big data and cognitive computing

MDPI

Article

Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation

Shouq Alrobaian [1], Saif Alshahrani [2] and Abdulaziz Almaleh [3,*]

[1] Technology and Information Security Department, Jazan University, Jazan 82817, Saudi Arabia
[2] Technical and Vocational Training Corporation, Bisha College, Bisha 67714, Saudi Arabia
[3] Information Systems Department, King Khalid University, Abha 62529, Saudi Arabia
* Correspondence: ajoyrulah@kku.edu.sa; Tel.: +966-533-212-174

Abstract: People are the weakest link in the cybersecurity chain when viewed in the context of technological advancement. People become vulnerable to trickery through contemporary technical developments such as social media platforms. Information accessibility and flow have increased rapidly and effectively; however, due to this increase, new electronic risks, or so-called cybercrime, such as phishing, scams, and hacking, lead to privacy breaches and hardware sabotage. Therefore, ensuring data privacy is vital, particularly in an educational institute where students constitute the large majority of users. Students or trainees violate cybersecurity policies due to their lack of awareness about the cybersecurity environment and the consequences of cybercrime. This paper aims to assess the level of awareness of cybersecurity, users' activities, and user responses to cybersecurity issues. This paper collected data based on a distributed questionnaire among trainees in the Technical and Vocational Training Corporation (TVTC) to demonstrate the necessity of increasing user awareness and training. In this study, quantitative research techniques were utilized to analyze the responses from trainees using tests such as the Chi-Squared test. Proof of the reliability of the survey was provided using Cronbach's alpha test. This research identifies the deficiencies in cybersecurity awareness among TVTC trainees. After analyzing the gathered data, recommendations for tackling these shortcomings were offered, with the aim of enhancing trainees' decision-making skills regarding privacy and security using the Nudge model.

Keywords: cybersecurity; awareness; survey; information security; cybercrime

Citation: Alrobaian, S.; Alshahrani, S.; Almaleh, A. Cybersecurity Awareness Assessment among Trainees of the Technical and Vocational Training Corporation . *Big Data Cogn. Comput.* **2023**, *7*, 73. https://doi.org/10.3390/bdcc7020073

Academic Editors: Peter R.J. Trim and Yang-Im Lee

Received: 24 February 2023
Revised: 8 April 2023
Accepted: 11 April 2023
Published: 12 April 2023

1. Introduction

The internet has become significantly connected to our lives as our economy and infrastructure have become heavily dependent on internet networks and modern technology [1]. The use of the internet has spread, especially with the digital transformation that depends on managing operations for the public and private sectors by integrating modern technology and taking advantage of it in all aspects of life and social circles [2]. The digital transformation has caused a vast revolution, especially among educational circles, mainly through the use of technology to obtain and disseminate information, which has led to an increase in the use of the internet [3].

The ease of sharing and finding personal information via social media or online searches has increased, but without adequate cybersecurity awareness, users may encounter challenges in determining whether to disclose their data. Factors such as cognitive biases, time limitations, and emotional influences can complicate the selection process of appropriate privacy protection options. This is especially true when interacting with user interfaces on websites that necessitate registration or involvement [4].

Therefore, users will not have complete control over the privacy of their data, which may lead to its violation [5]. Conversely, internet usage may involve certain processes or elements that necessitate user consent, often without them being fully aware that some of

these aspects could be detrimental to their personal data [6]. Therefore, there are so-called "Service Terms" that are included in every service provided to the user, whether in the social or educational aspect, and they explain to the user how to benefit from and control their data when using this service. It is often ignored and unread by the user, usually due to a lack of awareness on behalf of the user in protecting their data [7].

As a result of the increased use of the internet, cybercrime and electronic fraud cases have increased. Cybercrimes are similar traditional crimes in terms of different aspects and groups, but their development is related to computer use and geographical diversity [8]. They are carried out by programmers called hackers, and they are divided according to their actions, which may be on a personal level, i.e., for personal benefit by causing harm to others, or for the general use, for example, for testing systems or trying something to help [9]. Hackers have developed new methods and techniques that may lead to financial gain and psychological harm, or they may just sabotage for fun [3]. These cyber attacks are cheaper and less dangerous than physical attacks, in addition to some other advantages, such as the irrelevance of the distance to or place of an attack and the difficultly in identifying and prosecuting the attacker. Accordingly, cyber attacks may continue to increase [1], which may lead to violations of cybersecurity systems that protect the automation of the economy and infrastructure [3].

Cybersecurity includes the process of providing protection for cyberspace and organizing all resources and processes related to cyber attacks [10]. The primary cause leading to the increase in cyber attacks is the failure to follow the cybersecurity guidelines offered by organizations. In [3], the authors stress the critical nature of implementing and adhering to cybersecurity guidelines across all divisions of an organization. They highlight the need to focus on the organization's members, representing the most vulnerable point in the security chain. This underscores the significance of cultivating strong cybersecurity practices among employees to bolster overall organizational security. The authors of [4] also emphasize the value of gently motivating users to make optimal choices regarding the sharing of their personal data in the context of online privacy and security. By utilizing non-intrusive interventions, individuals can be guided toward making better-informed decisions about their data protection and online safety.

As cyber attacks have increased around the world, cybersecurity has become a priority in many countries. Accordingly, the Kingdom of Saudi Arabia has strengthened its investments and efforts to develop cybersecurity and its related procedures in the public and private sectors by 2030. The Kingdom of Saudi Arabia has established the National Authority for Cybersecurity (NCA) [11] to strengthen the position of cybersecurity and control the procedures and operational processes associated with it. The Saudi Federation for Cybersecurity and Drones (SAFCSP) [12] is another Saudi association that applies international standards, regulations, and practices to help improve the cybersecurity of the Kingdom of Saudi Arabia for it to become one of the leading countries in the technology revolution [13].

The rapid development of technology has led to an increase in the use of intelligent devices connected to the internet, especially in the educational sector. The number of smart devices exceeded 4 billion in 2020, leading to increased cyber attacks and new challenges [14].

The main reason for the increase in cybercrime in the educational sector is the poor awareness among users, as experts have shown in [15]. Cybersecurity awareness and policies in Saudi Arabia have not received enough attention among university students and institute trainees. This entails protecting individuals and university and school students by raising awareness about cybersecurity, providing training programs and educational means on the challenges of cybersecurity and the consequences of information crimes, and increasing the knowledge of risks of losing sensitive information [3,15]. This work assesses the level of awareness of cybersecurity and users' activities and their reaction to cybersecurity aspects. The contribution of this paper is as follows:

- The level of cybersecurity awareness is explored among trainees at the TVTC by evaluating and measuring many security factors while using the internet.
- Gaps are found in awareness of trainees at the educational organization (TVTC) after examining and analyzing the results and strategies are proposed to enhance this awareness.
- Awareness about cybersecurity is enhanced by presenting a theoretical framework appropriate for the TVTC to educate trainees about the risks and consequences of cybercrime.
- The approach is developed in the TVTC and proposals are made commensurate with the gaps we found through analyses of the results to improve the security environment and the decision-making process of individuals and the organization.

