TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Ankit Rana 214161IVCM

Assessment of Cyber Security Awareness Among Delhi Students

Master's Thesis

Supervisor: Kaie Maennel

Tallinn 2023

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Ankit Rana 214161IVCM

Delhi üliõpilaste küberturvalisuse teadlikkuse hindamine

Magistritöö

Juhendaja: Kaie Maennel

Tallinn 2023

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the materials used, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Ankit Rana

Abstract

The internet and the technologies that are associated with it are constantly changing. It is estimated that India will have an estimated 900 million internet users by 2025 [1]. According to a survey conducted between November and December 2022, internet users in India were the most likely to have been victims of cybercrime, with nearly 70% of respondents claiming to have ever been victims of cybercrime [2]. At this point, awareness in cybersecurity plays a vital role in defending against cyber-attacks. The goal of this study is to first assess the cybersecurity awareness levels of Delhi university students to determine where they fall short. Another goal of this study is to develop cybersecurity training course using Successive Approximation Model (SAM) [3] and run a pilot training to improve cybersecurity awareness levels of the students and finally check whether there has been any improvement through a post-training questionnaire. The results of the questionnaire are compared with a similar study conducted in Malaysia [4].

It is observed from pre-training questionnaire responses that although Delhi students are more aware than Malaysian students, they are having moderate or average level of cybersecurity awareness. Based on the results, a short cybersecurity training is developed as a pilot test which uses SAM [3] as instructional design. Finally, students are assessed after training, and the results of pre-training and post-training questionnaire are compared.

The comparison between results of pre-training and post-training questionnaire shows there is significant improvement in cybersecurity awareness of Delhi students after training showing SAM as instructional design is effective in creating short cybersecurity awareness trainings.

This thesis is written in the English language, and is 86 pages long, including 9 chapters, 46 figures and 13 tables.

List of abbreviations and terms

SAM	Successive Approximation Model
NCRB	National Crime Records Bureau
RQ	Research Question
NCR	National Capital Region
IT	Information Technology
ADDIE	Analyze Design Development Implementation Evaluation
CSV	Comma-Separated Value
MQ	Malware Question
PQ	Password Question
PHQ	Phishing Question
SQ	Social Engineering Question
UQ	User Behavior Question
2FA	2 Factor Authentication
SETA	Security Education Training and Awareness
PT	Post-Training Question
GIF	Graphics Interchange Format

Table of contents

List of Figures

List of tables

1 Introduction

The internet and the technologies that are associated with it are constantly changing. India currently has 692 million internet users, and their reliance on the internet is steadily increasing, with an estimated 900 million internet users by 2025 [1]. Constant connectivity increases the risks. Cyber-attacks on critical infrastructure and the economy are a threat to all. Individually, cyber security risks can put one's finances, identity, and privacy at risk. The personal information that is transferred and stored, resulting in people's growing reliance on digital devices and applications that control our everyday lives, has made cybersecurity awareness increasingly relevant and vital. This digital age offers numerous conveniences but introduces new challenges and threats that sometimes remain unseen or unrecognized to the untrained eye, increasing the importance of education and training in this field. As Delhi is India's capital, this thesis will investigate the level of cybersecurity awareness among Delhi students, which will aid in designing and implementing a short cybersecurity awareness training which will attempt to create an impact on the levels of cybersecurity awareness among Delhi students.

1.1 Problem Statement

According to Google's VP-Engineering for Privacy, Safety, and Security, India experienced 18 million cyber-attacks and 200,000 threats per day in the first quarter of 2022 [5]. According to the National Crime Records Bureau's (NCRB) most recent report, in 2021, cybercrimes in Delhi increased by 111% from 2020 [6]. This exhibits that cybersecurity incidents have become a source of concern with increased access to the internet and the web. Most incidents in India have targeted a specific range of ages, including the youth. Humans are frequently called "the first line of defense" against various information security threats [7]. Prior studies have shown that managing the risks associated with information security breaches depends on employee information security awareness [8], [9]. The current generation of students will work in various organizations. Therefore, we must ensure that students are educated about cyber security awareness early to protect themselves and the organization where they will work. To do that, we must first understand students' cybersecurity awareness levels, which will help design effective training.

1.2 Research Questions

RQ1: What is an appropriate methodology to measure cybersecurity awareness levels?

a) Are there any studies done before in Delhi or India which assess the cybersecurity levels?

RQ2: Are different cybersecurity awareness measurement methods and study results comparable?

a) How much cybersecurity awareness do Delhi university students possess compared to Malaysian students [4]?
b) What critical aspects must we consider when analyzing and comparing awareness studies?
c) What are the critical aspects to consider when designing the new awareness measurement instruments to ensure keeping up to date with technology and cybersecurity advancements?

RQ3: When designing a short awareness training for students, what methodology is appropriate and

a) Can the Successive Approximation Model instructional design method be appropriate for developing short but effective cybersecurity learning for students in changing environments and learning needs?
b) How does implementing short training sessions developed using SAM methodology impact the students' cybersecurity awareness?

1.3 Scope and Goal

The first goal of this study is to determine an appropriate methodology that can be used to assess the current state of cybersecurity awareness levels and to check if there have been any studies done before in Delhi or India or Worldwide which assess the cybersecurity levels.

Second goal is to assess the current state of cybersecurity awareness levels among university students in Delhi. Research has been done in different Indian states to assess students' cyber security awareness levels [10]–[16], including Delhi. Still, the results are all different where [11]–[13] showed students having an awareness of cybersecurity, whereas [10], [14]–[16] showed the opposite, showing students had a low level of cybersecurity awareness. This could be influenced because of the demographics and cultures of that region. India has a population of 1.41 billion [1] with diverse cultures in various parts. Delhi offers a population of 16 million, according to the 2011 census. This population comes from different parts of India, including migrants from adjacent states like Uttar Pradesh and Haryana and states like Uttarakhand, Rajasthan, Bihar, Punjab, and many more [17]. The assumption is that this may result in different mindsets and perspectives on cybersecurity hygiene and awareness, particularly among students.

Third goal is to check if different cybersecurity awareness measurement methods and study results are comparable and which critical aspects must be considered when analyzing and comparing awareness studies. This can be done by comparing the cybersecurity awareness levels reported in this study by Delhi students with that of Malaysian students. This is because the current study employs a questionnaire similar to that used in Muniandy et al.'s study [4]. So, this will help in checking what aspects of cybersecurity Delhi and Malaysian students share or lack awareness of.

The fourth goal is to check what methodology is appropriate when designing a short awareness training for students and if Successive Approximation Model (SAM) [3] can be appropriate methodology for designing short cybersecurity awareness training. This can be achieved by creating a short cybersecurity awareness training using SAM as a pilot test.

The final goal is to check if the SAM oriented short cybersecurity training can impact students' cybersecurity awareness. This can be achieved by evaluating the students after the training and check whether there is any improvement in cybersecurity awareness of students. If there is any improvement, the training can be further improved in the future, and the universities can be approached about including some subjects of cyber security awareness, either mandatory or elective, in their curriculum so that knowledge about cyber security awareness can be effectively increased from the ground level and to design a full-fledged cyber hygiene training

The study included students from three universities in Delhi, namely Jamia Hamdard University, Delhi Skill and Entrepreneurship University, and Al-Falah University, and also students from non-IT backgrounds to avoid influencing the results. However, many students shared the questionnaire with peers from different universities, thus resulting in snowball sampling. Snowball sampling is a non-probability sampling method in which new units are recruited to form part of the sample by existing units [18].

1.4 Limitations

Limitations of the study include a smaller raw dataset, which could occur if the questionnaire fails to reach the participant or the participant does not attempt either a pre-training or post-training questionnaire or both. Similarly, due to time constraints, only 27 responses were recorded in the post-training questionnaire, so comparing responses between the pre-training and post-training questionnaires may not provide the utmost accuracy.

While there is a versatility factor in demographics in Delhi, the results of the questionnaire analysis may not show conclusions aligned with the actual scenario within India or any other part of India in terms of the existing population.

Another limitation is response bias because respondents may randomly click on the best available option to demonstrate their knowledge, which can affect the results [19], [20].

A comparison with Muniandy et al. study [4] may not be accurate with today's standards because the study by Muniandy et al. [4] was conducted in 2017, and there might be an improvement in the cybersecurity awareness levels of Malaysian students by now. Additionally, accuracy may be impacted because the Muniandy et al. study [4] used a 3-point Likert Scale in the questionnaire, whereas the current study uses a 5-point Likert Scale.

1.5 Contributions by Author

One of the author's contributions to this thesis is the development of a questionnaire to assess cybersecurity awareness levels among Delhi students. This questionnaire will assist in determining which areas of cybersecurity the students are unaware of, and the results will aid in the development of appropriate training.

The second contribution is the modification, improvement, and adaptation of an existing questionnaire [4] to be compatible with the demographics of Delhi. In addition, some new questions were added, covering topics like user permissions and user behavior, as these were originally not present in the Muniandy et al. questionnaire [4].

The third contribution from the author is the reperformance of similar questions from the Muniandy et al. questionnaire [4] on a different population, along with newly added questions.

The fourth contribution is the development of SAM oriented experimental short training through online videos to educate students on basic cybersecurity awareness topics and the development of a post-training questionnaire to assess and report any changes in cybersecurity awareness levels. All of the pre-existing studies reported their findings on cybersecurity awareness and made general recommendations, but none attempted to improve it.

Another contribution made by the author is the provision of cybersecurity training in two languages: English and Hindi. This will aid in determining whether or not students prefer to take the course in their native language.

The author's final contribution is to keep the training materials available to the public with Iterative Design and Development phase in mind, which can aid in expanding the current experimental short training if used as a foundation.

In conclusion, the contributions above demonstrate the work's novelty and importance in the academic field. Furthermore, the research provides insight into university students' cybersecurity awareness, which can be used as motivation for introducing cybersecurity subjects or full-fledged training or workshops at the university level.

2 Related Work

Cybersecurity awareness has recently become very important due to increased cyber-attacks and threats, which has resulted in significant research on cybersecurity awareness.

This chapter aims to comprehensively understand the existing cybersecurity awareness literature and identify the gaps this thesis will address. In this chapter, we first explore pre-existing studies on cybersecurity awareness in different regions within India, then move towards the Indian subcontinent and Worldwide, and then look into different instructional designs to develop the cybersecurity training materials.

2.1 Research from India

Sadashivam [21] attempts to research and analyze cybercrime in India from 2014 to 2018. According to reports, in the preceding bracket of years, two Indian states, Uttar Pradesh and Jharkhand, reported increases in cybercrime cases above the national average, with 2017 being the year with the most significant rise in cybercrime cases, 9479 cases, which was true for almost all states and union territories. The article also acknowledges existing government initiatives in India to combat cybercrime. However, the paper needs more information on cybercrime in India after 2018. According to the National Crime Record Bureau India, cybercrime increased significantly in 2019 and 2020, with 44735 and 50035 cybercrimes, respectively [22]. The study concluded that cybercrime is growing in all countries, including India. The major challenge here is the dynamic nature of cybercrime, which arises from the ongoing evolution of digital technology. As a result, new strategies and approaches for cybercrime are being created. However, as the most significant stakeholder in our society, the government is taking numerous initiatives to combat cybercrime. The study also demands that cybercrime be given the same priority as other crimes, such as theft and homicide.

Rajan and Babu [23] shed light upon the youth’s current knowledge, personality traits, practice, and attitude in cyber worlds and suggest that the youth must use cyberspaces effectively.

In India, studies on cyber security awareness of employees and students from various states and regions have been conducted, with varying results on cyber security awareness.

Senthilkumar and Easwaramoorthy [11] examined the cybersecurity awareness and level of understanding about security issues among 500 Tamil Nadu college students and proposed some solutions. The survey questions in this study were designed to include a wide range of cybersecurity subjects such as viruses, email, phishing, and popups, as well as a mix of multiple choice, matrix, and demographic questions. The study showed that 69.45% of students in Tamil Nadu are aware of cyber security issues, including 38.6% of men and 30.85% of females, indicating that students have more knowledge than average regarding cyber security, which can help them defend themselves against cyberattacks.

Garg et al. [12] used an online survey to learn about the level of knowledge of cybercrime among 150 technical and non-technical students at Parul University in Vadodara. The data were tabulated and analyzed using the SPSS software (Statistical Package for Social Sciences). According to the findings, the most common cybercrime among students is hacking (17.3%), followed by cyberbullying (13.3%). As a protective step against cybercrime, the majority of students use strong passwords. In addition, anti-virus software is installed on 83.3% of the pupils' computers. As a result of the statistics, we may conclude that many students in Vadodara are aware of cybercrime.

Rathod and Potdar [13] conducted a similar study at D. Y. Patil Medical College in Maharashtra, India, to examine 200 medical students' cyber security awareness and recommend how to address these issues. The study concluded that most students spent nearly 3-4 hours online and used online transactions every month. Still, only the majority were aware of using a secure website based on the responses. Furthermore, roughly half of the students were mindful of societal cybercrime. Approximately 60% of those polled used antivirus software. Most students rarely changed passwords, and 8% admitted to sharing them. The analysis's strength is that it considers non-IT students, as cyber security awareness, differs. The disadvantage is that it is only conducted at one medical school, and the results may vary when multiple colleges are evaluated. In addition, this study's questionnaire does not account for other types of cybercrime, such as phishing, web advertising, etc.

The following studies' assessments produced contrasting results.

Chhibber and Thapar [14] used a questionnaire with 14 questions to collect data on cybersecurity awareness among 60 college students in Delhi. This study concluded that internet users in Delhi must be fully aware of cybercrime, cyber security issues are rising, and cities like Delhi are becoming more reliant on the internet. However, the questionnaire focuses on the user's cybercrime experience and knowledge of cyber security rather than the cyber security behaviors they include, which is the study's main limitation. This defeats the purpose of assessing cyber security awareness by instead assessing cybercrime experience.

Another study in the Delhi/NCR region was conducted by Mokha [15] by analyzing cyber-crime awareness among internet users, as opposed to Chhibber and Thapar [14], with different age groups and educational qualifications using a questionnaire survey with 160 respondents. Similar findings were found in this study, where people were only aware of hacking and viruses, but not phishing identity theft, and other issues. According to the survey, 48% of respondents share personal information with people they do not know, and 55% have their PCs frequently destroyed by viruses. However, one issue with this study is that it needs to specify its demographics or whether the respondents have an IT background, which could change the overall conclusions.

Shah [16] conducted a similar study in a Gujarat region to determine the levels of cybercrime awareness among 100 young internet users and to build a framework to sustain cybercrime and cyber security awareness programs among internet users. Despite the region's apparent increase in net addiction, the research found that internet users need to be better versed in cybercrime and cyber security. In addition, this study proposes a conceptual framework for maintaining and implementing cybercrime awareness programs among internet users.

Sreehari A et al. [10] researched cybercrime awareness among 200 college students in Kochi using a questionnaire survey to assess college students' understanding of different types of cybercrime and government schemes. According to the findings, most users are only marginally familiar with cybercrime, with a high ratio of awareness for hacking when compared to other types of cyber threats. However, it also revealed that most of those who responded were unaware of cyber laws.

One significant research gap for most of these studies is that they only show awareness from a single Indian state, and cultural factors may influence the results. Because India is such a vast and diverse country, perspectives and approaches to increasing cyber security awareness may vary. In addition, according to a study conducted in India by Mehta and Singh [24], male internet users are more knowledgeable about cyber regulations than female users, and employed users are more knowledgeable about Indian cyber laws than non-employees, demonstrating gender and institutional differences.

Chitrey et al. [25] showed the presence of Social Engineering in India and exhibited an analytical approach to Social Engineering. A proposed model of Social Engineering-based Attacks was developed based on the questionnaire responses. Humans, Organizational Security Policy, Technology, and Government Laws were identified as vulnerable entities in this model. As safeguards against social engineering attacks, the model recognizes information security awareness and training programs, organizational security policy, physical security, access control, technological control, and secure application development. Three different sorts of social engineering attacks are the subject of the study. First, it starts by developing a conceptual model based on the data to put the modeling of social engineering attacks into practice. Second, it enables the evaluation of the consequences of Social Engineering Attacks on businesses and individuals. Third, it presents a multidimensional approach to developing a security plan that employs defense-in-depth techniques to mitigate Social Engineering attacks. The survey participants were exclusively IT professionals. Hence this study does not represent the non-IT perspective on social engineering.

Shah and Agarwal [26] discovered 28 cybersecurity behaviors and practices after an empirical study of 300 smartphone users' cybersecurity behavior in India. According to the survey, smartphone users only sometimes act responsibly regarding cyber security. Some use standard security features such as screen locks but must be aware of more sophisticated security measures such as remote wiping and encryption. Language, gender, age, and operating system significantly impacted cybersecurity behavior and practices. Respondents generally strongly desired to protect their devices but demonstrated only moderate danger awareness. However, the overall sample size could be more significant than the number of smartphone users in India, limiting generalizability.

2.2 Research Worldwide

Bada et al. [27] concentrate on cybersecurity awareness campaigns and highlight crucial security variables that may fail to change people's behavior in a correct manner. From a psychological perspective, the study focuses on understanding failure since researchers believe that understanding individuals' risk perception is vital to developing effective awareness efforts.

Studies have been conducted outside of India to assess Cyber Security Awareness, with contrasting results on cybersecurity awareness with one.

Nagahawatta et al. [28] surveyed 121 Sri Lankan university students to assess their level of cybersecurity awareness. The findings of this study indicated that, while Sri Lankan students' experience and cybersecurity awareness are relatively good, there are some gaps in knowledge regarding current risks. The findings also revealed that the students could identify cybercrime as a threat. This may be consistent with the results of Senthilkumar and Easwaramoorthy [11] because Tamil Nadu and Sri Lanka have nearly identical cultural demographics.

Ahmed et al. [29] conducted a similar study to assess the level of cybercrime awareness among Bangladeshis comprehensively. According to the survey, Bangladeshis' cybersecurity awareness is at an all-time low, and immediate action is required. It also implies that people with prior knowledge of cybersecurity vulnerabilities can find ways to defend themselves. In addition, the study suggests strategies for implementing cybersecurity education in schools and institutions.

Khan et al. [30] investigated Pakistani undergraduates' cyber security and risky Internet behaviors. The findings revealed significant gender, age, and digital divide disparities in cybersecurity posture. The student profiles show three groups based on risky Internet behaviors and cyber-security, with the majority falling into the low cyber-security but risk-averse category. Furthermore, proactive cyber-security awareness affects risk-averse behavior. However, the results of the study need to be more generalizable. Because the study was conducted within a single country, cultural influences may have influenced it.

Muniandy et al. [4] investigated participants' online activities on social networking websites and then evaluated their cybersecurity activity to determine Malaysian university students' current state of cybersecurity behavior. Based on the questionnaire results, the researchers concluded that participants needed better practices to protect themselves from security threats. However, a similar study conducted in Tamil Nadu and Sri Lanka discovered an above-average level of awareness, which could be attributed to the different cultures and practices people use to protect themselves from cyber-attacks.

Alharbi and Tassaddiq [31] examined and evaluated the cybersecurity awareness levels of 576 Majmaah University students and reviewed their cybersecurity compliance using a scientific questionnaire based on various Internet safety elements. The survey has 50 specific questions that gave people without IT expertise extensive explanations and definitions of some cybersecurity technical jargon. The survey found that Majmaah University students knew about phishing, encryption, security tools, social networking, browser safety, and other related information. However, various factors may influence the outcome. For instance, answers from students between 18 and 25 were included in the sample, showing that the younger generation is becoming more aware of cyber threats and associated issues. Additionally, men comprised more than 60% of the responders, and males are more knowledgeable of cyber security risks than females, according to Alotaibi et al. [31]. A similar conclusion was made by Mehta and Singh [24], showing that male internet users are more knowledgeable about cyber laws than female users.

