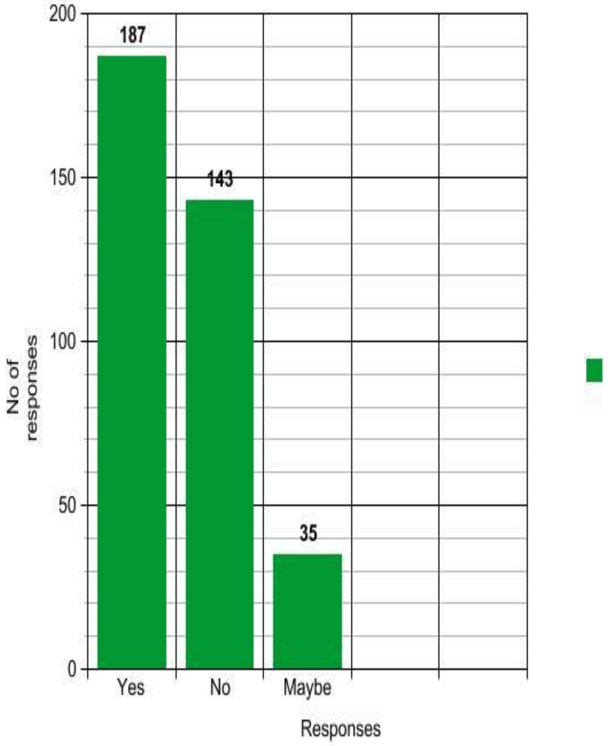

Fig. 4 Reaction to on Trust

Figure 4 demonstrates that kids are trustworthy while using the internet; 187 responded "Ok," 143 "No," and 35 "Mighty." The majority of people did not trust the internet, as seen by this statistic, which is close to 50%. This demonstrates that not all pupils relied on the internet. Do you believe your data is safe on the university system, we questioned in a second. Out of 367 students, 198 answered they felt their data was safe, 103 said no, and 64 said maybe, according to the statistics. According to the findings, the majority of its programmes think their data is safe, but altogether, more shows feel this way than the majority, with 207 showing that they do not. This makes the ICT staff aware that a workshop is needed to inform students on how their data is kept in the university systems.

Cybersecurity Awareness Program as a Course

Knowing whether students are eager to attend a cybersecurity course when it is included into a curriculum is one of the research's goals.

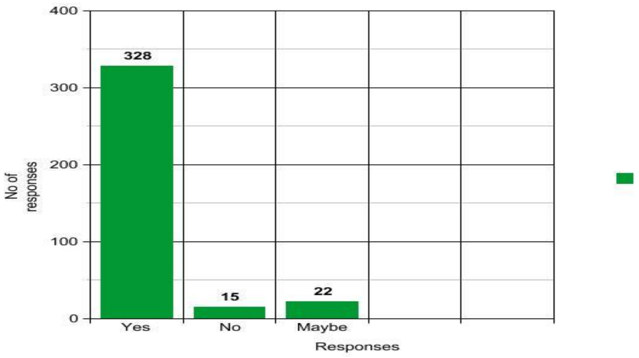

Figure 6: Reaction to the University of California's inclusion of a course on cybersecurity

Figure 5 reveals an astounding finding about students' willingness to enrol in a cybersecurity course in their curriculum, and the outcome reveals a strong consensus. A total of 328 out of 367 respondents said that they did, demonstrating the absence of a cybersecurity course at colleges and raising management's understanding. You were also asked if you thought it was crucial for academic institutions to have an information security officer. There are now no security officials at the institutions, as shown by the fact that 325 out of 367 students agreed with that conclusion.

Conclusion

The results of the poll indicate that university students don't have a basic grasp of cybersecurity. This is accurate despite the fact that 193 students selected "yes" in response to the survey's first question, 82 selected "no," and 90 selected "unsure." The survey's second question, however, demonstrated a lack of cybersecurity understanding. When asked if they opened emails from strangers, 219 out of 367 respondents said "yes," while 110 said "no" and 36 said they may. Analysis of the responses to the question concerning password management reveals that 204 respondents chose "No," 139 chose "Yes," and 22 chose "Maybe." This result indicates that the majority of students are not aware of phishing schemes. The results show that none of the universities seem to offer cybersecurity programmes, and 346 out of 367 respondents indicated a strong desire in learning more about cybersecurity. Furthermore, 328 of the 367 respondents believe that cybersecurity training should be a requirement for admission to their university. The findings show that, while being aware of the risks involved with disclosing credit card information or making purchases online, 276 out of 367 students do not comprehend what phishing is. According to the study, 346 of the 367 students who participated expressed a desire to learn more about cybersecurity, and 328 said they would be open to taking a cybersecurity course at university. This indicates that students are seeking such cybersecurity awareness courses. The survey's findings ultimately demonstrate that there is no cybersecurity awareness programme offered in Indian tertiary institutions, as well as a lack of fundamental cybersecurity skills like password management and a demand from students for such a programme.

***Department of Zoology**
Government P.G. College
Gangapurcity (Raj.)
****Student MCA**

References

1. A McDaniel, E. (2013). Securing the Information and Communications Technology Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness. Issues in Informing Science and Information Technology, 10(2012), 313–324. https://doi.org/10.28945/1813
2. Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. Journal of Information and Knowledge Management, 15(1). https://doi.org/10.1142/S0219649216500076
3. Aloul, F. A. (2012). The Need for Effective Information Security Awareness. Journal of Advances in Information Technology, 3(3). https://doi.org/10.4304/jait.3.3.176-183
4. Chan, H. (2012). Significance of Information Security Awareness in the Higher Education Sector. 60(10), 23–31.
5. Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. Computers and Security, 26(1), 63–72. https://doi.org/10.1016/j.cose.2006.10.005
6. Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security. Proceedings of the 2005 Information Security Curriculum Development Conference, InfoSecCD '05, 43–48. https://doi.org/10.1145/1107622.1107633
7. Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Management and Computer Security, 22(1), 115–126. https://doi.org/10.1108/IMCS-01-2013-0005
8. Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. Information Management and Computer Security, 14(1), 24–36. https://doi.org/10.1108/09685220610648355