The rest of this paper is structured as follows: the relevant works are put forward in Section 2. Section 3 presents the methodology for assessing cybersecurity awareness among trainees and describes the dataset collected in this study. The results are shown in Section 4 based on the analysis and examination of the data. This paper concludes with a review of the study's data and findings in Section 5, followed by Section 6 with a conclusion.

2. Related Work

Few studies have covered cybersecurity awareness in the educational community and among students, which depends on people's understanding and knowledge of cybersecurity or information security and the consequent risks and methods of protection from them [16]. Many relevant works have determined the awareness level by assessing the understanding of cybersecurity concepts among students. Alharbi et al. [3] showed how Majmaah University students [17] understand cybersecurity, cyberattacks, and their consequences. Based on the questionnaire conducted by researchers, they found that awareness about cybersecurity must be increased among university students, advanced educational methods should be used and combined with traditional methods, and videos and games can be used to provide awareness to students. However, the length of the questions in the questionnaire was one of the defects of this study, which may have led to ambiguity in understanding basic terms and concepts.

Khader et al. [18] suggested a theoretical cybersecurity awareness framework that directs the implementation of programs to raise graduates' cybersecurity awareness in any academic setting. The CAFA [19] can be a jumping-off point for educational institutions looking to establish new policies and procedures.

The study in [20] aimed to determine the level of understanding of threats related to online security and comprehension of the preventive measures used to protect young people from online dangers. Data were collected from youths enrolled in classes of children aged eleven and higher at random. According to the survey findings, most young people are unaware of internet security risks and hazards. This survey sample did not adhere to the universal frameworks used to produce acceptable results, which can be enhanced to reflect solid findings [21].

Another work performed by Taha et al. [22] compared college students' knowledge and behavior regarding information security awareness. The main objective was to compare students' understanding of information security when using smartphones versus computers to see where there are differences. As a result of their work, they encourage academic institutions to exercise caution and run information security awareness campaigns. The creation of the necessary level of awareness among all Jordanian students would be facilitated by including an information security course as a university requirement. However, the survey question count needed to be improved, which resulted in inaccurate measurements of all relevant factors considering cyber attack evolution and the tools available to defend against them.

The authors of [23] assessed students' cybersecurity knowledge in developing countries by examining the understanding of the effects of software and email security. The study was conducted through a scientific questionnaire containing eleven questions, which could be considered as of the defects of this study, as the number of questions needed to be increased to include all essential aspects of cybersecurity. However, through this questionnaire, the researchers found that awareness of email security increases awareness about cybersecurity more than software security.

Likewise, researchers [24] investigated the increasing awareness of cybersecurity with the spread of social engineering attacks targeting users as they are the weakest link according to their level of understanding about this type of attack. The researchers discovered that education programs are an effective method to raise awareness among users and employees. Nevertheless, the work could have included the study and comparison of laws and regulations legislated by governments.

3. Materials and Methods

3.1. Research Method

This study used a survey method to gather qualitative data about the Technical and Vocational Training Corporation trainees and assess their level of cyber security knowledge. The survey was conducted online to efficiently and ethically collect a sizable sample of male and female trainees. There were 40 questions in total, covering a variety of cybersecurity topics, such as demographics (4 questions), technical information (2 questions), internet usage (2 questions), information about prior hacks (1 question), use of security tools such as antivirus [25], two-factor authentications (2FA) [26], firewalls [27] (9 questions), password policy (9 questions), browser security (3 questions), social networking (5 questions), and cybersecurity knowledge (9 questions). The survey questions were chosen based on mechanisms designed by other cybersecurity researchers [3,23].

The internet serves as a worldwide platform for information and commerce, offering numerous benefits to users. However, as individuals spend more time online, they may encounter various infringements, including privacy concerns that necessitate increased awareness of responsible internet usage [28]. To better understand this phenomenon, questions were designed to gather insights into the online behavior of trainees, ultimately shedding light on their internet usage habits and potential vulnerabilities.

Awareness questions about security tools, which in turn help individuals to protect themselves from cybercrime-related threats during personal use of the internet, noting that it is not enough to rely on them alone [29], have been created to examine the current security practices among Technical and Vocational Training Corporation trainees.

The browser security segment questions aim to assess the trainees' comprehension of how secure their standard web browser is. A web browser is the gateway to information and services via the internet, through which accounts are accessed via e-mail, social media, and downloading various files. Hence, it counts as a sensitive gateway to attack and cybercrime [30].

The networking and cyberspace knowledge questions assess the trainees' understanding of the dangers of accessing a variety of social networks, as it is the main basis for communication between individuals and access to various websites, which increases the risk of attacks on their personal data and information accessed through it. The questions also assessed the trainees understanding of how to respond to cybercrime events [31]. Therefore, we examined the trainees' cybersecurity knowledge, abilities, behavior, beliefs, and self-perception.

The questionnaire was selected from other survey questions created by other researchers in [3], with adjustments to reduce the number of questions (which is mentioned as a limitation in [3]) according to a random sample of 50 male and female trainees who recommended reducing the number of questions to maintain some degree of satisfaction.

3.2. Study Model

The survey depends on the scientific questionnaire standards used in related works [3] and [23] with a few modifications in several questions due to limitations in previous works, such as responses of a random sample of trainees. The modified questions were reviewed and analyzed based on the questionnaire standards [32]. The survey questions also include additional scientific explanations for each section to make it easier for non-technical trainees to understand the questions. The first page of the questionnaire also contained the aim of the study, explaining the meaning and some basic information to the user. After obtaining the required approval from the TVTC, the survey was distributed through the questionnaire link among trainees with the help of heads of department. The sample size of this study followed the standard guidelines [21], which resulted in 739 complete responses from TVTC trainees with limited responses to one answer for each sample by requesting signing in to a Google account.

3.3. Data Collection

The data were collected in electronic form by sharing an official link through the organization to give respondents access to the designed question on the Google Form, answer, and submit their responses. The responses were exported to Microsoft Excel after the questionnaire had been administered. The total number of collected responses exported to Excel was 739. The data were cleaned in Excel, and after cleaning, the data were exported and coded in Statistical Package for the Social Sciences (SPSS) for further analysis.

4. Results

The entire population of trainees was selected for this study, and the respondent trainees served as the chosen sample. The study focuses on trainees' knowledge of cybersecurity issues, including phishing attacks, which is based on targeting specific people through their available data or exploiting errors caused by these people through their use of systems [33]; malware, which is programming code that helps perform malicious actions used by attackers to steal information or harm others without user permission [34]; patching, which is intended to fix defects in programs; and adding features, including improving the security of programs by identifying, verifying, and installing updates [35]. The actions of trainees exposed to cybercrime were also studied. The survey also gathered information from trainees regarding cybersecurity concepts such as countermeasures, password protection, website security, and social media platforms.