Neigel et al. [32] concluded that current cyber education is under-preparing graduates in considering the human factors associated with cybersecurity breaches. Human error may be the root cause of such security breaches and the weakest link regarding cyber resilience.

A recurring issue is the generalizability of the data generated by these studies. Cultural factors may have influenced the results because each study was conducted in a single country. According to Lowry et al. [33], there are significant differences in the context of information technology between Asian and Western cultures, which can be agreed upon here as well.

2.3 Instructional design methods

The following are few of the most commonly used instructional design approaches:

2.3.1 Bloom’s Taxonomy:

Bloom’s taxonomy was created in 1956 by Benjamin Bloom and others. It was revised in 2001 by cognitive psychologists, curriculum theorists, instructional researchers, and testing and assessment specialists [34]. The following are simple definitions of the taxonomy stages and what each level stands for [35]:

Remembering: “To recall the information learned, such as memorizing and defining the terms and facts.”[35]
Understanding: “To know and understand a concept so it can be explained to someone else.”[35]
Applying: “To apply the concepts learned to solve a problem.” [35]
Analyzing: “The ability to breakdown the knowledge into parts and effectively analyze a situation to apply the concepts learned to solve a problem.” [35]
Evaluating: “The ability to judge, criticize and have recommendations for an idea” [35]
Creating: “The ability to concatenate ideas to form a new solution.”[35]

2.3.2 ADDIE:

ADDIE is a leading learning development model for instructional design, encompassing designing, developing, and delivering learning content [36]. The model is frequently used in organizations to design training and learning, and development programs [36]. It has five phases which are [37]:

Analyze: Identifying students' knowledge and evaluating what they should know
Design: Planning to meet the needs, including, but not limited to, deciding on the learning objectives, evaluation criteria, tools used, and so on.
Development: Based on the plan, create learning materials and activities. Content, audio, and graphical materials [37] are written during this phase.
Implementation: Incorporate learning materials and activities designed into the learning environment [37].
Evaluation: To determine overall effectiveness, conduct formative and summative content evaluations.

3 Research Methodology

Several research methods were used to answer the outlined research questions in Section 1.2. These are summarized in Table 1 and depicted in Figure 1 and discussed in detail in this Section.

Research Questions	Purpose of the Question	Research Method
What is an appropriate methodology to measure cybersecurity awareness levels? a) Are there any studies done before in Delhi or India which assess the cybersecurity levels?	To use the appropriate methodology to measure the cybersecurity awareness levels based on existing literature in Delhi or India	Literature Review
Are different cybersecurity awareness measurement methods and study results comparable? a) How much cybersecurity awareness do Delhi university students possess compared to Malaysian students [4]? b) What critical aspects must we consider when analyzing and comparing awareness studies? c) What are the critical aspects to consider when	To develop a questionnaire to understand where Delhi university students lack awareness. Since the questionnaire of the current study employs similar questions to Muniandy et al. [4], this will help check what aspects of cybersecurity Delhi and Malaysian students share or lack awareness of.	Interviews with an IT expert, Questionnaire and Comparative Analysis

designing the new awareness measurement instruments to ensure keeping up to date with technology and cybersecurity advancements?		
When designing a short awareness training for students, what methodology is appropriate and a) Can the Successive Approximation Model instructional design method be appropriate for developing short but effective cybersecurity learning for students in changing environments and learning needs? b) How does implementing short training sessions developed using SAM methodology impact the students’ awareness?	To design a pilot cyber security awareness training using SAM and check its effectiveness on Delhi university students.	Interviews with expert, Successive Approximation Model, and Questionnaire Comparative Analysis

Table 1. Research questions, purpose and methods

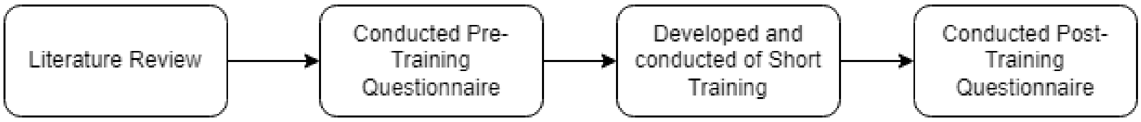

Literature Review
Conducted Pre-Training Questionnaire
Developed and conducted of Short Training
Conducted Post-Training Questionnaire

Figure 1. Process of Research

Figure 1 shows the current research process, which begins with a literature review, in which the researcher gathered information on existing knowledge relevant to the research questions. Following that, a questionnaire was created and distributed to university students in Delhi. Following the collection of data from the questionnaire, knowledge gaps in cybersecurity security awareness were identified, and a short cybersecurity training was developed as a result. To validate the effectiveness of this training and check if there are any improvements in cybersecurity awareness levels of students, a post-training questionnaire was executed.

A literature review was done to check pre-existing cybersecurity awareness and training studies. This literature review is used to identify the gaps in existing research. The initial keywords for this literature review were broad terms like ‘cybersecurity awareness of students’, ‘cybersecurity awareness training’, ‘cybersecurity awareness training in India’, and ‘cybersecurity awareness in India.’ Later, the keywords were broken down into 'cyber', 'security', 'awareness', and 'students' or without 'students' together with 'Delhi', 'Gujarat,’ other Indian states, and then increasing my search region from states to country and then inside the Indian subcontinent and Asia. The study utilizes forward and backward snowballing to find relevant publications.

Regarding libraries, relevant research publications were searched using ScienceDirect, Scopus, Google Scholar, IEEE Xplore, and ResearchGate. The primary inclusion criteria were finding papers on cyber security awareness published after 2010. The main exclusion criteria were to eliminate studies on cyber security awareness published before 2010 in a language other than English.

The quantitative analysis research methodology is used to create and execute the pre-training and post-training surveys via questionnaires and collect data from various participants. A quantitative methodology was used because it aids in the understanding of an issue or phenomenon by gathering objective data that can be communicated and analyzed using statistics and metrics (Aliaga, M. & Gunderson, B. (2002), as cited in

[38]). Telephonic interviews and discussions with an IT expert were conducted to develop the pre- and post-training questionnaire.

The IT expert is Mr. Sufiyan Malik, a Cybersecurity Consultant in an organization in India, with approximately three years of experience. Telephonic interviews and consultations with the expert were conducted to develop the content structure and learning objectives for the short cyber security awareness training. The short cyber security awareness training follows the Successive Approximation Model [3], further explained in Chapter 3.2.

3.1 Questionnaire Description

A new questionnaire was developed after a review of some existing questionnaires from previous studies and a telephonic interview with an industry expert. The questionnaire contains a total of 38 questions. Among these are five demographic questions about educational level, type of school (private or public), the current field of study, age group, and gender, along with three questions about if the respondents have received any training related to cybersecurity, their preference for attending any cybersecurity training and asking them to insert email if they are interested in participation for future research surveys. The remaining questions are divided into topics based on the identified broad areas consisting of six questions on Malware, five on Password security, five on Phishing, five on Social Engineering, and nine on general user behavior. The final section includes questions about cybersecurity trainings, such as whether participants have had any prior cybersecurity trainings or studies, their preferred platform for attending cybersecurity training, and whether they want to be contacted again for future similar surveys.

The reason for using 5-9 questions per section is that participants are more likely to respond to a short questionnaire than a lengthy questionnaire [39]. It has also been reported by Kost et al. [40] that a more concise survey using a short questionnaire is more reliable and produces higher response and completion rates than a long survey.

The questionnaire used a 5-point Likert scale to collect responses for the following reasons:

- Because Likert scales are simple to understand and apply, they are the most commonly used instrument in measuring attitudes and beliefs toward mathematics [41]. In addition, Likert scales can ask participants to indicate their agreement or disagreement with a statement using a standardized response format which can be used to measure attitude, providing a higher sensitivity level than yes or no responses [42].

- Researchers can gather quantitative estimates of subjective traits using Likert scales, which generate numeric data that can be summarized and visualized similarly to other quantitative data collected during an evaluation [43].

3.1.1 Common and Modified Questions:

As previously stated, the Delhi demographic is unique in many ways, including how students in Delhi use technology, which means that some of the existing questionnaires cannot be fully utilized because they do not cover every aspect of cyber security awareness that must be followed within Delhi and require some additional questions that are suited for the Delhi demographic. Therefore, following a review of some existing questionnaires from previous studies, a new questionnaire was developed with the assistance of an industry expert, some of which are also similar to the questions from the Muniandy et al. questionnaire [4] used in their study.

In addition, 18 questions were modified and used from the Muniandy et al. questionnaire [4], which the expert and the researcher believe can be more commonly asked questions and are not exclusive to the Malaysian demographic, thus also suiting the Delhi demographic. Some of these questions from the Muniandy et al. questionnaire [4] are also used to gauge cybersecurity awareness, for instance, in studies by Senthilkumar and Easwaramoorthy [11], Alharbi and Tassaddiq [44], Khan et al. [30], Alotaibi et al. [31], Nagahawatta et al. [28], Sreehari A et al. [10], and Shah and Agarwal [26]. The expert also suggested combining questions P4 and P5, Ph6 and Ph10, and S2 and S6 as they may yield similar response trends. Table 2 shows the questions that were used.

ID	**Questions from Muniandy et al.** [4]	**Modified version**
M1	Willing to open email attachments from strangers	You open email attachments from unknown persons.

M2	Interesting subject line causes the of opening an email attachment	You open an email attachment because of the intriguing subject line.
M7	Scan removable drives prior to using it on my personal computer	How often do you scan your files whenever you insert a flash drive or download files from any website or email attachments?
M9	Willing to download materials from unsecure sites	Are you willing to download files from untrustworthy websites?
M10	Apply security patches as soon as possible.	How frequently do you update and install the latest security updates for your devices?
P2	Sharing password with other people	How often do you share passwords with others, such as family or friends?
P3	Different passwords for different applications	You keep different passwords for different accounts.
P4	Password consists of lowercase, uppercase, numbers, special characters	Your passwords contain a combination of lowercase, uppercase, numbers, special characters, and a minimum of eight characters.
P5	Passwords longer than 8 characters	
P7	Never change password	Do you frequently change passwords for your accounts, including your Internet banking?
Ph4	Willing to click hyperlinks in email messages	You should click hyperlinks in every email message.
Ph6	URL must be "https" if I'm transmitting confidential information	You check URLs before visiting any website (e.g., checking 'https,' checking any spelling errors in the domain name)
Ph10	Check URL spelling prior to any types of transactions.	
Ph8	I prefer to type URL in the new browser rather than clicking it on hyperlinks.	How often do you prefer to type the URL in a new browser rather than clicking it on a hyperlink?

Ph3	Willing to provide confidential information to any types of emails	How often do you provide personal information in response to any email request?
S2	Willing to reveal username and password to anyone claiming to be system administrator	How frequently will you give your username and password to anyone claiming to be a system administrator/help desk representative?
S6	Willingness to provide password to a help desk	
S7	Check the authorization or identity of someone before talking on any issues	How often do you verify the identity of an unknown caller or email sender before providing any information?

Table 2. Comparing the questionnaire questions from the Malaysian study and the current study

3.1.2 Data Collection

Delhi had approximately 281,983 university and college students as of 2020 [45]. As previously stated, the questionnaire was initially distributed to students from Jamia Hamdard University, Delhi Skill and Entrepreneurship University, and Al-Falah University, with a combined student population of over 10,000 [46], [47]. According to [48], the sample size for a population of 10,000 to 15,000 should be 370 or 375. According to most statisticians, the minimum sample size for any meaningful result is 100 [49].

The research data for Delhi students was gathered by distributing a Google Forms-designed questionnaire among the students currently studying in Delhi. The questionnaire was distributed through social media platforms and workshops with university and high school students who study in Delhi. In addition, the questionnaire was distributed to students from various universities in Delhi and different study fields, considering the non-IT perspective to collect data while avoiding response bias. Topics like malware, password security, phishing, social engineering, and general user behavior were all covered in the questionnaire.

The links of pre-and post-training questionnaires below:

Pre-Training Questionnaire: https://forms.gle/pAuExEf34UmGXxzH7

Post-training Questionnaire: https://forms.gle/eZBLgQtqvEA4c2gn9

3.1.3 Reliability of the Questionnaire

Creswell [50] defines Cronbach's alpha as a measure of reliability, precisely internal consistency. Taber [51] describes Alpha Cronbach's alpha values as excellent (0.93–0.94), strong (0.91–0.93), reliable (0.84–0.90), robust (0.81), fairly high (0.76–0.95), high (0.73–0.95), good (0.71–0.91), relatively high (0.700.77), slightly low (0.68), reasonable (0.67–0.87), adequate (0.64–0.85), moderate (0.610.65), satisfactory (0.58–0.97), acceptable (0.45–0.98), sufficient (0.45–0.96), not satisfactory (0.4–0.55) and low (0.11). Cronbach's alpha values between 0.60 and 0.70 are acceptable, and 0.8 or greater are excellent [39], [41]. Cronbach's alpha values for the questionnaire were determined through pilot testing with 20 students and are shown in Table 3.

Subscales	**Reliability (Cronbach Alpha)**
Malware	0.7407
Password	0.7155
Phishing	0.6168
Social Engineering	0.7484
User behavior	0.6402

Table 3. Reliability of the questionnaire

3.2 Successive Approximation Model (SAM)

Once the questionnaire responses were received, developing a short training course, as pilot training, to educate students about basic cybersecurity awareness was considered. The learning design was considered using several options, including ADDIE and others, but because the researcher felt there was a need for a fast-paced iterative design, SAM was explored as an option.

The Successive Approximation Model (SAM) is a simplified version of the ADDIE Model (Analysis, Design, Development, Implementation, and Evaluation) [37], designed to elicit feedback and build working models early [3]. This model, created by Dr. Michael Allen of Allen Interactions, employs a recursive rather than a linear process for course development [3]. SAM is a widely used method for designing and developing e-learning content [52]. It is based on the notion that the development process should be iterative, with e-learning content tested and refined until it meets the needs of the learners [52]. The SAM model is divided into three stages: Preparation, Iterative Design, and Iterative Development.

A group is responsible for creating the course and deciding the course's learning objectives, audience needs, and content specifications during the Preparation phase [53].

The Iterative Design phase is focused on designing, prototyping, and evaluating rotate iteratively in small steps [54]. Feedback from the learners is incorporated into the design, and the process is repeated until the course meets the objectives set out in the Preparation phase.

The Iterative Development phase involves a continuous loop of developing, implementing, and assessing until the final training program is ready for large-scale implementation [54]. Following implementation, the program's impact is evaluated through audience feedback, and further design and development may occur [53].

The primary advantage of using SAM over ADDIE or Bloom Taxonomy is its iterative process and non-linear approach, which allows for opportunities to experiment, test, and revise designs [54]; making SAM more flexible makes it easy to update.

The questionnaire responses will show which areas of cybersecurity the students lack awareness in, as well as whether the students have received any prior cybersecurity training, their preferred platform for training if they wish to attend one, and the emails of students who wish to participate in these training and be a part of future surveys. Once the responses were received, students who entered their email addresses to participate in these training were sent an email with links to video playlists and a post-training questionnaire to see if their cybersecurity awareness had improved. Further is explained in Chapter 5.

4 Questionnaire Results and Analysis

The questionnaire generated a total of 139 responses. The following sections provide a detailed analysis of various areas of the questionnaire. In addition, the responses from Muniandy et al. study [4] are also compared with Delhi students, where the questions are similar, as shown in Table 2 above. The responses to this questionnaire are stored as a comma-separated value (CSV) file in the following drive storage:

Pre-Training questionnaire responses:
https://drive.google.com/file/d/1L6geBJJwcZXB4fUtWqQCRwUWXaIvmTmP/view?usp=share_link

4.1 Demographic Profile

Variable	Response	%
Gender	Male	53.24
	Female	44.6
	Prefer not to say	2.16
Age Group	18-24 years	68.35
	25-30 years	24.46
	30+ years	7.19
Level of education pursuing	Bachelors	75.54
	Masters	23.02
	Doctorate	1.44
University	Government-owned/managed	47.78
	Private Owned	52.52
Current field of study or have studied	Computer Science or IT study	42.45
	Non-IT study	57.55
Region of current studies	Delhi	98.56
	Outside Delhi	1.44

Table 4. Demographic question responses

One intriguing finding is that, although the study was aimed at university students in Delhi, it reached 1.44% of students outside of Delhi. The researcher believes this may result from snowball sampling, as discussed before.

4.2 Malware Awareness

This section consists of 6 questions based on essential awareness of malware threats. The following Table 5 contains the questions based on malware awareness.

S.No.	Questions
MQ1.	You open email attachments from unknown persons.
MQ2.	You open an email attachment because of the intriguing subject line.
MQ3.	How often do you connect your personal or professional devices on open/public networks?
MQ4.	Are you willing to download files from untrustworthy websites?
MQ5.	How often do you scan your files whenever you insert a flash drive or download files from any website or email attachments?
MQ6.	In case the website certificate is expired or invalid for your most visited websites, will you still proceed to such websites?

Table 5. Malware Questions

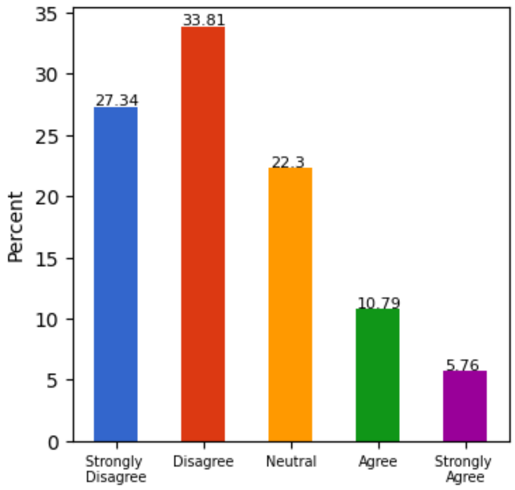


Figure 2. You open email attachments from unknown persons.

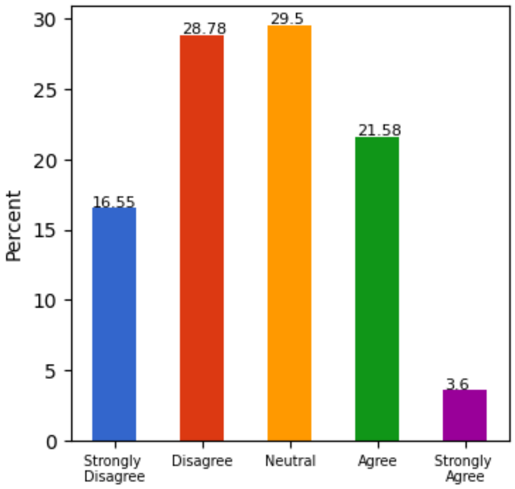


Figure 3. You open an email attachment because of the intriguing subject line

4.2.1 Malware Question 1 (MQ1)

Figure 2 shows that the majority of the students disagree. In contrast, 22.3% of students are neutral about opening email attachments from unknown people, with 10.79% and 5.76% agreeing and strongly agreeing, respectively, which is very concerning. 33.81% of students disagreed but did not strongly disagree about opening email attachments from unknown people. The number of disagreeing students can be reduced and shifted toward strongly disagreeing.

As per M1 responses, Malaysian students had 16.41% agreeing and 71.88% disagreeing [4], showing a similar trend.