4.1. Descriptive Analysis

This section focuses on data analysis, which is presented as frequency distribution tables, bar charts, percentages, and proportions using Chi-square test techniques [36]. Tests were conducted at a 95% confidence level, and the decision rule was based on the null hypothesis; if the p-value was less than 0.05 we reject the null hypothesis and conclude that the two groups are dependent on each other, and if the p-value is greater than 0.05, we do not reject the null hypothesis and conclude that the two groups are independent of each other [37].

The accuracy of the assessment of cybersecurity knowledge of trainees depends on measuring the influence of the life cycle variables of the trainees. Therefore, variables such as sex, the level of qualification, specialization, and the operating system used were selected to help the assessment. Table 1 summarizes the variable information of the sampled population in more detail.

Table 1. Shows the respondents' gender, level of qualification, operating system, and specializations.

Variables		Freq.	Percentage %
Sex	Male	281	38.02
	Female	458	61.98
Degree	BA	19	2.57
	Diploma	720	97.43
Specialization	Accounting	4	0.54
	Administrative technology	194	26.25
	Arabic language	1	0.14
	Chemical technology	4	0.54
	Civil and architectural technology	4	0.54
	Computer technology	281	38.02
	Decoration, beauty technology, and clothing design	146	19.76
	Electrical technology	2	0.27
	Electronic technology	53	7.17
	Food technology and the environment	2	0.27
	Human resources	5	0.68
	Insurance	8	1.08
	Library administration	11	1.49
	Mechanical technology	16	2.17
Operating Systems used	Linux	8	1.08
	Mac	123	16.64
	Windows	403	54.53
	Unknown	163	22.06
	Windows system, Linux system (Linux)	13	1.76
	Windows system, Mac system (Mac OS)	24	3.25
	Windows, Mac OS, Linux	5	0.68

As the table shows, most of the respondents were female (458 (61.98%)), while there were 281 male respondents (38.02%). It was recorded that the majority of the respondents, 720 (97.43%), had a diploma, while the rest of the respondents, 19 (2.57%), had bachelor degrees. The specialization area in Table 1 shows that 4 (0.54%) respondents were accounting specialists, 194 (26.25%) respondents belong to administrative technology (either marketing and innovation, human resources, or logistics), one respondent specialized in the Arabic language, 4 (0.54%) respondents specialized in both chemical technology (chemical production and chemical laboratories) and civil and architectural technology (such as surveying, civil construction, and architectural construction). At total of 281 (38.02%) respondents specialized in computer technology (such as networking, software, technical support, and multimedia). A total of 146 (19.76%) respondents specialized in decoration, beauty technology, and clothing design (e.g., cosmetology, hair care, fashion manufacturing, and fashion design). Two (0.27%) respondents specialized in both electrical technology (such as electrical machines, electric power, and renewable energy) and food technology and the environment (e.g., food safety, occupational safety, and health, and environmental protection). A total of 53 (7.17%) respondents specialized in electronic technology (such as electronics and control systems, precision instruments and machines, and medical devices). Five (0.68%) respondents specialized in human resources, 8 (1.08%) respondents specialized in insurance, 11 (1.49%) respondents were library administration specialists, 16 (1.17%) respondents specialized in mechanical technology (such as manufacturing, engines and vehicles, and refrigeration and air conditioning), and lastly, 8 (1.98%) respondents specialized in tourism and hospitality technology (e.g., travel and tourism, hotels, and

event management). Regarding the type of operating system on respondents' devices, the majority of the respondents had Windows on their device (403 (54.53%) respondents), followed by 123 (16.64%) respondents who had Mac on their devices, 8 (1.08%) had Linux on their devices, about 163 (22.06%) respondents did not know the type of operating system on their device, 13 (1.76%) respondents had both Windows and Linux on their device, and 24 (3.25%) had both Windows and Mac on their system device. The respondents were not asked about a specific device type due to the various vendors, which is out of the scope of this research. In comparison, 5 (0.68%) respondents had all three types of operating systems on their system devices, as shown in Figure 1.

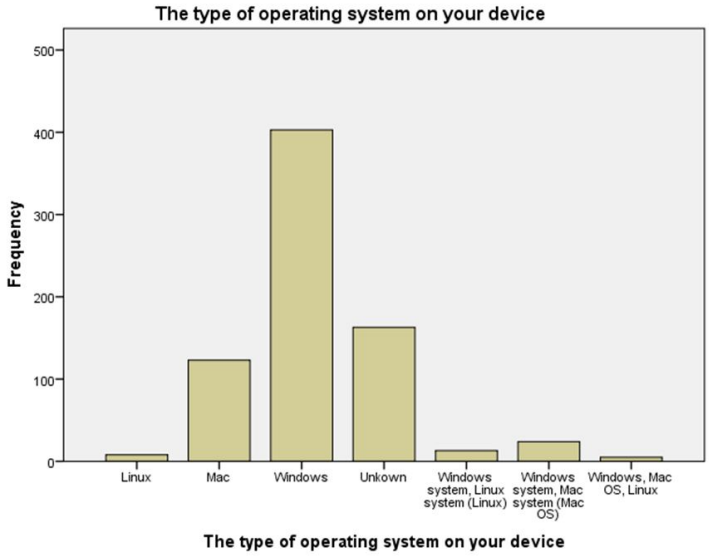

Figure 1. Respondents' Operating Systems.

4.2. Cybersecurity Concepts

In cybersecurity, the term CIA, which indicates confidentiality, integrity, and availability [38], is utilized as the main principle required to maintain the essential knowledge of cybersecurity concepts by applying specific processes to systems and services connected to the internet. Organizations, even academic institutions, protect the cyberspace by protecting weaknesses in the chain (trainees) and should take measures to educate them on how to protect their critical data and networks [38,39]. Based on the weakness in the chain (the trainees), this paper aims to assess the CIA concept among them. The questionnaire in this paper contains 40 questions, of which 26 focus on the cybersecurity aspects of the CIA (Table 2). It includes 14 questions about confidentiality, passwords, and revealing personal information on social networking sites. Twelve integrity, firewall, email policy, browser, and antivirus software questions were included in the evaluation. In addition, all 26 questions were related to measuring availability.

A small percentage of respondents (0.41%) spent the most time on Facebook [40], 27 (3.65%) respondents spent the most time on Instagram [41], 4 (0.54%) respondents spent the most time on LinkedIn [42], and a high percentage of 159 (21.52%) respondents spent the most time on Snapchat [43]. Moreover, 14 respondents spent the most time on both Instagram and Twitter [44], 11 respondents spent the most time on Instagram and YouTube [45], 2 respondents spent the most time on both Snapchat and Facebook, 78 respondents spent the most time on both Snapchat and Instagram, 27 respondents spent the most time on Snapchat and Twitter, 10 respondents spent the most time on Snapchat and YouTube, 3 respondents spent the most time on WhatsApp [46] and Facebook, 13 respondents spent the most time on WhatsApp and Instagram, a high percentage of the respondents (276, 37.35%) spent the most time on WhatsApp and Snapchat, and lastly, four respondents spent the most time on WhatsApp and YouTube.

Table 2. Time respondents spent on social media platforms.

Which Social Network Do You Spend the Most Hours on?	Freq.	Percentage %
Facebook	3	0.41
Instagram	27	3.65
LinkedIn	4	0.54
Snapchat	159	21.52
Twitter	41	5.55
WhatsApp	31	4.19
YouTube	27	3.65
Instagram, Twitter	14	1.89
Instagram, YouTube	11	1.49
Snapchat, Facebook	2	0.27
Snapchat, Instagram	78	10.55
Snapchat, Twitter	27	3.65
Snapchat, Youtube	10	1.35
WhatsApp, Facebook	3	0.41
WhatsApp, Instagram	13	1.76
WhatsApp, Snapchat	276	37.35
WhatsApp, Twitter	9	1.22
WhatsApp, YouTube	4	0.54

About 555 (75.1%) respondents have email and do use their email, while a small amount of 184 (24.9%) respondents sometimes used their email (Table 3).

Table 3. Respondents reply to email usage.

Do You Use E-Mail?	Freq.	Percentage %
Yes	555	75.1
Sometimes	184	24.9

4.2.1. System Update

Table 4 reveals that the majority of the respondents', 392 (53.04%), devices have automatic updates enables, i.e., the device updates the system if it detects a new update, which helps them keep their devices safe. A total of 258 (34.91%) respondents performed manual updates, i.e., the auto update feature is disabled and they update the device themselves when it asks for an update. A total of 59 (7.98%) respondents do not use the update feature, i.e., they use their devices without an update; this makes their devices more vulnerable to threats and hacking than others. A total of 30 (4.06%) respondents had got received device and had not updated it yet. To better understand the percentages, Figure 2 shows the responses regarding the operating system updates.

Table 4. Respondents ways of updating their OS device.

How to Update the Operating System of Your Device?	Freq.	Percentage %
Automatic update (the automatic update feature is enabled and the device updates the system if it detects a new update)	392	53.04
I do not know the update feature	59	7.98
Manual update (the auto update feature is disabled and I update the device myself when it asks for an update)	258	34.91
Never (the device is new)	30	4.06

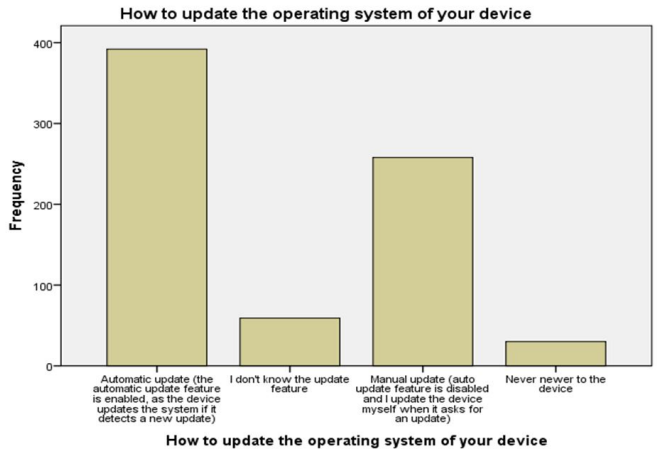

Figure 2. How respondents update their operating system.

4.2.2. Devices Attacked

The following Figure 3 shows the results of whether the trainees' devices had been attacked before. A total of 660 (89.31%) respondents' devices had not been attacked before, which means they apply proper security practices, while a virus had attacked 33 (4.47%) respondents' devices, 31 (4.19%) respondents' accounts had been hacked, and 15 (2.03%) respondents had been scammed.

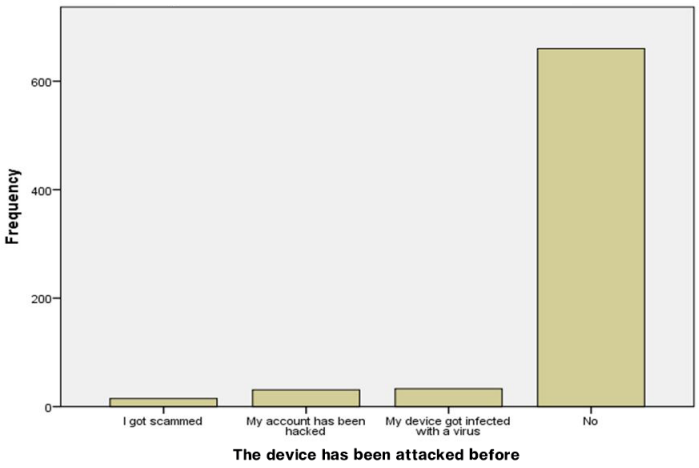

Figure 3. Previously attacked devices.

Although those who implement security measures make up the majority, this survey asked follow-up questions to the respondents whose devices had been hacked and deceived before, as Table 5 shows.

Of the respondents who had been scammed, 3 (0.4%) did nothing and 12 (1.6%) informed the concerned authorities and their card was suspended. Out of the respondents who informed us that their account was hacked, 10 (1.4%) contacted support for the hacked program, 6 (0.8%) did nothing to it, and 6 (0.8%) informed everyone that their account was hacked and contacted the support for the hack program. Eight (1.1%) only told everyone that their account was hacked. However, of respondents that said that their device was infected with a virus, 10 (1.4%) ran a device scan program (programs to detect viruses inside the device), 9 (1.2%) deleted virus-related files, 7 (0.9%) ran a device scan program (programs to detect viruses inside the device) and deleted the files associated with the virus, and 6 (0.8%) went to tech support.

Table 5. Respondents reactions to the device being attacked.

When You Were Scammed?	Freq.	Percentage %
Did not do anything	3	0.4
Informed the concerned authorities, the bank card was suspended	12	1.6
When my account was hacked		
I contacted support for the hacked program.	10	1.4
I did not do anything	6	0.8
I informed everyone that my account was hacked and I contacted support for the hacked program	6	0.8
I told everyone that my account was hacked	8	1.1
I told everyone that my account was hacked, I contacted support for the hacked program, and I did nothing	1	0.1
When my device got infected with a virus		
I did not do anything	1	1
I ran a device scan program (programs to detect viruses inside the device) and I deleted the files associated with the virus	7	0.9
I went to tech support	6	0.8
I ran a device scan program (programs to detect viruses inside the device)	10	1.4
Virus-related files were deleted	9	1.2

4.2.3. Antivirus Software

The default protection on computers enforces some countermeasures related to the security of devices, such as protection mechanisms. One of the protection mechanisms is software that detects malicious websites when visiting or downloading files containing a virus. This software, called antivirus software, detects malicious files, depending on their signature or behaviors and compares the findings with a huge related database. This type of software helps trainees protect their devices [47]. As expected, most trainees did not have antivirus software installed, as shown in Table 6. A total of 273 (36.94%) respondents had antivirus software installed on their devices, 164 (22.19%) respondents sometimes installed antivirus software on their devices, while 302 (40.87%) did not have antivirus software installed.

Table 6. Installation of antivirus software.