4.2.2 Malware Question 2 (MQ2)

As shown in Figure 3, 18.6% of students agreed, and 3.9% strongly agreed about opening an email attachment because of the intriguing subject line. However, this statement fetched a neutral response from 29.5% of students, indicating that they may or may not agree, which is still concerning. While a tempting subject line may hook your interest in the email attachment, it is essential to use caution when opening attachments, especially if they come from unknown senders or the subject seems suspicious. The researcher believes this area has some room for improvement.

According to M2 responses, Malaysian students seem more inclined to open attachments with catchy subject lines, with nearly 40% agreeing with the statement [4]. On the other hand, Delhi students appear to be more cautious than Malaysian students, with nearly 22% agreeing or strongly agreeing with the statement. However, almost the same disagreement with the statement is seen in both sets of students.

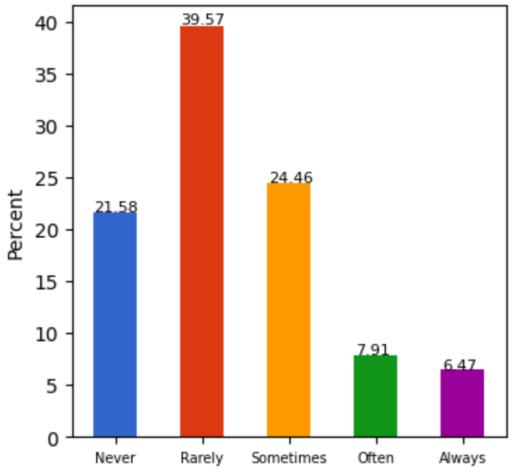


Figure 4. How often do you connect your personal or professional devices on open/public networks?

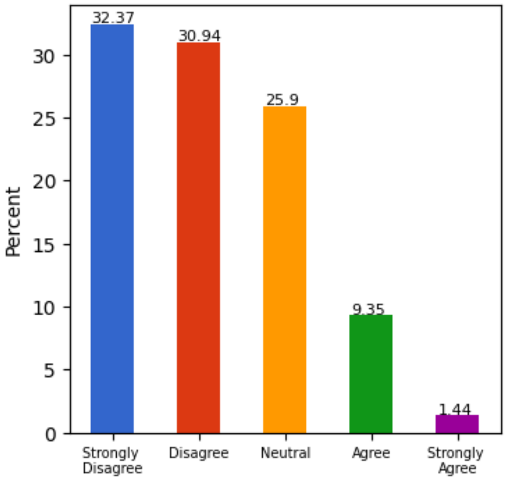


Figure 5. Are you willing to download files from untrustworthy websites?

4.2.3 Malware Question 3 (MQ3)

According to Figure 4, 24.5% of students sometimes, 8% frequently, and almost 6.5% always connect their personal or work devices to public/open networks. Almost 40% of those polled rarely connect their devices to open networks, but this figure can be reduced and shifted to those who never join open networks.

4.2.4 Malware Question 4 (MQ4)

Figure 5 shows that most students strongly disagree, almost 26% were neutral, 9.35% agreed, and almost 1.5% strongly agreed about being willing to download files from untrustworthy websites, which is a concerning issue. Almost 31% of students partially disagreed on the same topic, but this figure can also be reduced. Shady websites can source infected files, causing your device to malfunction and compromising your data.

The survey results show that Delhi students are more cautious when downloading files from untrustworthy websites, with only a tiny percentage strongly agreeing or agreeing. On the other hand, Malaysian students appear to be less cautious, with a higher percentage agreeing to download files and a lower percentage disagreeing than Delhi students as per M9 responses [4]. Overall, results suggest that Delhi students are more aware than Malaysian students of this statement.

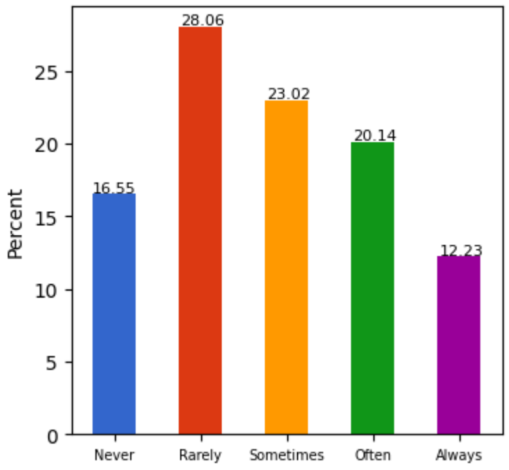


Figure 6. How often do you scan your files whenever you insert a flash drive or download files from any website or email attachments?

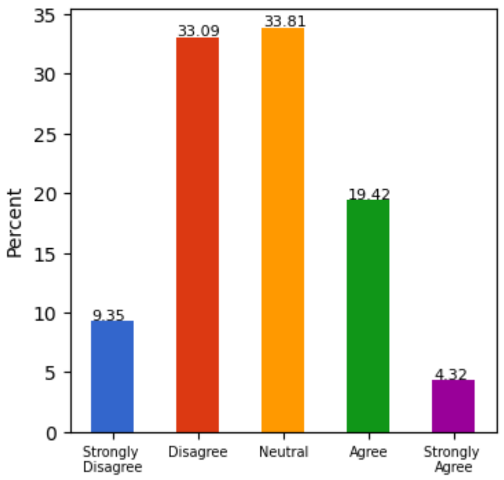


Figure 7. In case the website certificate is expired or invalid for your most visited websites, will you still proceed to such websites?

4.2.5 Malware Question 5 (MQ5)

Figure 6 shows that 23.02% of students scan their files occasionally, 28.06% rarely, and 16.5% never scan their files whenever they insert a flash drive or download a file from the internet, increasing the risk of introducing viruses, malware, or other malicious software onto their devices, which leaves room for improvement.

As per M7 responses, 46.88% of Malaysian students disagreed with the same statement [4]. On the contrary, only 16.55% of Delhi students never scanned their files, showing less awareness than Malaysian students.

4.2.6 Malware Question 6 (MQ6)

As shown in Figure 7, almost 33% of the students partially disagreed, and only 9% strongly disagreed with continuing to their most visited website, even if the certificate expired or was invalid. Nearly 34% of students were neutral, 19.42% agreed, and almost 5% strongly agreed, which leaves room for improvement. A website with an expired or invalid SSL certificate cannot be verified, making it vulnerable to attacks by hackers who may intercept or modify the data being transmitted between your device and the website and making you susceptible to phishing attacks.

4.3 Password Awareness

This section consists of 5 questions based on essential password security awareness. The questions on password security awareness are listed in Table 6.

S.No.	Questions
PQ1.	How often do you share passwords with others, such as family or friends?
PQ2.	You keep different passwords for different accounts.
PQ3.	Your passwords contain a combination of lowercase, uppercase, numbers, special characters, and a minimum of eight characters.
PQ4.	You set up 2-factor authentication for accounts other than passwords.
PQ5.	Do you frequently change passwords for your accounts, including your Internet banking?

Table 6. Password Questions

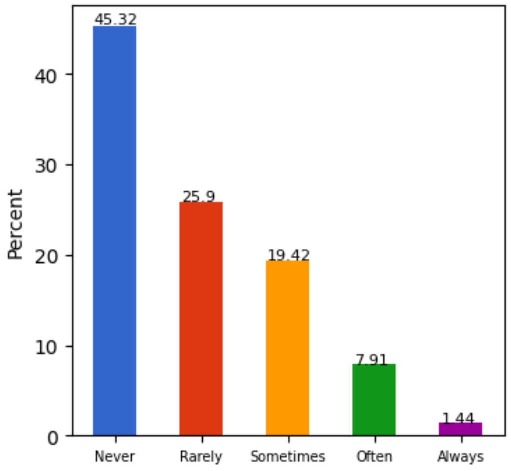


Figure 8. How often do you share passwords with others, such as family or friends?

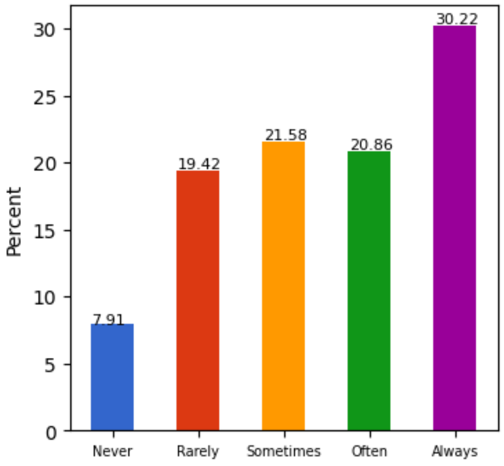


Figure 9. You keep different passwords for different accounts.

4.3.1 Password Question 1 (PQ1)

As illustrated in Figure 8, most students never share their passwords with friends or family, while 19.4% share them occasionally, nearly 8% frequently, and 1.4% always do. Almost 26% of students rarely share them, but this also counts as sharing, which can jeopardize the user's account. Your password could be exposed if any people you have shared it with use poor security practices or have their own devices compromised by hackers.

According to the P2 responses, most Malaysian students (85.94%) disagreed with sharing passwords, while 11.72% agreed [4]. In contrast, only 45% of Delhi students never share their passwords, suggesting they are likelier to share passwords than their Malaysian counterparts.

4.3.2 Password Question 2 (PQ2)

According to Figure 9, 21.5% of students sometimes keep different passwords for different accounts, 19.4% rarely, and about 8% never. 30.22% of students use different passwords for other accounts, while 20.86% often. Despite many students displaying awareness, much room remains for improvement. Using the same password for all your accounts may lead to the compromise of all your accounts using the same password if one of the accounts gets compromised.

As per P3 responses, almost 60% of Malaysian students disagreed with having different passwords for different applications [4]. On the other hand, only around 8% of the Delhi students never keep a different password for different accounts and applications, showing less awareness among Malaysian students on this statement.

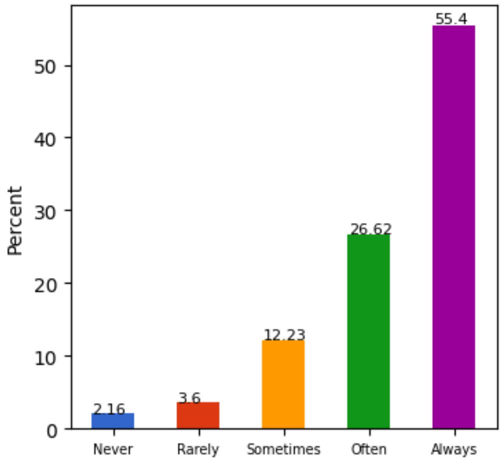


Figure 10. Your passwords contain a combination of lowercase, uppercase, numbers, special characters, and a minimum of eight characters.

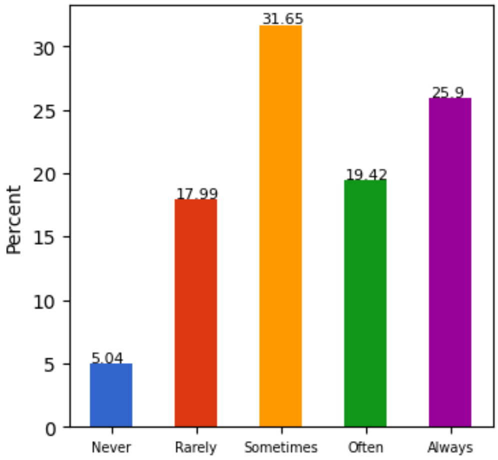


Figure 11. You set up 2-factor authentication for accounts other than passwords.

4.3.3 Password Question 3 (PQ3)

55% of the students always have passwords containing a combination of lowercase, uppercase, numbers, special characters, and a minimum of eight characters, with 26.6% often, almost 12% sometimes, 3.6% rarely, and only 2% never having the same pattern as seen in Figure 10. This positive trend is seen because most websites keep password requirements mandatory these days, where the user must always comply and save a password with a minimum requirement.

Most Delhi and Malaysian students recognize the importance of using a combination of lowercase, uppercase, numbers, and special characters in passwords. However, while many Delhi students claim to always follow this practice, Malaysian students appear to be more unsure, with a significant percentage indicating that they do not know or disagree [4].

4.3.4 Password Question 4 (PQ4)

Figure 11 shows that a significant percentage of students (almost 45%) use two-factor authentication (2FA) for accounts other than passwords, either "often" or "always". However, almost 31% of the students sometimes use it, while many rarely (17.99%) or do not use 2FA (5.04%), leaving room for improvement. In addition, not enabling 2FA increases the risk of unauthorized account access, which could lead to data theft, financial loss, and other security breaches.

4.3.5 Password Question 5 (PQ5)

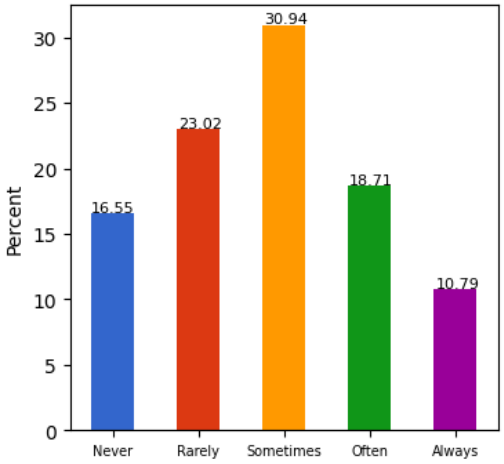


Figure 12. Do you frequently change passwords for your accounts, including your Internet banking?

Figure 12 shows that 16.55% of students never and 23.02% rarely change passwords. Around one-third of students (30.94%) said they sometimes change their passwords, and 18.71% change them often. Only 10.79% of students reported consistently changing their passwords. These results suggest that many people do not prioritize changing their passwords frequently, which could put their accounts at risk of being compromised, which leaves room for improvement.

According to P7 responses, almost 45% of Malaysian students agreed upon never changing passwords [4]. On the other hand, only 16.55% of Delhi students never changed their passwords, showing that most Delhi students know the risks of not changing passwords more than Malaysian students.

4.4 Phishing Awareness

This section contains five questions about phishing awareness. Table 7 lists the phishing awareness questions.

S.No.	Questions
PHQ1.	You should click hyperlinks in every email message.
PHQ2.	You should check URLs before visiting any website (e.g., checking 'https,' checking any spelling errors in the domain name)
PHQ3.	How often do you prefer to type the URL in the new browser tab rather than clicking it on the hyperlink?
PHQ4.	How often do you check the sender's email address before opening an email?
PHQ5.	How often do you provide personal information in response to any email request?

Table 7. Phishing Questions

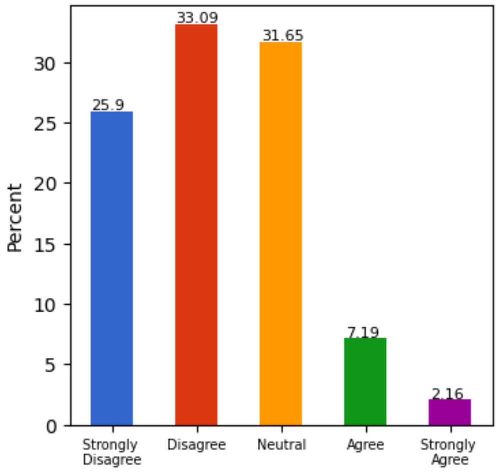


Figure 13. You should click hyperlinks in every email message.

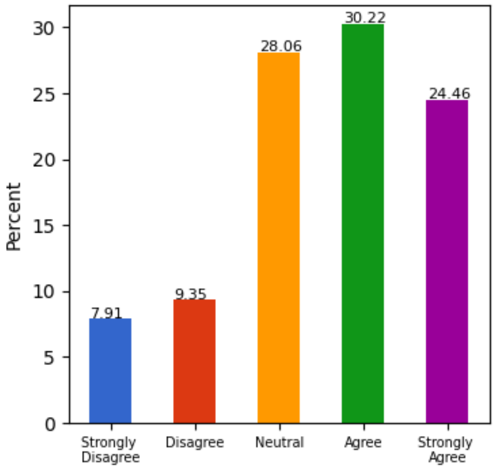


Figure 14. You should check URLs before visiting any website

4.4.1 Phishing Question 1 (PHQ1)

Figure 13 shows that only 2.16% of students strongly agree, and 7.19% agree that one should click hyperlinks in every email. Around 33% of the students disagree, and approximately 26% strongly disagree with this statement. These results show that most students know the risks of clicking email hyperlinks. Also, a significant amount (31.65%) of the students were neutral on this statement, leaving room for improvement. This is concerning because some hyperlinks may direct you to fraudulent websites or login pages that steal your personal and financial information.

According to the Ph4 responses, 25.7% of Malaysian students agree, and nearly 51% disagree with clicking on hyperlinks in all email messages [4]. In comparison, only 9% of Delhi students agree and strongly agree with the statement, while 58% strongly disagree and disagree, indicating that Delhi students are more aware than Malaysian students. As previously stated, a sizable proportion (31.65%) of Delhi students were neutral on this statement. Therefore, Delhi students may or may not click on email hyperlinks, depending on the circumstances.

4.4.2 Phishing Question 2 (PHQ2)

According to Figure 14, 30.22% of the students agree, and 24.46% strongly agree that they check the URLs before visiting any website, like checking any spelling errors in a domain name or checking ‘https.’ However, nearly 28% of students are neutral, 9.35% disagree, and 7.91% strongly disagree with this statement. These findings imply that many people know the significance of verifying URLs to safeguard online activity, but there is still room for improvement.

According to the Ph6 and Ph10 responses, 35.16% and 26.56% of Malaysian students agree on checking the 'https' status and URL spelling, respectively, while 36.72% and almost 47% disagree with the same [4]. On the contrary, almost 54% of Delhi students agree and strongly agree on checking the URL before visiting any website. In comparison, only 17% strongly disagree and disagree on the same, showing Delhi students are more cautious than Malaysian students.

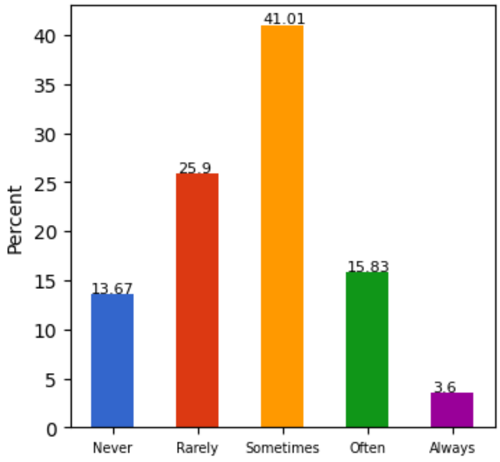


Figure 15. How often do you prefer to type the URL in the new browser tab rather than clicking it on the hyperlink?

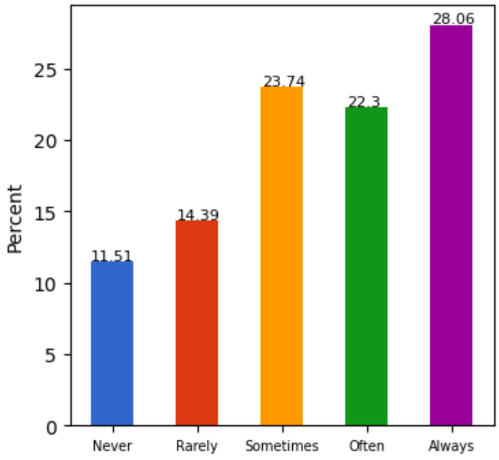


Figure 16. How often do you check the sender's email address before opening an email?

4.4.3 Phishing Question 3 (PHQ3)

According to Figure 15, most students prefer to click hyperlinks instead of typing the URL in a new browser tab. Around 41% of students sometimes type the URL, while almost 26% rarely do so. About 16% often choose to type the URL, while only 3.6% always do. Notably, 13.67% never type the URL in a new browser tab. These findings indicate that there is quite room for improvement since most people rely on hyperlinks rather than manually entering URLs, which is a significant concern because typing URLs manually can help you verify that you are visiting the correct website and reduce the risk of falling for phishing scams or other types of online fraud.