Have You Installed Antivirus Software (Protection Software to Detect and Protect against Viruses) on Your Devices	Freq.	Percentage %
No	302	40.87
Sometimes	164	22.19
Yes	273	36.94

Trainees need to know about cybersecurity countermeasures that help to keep their devices and information secure. Table 7 shows the rate in which respondents agree with the research questions on a Likert scale. A total of 558 (75.51%) respondents completely agree that antivirus and security software must be downloaded from licensed and trusted sources, 124 (16.78%) respondents agreed, and 49 (6.63%) respondents are neutral regarding whether antivirus and security software should be downloaded from licensed and trusted sources. A total of 3 (0.41%) respondents disagreed and 5 (0.68%) respondents strongly disagreed that antivirus and security software must be downloaded from licensed and

trusted sources. The majority of the respondents (509 (68.88)) completely agreed that antivirus software must be up to date; similarly, 162 (21.92%) also agreed that antivirus software must be up to date. A total of 58 (7.85%) respondents did not know (i.e., neutral to the research question), 6 (0.81%) respondents disagreed and 4 (0.54%) respondents strongly disagreed that antivirus software must be up to date. A total of 267 respondents (36.13%) completely agreed that they were able to recognise sites that will infect their computer with viruses if they visit them and download their programs; similarly, 227 (30.72%) respondents agreed with this statement. A total of 198 (26.79%) respondents did not know (i.e., neutral), 30 (4.06%) respondents disagreed and 17 (2.30%) respondents strongly disagreed that they were able to recognise sites that will infect their computer with viruses if they visit them and download their programs. A total of 360 respondents (48.71%) completely agreed that the firewall (a program that protects the network (the internet)) must be activated in all the devices they use. Similarly, 242 (32.75%) respondents agreed with this statement. A total of 125 (16.91%) respondents did not know (i.e., neutral), 11 (1.49%) respondents disagreed, and 1 (0.14%) respondent strongly disagreed that the firewall must be activated in all the devices they use. A total of 240 respondents (32.48%) completely agreed that they felt that all the devices they used were safe. Similarly, 281 (38.02%) respondents agreed with this statement. A total of 140 (18.94%) respondents did not know (i.e., neutral), 70 (9.47%) respondents disagreed, and 8 (1.08%) respondents strongly disagreed that they felt that all the devices they used were safe. A total of 480 respondents (64.95%) totally agreed that they must use two-factor verification (for example, the method of entering Mubashir for the Al Rajhi Bank application and entering the verification code sent by text message) if it is available. Similarly, 187 (25.30%) respondents also agreed with this statement. A total of 55 (7.44%) respondents did not know (i.e., neutral), 13 (1.76%) respondents disagrees, and 4 (0.45%) respondents strongly disagrees that they must use two-factor verification if it is available. A total of 173 (23.4%) respondents completely agreed, 158 (21.4%) respondents agreed, 129 (17.5%) respondents did not know, 162 (21.9%) respondents disagreed, and 117 (15.8%) respondents strongly disagreed with the statement that public networks (internet located in airports, parks, and malls) can be used and are safe to use on personal devices. A total of 144 (19.5%) respondents totally agreed, 201 (27.2%) respondents agreed, 126 (17.1%) respondents did not know, 179 (24.2%) respondents disagreed, and 89 (12.0%) respondents strongly disagreed with the statement that attachments (sent files such as Word files or others) sent to your email or social networks may be opened without worry. Lastly, 224 (30.3%) respondents totally agreed, 209 (28.3%) respondents agreed, 110 (14.9%) respondents did not know, 171 (23.1%) respondents disagreed, and 25 (3.4%) respondents strongly disagreed with the statement that their passwords must be changed periodically.

4.2.4. Password Mechanism

Cybersecurity countermeasures include strong passwords to protect accounts and information. Passwords are one of the authentication methods which needs to be strong. Characteristics that are recommended for a strong password are a password length of at least 12 characters and a password that contains alpha (capital and small letters), numeric, and at least one special character (symbols) [48]. Therefore, in this survey, we assessed how the trainees manage their passwords and their knowledge about them, with the data summarised in Table 8.

Table 7. Respondents perception of cybersecurity countermeasures.

Questions	Totally Agree	Agree	Do Not Know	Disagree	Strongly Disagree	Total
Antivirus and security software must be downloaded from licensed and trusted sources.	558	124	49	3	5	739
%	75.51	16.78	6.63	0.41	0.68	100.00
Antivirus software must be up to date.	509	162	58	6	4	739
%	68.88	21.92	7.85	0.81	0.54	100.00
I feel that all the devices I use are safe.	240	281	140	70	8	739
%	32.48	38.02	18.94	9.47	1.08	100.00
I am familiar with sites that will infect my computer with viruses if I visit them and download their programs.	267	227	198	30	17	739
%	36.13	30.72	26.79	4.6	2.30	100.00
The firewall (a program that provides protection for the network (the internet)) must be activated in all the devices we use.	360	242	125	11	1	739
%	48.71	32.75	16.91	1.49	0.14	100.00
We must use two-factor verification (example: the method of entering Mubashir for the Al Rajhi Bank application and entering the verification code sent by text message) if it is available.	480	187	55	13	4	739
%	64.95	25.30	7.44	1.76	0.54	100.00
Public networks (internet located in airports, parks, and malls) can be used and are safe to use on personal devices.	173	158	129	162	117	739
%	23.4	21.4	17.5	21.9	15.8	100.00
You can open any attachments (sent files such as Word files or others) sent to your email or social networks without worry.	144	201	126	179	89	739
%	19.5	27.2	17.1	24.2	12.0	100.00

Table 8. Respondents perception of data protection and security regarding passwords.

Questions	Totally Agree	Agree	Do Not Know	Disagree	Strongly Disagree	Total
I can use passwords that were previously used.	118	205	94	231	91	739
%	16.0	27.7	12.7	31.3	12.3	100.00
One password can be used for multiple sites.	145	224	72	186	112	739
%	19.6	30.3	9.7	25.2	15.2	100.00
Our passwords can be shared with others.	51	46	34	145	463	739
%	6.9	6.2	4.6	19.6	62.7	100.00
What annoys me is that I have long, strong, and different passwords for several sites, and it is hard for me to remember them all.	259	221	78	120	61	739
%	35.0	29.9	10.6	16.2	8.3	100.00
We must log out of our accounts (e.g., email, university website, bank applications, etc.) when work is complete.	365	200	80	71	23	739
%	49.4	27.1	10.8	9.6	3.1	100.00
Private passwords should not be recorded on paper or in device notes.	226	173	108	162	70	739
%	30.6	23.4	14.6	21.9	9.5	100.00
We have to remember passwords without going back to the device, and we do not let the device remember our passwords.	278	238	103	96	24	739
%	37.6	32.2	13.9	13.0	3.2	100.00
We must update the internet browser (the browser we use to visit sites such as Chrome, Safari, and others) and make sure to update it constantly.	381	251	92	10	5	739
%	51.6	34.0	12.4	1.4	0.7	100.00
We must constantly check browser links (the URLs that appear at the top of the page, i.e., https://www.google.com/ (accessed on 1 March 2023))	379	225	100	26	9	739
%	51.3	30.4	13.5	3.5	1.2	100.00