Delhi students tend to type URLs in a new browser sometimes or rarely. In contrast, Malaysian students have mixed opinions, with almost 60% disagreeing that they prefer to type URLs according to Ph8 responses [4]. Delhi students are more likely to type URLs than Malaysian students.

4.4.4 Phishing Question 4 (PHQ4)

Figure 16 shows that a significant number of students (almost 25% combining ‘never’ and ‘rarely’) do not regularly check the sender's email address before opening an email. On the other hand, about a quarter of respondents (23.74%) sometimes check, while 50.36% check often or always. This shows that students know the risks of not checking the sender’s email address. However, according to the responses, there is room for improvement. Many people do not check the sender's email address before opening an email which may lead to email scams and phishing attempts.

4.4.5 Phishing Question 5 (PHQ5)

As shown in Figure 17, 38.85% of the students reported never providing personal information in response to email requests. Meanwhile, 35.25% reported rarely doing so, indicating that they have done so at some point. 15.11% of the students reported that they sometimes provide personal information, and only 6.47% reported often doing so. A small group of students (4.32%) reported always providing personal information in response to email requests. This tells that many people are alert of sharing personal information online and only do so in certain circumstances.

According to Ph3 responses, almost 78% of Malaysian students disagree, and only 9.38% agree on willingness to provide confidential information to any emails [4]. On the other hand, 38.85% of Delhi students reported never providing personal information in response to email requests. When the figures are compared, Malaysian students appear more aware of the risks than Delhi students.

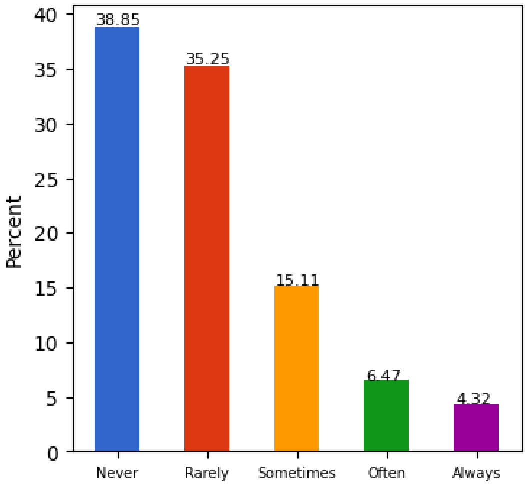


Figure 17. How often do you provide personal information in response to any email request?

4.5 Social Engineering Awareness

This section contains five questions about social engineering. Table 8 lists the phishing awareness questions.

S.No.	Questions
SQ1.	How frequently are you willing to give your username and password to anyone claiming to be a system administrator/help desk representative?
SQ2.	How often have you been tricked into giving away personal information to a caller or emailer, even though you knew it was suspicious?
SQ3.	How often do you verify the identity of an unknown caller or email sender before providing any information?
SQ4.	You are comfortable in refusing to provide information to individuals who do not have a legitimate need to know it.
SQ5.	How often do you post your work-related data on Instagram/Snapchat stories (social media)?

Table 8. Social Engineering Questions

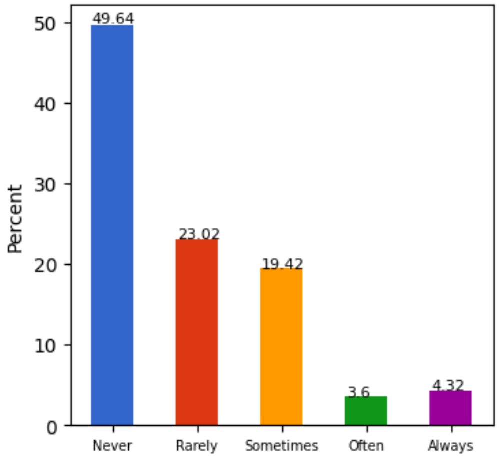


Figure 18. How frequently are you willing to give your username and password to anyone claiming to be a system administrator/help desk representative?

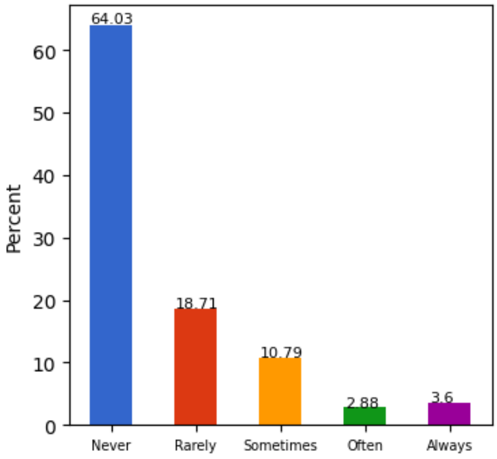


Figure 19. How often have you been tricked into giving away personal information to a caller or emailer, even though you knew it was suspicious?

4.5.1 Social Engineering Question 1 (SQ1)

Figure 18 shows that almost half of the students would never give their user credentials to someone claiming to be a system administrator or a help desk representative. Nearly 23% would rarely, while 19.42% would sometimes comply. Only 3.6% of the students would often, and 4.32% always give away their login credentials. This suggests that these students are generally cautious about sharing their sensitive information and aware of the potential risks associated with such actions.

According to S2 and S6 responses, almost 83% and 71% of Malaysian students disagree on sharing credentials with anyone claiming to be a system administrator or help desk, respectively [4]. On the other hand, almost 50% of Delhi students will never give credentials to anyone claiming to be a system admin or helpdesk. On comparison of statistics, more Malaysian students are cautious than Delhi students.

4.5.2 Social Engineering Question 2 (SQ2)

Figure 19 shows that most students have never been tricked into giving away personal information to suspicious callers or emailers. 18.71% of students indicated they rarely fall for such tricks, while 10.79% said they would sometimes fall for such schemes. Only 2.88% of the students reported they often, and 3.6% indicated that they always give away personal information despite suspecting fraud. Sharing personal data with someone with bad intentions can lead to identity theft.

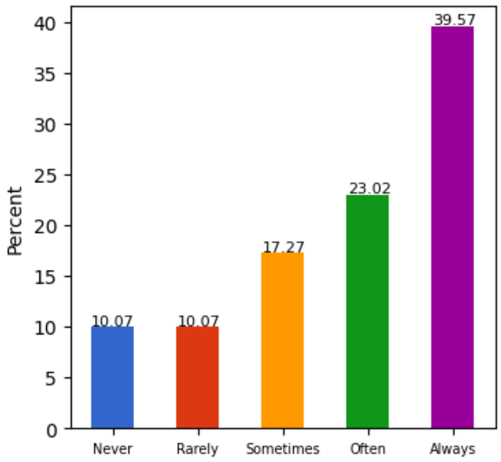


Figure 20. How often do you verify the identity of an unknown caller or email sender before providing any information?

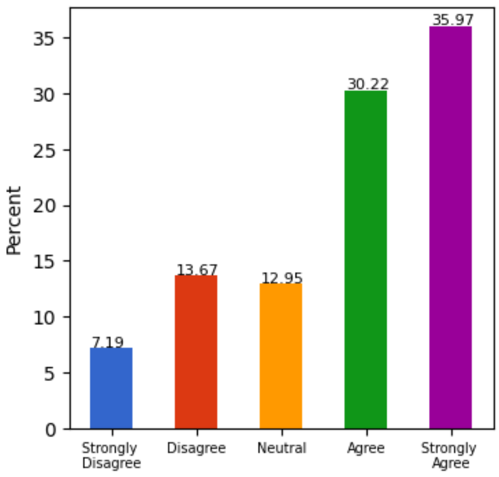


Figure 21. You are comfortable in refusing to provide information to individuals who do not have a legitimate need to know it

4.5.3 Social Engineering Question 3 (SQ3)

Figure 20 shows that most students (39.57%) always verify the identity of unknown callers or email senders before providing any information. A significant proportion of students (23.02%) said they often verify identity, while 17.27% do so sometimes. Only a small percentage of students (10.07%) reported rarely or never verifying identity. These findings suggest that most students are cautious when sharing sensitive information with unknown people. However, there is still room for improvement in verifying identity consistently.

Based on the responses, Delhi students are generally more aware of the importance of verifying the identity of unknown callers or email senders, with 62.59% responding with "Often" or "Always". In comparison, only 33.59% of Malaysian students agreed to check the authorization or identity of someone before talking on any issues, according to S7 responses [4].

4.5.4 Social Engineering Question 4 (SQ4)

Figure 21 shows that most students agree and strongly agree that they are comfortable refusing to provide information to individuals who do not have a legitimate need to know it. This indicates that students are willing to take a stand to prevent unauthorized access. Meanwhile, a smaller portion of students disagree, strongly disagree, or are neutral with this statement, showing that they may be open to providing information, thus unintentionally giving unauthorized access.

4.5.5 Social Engineering Question 5 (SQ6)

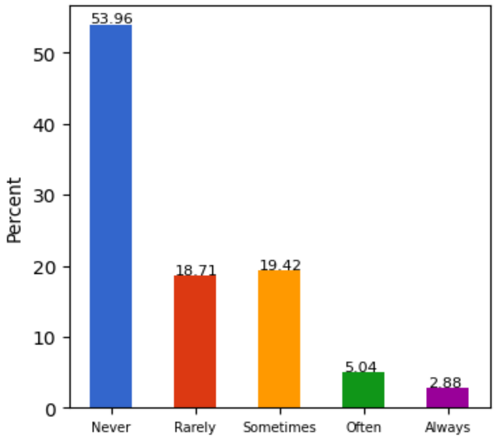


Figure 22. How often do you post your work-related data on Instagram/Snapchat stories (social media)?

Figure 22 shows that 53.96% of students never post work-related data on Instagram/Snapchat stories, while 18.71% do it rarely, 19.42% sometimes, 5.04% often, and 2.88% always. These results show that most students know the risk of posting work-related information on social media. It may make the organization vulnerable to data breaches or cyber-attacks because hackers and cybercriminals constantly seek sensitive information or software to exploit. Work-related media on social media may help them get that information.

4.6 User Behavior Awareness

This section contains nine questions about user behavior awareness. Table 9 lists the phishing awareness questions.

S.No.	Questions
UQ1.	You should backup your data at regular intervals (monthly, quarterly, or annually)
UQ2.	How frequently do you lock your device before leaving it unattended?

UQ3.	You post your vacation pictures during the vacation itself with a location tag (in real-time)
UQ4.	Before installing an app from App Store/Play Store/website, how often do you read the terms and conditions?
UQ5.	How often have you installed any third-party application from external sources?
UQ6.	You grant all the devices permissions the application will use while installing the application.
UQ7.	How frequently do you update and install the latest security updates for your devices?
UQ8.	How often do you access your personal emails on school/work computers?
UQ9.	How often do you install any third-party software on school/work computers?

Table 9. User Behavior Questions

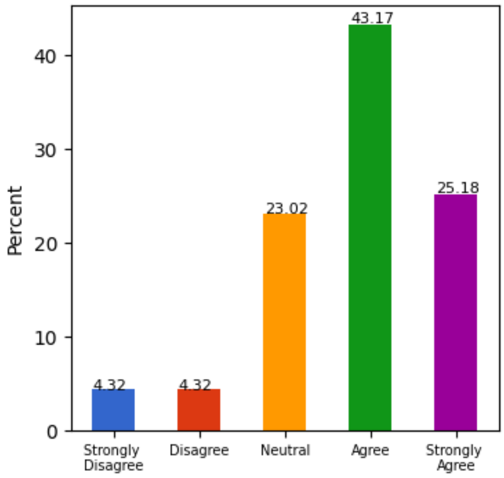


Figure 23. You should backup your data at regular intervals

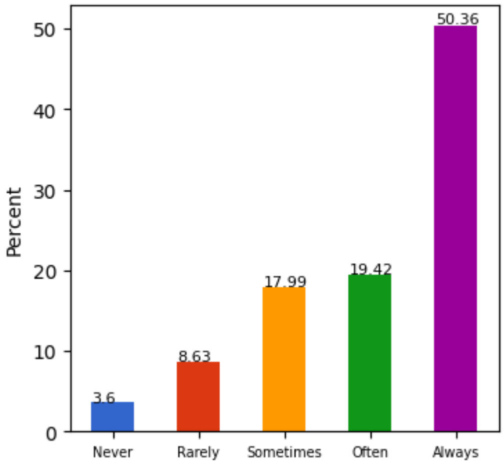


Figure 24. How frequently do you lock your device before leaving it unattended?

4.6.1 User Behavior Question 1 (UQ1)

Figure 23 shows that most students partially agreed to back up their data regularly, with 25.18% strongly agreeing and 23.02% neutral. In comparison, 4.32% of students disagreed and strongly disagreed on the same topic. The data backups should be done regularly to prevent data loss.

4.6.2 User Behavior Question 2 (UQ2)

Figure 24 shows that 50.36% of students lock their devices before leaving them unattended. 19.42% of the students often, 17.99% sometimes, 8.63% rarely, and 3.6% never lock their devices before leaving them unattended. These results show that many students know that leaving their unlocked devices unattended is a security risk. However, leaving the devices unlocked and unattended increases the chances that someone you do not know or someone you know gains access to your personal or organizational files, putting you at risk.

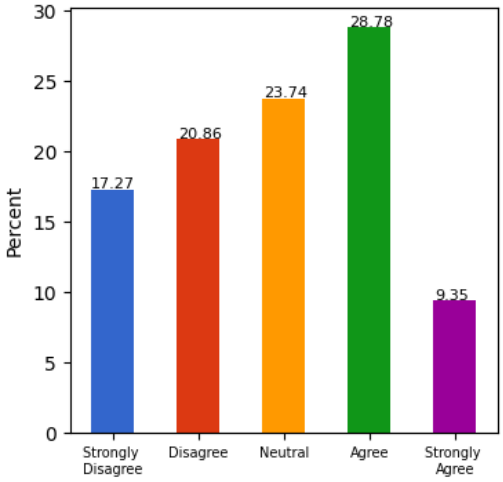


Figure 25. You post your vacation pictures during the vacation itself with a location tag

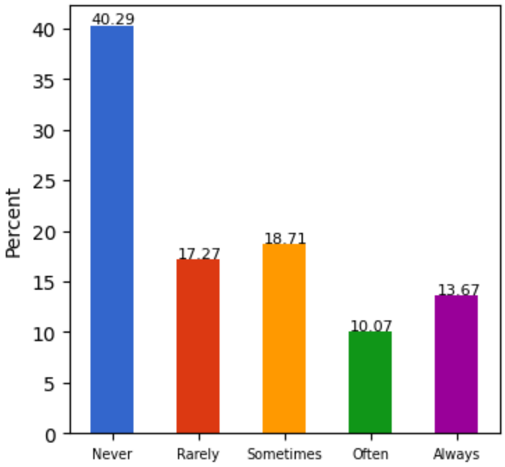


Figure 26. Before installing an app from App Store/Play Store/website, how often do you read the terms and conditions

4.6.3 User Behavior Question 3 (UQ3)

Figure 25 shows that most students either agree (28.78%) or are neutral (23.74%) about posting vacation pictures with location tags during the vacation itself. However, many students disagree (20.86%) or strongly disagree (17.27%) with this practice. However, 9.35% of the students strongly agree with the same. It shows people have different opinions on sharing vacation pictures in real-time. This is concerning and needs improvement because posting your vacation photos in real-time with location tags reveals your location and may expose you to theft or burglary.

4.6.4 User Behavior Question 4 (UQ4)

Figure 26 shows that most students (40.29%) never read the terms and conditions before installing an app from the App Store/Play Store/website. 17.27% rarely read them, while 18.71% sometimes read them. Only 13.67% always and 10.07% often read them. This is concerning because failure to read the terms and conditions may result in ignorance of some terms, which may say that the application or software will share personal data with third parties or process the personal data. This aspect of user behavior needs significant improvement.

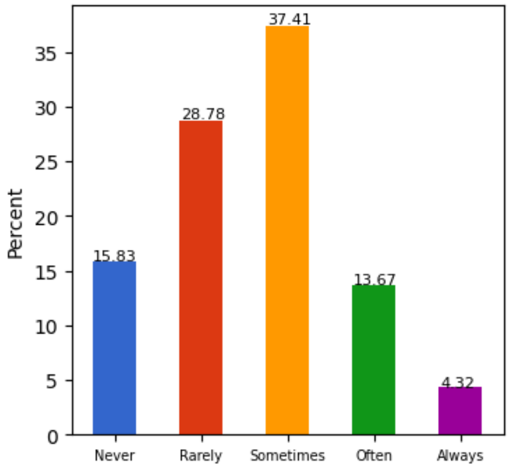


Figure 27. How often have you installed any third-party application from external sources?

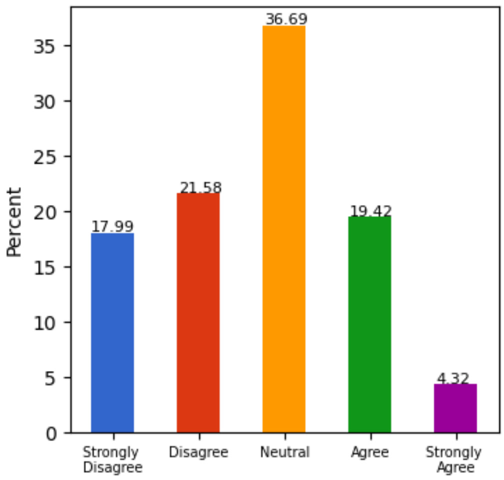


Figure 28. You grant all the devices permissions the application will use while installing the application

4.6.5 User Behavior Question 5 (UQ5)

Figure 27 shows that most students (37.41%) occasionally install any third-party application from external sources, followed by 13.67% who do so frequently and 4.32% who always do so. However, 28.78% of the students rarely and 15.83% never install any third-party application from external sources. This needs improvement because not all third-party sources are reliable. In addition, some may contain malicious or modified applications that could harm your device or steal your personal information.

4.6.6 User Behavior Question 6 (UQ6)

According to Figure 28, most students (36.69%) are neutral regarding granting all device permissions when installing an application. However, a significant portion disagreed

(21.58%) or strongly disagreed (17.99%). A smaller percentage agreed (19.42%) or strongly agreed (4.32%) on granting all permissions. These findings indicate that students' comfort levels with granting application permissions vary, highlighting the importance of educating users on the potential risks of such practices. Allowing every permission when installing apps is risky because it may give the app access to your data and device features that it does not require to function correctly.

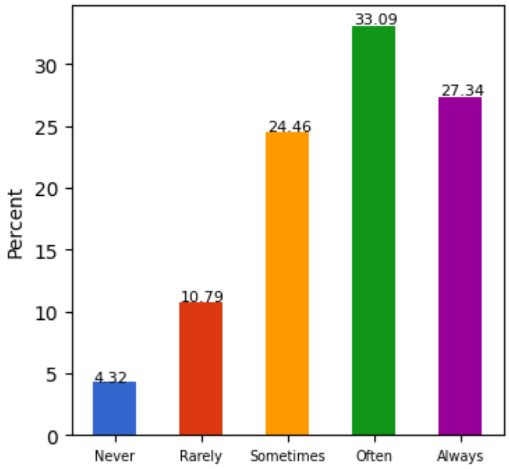


Figure 29. How frequently do you update and install the latest security updates for your devices?

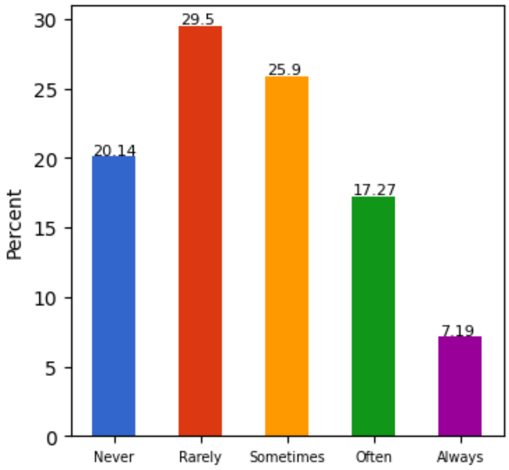


Figure 30. How often do you access your personal emails on school/work computers?

4.6.7 User Behavior Question 7 (UQ7)

Figure 29 shows that most students install security updates on their devices often (33.09%) or always (27.34%). However, 10.79% of the students rarely and 4.32% never update their devices. Meanwhile, almost a quarter of students (24.46%) reported updating their devices sometimes. These results suggest that while many students prioritize security updates, many still neglect them, leaving them vulnerable to potential security breaches.

According to M10 responses, almost 29% of Malaysian students agree with applying security patches as soon as possible, with 25% disagree [4]. As stated before, most Delhi students install security updates often or always, with only 4.32% never installing security updates. Comparing the statistics, Delhi students seem more aware of the risks of not updating devices than Malaysian students.

4.6.8 User Behavior Question 8 (UQ8)

According to Figure 30, most students access their personal emails on school or work computers rarely or never. However, about a quarter (25.9%) access their personal emails sometimes. In comparison, a smaller percentage (24.46%) access them often or always, which needs improvements because accessing personal emails on school or work computers can be dangerous as it may violate your school or workplace's policies. In addition, they may be able to monitor your communications.

4.6.9 User Behavior Question 9 (UQ9)

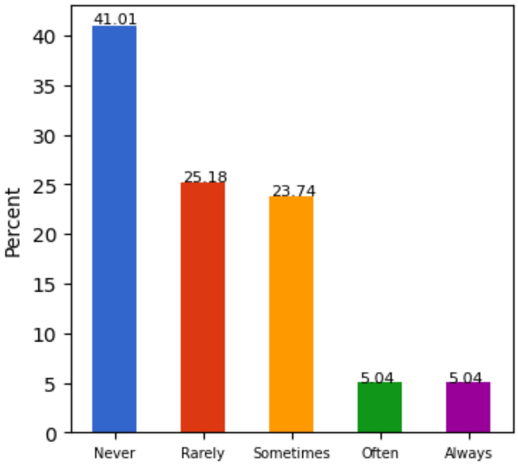


Figure 31. How often do you install any third-party software on school/work computers?

Figure 31 shows that 41.01% of students reported never installing third-party software on school or work computers. 25.18% reported doing so rarely, while 23.74% install third-party software sometimes. Only 5.04% of the students always and often install third-party software on school or work computers. It can be said that students are aware of the risks.

4.7 Cyber Security Training

The purpose of this section was to ask students if they had any prior training related to cyber security, as well as their preferred platform of cyber security training if they wanted to attend one, and finally, to write their emails if they wanted to participate in future research surveys. Finally, the emails will be used to contact the students for a post-training survey.

Variable	Response	%
Prior studies or training related to cybersecurity	Yes	30.94
	No	51.08
	Maybe	17.99
Preferred platform for attending training	Self-study through online study materials	16.55
	Online Lectures	32.37
	Short Video (5-7 mins)	51.08

Table 10. Responses for cybersecurity training questions

Table 10 shows that approximately 30.94% of students have prior cybersecurity study or training, while the majority, 51.08%, do not. The remaining 17.99% are unsure if they have any prior cybersecurity knowledge. This data suggests that a sizable portion of the population may lack cybersecurity knowledge due to no cybersecurity training, emphasizing the need for more education and awareness.

The majority of students (51.08%) prefer short 5–7-minute videos for cybersecurity training, according to Table 10. 32.37% of students prefer online lectures with varying lengths, while 16.55% prefer self-study using online study materials. These findings indicate that shorter, more digestible content is preferred over extended, traditional lecture formats. The short videos' popularity can be attributed to their ease of use and ability to fit into busy schedules.

4.8 Comparison with Malaysian students

The questionnaire for this thesis shared many similar questions to the Muniandy et al. questionnaire [4]. As stated before, the researcher and the expert believe that the questions used in Muniandy et al. study can be standard and not exclusive to the Malaysian demographic. The responses to questions common with Muniandy et al. questionnaire [4] are in Appendix 1. Furthermore, these common questions can be asked of Delhi students. Therefore, the observations and comparisons of 128 Malaysian and 139 Delhi students' responses to questions common to both studies were made.

A similar pattern was observed in response to question M1 compared to Delhi students' responses, showing similar cybersecurity awareness levels among Malaysian and Delhi students.

The responses to questions M2, M7, M9, M10, P3, P4, and P5, P7, Ph1, Ph6, Ph10, and Ph8, compared with Delhi students' responses, revealed that Delhi students are more aware of cybersecurity than Malaysian students.

M7, P2, Ph3, S2, and S6 responses, compared with responses of Delhi students, revealed that Malaysian students are more aware than Delhi students.

One limitation is that comparison with Muniandy et al. study [4] may not be accurate with today's standards because the Malaysian study [4] was conducted in 2017, and there might be an improvement in the cybersecurity awareness levels of Malaysian students by now.

Overall, it was discovered that Delhi students are more aware than Malaysian students in most aspects. However, the Delhi students appear to have an average level of cybersecurity awareness, as seen from the responses. This may be because most of the students have not attended any training related to cybersecurity, as seen earlier from the responses. Improvements can be made with the help of a pilot run of short cyber security training. Any changes in cybersecurity awareness can be assessed after the training through a questionnaire and compared to the previous responses to see if there is any improvement in cybersecurity awareness among Delhi students.

5 Cybersecurity Awareness Training

This chapter discusses the short cybersecurity training developed by the researcher as a pilot experiment. It has been observed that many people become victims of various cybercrimes due to a lack of cyber awareness. As a result, we all must have a basic understanding of cybersecurity best practices to protect ourselves and our organizations from cyber threats, which can help prevent cybercrimes. Therefore, rather than simply making recommendations to students, and given that almost half of the students have not attended any training on cybersecurity as reported in the questionnaire results, the researcher attempts to educate them through brief cybersecurity awareness training, designed using the input from the questionnaire results.

In a recent study by Reeves et al. [55], the researcher examined employee responses to a series of Security Education Training and Awareness (SETA) videos. The participants reported the following things [55]:

- Videos moved too quickly for some participants to keep up with the content or were too lengthy, resulting in dullness [55].
- Videos lacked any introduction or context [55].
- Videos took too long to get to their point, and some videos were too long [55]. Videos which were short, simple, and informative were more positively received [55].
- The style of presentation seemed outdated. Some videos were deemed lower quality than others, with common complaints that they lacked visual appeal [55].
- Because participants believed that the presented cyberattack would never happen to them, they were unmotivated to adopt the suggested mitigation behavior [55].
- While relevant, the information was too advanced for some participants' current understanding [55].
- Features that made videos more engaging include the use of relevant/interesting statistics, the appropriate (but not overpowering) use of fear, a sense of interactivity with the content, and the avoidance of simply lecturing the viewer [55].

According to the study's findings, themes in the content, design, and style of cybersecurity training videos are essential in explaining employee appraisal and engagement [55]. Furthermore, multiple themes were acknowledged unrelated to the videos, such as the employees' perceptions of the intended audience and their general biases of cybersecurity principles [55]. The findings also show that some employees will form an opinion about the corporate motivations whenever they are exposed to any SETA program [55]. These viewpoints may influence their comprehension of the material [55]. The researcher of the current study believes that a similar perception can be applied to university students.

The researcher has developed a short cybersecurity training as a pilot experiment or an alpha version based on SAM which also tries to cover the observations made by participants in the study by Reeves et al. [55]. This section will review the SAM model’s three stages, as seen in Figure 32, in context with this cybersecurity training.

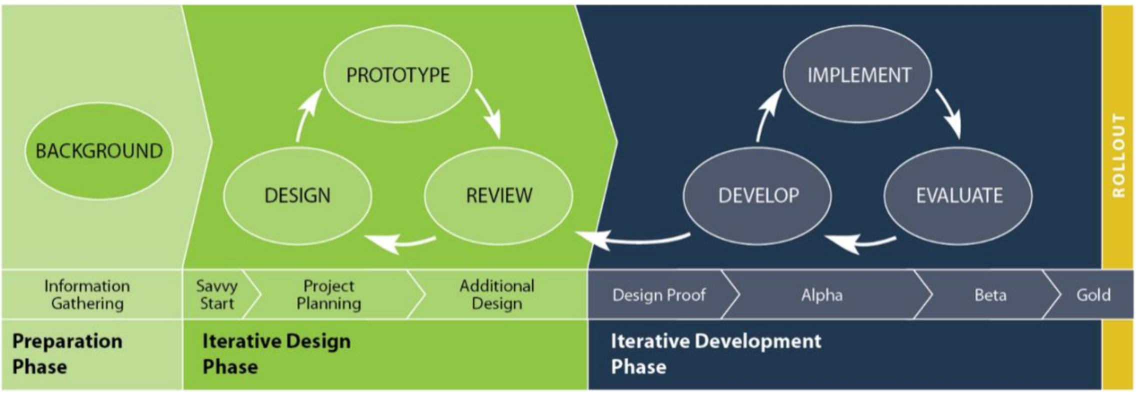


Figure 32. Successive Approximation Model [3]

5.1 Preparation Phase

SAM begins by gathering all relevant project information and background knowledge. This phase aims to gather all the needed information, assign and analyze roles, and understand learners’ needs (Sites & Green, 2014, as cited in Jung et al. [54]). The conclusion of the first phase of this model is referred to as a "savvy start". As you develop the material, engage as many interested parties as possible in brainstorming, sketching, and prototyping [3]. The Pre-Training questionnaire is the first step in this Preparation Phase, and utilized to gather the necessary information from the students. Following that, a training structure is required in this phase.

The researcher, in this phase, added an external expert. Dr. Farzana Munawwar is an Assistant Professor, having more than 13 years of experience teaching at the university level in India.

The expert's contribution to the creation of training was assisting in defining a structure for the training, including learning objectives and identifying and suggesting improvements in the training to the researcher to solidify the training as possible through telephonic interviews.

Given that nearly half of the students preferred to attend training that was short videos ranging from approximately 5-7 minutes, the short cybersecurity training was designed to be bite-sized learning modules that were short videos. As for the platform for these videos, initially, it was decided to upload them to Google Drive and share the link with the students.

The training content primarily covers the topics covered in the questionnaire and will extend to some topics according to the training structure. Initially, ten videos based on topics covered in the questionnaire were planned. However, the expert suggested reducing the number of videos as the students might prefer fewer videos, and ten videos might make them lose interest in the topic. Finally, it was decided to use five videos on each awareness topic: Malware, Phishing, Password Attacks, Social Engineering, and User Behavior. Each training video includes a definition of the topic with some explanations, different types if applicable, real-life cases related to the topic if applicable, and precautions to be taken to protect yourself.

The initial learning objectives of the training were discussed with the expert and stated in Table 11.

Topic	**Learning Objective**
Malware Awareness	The students will learn about ● what malware is ● how malware is spread ● different types of malwares and how to differentiate between them

	● precautions to take to protect themselves from malware
Phishing Awareness	The students will learn about ● what phishing is ● how to detect lousy formatting, fake and masked links in emails ● how to detect phishing attempts that involve impersonation, fear tactics, and email attachments
Password Attacks Awareness	The students will learn about ● what password attacks are ● different types of password attacks and how to differentiate between them ● importance of 2FA and password managers ● some other precautions to protect yourself from password attacks
Social Engineering Awareness	The students will learn about ● what social engineering is ● different tactics used in social engineering and how to differentiate between them ● how to detect social engineering attempts and take precautions to protect themselves from social engineering attacks
User Behavior Awareness	The students will learn about ● different user behaviors that can potentially affect cybersecurity and precautions that can be taken to protect themselves

Table 11. Learning Objectives

5.2 Iterative Design

In this phase of SAM, the goal is to design the first iteration of training so that the students can evaluate it and the changes can be incorporated to improve the course. According to (Sites & Green, 2014, as cited in Jung et al. [54]), all design, prototyping, and evaluation rotate iteratively in small steps. A crucial step in the design phase is prototyping since each evaluation results in the development of several prototypes (Sites & Green, 2014, as cited in Jung et al. [54]). A similar approach was taken in designing this short cybersecurity training.

The training was created using Microsoft PowerPoint presentations. Initially, it was planned to use automated voice for teaching and explanations. However, after consulting with the expert, it was decided that the researcher would record their voice because it can help make the training more conversational, which can help increase engagement [56].

The first prototype was based on 'Malware Awareness' and was pilot tested on five students who indicated an interest in participating in this training via questionnaire responses. Students gave feedback saying the conversational style was engaging. However, too much text and insufficient graphics made the presentation appear like a short lecture, which would not be an excellent way to engage students. Students also reported that the video was not viewable directly in Google Drive due to the large storage size of the video, so they had to download the video, which is not ideal. The expert recommended using YouTube to share the finalized training videos because, firstly, it will be easy to share and view, and also, it can help see how many people have viewed the training.

The second prototype was based on the same topic, but the slides were improved with as little text as possible and more graphical elements, such as adding Graphics Interchange Format (GIF) images, to help students understand the context of the topic. Jung et al. [54] also used multimedia such as images and GIF files in order to decrease the cognitive overload. The second prototype was tested with the same students. Students provided positive feedback, but they expressed a lack of motivation to follow the precautions outlined in training. After discussion with the expert, adding real-life cases related to the topic was decided to help with the motivation. A recent study by Gero et al. [57] discovered a significant difference in intrinsic motivation to study between electrical engineering students who attended the course that included real-world examples and those who completed the course in its original format, without examples, with the former outperforming the latter. The supervisor and the expert also suggested making the training in the native language as well, which may provide a better understanding of the topic to the students. The first official languages of Delhi are Hindi and English [58]

The learning objectives were updated prior to the final iteration's rollout due to the addition of teaching real-life examples. Table 12 contains the updated learning objectives.

Topic	**Learning Objective**
Malware Awareness	The students will learn about ● what malware is ● how malware is spread ● different types of malware and how to differentiate between them ● three real-life cases which involve malware ● precautions to take to protect themselves from malware
Phishing Awareness	The students will learn about ● what phishing is ● four real-life cases which involve phishing ● how to detect lousy formatting, fake and masked links in emails ● how to detect phishing attempts that involve impersonation, fear tactics, and email attachments
Password Attacks Awareness	The students will learn about ● what password attacks are ● different types of password attacks and how to differentiate between them

	● five real-life data breach cases which involve password attacks ● importance of 2FA and password managers ● some other precautions to protect yourself from password attacks
Social Engineering Awareness	The students will learn about ● what social engineering is ● different tactics used in social engineering and how to differentiate between them ● how to detect social engineering attempts and take precautions to protect themselves from social engineering attacks
User Behavior Awareness	The students will learn about ● different user behaviors that can potentially affect cybersecurity and precautions that can be taken to protect themselves

Table 12. Updated Learning Objectives

5.3 Iterative Development

The finished prototype is developed and implemented during this Iterative Development phase [3]. Once used, it can be evaluated and, if necessary, re-run through the development and implementation phases [3]. An instructor can use an Iterative Development phase to use feedback directly from students to continuously reevaluate the design of the online course to meet the needs of the student [59].

The training was uploaded to YouTube after receiving initial feedback from pilot testing the prototype with a small group of students and suggestions from the expert and supervisor. The training included two playlists, English and Hindi language, each with five videos on the topics above.

Students who shared their email addresses in the initial questionnaire responses received an email containing both the playlists and the post-training questionnaire for the course evaluation. This will help us understand if this alpha training improved the students' cybersecurity awareness.

The playlist containing the Hindi version of the training has 106 views compared to its English counterpart, which has 73 views showing the students preferred the training, which the researcher believes may lead to a better understanding of the concepts since Hindi is the native language.

Links for both the playlists are attached below:

YouTube Playlist for Cybersecurity Training in English

https://youtube.com/playlist?list=PLH33dhtocINmZ2FGS1PSBm-cyhZVhzQCM

YouTube Playlist for Cybersecurity Training in Hindi

https://youtube.com/playlist?list=PLH33dhtocINlcyIaJpiRGWHvh6sl8OQk2

As previously stated, SAM employs a recursive rather than a linear process for course development, so the presentation files in the link below for any future improvements or developments in training.

Presentation Files Link:

https://drive.google.com/drive/folders/1D32813CIb0g7it8kzbxEdQHvsAWvYI_Q?usp=sharing

5.4 Post-Training Questionnaire

To see if there were any improvements in the students' cybersecurity awareness levels, a post-training questionnaire was developed with the help of the same industry expert. The post-training questionnaire asked the same questions as the pre-training questionnaire. However, it was slightly modified to see if they would have the same behavior to issues in the future and check if the training impacted the cybersecurity awareness of the students who attended the training.

The post-training questionnaire contains 15 questions in total. These are questions nearly identical to those asked in the pre-training questionnaire, where the researcher observed and concluded that students need improvement.

The responses are again collected on a 5-point Likert Scale to compare responses from post-training questionnaires with the corresponding questions in pre-training questionnaires.

Table 13 contains all the questions used in the post-training questionnaire.

S.No.	Post-Training Questions
PT1.	Will you open an email attachment because of the intriguing subject line?
PT2.	How frequently will you scan your files whenever you insert a flash drive or download files from any website or email attachment?
PT3.	Will you still proceed to the websites whose website certificate is expired or invalid?
PT4.	How frequently are you willing to keep different passwords for different accounts?
PT5.	How frequently will you set up 2-factor authentication for accounts?
PT6.	How frequently will you change passwords for your accounts?
PT7.	Will you click on hyperlinks in every email message?
PT8.	How often will you prefer to type the URL in the new browser rather than clicking it on a hyperlink?
PT9.	How often will you check the sender's email address before opening an email?
PT10.	Will you post your vacation pictures with location tags during the vacation itself?
PT11.	How often will you read the terms and conditions before installing an app?
PT12.	How often will you install any third-party apps from external sources?
PT13.	Will you grant all the device permissions while installing the application?
PT14.	How often will you access your personal emails on school/work computers?
PT15.	Would you like to give feedback or comments about the training or questionnaire? The feedback or comment will be used to improve the course content or presentations for the future.

Table 13. Post-Training Questions

5.5 Post-Training Questionnaire Responses

The Post-Training Questionnaire received 27 responses to date, based upon which a comparison between the previous pre-training and post-training questionnaires is made. The responses to this questionnaire are stored as a CSV file in the following link:

Post-Training questionnaire responses:

https://drive.google.com/file/d/1L7_ovy3xUTeuymrrZwy5HENV9vmatYvj/view?usp=share_link

5.5.1 Post-Training Question 1 (PT1)

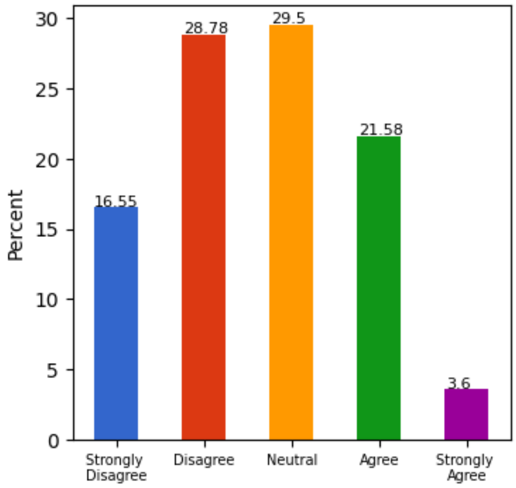


Figure 3. You open an email attachment because of the intriguing subject line

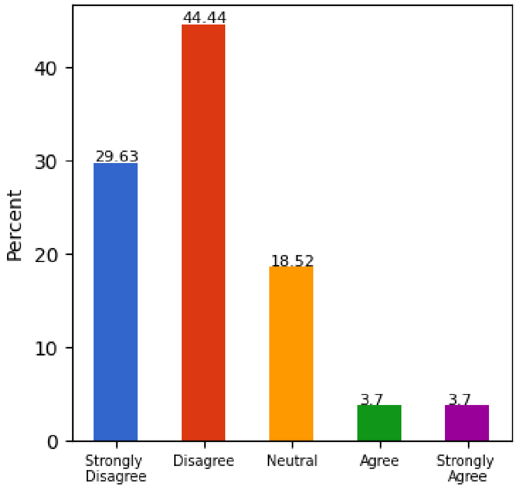


Figure 33. Will you open an email attachment because of the intriguing subject line?