Table 8. *Cont.*

Questions	Totally Agree	Agree	Do Not Know	Disagree	Strongly Disagree	Total
Always use the incognito browser (users usually activate it when they connect to the internet from public networks such as coffee shops, airports, or public offices as it contributes to protecting privacy and your search history will not be saved after.	235	220	217	48	19	739
%	31.8	29.8	29.4	6.5	2.6	100.00
Passwords are secure if they are 12 characters long and contain lowercase and uppercase letters, numbers, special characters ($, &, ;, @, etc.), and punctuation.	430	218	45	43	3	739
%	58.19	29.50	6.09	5.82	0.41	100.00
Our passwords must be changed periodically.	224	209	110	171	25	739
%	30.3	28.3	14.9	23.1	3.4	100.00

Respondents were asked some security questions about their user password and the necessity to protect them. A total of 118 (16.0%) respondents totally agreed that they could use the passwords that have been previously used, 205 (27.7%) respondents agreed, 94 (12.7%) respondents dis not know, 231 (31.3%, the highest percentage) disagreed, and 91 (12.3%) respondents strongly disagreed. A total of 145 (19.6%) respondents agreed that one password could be used for multiple sites, 224 (30.3%, the highest percentage) respondents agreed, 72 (9.7%) respondents did not know, 186 (25.2%) respondents disagreed, and 112 (15.2%) respondents strongly disagreed. A total of 51 (6.9%) respondents totally agreed that passwords could be shared with others, 46 (6.2%) respondents agreed, 43 (4.6%) respondents did not know, 145 (19.6%) respondents disagreed, and 463 (62.7%) respondents (the highest percentage) strongly disagreed. A total of 259 (35.0%) respondents agreed that it is annoying to have long, strong, and different passwords for several sites and it was hard for them to remember them all, 221 (29.9%) respondents agreed, 78 (10.6%) respondents did not know, 120 (16.2%) respondents disagreed, and 61 (8.3%) respondents strongly disagreed. A total of 365 (49.4%) respondents (the highest percentage) totally agrees that they must log out of their accounts (e.g., email, university website, bank applications, etc.) when work is complete, 200 (27.1%) respondents agreed, 80 (10.8%) respondents did not know, 71 (9.6%) respondents disagreed, and 23 (3.1%) respondents strongly disagreed.

4.2.5. Data Protection Through Social Media Privacy

The last area of cybersecurity countermeasures this survey assesses is data protection and privacy. Table 9 shows the responses to data protection through social media privacy in detail.

Table 9. Respondents' perception of social media privacy.

Questions	Totally Agree	Agree	Do Not Know	Disagree	Strongly Disagree	Total
There is no harm in posting personal photos on social media.	131	154	149	154	151	739
%	17.7	20.8	20.2	20.8	20.4	100.00
There is no harm in accepting an extension from anyone on social media.	123	161	131	176	148	739
%	16.6	21.8	17.7	23.8	20.0	100.00
There is no harm in sharing your current location on social media.	105	121	107	174	232	739
%	14.2	16.4	14.5	23.5	31.4	100.00
There is no harm in sharing current job information on social media and updating the information continuously.	113	111	128	175	212	739
%	15.3	15.0	17.3	23.7	28.7	100.00
I know how to report any risks or threats (such as harassment or bullying) that I face when using social media.	323	238	120	36	22	739
%	43.7	32.2	16.2	4.9	3.0	100.00

Respondents were further asked some questions on data protection through social media. A total of 131 (17.7%) respondents agreed that there was no harm in posting personal photos on social media, 154 (20.8%) respondents agreed, 149 (20.2%) respondents did not know, 154 (20.4%) disagreed, and 151 (20.4%) respondents strongly disagreed. A total of 123 (16.6%) respondents totally agreed that there was no harm in accepting an extension from anyone on social media, 161 (21.8%) respondents agreed, 131 (17.7%) respondents did not know, 176 (23.8%) disagreed, and 148 (20.%) respondents strongly disagreed. A total of 105 (14.2%) respondents agreed that there was no harm in sharing your current location on social media, 121 (16.4%) respondents agreed, 107 (23.5%) respondents did not know, 174 (23.5%) respondents disagreed, and the highest percentage (31.4%, 232 respondents) strongly disagreed. About 113 (15.3%) respondents agreed that there was no harm in sharing current job information on social media and updating the data continuously., 111 (15.0%) respondents agreed, 128 (17.3%) respondents did not know, 175 (23.7%) respondents disagreed, and the highest percentage (28.7%, 212 respondents) strongly disagreed. Lastly, the highest percentage of respondents (323, 43.7%) totally agreed that they knew how to report any risks or threats (such as harassment or bullying) that they may face when using social media, 238 (32.2%) respondents agreed, 120 (16.2%) respondents did not know, 36 (4.9%) respondents disagreed, and 22 (3.0%) respondents strongly disagreed. At the end of this survey, we conducted an analysis to find out the extent to which trainees are attracted to matters related to cybersecurity and attend seminars, and the importance of raising awareness about cybersecurity, with the results shown in Tables 10–12.

Table 10. Previously attended or participated in an awareness program on cybersecurity.

Have You Previously Attended or Participated in an Awareness Program on Cybersecurity?	Freq.	Percentage %
No	507	68.6
Yes	232	31.4
Total	739	100.00
How long was the program you attended?		
1 to 3 days	40	5.4
3 to 5 days	21	2.8
Less than a day	142	19.2
More than 5 days	29	3.9
Total	232	31.4

Table 10 shows that 232 (31.4%) respondents had previously attended or participated in an awareness program on cybersecurity, while a higher percentage of respondents (507, 68.6%) had not previously attended or participated in an awareness program on cybersecurity. Out of the 232 respondents that had participated in an awareness program on cybersecurity, 40 respondents attended an awareness program that lasted for one to three days, 21 respondents attended an awareness program that lasted for three to five days, 142 respondents attended an awareness program that lasted for less than a day, and lastly, 29 respondents participated in an awareness program on cybersecurity that lasted for more than five days.

Table 11. Participant perceptions on the necessity of awareness programs.

Questions	Totally Agree	Agree	Do Not Know	Disagree	Strongly Disagree	Total
It is necessary to have an awareness program on cyber security these days to protect others from falling victim to hacking	506	164	58	8	3	739
%	68.5	22.2	7.8	1.1	0.4	100.00
Filling out this questionnaire was interesting	352	261	69	43	14	739
%	47.6	35.3	9.3	5.8	1.9	100.00

Respondents were questioned on the necessity of an awareness program on cybersecurity; 506 (68.5%) respondents totally agreed that it was necessary to have an awareness program on cybersecurity these days to protect others from falling victim to hacking, 164 (22.2%) respondents agreed, 58 (7.8%) respondents did not know, 8 respondents disagreed, and a very low proportion of respondents (3, 0.4%) strongly disagreed. However, the majority of the respondents (352, 47.6%) totally agreed that filling out this questionnaire was interesting and exciting, 261 (35.3) respondents agreed, 69 (9.3%) respondents did not know, 43 (5.8%) respondents disagreed, and very few respondents (14, 1.9%) strongly disagreed.