Figure 33 shows that nearly 75% of students strongly disagree or disagree with opening an email attachment because of intriguing subject lines in the future. In contrast, nearly 45% previously disagreed or strongly disagreed on the same topic before training as seen in Figure 3. As observed, there is a nearly 30% improvement. Furthermore, 29.5% of neutral students on the take have decreased to only 18.52%, and 21.58% who agreed previously have decreased to 3.7%. The students who were previously neutral and agreed with the statement have shifted to those who disagree and strongly disagree.

5.5.2 Post-Training Question 2 (PT2)

Before training, most Delhi students responded that they never or rarely scanned their files when inserting a flash drive or downloading files from the internet. Only a tiny percentage reported doing so always or often as seen in Figure 6. However, as seen in Figure 34, there was a significant shift in these responses, with no one reporting that they would never scan their files anymore. Instead, most students reported they would scan their files often (40.74%), showing a 20% increase and a decrease in those who responded 'rarely.'

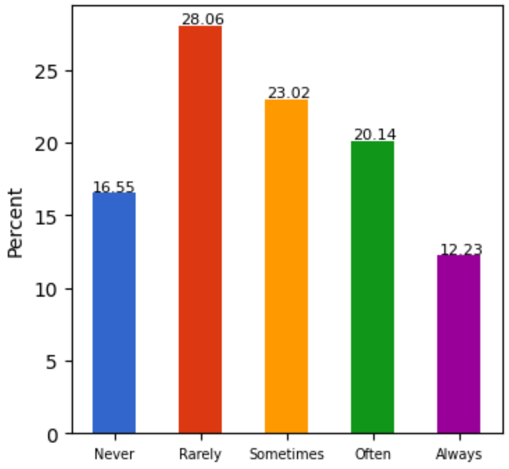


Figure 6. How often do you scan your files whenever you insert a flash drive or download files from any website or email attachments?

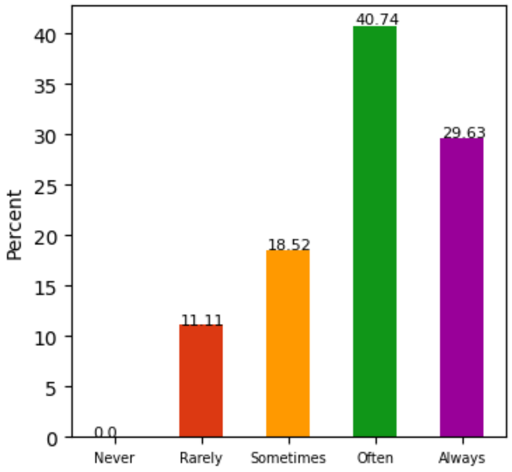


Figure 34. How frequently will you scan your files whenever you insert a flash drive or download files from any website or email attachment?

5.5.3 Post-Training Question 3 (PT3)

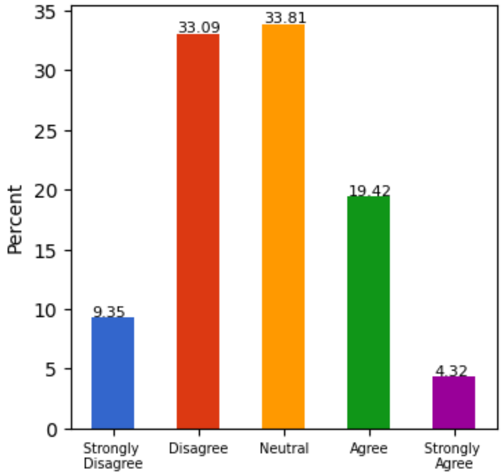


Figure 7. In case the website certificate is expired or invalid for your most visited websites, will you still proceed to such websites?

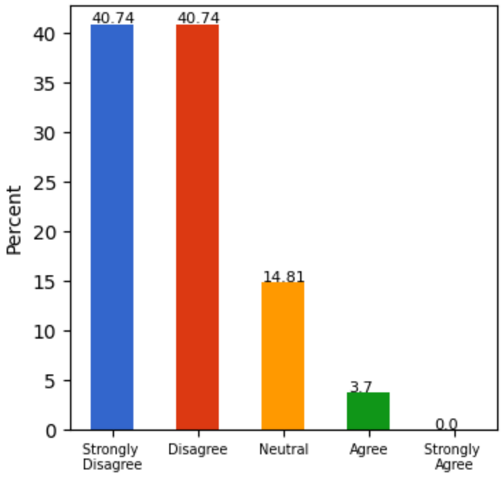


Figure 35. Will you still proceed to the websites whose website certificate is expired or invalid?

Before training, most Delhi students hesitated to proceed to websites with expired or invalid certificates, with 42.44% indicating disagreement or strong disagreement. However, a significant percentage (33.81%) remained neutral. After training as per Figure 35, 81.48% indicated strong disagreement or disagreement towards the same in the future. Also, after training, there was a significant reduction in the percentage of people with a neutral take on this statement.

5.5.4 Post-Training Question 4 (PT4)

According to Figure 9, before training, most Delhi students (30.22%) reported consistently using the same password for different accounts, while only 7.91% said they never did so. However, after training, the percentage of student responses for the same statement reduced to 0%, and those who reported doing it rarely decreased to 3.7%, as seen in Figure 36. Meanwhile, the percentage of students who reported 'often' for the same increased to 44.44%, indicating a positive shift in their password management habits.

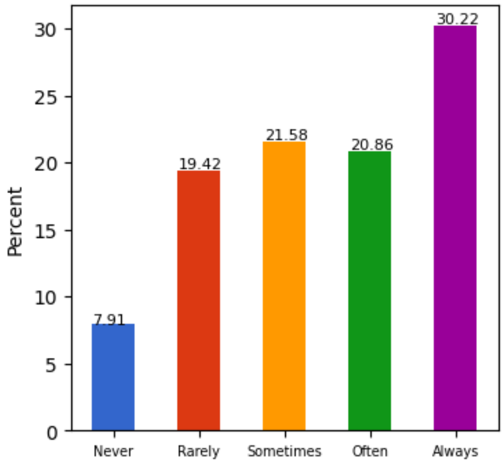


Figure 9. You keep different passwords for different accounts

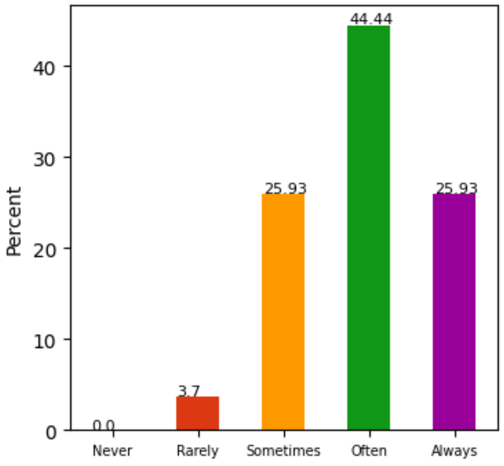


Figure 36. How frequently are you willing to keep different passwords for different accounts?

5.5.5 Post-Training Question 5 (PT5)

Before training, most Delhi students (31.65%) reported only setting up two-factor authentication sometimes, while 25.9% reported always using it. Only 5.04% reported never using it. However, there is a significant change after training, with 48.15% reporting they would use two-factor authentication often and 37.04% always. The percentage of students who would never use it dropped to 0%, indicating that the training positively impacted their security habits. There was also a decrease from 17.99% to 3.7% of students who reported they would rarely use it.

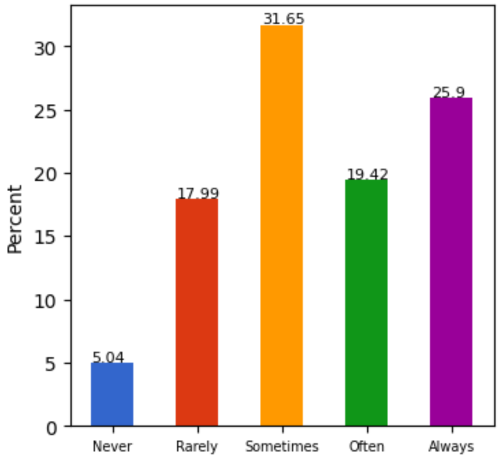


Figure 11. You set up 2-factor authentication for accounts other than passwords

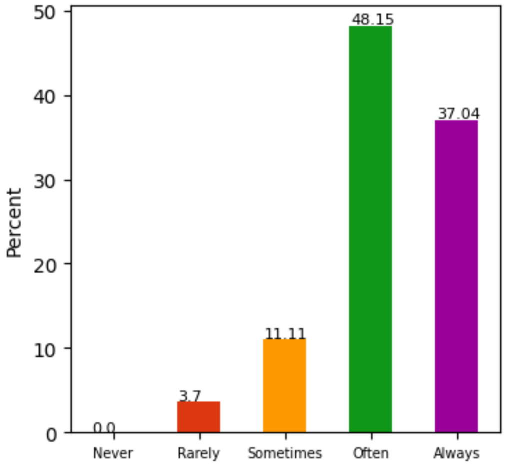


Figure 37. How frequently will you set up 2-factor authentication for accounts?

5.5.6 Post-Training Question 6 (PT6)

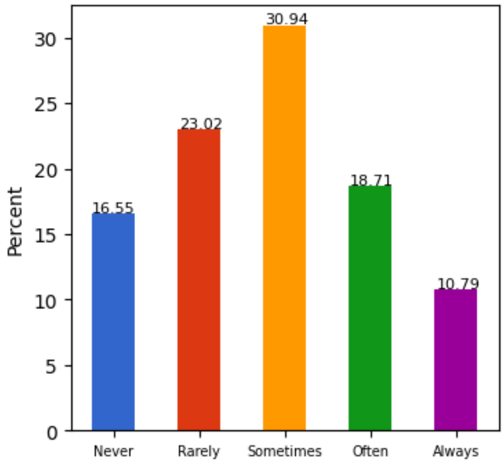


Figure 12. Do you frequently change passwords for your accounts, including your Internet banking?

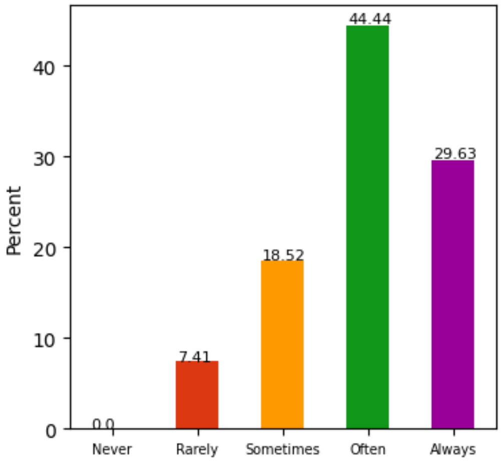


Figure 38. How frequently will you change passwords for your accounts?

Before the training as seen in Figure 12, many Delhi students reported either never changing their passwords or only changing them rarely or sometimes. In contrast, after the training as observed in Figure 38, no one reported that they would never change their passwords, and the majority reported they would be changing them either often or constantly. This suggests the training positively impacted students' attitudes and behaviors toward password security.

5.5.7 Post-Training Question 7 (PT7)

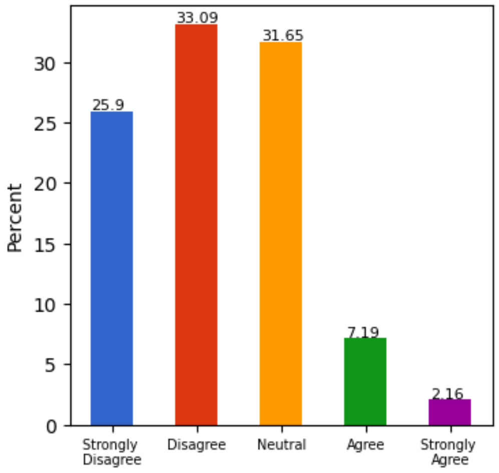


Figure 13. You should click hyperlinks in every email message.

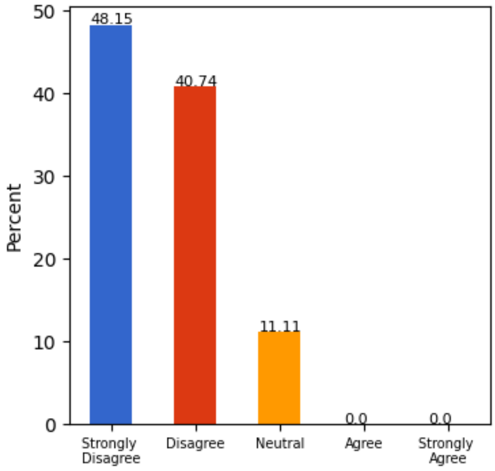


Figure 39. Will you click on hyperlinks in every email message?

Before training, 58% of Delhi students hesitated to click hyperlinks in email messages by either disagreeing or strongly disagreeing with the statement. Only a tiny percentage (9.35%) agreed to the same. However, as seen in Figure 39, after training, there was a significant shift in attitudes, with almost 90% of students now disagreeing and none agreeing with doing the same in the future. This indicates that the training positively impacted their understanding of email safety and cybersecurity, leading to a more cautious approach when interacting with email messages.

5.5.8 Post-Training Question 8 (PT8)

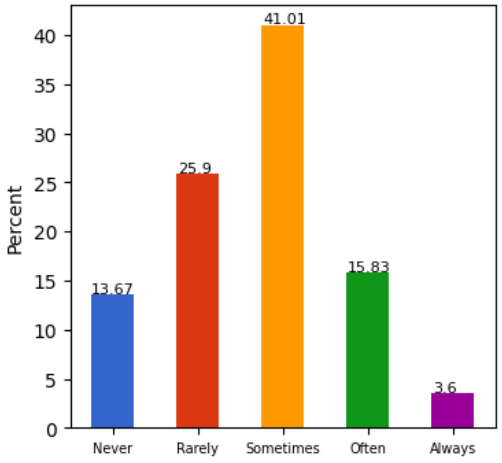


Figure 15. How often do you prefer to type the URL in the new browser tab rather than clicking it on the hyperlink?

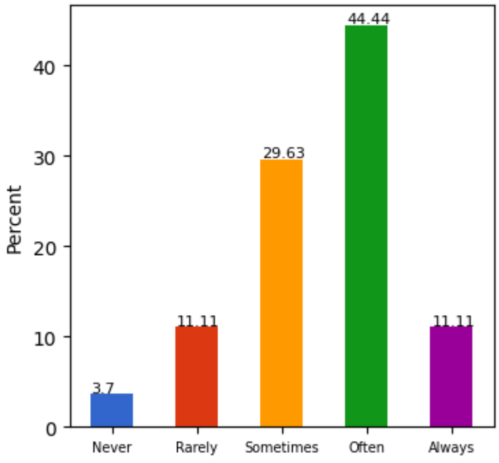


Figure 40. How often will you prefer to type the URL in the new browser rather than clicking it on a hyperlink?

Most Delhi students preferred to click on hyperlinks rather than typing URLs, with 41.01% doing so sometimes, with only 3.6% of students constantly typing URLs before the training. However, after the training, 44.44% of students reported they would often type URLs instead of clicking hyperlinks, as seen in Figure 40. In addition, the percentage of students who reported never or rarely typing URLs in the future also decreased, while the percentage of those who will now sometimes type URLs increased slightly.

5.5.9 Post-Training Question 9 (PT9)

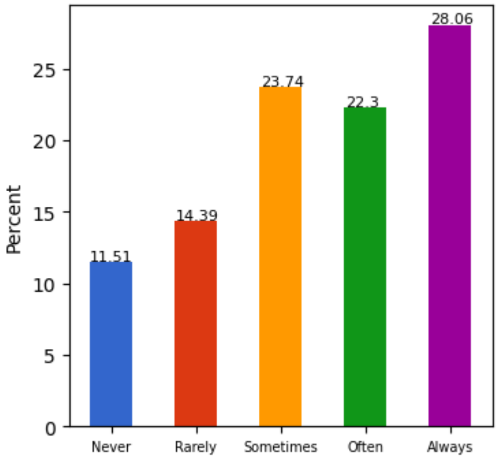


Figure 16. How often do you check the sender's email address before opening an email?

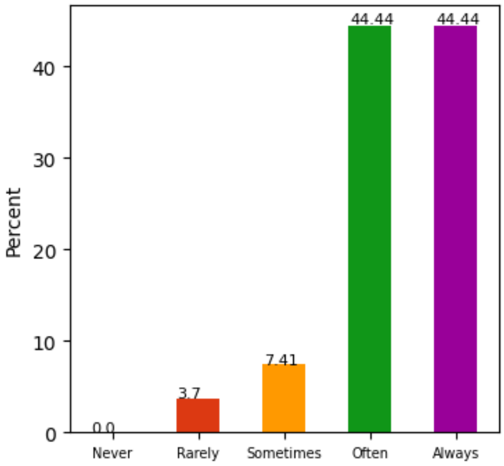


Figure 41. How often will you check the sender's email address before opening an email?

Before the training, most Delhi students did not check the sender's email address before opening emails. Only 28.06% always checked the sender's email, while 25.9% rarely or never did. However, as seen in Figure 41, there was a significant increase in students who reported that they would check the sender's email address after training. 44.44% of students reported they would check for the same often or always in the future, while the percentage of those who will never check dropped to 0%.

5.5.10 Post-Training Question 10 (PT10)

Before the training, a significant proportion of Delhi students expressed some level of agreement with posting vacation pictures with location tags during their vacation, with around 38% expressing agreement or strong agreement. However, after training, the proportion of students agreeing or strongly agreeing with the statement has dropped to 3.7% collectively. Also, the percentage who 'disagree' or 'strongly disagree' increased to nearly 78%, as seen in Figure 42.

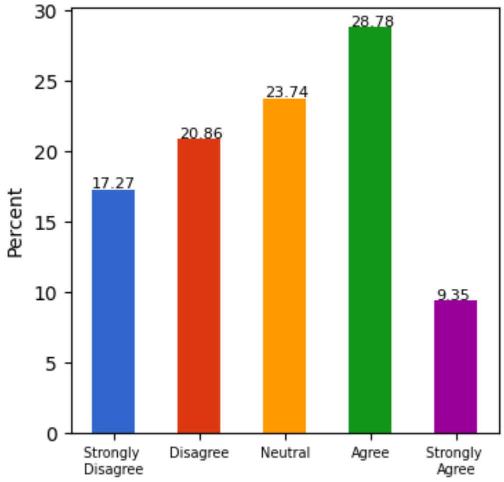


Figure 25. You post your vacation pictures during the vacation itself with a location tag

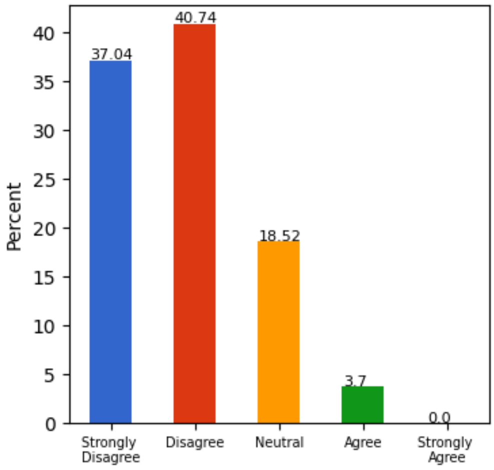


Figure 42. Will you post your vacation pictures with location tags during the vacation itself?