Table 12. Previous discussions of security aspects

This Is the First Time I Have Discussed the Security Aspects of the Devices I Have Used Regularly.	Freq.	Percentage %
No	60	8.1
Sometimes	205	27.7
Yes	474	64.1
Total	739	100.00

A total of 474 (64.1%) respondents said that this was the first time they had discussed the security aspects of the devices they use on a regular basis, 205 (27.7%) respondents said that they sometimes discuss the security aspects of the devices they use on a regular basis, while 60 (8.1%) respondents do not discuss the security aspects of the devices they use on a regular basis.

Figure 4 shows a bar graph between the type of operating system on respondents' devices and the tendency of being attacked, which was extracted from this survey. The chart shows that respondents with Windows devices are more likely to be either attacked by viruses, scammed, or hacked.

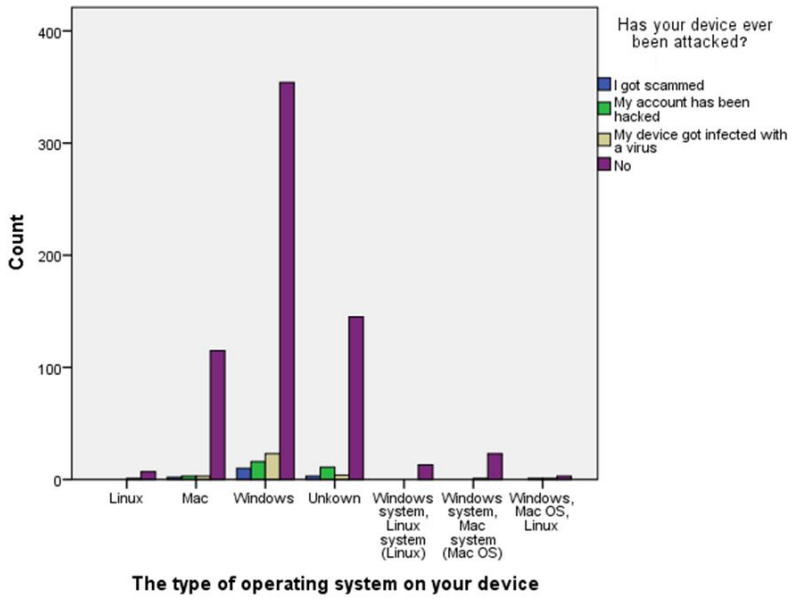

Figure 4. Relationship between type of operating systems and attacks.

4.3. Chi-Square Tests to Hypothesis Statement

This part of the study was conducted to help assess whether the likelihood of attacks on respondents' devices is dependent on the operating system they have installed on their devices. A Pearson's chi-squared test was used to evaluate the differences, where chi-square test use two categorical variables of independence: null hypothesis (0) if the variables are independent, and alternative hypothesis (a) if the variables are dependent. If the *p*-value is less than 0.05, we will reject the null hypothesis and can conclude that the two groups are dependent on each other. If the *p*-value is greater than 0.05, we will not reject the null hypothesis and can conclude that the two groups are independent of each other [36]. The *p*-value in Table 13 is greater than the 0.05 significance level and thus we do not reject the null hypothesis and conclude that the respondents' type of operating system they use, either Windows, Linux, or Mac, is not linked to the likelihood of being attacked.

That is, there is no relationship between the operating system and the whether the device will be attacked.

Table 13. Chi-Square Tests on OS and hacking.

Chi-Square Tests	Value	df	*p*-Value
Pearson Chi-Square	19.448a	18	0.365

In order to evaluate if respondents' perceptions of an awareness program on cyber security is dependent on their educational system, we used the chi-squared test of independence. chi-square test use two categorical variables of independence: null hypothesis (0): if the variables are independent, and alternative hypothesis (a): if the variables are dependent. Furthermore, this test was used to assess if respondents' perceptions on the necessity to have an awareness program on cyber security were dependent on their educational system or not. The *p*-value for both research questions in Table 14 is greater than the 0.05 significance level. We reject the null hypothesis and conclude that respondents who attended or participated in an awareness program on cybersecurity are not dependent on their educational system. Similarly, respondent perception of the necessity of having an awareness program on cybersecurity is not dependent on their educational system.

Table 14. Chi-squared test on security awareness.

Chi-Square Tests, Pearson Chi-Square Educational System	Value	df	*p*-Value
Previously attended or participated in an awareness program on cyber security?	0.348	2	0.840
It is necessary to have an awareness program on cybersecurity these days to protect others from hacking and falling victim.	10.989	8	0.202

5. Discussion and Limitations

The analyses were presented in frequency distribution tables, charts, percentages, and proportions using Chi-square test techniques. However, most of the respondents were female (61.98%), followed by males (38.02), out of which 98.78% attended the Technical and Vocational Training Corporation. The results in Table 1 report that most respondents were diploma holders (97.43%), while very few were bachelor degree holders (2.57%). Most respondents (54.53%) had a Windows operating system on their device, 16.64% had a Mac operating system, and few had a Linux operating system. In contrast, some respondents 5.69% had more than one operating system on their device. However, the majority of the respondents operating systems on their devices were updated automatically as the auto update feature was enabled, while 34.91% of respondents updated the operating systems on their devices manually, few respondents 4.06% had not updated their operating system on their device before because it was new, and 7.98% had never updated the operating system on their device. A higher percentage of the respondents used email, while few respondents only sometimes used email. The time respondents spent on social media was assessed, and the majority spent most of their time on Snapchat, WhatsApp, Instagram, and YouTube. The result reveal that the majority of respondents' devices have not been attacked before, at about 89.31%, while 4.47% had been infected by a virus, 4.19% had been hacked, and 2.03% had been scammed. A total of 0.4% of respondents who had been scammed did nothing afterwards and 1.6% informed the concerned authority and their bank card was suspended to secure their account from losing money without their authentication. A total of 1.4% of respondents who had had their account hacked also contacted the support for the hacked program, 0.8% did nothing, 0.8% informed everyone that their account had been hacked at the same time as contacting the support for the hacked program, while only 1.1% told everyone that their account was hacked. Some respondents' devices were infected

with a virus, and of these respondents, 0.9% ran a device scan program and deleted the files associated with the virus as a solution and 0.8% of these respondents went to tech support this while also running a device scan program to detect the viruses in the device. In contrast, 1.2% of respondents deleted the related virus files. In order to provide and build solutions to enhance protection, 36.94% of respondents had antivirus software installed to detect and protect devices against viruses, while 22.19% had only once or sometimes installed it on their devices. Respondents were assessed on their perception of the use and importance of antivirus software. Most agreed that antivirus and security software must be downloaded from licensed and trusted sources, while very few disagreed. A higher percentage of the respondents also agreed that antivirus software must be up to date, and very few disagreed. The responses to security questions showed that the majority disagreed with reusing previously used passwords and the majority agreed that one password can be used for multiple sites. In contrast, most of the respondents strongly disagreed with sharing their passwords with others. Finally, the perceptions of social media privacy were accessed, and most of the respondents strongly disagreed with the statement that there is no harm in sharing their current location on social media. Similarly, most respondents strongly disagreed that there was no harm in sharing current job information on social media and updating the information continuously. Theses results further reveal that most respondents know how to report any risks or threats faced on social media. Finally, respondents were asked about their awareness of cyber security programs. The results revealed that only 31.4% of respondents had previously attended or participated in an awareness program on cyber security. In contrast, the rest (68.6%) have never attended or participated in any awareness program on cyber security.