5.5.11 Post-Training Question 11 (PT11)

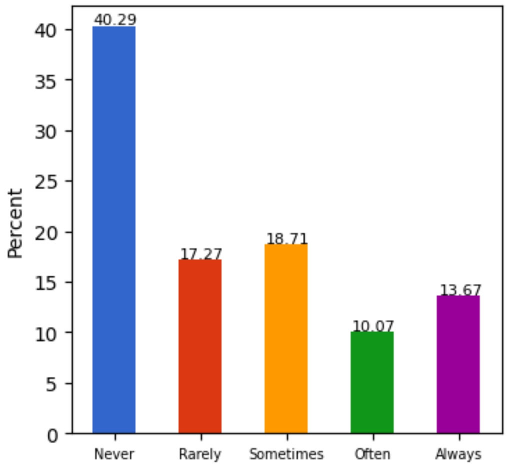


Figure 26. Before installing an app from App Store/Play Store/website, how often do you read the terms and conditions?

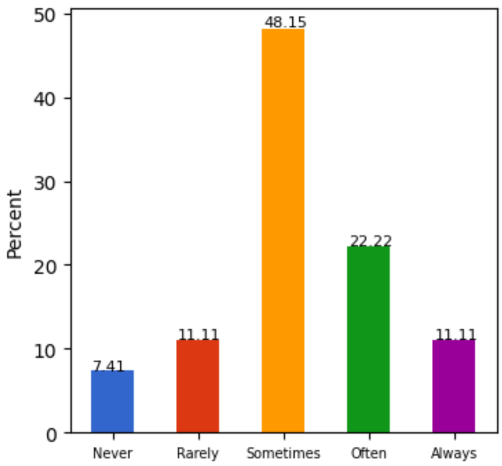


Figure 43. How often will you read the terms and conditions before installing an app?

Before the training, 40.29% of Delhi students admitted to never reading the terms and conditions before installing an app, while only 13.67% claimed always to read them. After the training, the percentage of students who will never read the terms and conditions decreased drastically to 7.41%, while the percentage of those who will sometimes read them increased to 48.15%, as seen in Figure 43. The percentage of students who may often read them also increased to 22.22%. The percentage of students who will always read them in the future remained almost the same as before.

5.5.12 Post-Training Question 12 (PT12)

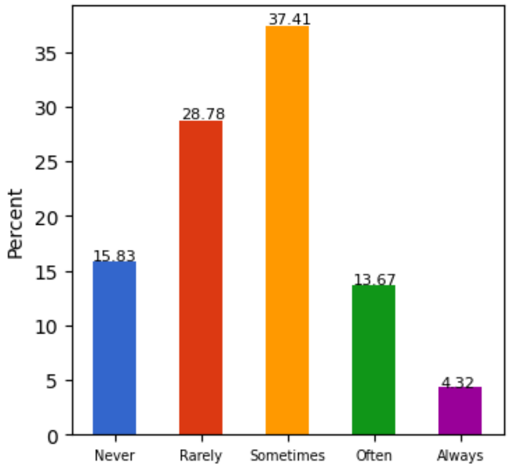


Figure 27. How often have you installed any third-party application from external sources?

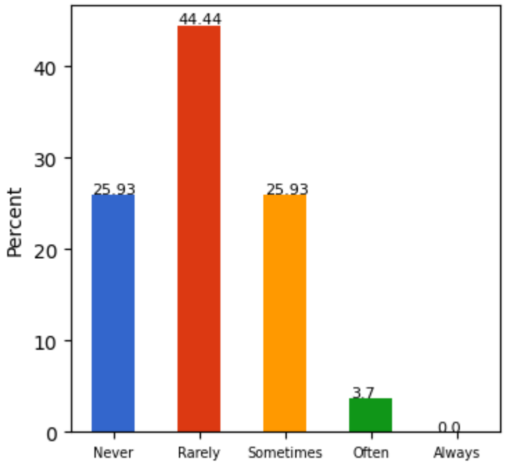


Figure 44. How often will you install any third-party apps from external sources?

Based on the pre-training survey of Delhi students, 15.83% reported never installing third-party apps from external sources. Almost 29% reported doing it rarely, 37.41% sometimes did, 13.67% often did, and 4.32% always did the same as observed in Figure 27. After the training, as seen in Figure 44, the percentage of students who will never install third-party apps from external sources increased to 25.93%, while the percentage who rarely do increase to 44.44%. The percentage of students who will sometimes decrease to 25.93%, while the percentage who will often do the same decrease to 3.9%, and no students reported they will always install third-party apps from external sources.

5.5.13 Post-Training Question 13 (PT13)

Before the training, most Delhi students were neutral or disagreed with granting all device permissions while installing an application. However, a significant percentage agreed or strongly agreed with this statement. After the training, there was a clear shift in opinions, with a higher percentage of students disagreeing or strongly disagreeing with granting all device permissions in the future. The proportion of neutral students also decreased, while the proportion who strongly agreed dropped to zero, as seen in Figure 45.

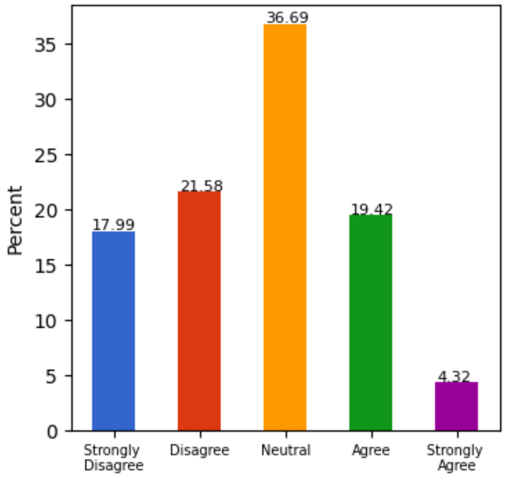


Figure 28. You grant all the devices permissions the application will use while installing the application.

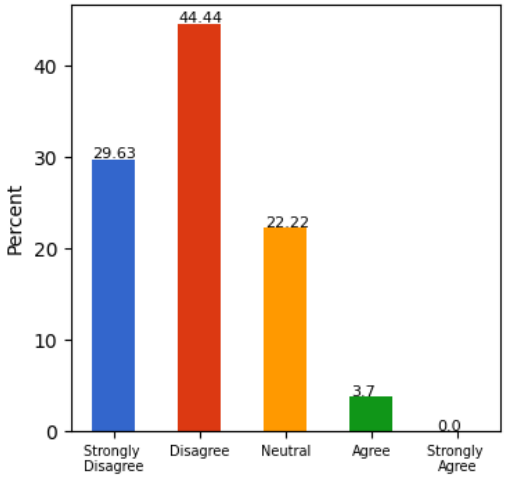


Figure 45. Will you grant all the device permissions while installing the application?

5.5.14 Post-Training Question 14 (PT14)

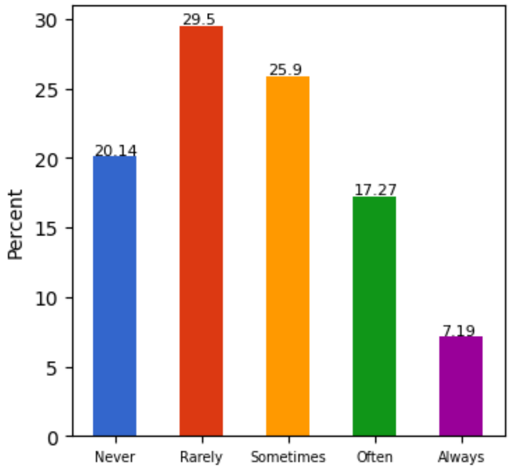


Figure 30. How often do you access your personal emails on school/work computers?

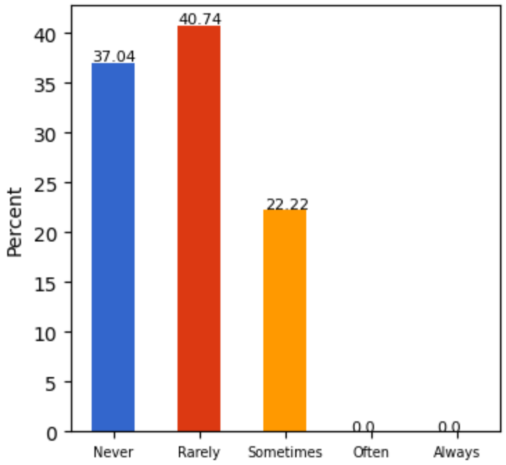


Figure 46. How often will you access your personal emails on school/work computers?

The pre-training questionnaire showed that most students rarely or never accessed their personal emails on school/work computers, with 20.14% never accessing and 29.5% rarely accessing. Only a small percentage (7.19%) reported consistently accessing their emails. As seen in Figure 46, after the training, the percentage of students who reported never accessing their personal emails on school/work computers in the future increased significantly to 37.04%. In contrast, the percentage of students who reported they would rarely do the same also increased to 40.74%. The percentage of students who reported sometimes accessing their personal emails in the future decreased to 22.22%, while no students reported often or always for the same.

5.5.15 Post-Training Question 15 (PT15)

Only five helpful responses were collected as feedback to either training or questionnaire. The five feedback comments are listed below:

Participant 7: “The course was constructed in a way that it clarifies a lot of doubts and usual practices that was ignored before and made me aware about a lot of potential risks within the internet world.”

Participant 10: “The training was useful to understand the impact of smallest mistake or habit of an individual online.”

Participant 11: “Voice quality can be improved in the videos”

Participant 24: “Overall, I found the questionnaire to be relevant.”

Participant 26: “This training provided some valuable suggestions and insights on the do’s and don'ts to maintain a better security posture. It is curated very well for the beginner who are often the main target for the attacker.”

6 Discussion

Key findings from the questionnaires and training could be summarized in following items:

- Responses from Pre-Training Malware awareness show that students are more likely to open email attachments due to interesting subject lines than from unknown people.
- A similar trend is seen from responses of Pre-Training Social Engineering awareness questions where it is observed that students often verify the identity of an unknown caller or email sender before providing any information and are comfortable in refusing to provide information to individuals who don’t have the authority to know it. Majority of the students also don't give out personal info such as username and password to those claiming to be system administrators, and therefore haven't been tricked into giving out that info. This results in majority of the students reporting they have never been tricked into giving out information.
- The students possess high Social Engineering awareness as per Pre-Training questionnaire. The hypothesis is that the most questions asked in Social Engineering awareness sections can also show awareness on online scams. Indian students have been taught early in schools regarding online scams and precautions which can be taken, due to which this result is influenced.
- According to the Pre-Training Password Awareness responses, which show nearly similar percentages, the majority of students sometimes change their passwords and set up 2FA other than passwords sometimes.
- It was discovered from Pre-Training questionnaire that while most students sometimes install third-party applications from external sources, they rarely scan their files whenever they insert a flash drive or download files from any website.
- As per Pre-Training questionnaire responses, majority of the students never share work-related data on social media but agree on sharing vacation pictures during the vacation itself with a location tag. This shows a sense of differentiation created by the students between work and social life.
- According to Pre-Training questionnaire responses, male students and non-IT students were more aware than female students and IT students, which could be due to more responses from one group than the other.

- Despite receiving fewer responses from female students than male students in the Pre-Training questionnaire, female students reported higher Malware awareness than male students.
- Almost exactly the same percentage of respondents strongly agree on opening email attachments with intriguing subject lines before and after training as per the Pre- and Post-Training questionnaire.
- Similar trend is observed in Post-Training questionnaire where students reported they will often and always keep different passwords for different accounts, will enable 2FA and will frequently change their passwords.
- According to Post-Training questionnaire responses, students will often prefer to type the URL in the new browser rather than clicking it on a hyperlink but not always. Exact same percentage of students is observed who will rarely or always prefer to type the URL in the new browser.
- The percentage of students who reported always reading terms and conditions in the Pre-Training Questionnaire has decreased by nearly 2% in the Post-Training Questionnaire.
- According to training video view counts, more students preferred to watch the Hindi version of the training than the English version. The combined views from the Hindi versions of the videos are 106, while the combined views from the English versions are 79. This demonstrates that Delhi university students prefer to learn in their native language, which may be in order to better understand the concepts.

The following are some comparisons of results of similar questions from different studies in India:

- Another study in Delhi [14] reported that nearly 80% of Delhi students agreed that reading terms and conditions is important, whereas current research contradicts showing that nearly 40% never read terms and conditions and 17% do so only occasionally as per Pre-Training questionnaire results.
- According to Chhibber and Thapar [14], 42% of students were either neutral or disagreed with giving device permissions when installing an application, with approximately 12% agreeing. According to the current study’s Pre-Training questionnaire results, nearly the same percentage of students disagreed or were neutral

on this point. Interestingly, nearly 23% of students agreed, which is nearly double what was reported earlier.

- The same study in Delhi [14] and another in Kochi [10] found that nearly 73% and 76% of students, respectively, had never lost money due to cybercrime, demonstrating good awareness of online scams and social engineering which is surprisingly, in line with current study's Pre-Training questionnaire results, considering the demographic and locations are totally different. This shows that both set of students are very aware of social engineering.
- According to Sreehari et al. [10], nearly 12% of Kochi students check the verification of websites, whereas the current study finds that nearly 54% of students agree on verifying the URL before entering any website as per Pre-Training questionnaire results. The same study reports that almost 60% of the students rarely change their passwords whereas this study reported before training that only 23% of the students do the same. As previously stated, this could be due to different demographics resulting in different mindsets and perspectives on cybersecurity hygiene and awareness.

One of the lessons learned from this study is that when different scales are used in different questionnaires, the parameters for comparing the findings of different studies can differ. Muniandy et al [4] uses 3-point Likert Scale whereas the current study uses 5-point Likert scale. This makes comparison of results difficult and may result in less accuracy during the comparative analysis. Furthermore, different studies use different questions in a questionnaire targeting different aspects of cybersecurity awareness, which could be due to demographic compatibility. Studies by Sreehari A et al. [10], Muniandy et al. [4], Khan et al. [30], and Chhibber and Thapar [14] attempt to assess respondents' cybersecurity awareness but use questionnaires that vary from study to study. This makes a full comparison with other studies difficult. This study suggests developing a streamlined or standardized questionnaire for assessing cybersecurity awareness, from which appropriate questions can be selected based on demographic compatibility. This can aid in increasing the efficiency of studies and the accuracy of comparative analysis, resulting in more trend analysis.

In comparison to studies that use more traditional instructional designs and models, there are fewer studies that use SAM to develop courses or trainings. Another lesson learned from this study is that non-traditional instructional designs can be effective as well. As a result, SAM could be used by different studies in the future and is a practical alternative to traditional instructional designs to design short online courses because it allows for quick changes based on student feedback and the creation of multiple courses based on the needs of the learners. A study also concluded that SAM was effective in terms of allowing agile revisions and meeting the needs of continuing learners throughout the course [54]. Short online courses help to increase engagement with students who are often working full-time and prefer a straightforward presentation of course material [59].

7 Conclusion and Future Work

7.1 Conclusion

This research analyzes university students’ knowledge of cybersecurity awareness in Delhi and attempts to improve their knowledge about it through training. The study’s main goal was to check the cybersecurity awareness level of university students of Delhi, compare the results with another study, and see if a short training based on SAM could impact the cybersecurity awareness of the students.

Following a review of the literature, it is concluded that quantitative analysis using a questionnaire can be used to assess cybersecurity awareness levels which answers the RQ1. The cybersecurity awareness of Delhi students was assessed using a newly designed questionnaire that was created by modifying, improving, and adapting an existing questionnaire [4] to be compatible with Delhi's demographics and also helps in reperforming similar questions on different demographic. The study concludes that when developing a new cybersecurity awareness measurement instrument, current common trends and demographic aspects should be taken into account which answers the RQ2 (c).

The responses of most of the questions were also compared with another study from Malaysia since they shared similarities. Although it was concluded that Delhi students had more cybersecurity awareness than Malaysian students, it was also concluded that Delhi students had an average level of cybersecurity awareness overall, answering the RQ2 (a), which could be due to the majority of the students having no prior cybersecurity training. The study also concludes that different cybersecurity awareness study results are comparable if the questions used in both studies are similar and scales are comparable which answers the RQ2 (b).

Based on the findings, cybersecurity awareness could be improved through training, so a short cybersecurity training was developed as a pilot test to improve Delhi students' cybersecurity awareness. With Iterative Design and Development phase in mind, training materials were kept available to the public, which can aid in expanding the current experimental short training if used as a foundation. SAM was used as an instructional design method to develop and implement this short cybersecurity training, making this study the first to use SAM as an instructional design method on Delhi students. The training was designed, and prototypes were made and tested on a small set of students for instant feedback.

The final training was uploaded in two languages on YouTube. The post-training questionnaire was developed with the help of an expert, which used some questions from the pre-training questionnaire to compare and see if there are improvements in the cybersecurity awareness of Delhi students. The responses showed a significant shift in attitudes. The training seems to have a positive impact and influenced students to be more cautious about the issues discussed which answers the RQ3 (b). The study concludes that SAM is an appropriate instructional design method for developing short but effective cybersecurity learning in changing environments, and that SAM-oriented short training sessions can be effective in raising student awareness which answers the RQ3 (a).

According to Statista, approximately four out of every ten internet users worldwide have experienced a cybercrime by the end of 2022 [60]. According to a survey conducted between November and December 2022, internet users in India were the most likely to have been victims of cybercrime, with nearly 70% of respondents claiming to have ever been victims of cybercrime [2]. Since we are experiencing quite an increase in cybercrime, cybersecurity courses and training at various universities must be integrated into students' curricula.

7.2 Future Work

As the comparison of responses of both pre-training and post-training questionnaire show improvement in cybersecurity awareness levels with the short cybersecurity training, the training can be updated with the latest trends and their impacts. The training is an alpha rollout of the Iterative Development phase of SAM. Keeping that in mind, the course content is accessible to all, having the URL so that it can be iteratively developed to make more improvised versions to improve the training.

Also, universities that were chosen to collect the responses from can be approached about including some subjects of cyber security awareness, either mandatory or elective, in their curriculum so that knowledge about cyber security awareness can be effectively increased from the ground level and to design a full-fledged cyber hygiene training. In addition, delivering the course interactively offline in classes instead of online may result in more significant improvement. Therefore, the current cybersecurity training can be made more interactive in the future.

As suggested in another study [61], questionnaires used in the research can be updated in future as needed. It is possible to create a functioning app that will assess the cybersecurity awareness of students or anyone else before and after the training and give feedback directly to the creator of the training to help them improve or see where they fall short.

References

[1] Livemint, “India to have around 900 million internet users by 2025: Report,” *mint*, Jul. 29, 2022. https://www.livemint.com/news/india-to-have-around-900-million-internet-users-by-2025-report-11659063114684.html (accessed Feb. 28, 2023).

[2] A. Chatterjee, “India’s had its worst year of cyberattacks, but 2023 will see govt & firms ramp up defences,” *ThePrint*, Dec. 30, 2022. https://theprint.in/india/indias-had-its-worst-year-of-cyberattacks-but-2023-will-see-govt-firms-ramp-up-defences/1286441/ (accessed Apr. 16, 2023).

[3] “Successive Approximation Model (SAM).” https://dli.kennesaw.edu/resources/idmodels/sam.php (accessed Mar. 19, 2023).

[4] L. Muniandy, B. Muniandy, and Z. Samsudin, “Cyber Security Behaviour among Higher Education Students in Malaysia,” *J. Inf. Assur. Cybersecurity*, pp. 1–13, Feb. 2017, doi: 10.5171/2017.800299.

[5] “India saw 18 million cyber attacks in first quarter of 2022: Google’s Royal Hansen,” *Moneycontrol*. https://www.moneycontrol.com/news/business/india-saw-18-million-cyber-attacks-in-first-quarter-of-2022-google-executive-royal-hansen-9084911.html (accessed Feb. 28, 2023).

[6] “Delhi Witnessed 111% Rise in Cybercrime in 2021: NCRB Data,” *The Wire*. https://thewire.in/government/delhi-witnessed-111-rise-in-cybercrime-in-2021-ncrb-data (accessed Feb. 28, 2023).

[7] “How to raise information security awareness (EN),” *ENISA*. https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide (accessed Dec. 09, 2022).

[8] N. A. G. Arachchilage and S. Love, “Security awareness of computer users: A phishing threat avoidance perspective,” *Comput. Hum. Behav.*, vol. 38, pp. 304–312, Sep. 2014, doi: 10.1016/j.chb.2014.05.046.

[9] N. Sohrabi Safa, R. Von Solms, and S. Furnell, “Information security policy compliance model in organizations,” *Comput. Secur.*, vol. 56, pp. 70–82, Feb. 2016, doi: 10.1016/j.cose.2015.10.006.

[10] A. Sreehari, K. J. Abinanth, S. B, U. P.S, and Mrs. Jayashree, “A STUDY OF AWARENESS OF CYBER CRIME AMONG COLLEGE STUDENTS WITH SPECIAL REFERENCE TO KOCHI,” *Int. J. Pure Appl. Math.*, vol. Volume 119, no. No. 16 2018, pp. 1353–1360.

[11] K. Senthilkumar and S. Easwaramoorthy, “A Survey on Cyber Security awareness among college students in Tamil Nadu,” *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 263, no. 4, p. 042043, Nov. 2017, doi: 10.1088/1757-899X/263/4/042043.

[12] A. Garg, R. Patel, and R. Patel, “A Research of the awareness level among Technical and Non-technical students of cyber security in Parul University,” *Isara Solut.*, Jan. 2021, Accessed: Nov. 04, 2022. [Online]. Available: https://www.academia.edu/61581469/_A_Research_of_the_awareness_level_among_Technical_and_Non_technical_students_of_cyber_security_in_Parul_University_

[13] P. Rathod and A. Potdar, “Study of Awareness of Cyber-Security among Medical Students,” *Indian J. Forensic Med. Toxicol.*, vol. 13, p. 196, Jan. 2019, doi: 10.5958/0973-9130.2019.00040.9.

[14] R. Chhibber and R. Thapar, “A Survey on ‘Cyber Security Awareness among College Going Students in Delhi ,’” p. 9.

[15] A. Mokha, “A Study on Awareness of Cyber Crime and Security,” *Res. J. Humanit. Soc. Sci.*, vol. 8, p. 459, Jan. 2017, doi: 10.5958/2321-5828.2017.00067.5.

[16] J. Shah, “A Study of Awareness About Cyber Laws for Indian Youth,” *Int. J. Trend Sci. Res. Dev.*, vol. Volume-1, no. Issue-1, Jan. 2017, Accessed: Nov. 04, 2022. [Online]. Available: https://www.ijtsrd.com/humanities-and-the-arts/social-science/54/a-study-of-awareness-about-cyber-laws-for-indian-youth/jigar-shah

[17] National Capital Region Planning Board, “STUDY ON COUNTER MAGNET AREAS TO DELHI & NCR,” 2001. [Online]. Available: https://ncrpb.nic.in/pdf_files/05_chapter%202_cma.pdf

[18] K. Nikolopoulou, “What Is Snowball Sampling? | Definition & Examples,” *Scribbr*, Aug. 17, 2022. https://www.scribbr.com/methodology/snowball-sampling/ (accessed Mar. 16, 2023).

[19] D. Paulhus, “Social desirable responding: The evolution of a construct,” *Role Constr. Psychol. Educ. Meas.*, Jan. 2002.

[20] K. Bogner and U. Landrock, “Response Biases in Standardised SurveysResponse Biases in Standardised Surveys,” *GESIS Surv. Guidel.*, 2016, doi: 10.15465/GESIS-SG_EN_016.

[21] D. T. Sadashivam, “Cyber Crime in India: An Introspection,” vol. 40, no. 60, p. 6.

[22] “Crime in India Table Contents | National Crime Records Bureau.” https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents?field_date_value%5Bvalue%5D%5Byear%5D=2020&field_select_table_title_of_crim_value=20&items_per_page=All (accessed Apr. 18, 2022).

[23] M. Rajan and J. Babu, “CYBER KNOWLEDGE, ATTITUDE, PRACTICE AND PERSONALITY TRAITS OF COLLEGE STUDENTS,” pp. 2582–5208, Jun. 2020.

[24] S. Mehta and V. Singh, “A STUDY OF AWARENESS ABOUT CYBERLAWS IN THE INDIAN SOCIETY,” *Int. J. Comput. Bus. Res.*, vol. 4, Jan. 2013.

[25] A. Chitrey, D. Singh, M. Bag, and V. Singh, “A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model,” *Int. J. Inf. Netw. Secur.*, vol. 1, Jan. 2012, doi: 10.11591/ijins.v1i2.426.

[26] P. Shah and A. Agarwal, “Cybersecurity behaviour of smartphone users in India: an empirical analysis,” *Inf. Comput. Secur.*, vol. 28, no. 2, pp. 293–318, 2020, doi: 10.1108/ICS-04-2019-0041.

[27] M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber Security Awareness Campaigns: Why do they fail to change behaviour?” arXiv, Jan. 09, 2019. doi: 10.48550/arXiv.1901.02672.

[28] R. Nagahawatta, M. Warren, and W. Yeoh, *A Study of Cybersecurity Awareness in Sri Lanka*. 2020.

[29] N. Ahmed, Dr. M. R. Islam, U. Kulsum, Md. R. Islam, E. Haque, and S. Rahman, *Demographic Factors of Cybersecurity Awareness in Bangladesh*. 2019. doi: 10.1109/ICAEE48663.2019.8975603.

[30] N. F. Khan, N. Ikram, S. Saleem, and S. Zafar, “Cyber-security and risky behaviors in a developing country context: a Pakistani perspective,” *Secur. J.*, 2022, doi: 10.1057/s41284-022-00343-4.

[31] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, “A survey of cyber-security awareness in Saudi Arabia,” in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec. 2016, pp. 154–158. doi: 10.1109/ICITST.2016.7856687.

[32] A. R. Neigel, V. L. Claypoole, G. E. Waldfogle, S. Acharya, and G. M. Hancock, “Holistic cyber hygiene education: Accounting for the human factors,” *Comput. Secur.*, vol. 92, p. 101731, May 2020, doi: 10.1016/j.cose.2020.101731.

[33] P. Lowry, J. Cao, and A. Everard, “Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures,” *J. Manag. Inf. Syst.*, vol. 27, pp. 163–200, Apr. 2011, doi: 10.2307/41304596.

[34] “Bloom’s Taxonomy,” *Vanderbilt University*. https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/ (accessed Apr. 10, 2023).

[35] R. Karimnia, K. Maennel, and M. Shahin, “Kultuurilisi aspekte arvestava küberturvalisuse teadlikkuse koolitusprogrammi koostamine Iraani, Hormozgani regiooni keskkooliõpilastele,” May 2021, Accessed: Apr. 10, 2023. [Online]. Available: https://digikogu.taltech.ee/et/item/daff1e63-287b-4f4c-82ea-f467b7215e2f

[36] E. van Vulpen, “Understanding the ADDIE Model: All You Need to Know,” *AIHR*, Apr. 06, 2023. https://www.aihr.com/blog/addie-model/ (accessed Apr. 10, 2023).

[37] “ADDIE.” https://dli.kennesaw.edu/resources/idmodels/addie.php (accessed Apr. 10, 2023).

[38] O. D. Apuke, “Quantitative Research Methods : A Synopsis Approach,” *Kuwait Chapter Arab. J. Bus. Manag. Rev.*, vol. 6, no. 11, pp. 40–47, Sep. 2017, doi: 10.12816/0040336.

[39] S. Sahlqvist *et al.*, “Effect of questionnaire length, personalisation and reminder type on response rate to a complex postal survey: randomised controlled trial,” *BMC Med. Res. Methodol.*, vol. 11, no. 1, p. 62, Dec. 2011, doi: 10.1186/1471-2288-11-62.

[40] R. G. Kost and J. Correa da Rosa, “Impact of survey length and compensation on validity, reliability, and sample characteristics for Ultrashort-, Short-, and Long-Research Participant Perception Surveys,” *J. Clin. Transl. Sci.*, vol. 2, no. 1, pp. 31–37, Feb. 2018, doi: 10.1017/cts.2018.18.

[41] C. León-Mantero, J. C. Casas-Rosal, C. Pedrosa-Jesús, and A. Maz-Machado, “Measuring attitude towards mathematics using Likert scale surveys: The weighted average,” *PLOS ONE*, vol. 15, no. 10, p. e0239626, Oct. 2020, doi: 10.1371/journal.pone.0239626.

[42] G. Albaum, “The Likert scale revisited: An alternate version,” *Int. J. Mark. Res.*, vol. 39, pp. 331–348, Jan. 1997.

[43] L. South, D. Saffo, O. Vitek, C. Dunne, and M. Borkin, “Effective Use of Likert Scales in Visualization Evaluations: A Systematic Review,” Mar. 2021, Accessed: Apr. 11, 2023. [Online]. Available: https://osf.io/exbz8/

[44] T. Alharbi and A. Tassaddiq, “Assessment of Cybersecurity Awareness among Students of Majmaah University,” *Big Data Cogn. Comput.*, vol. 5, no. 2, Art. no. 2, Jun. 2021, doi: 10.3390/bdcc5020023.

[45] “Number of Students: Delhi: Colleges | Economic Indicators | CEIC.” https://www.ceicdata.com/en/india/number-of-students-colleges/number-of-students-delhi-colleges (accessed Mar. 18, 2023).

[46] “Delhi skill university to enrol 6,000 students in first round of admission process,” *The Indian Express*, Jun. 11, 2021. https://indianexpress.com/article/education/delhi-skill-university-to-enrol-6000-students-in-first-round-of-admission-process-7354857/ (accessed Apr. 10, 2023).

[47] “Jamia Hamdard,” *Top Universities*. https://www.topuniversities.com/universities/jamia-hamdard (accessed Apr. 10, 2023).

[48] R. V. Krejcie and D. W. Morgan, “Determining Sample Size for Research Activities,” *Educ. Psychol. Meas.*, vol. 30, no. 3, pp. 607–610, Sep. 1970, doi: 10.1177/001316447003000308.

[49] P. B. Bullen, “How to choose a sample size (for the statistically challenged),” *tools4dev*, Oct. 17, 2013. https://tools4dev.org/resources/how-to-choose-a-sample-size/ (accessed Mar. 18, 2023).

[50] J. W. Creswell, *Educational research: planning, conducting, and evaluating quantitative and qualitative research*, 4th ed. Boston: Pearson, 2012.

[51] K. S. Taber, “The Use of Cronbach’s Alpha When Developing and Reporting Research Instruments in Science Education,” *Res. Sci. Educ.*, vol. 48, no. 6, pp. 1273–1296, Dec. 2018, doi: 10.1007/s11165-016-9602-2.

[52] “Successive Approximation Model - Teachfloor.” https://www.teachfloor.com/elearning-glossary/successive-approximation-model (accessed Mar. 19, 2023).

[53] “SAM (Successive Approximation Model) for Instructional Design [2022],” *Valamis*, Jul. 19, 2022. https://www.valamis.com/hub/sam-model (accessed Apr. 11, 2023).

[54] H. Jung, Y. Kim, H. Lee, and Y. Shin, “Advanced Instructional Design for Successive E-Learning: Based on the Successive Approximation Model (SAM),” *Int. J. E-Learn. Corp. Gov. Healthc. High. Educ.*, vol. 18, Mar. 2019.

[55] A. Reeves, D. Calic, and P. Delfabbro, “‘Generic and unusable’1: Understanding employee perceptions of cybersecurity training and measuring advice fatigue,” *Comput. Secur.*, vol. 128, p. 103137, May 2023, doi: 10.1016/j.cose.2023.103137.

[56] C. J. Brame, “Effective Educational Videos: Principles and Guidelines for Maximizing Student Learning from Video Content,” *CBE—Life Sci. Educ.*, vol. 15, no. 4, p. es6, Dec. 2016, doi: 10.1187/cbe.16-03-0125.

[57] A. Gero, Y. Stav-Satuby, and N. Yamin, “Increasing motivation of engineering students: Combining ‘real world’ examples in a basic electric circuits course,” *Int. J. Eng. Educ.*, vol. 32, pp. 2460–2469, Dec. 2016.

[58] “Wayback Machine,” May 25, 2017. https://web.archive.org/web/20170525141614/http://nclm.nic.in/shared/linkimages/NCLM52ndReport.pdf (accessed Apr. 09, 2023).

[59] U. of L. at L. Colleen Wolverton and U. of L. at L. Brandi Guidry Hollier, “Guidelines for Incorporating Active Learning Into the Design of Online Management Courses Utilizing the Successive Approximation Model (SAM),” *International Journal of Education and Development using ICT, Vol. 18, No. 1, 2022*, Apr. 30, 2022. http://ijedict.dec.uwi.edu/viewarticle.php?id=2987 (accessed Mar. 19, 2023).

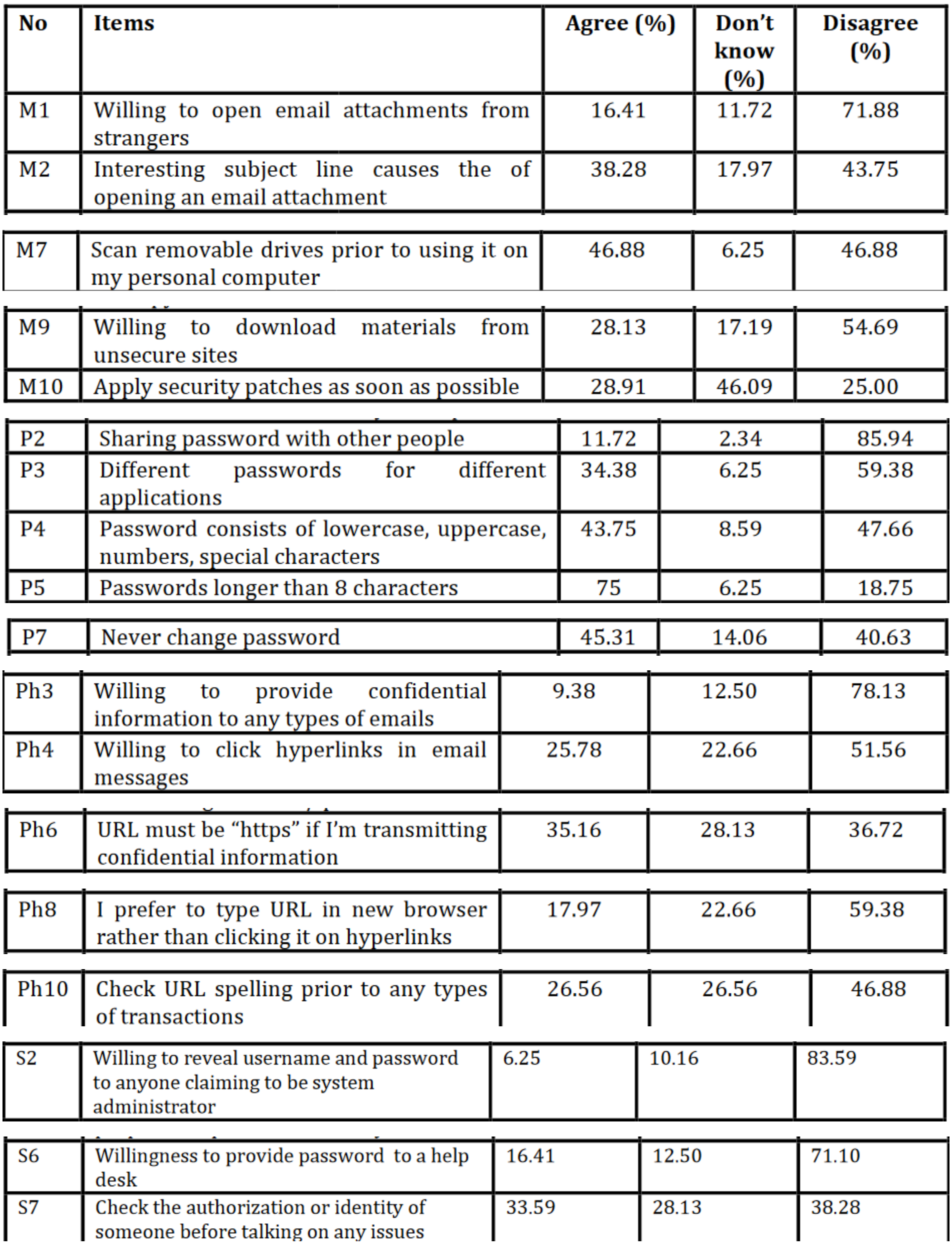
[60] “Cybercrime rate by country 2022,” *Statista*. https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/ (accessed Apr. 16, 2023).

[61] A. Ojha and S. Mäses, “Cybersecurity-Awareness-among-Engineering-students-of-West-Bengal-India,” Tallinn University of Technology.

Appendices

Appendix 1

Muniandy Question responses which are common/similar to current study questions



No	Items	Agree (%)	Don't know (%)	Disagree (%)
M1	Willing to open email attachments from strangers	16.41	11.72	71.88
M2	Interesting subject line causes the of opening an email attachment	38.28	17.97	43.75
M7	Scan removable drives prior to using it on my personal computer	46.88	6.25	46.88
M9	Willing to download materials from unsecure sites	28.13	17.19	54.69
M10	Apply security patches as soon as possible	28.91	46.09	25.00
P2	Sharing password with other people	11.72	2.34	85.94
P3	Different passwords for different applications	34.38	6.25	59.38
P4	Password consists of lowercase, uppercase, numbers, special characters	43.75	8.59	47.66
P5	Passwords longer than 8 characters	75	6.25	18.75
P7	Never change password	45.31	14.06	40.63
Ph3	Willing to provide confidential information to any types of emails	9.38	12.50	78.13
Ph4	Willing to click hyperlinks in email messages	25.78	22.66	51.56
Ph6	URL must be "https" if I'm transmitting confidential information	35.16	28.13	36.72
Ph8	I prefer to type URL in new browser rather than clicking it on hyperlinks	17.97	22.66	59.38
Ph10	Check URL spelling prior to any types of transactions	26.56	26.56	46.88
S2	Willing to reveal username and password to anyone claiming to be system administrator	6.25	10.16	83.59
S6	Willingness to provide password to a help desk	16.41	12.50	71.10
S7	Check the authorization or identity of someone before talking on any issues	33.59	28.13	38.28