The results indicate that a significant portion of the awareness and responses concerning security and data privacy hinges on individual behavior and decision making, followed by the policies and guidelines set by organizations for their members. Making informed decisions and devising strategies to protect individuals and raise awareness about privacy and security when using personal devices, or those owned by an organization, can be challenging due to factors such as commitment, cost, and suitability for the specific environment.

In response to these challenges, researchers [4] have proposed the Nudge model, an approach that focuses on gentle interventions or prompts to encourage users to make more advantageous choices, considering both individual behavior and organizational needs. Rooted in behavioral economics, the Nudge concept assists individuals by subtly guiding them toward better decisions rather than enforcing rigid rules or regulations. This approach enables users to make more informed choices about privacy and security, fostering a safer online environment for both individuals and organizations.

5.1. Reliability Test

We have addressed the quality criteria using a reliability test; the closer the coefficient is to 1.0, the greater the internal consistency of items that are variables in the scale. Table 15 provides the value for Cronbach's alpha [49], showing a value of 0.808, indicating a high internal consistency level for our scale for these data. The item for each question presents Cronbach's alpha if the item is deleted. The column would present the value of Cronbach's alpha if a particular item were deleted from the scale shown in Table 15.

Table 15. Reliability test statistics.

Cronbach's Alpha	N of Items
0.808	30

5.2. Limitations

Although there are some limitations, this survey provides help and guidance for the TVTC to increase cybersecurity awareness and enhance existing policies. Nevertheless,

several limitations have been faced and should be avoided in the future, such as the data collection time and the sample size. Another limitation of this work is the number of questions, which can be optimized in the future to cover the most suitable cybersecurity awareness information instead of expanding it to more dimensions, such as the behavior on social media.

6. Conclusions and Future Work

Cybersecurity awareness is one of the most significant aspects of modern life that should be recognized and improved, particularly at educational institutions due to their direct connection to the network and the internet. Therefore, awareness of cybersecurity concepts and mechanisms should be improved, such as establishing solid passwords, upgrading systems, and employing antivirus software with the main aims of preventing data leaks and device hacking. Therefore, this quantitative study was conducted on trainees at the TVTC institution in the Kingdom of Saudi Arabia utilizing questionnaires. The results indicated that the majority needed an appropriate foundation in cyber security expertise and statistical analysis. Therefore, awareness must be raised among TVTC trainees and training on cyber security strategies that help them protect their devices and data should be implemented. Furthermore, a focus should be placed on developing plans and strategies for cybersecurity awareness among students and trainees of educational institutions to enable users to understand the threats and factors that lead to weaknesses on their devices and data, and their effectiveness should be tested continuously. Based on the survey in our paper, we suggest the following:

- A course should be included in each foundation specialization to raise awareness of cybersecurity, which can be implemented as an electronic course.
- Trainees should be offered the chance to specialize in technology under the supervision of cybersecurity specialists who conduct awareness campaigns in the institution's departments (for example, during a week, each day is devoted to a section of the institution).
- Sensitive applications such as banks or university pages should contain an awareness list regarding the application's security, so the reader is encouraged to read it before opening the application.
- During job interviews, a set of cybersecurity questions and their basic concepts should be presented to test the applicability of the candidates.
- Cybersecurity awareness should be raised by conducting educational experiments to attempt to penetrate the trainees' devices to educate them about possible vulnerabilities and the usefulness of auxiliary programs such as antivirus software.
- The Nudge model [4] is a helpful factor to assist users in making better privacy and security decisions online for particular individuals who may not have the knowledge or motivation to make optimal choices on their own. The Nudge model includes several additional dimensions such as providing a realistic view of risks by making information clear and consistent, improving the user interface, which helps in increasing cognitive awareness, and also introducing incentives to encourage users to act. By providing gentle guidance, nudges can encourage users to take actions that will improve their online safety without feeling overwhelmed or burdened by complex decision-making processes.

A more scalable questionnaire can be implemented to increase the sample size and include more than one educational institution for comparison. Furthermore, another study could be conducted after providing a cybersecurity awareness course to measure its impact of on the respondents. The questionnaire also can be expanded to include members, employees, and trainees of industrial sectors to compare the results with academic institutions.

Author Contributions: Conceptualization, S.A. (Shouq Alrobaian) and A.A.; methodology, S.A. (Shouq Alrobaian); software, S.A. (Shouq Alrobaian); validation, S.A. (Saif Alshahrani) and S.A. (Shouq Alrobaian) and investigation, S.A. (Saif Alshahrani); resources, A.A.; writing—original draft preparation, S.A. (Shouq Alrobaian); writing—review and editing, A.A.; visualization, S.A. (Shouq Alrobaian); supervision, A.A.; project administration, A.A.; funding acquisition, A.A. All authors have read and agreed to the published version of the manuscript.

Funding: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through large group Research Project under grant number RGP.2/550/44.

Data Availability Statement: data is unavailable due to privacy or ethical re-strictions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* **2014**, *80*, 973–993. [CrossRef]
2. Reis, J.; Amorim, M.; Melão, N.; Matos, P. Digital transformation: A literature review and guidelines for future research. In Proceedings of the World Conference on Information Systems and Technologies ; Springer: Berlin/Heidelberg, Germany, 2018; pp. 411–421.
3. Alharbi, T.; Tassaddiq, A. Assessment of cybersecurity awareness among students of Majmaah University. *Big Data Cogn. Comput.* **2021**, *5*, 23. [CrossRef]
4. Acquisti, A.; Adjerid, I.; Balebako, R.; Brandimarte, L.; Cranor, L.F.; Komanduri, S.; Leon, P.G.; Sadeh, N.; Schaub, F.; Sleeper, M.; et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 1–41. [CrossRef]
5. Guarino, A.; Malandrino, D.; Zaccagnino, R. An automatic mechanism to provide privacy awareness and control over unwittingly dissemination of online private information. *Comput. Netw.* **2022**, *202*, 108614. [CrossRef]
6. Lippi, M.; Pałka, P.; Contissa, G.; Lagioia, F.; Micklitz, H.W.; Sartor, G.; Torroni, P. CLAUDETTE: An automated detector of potentially unfair clauses in online terms of service. *Artif. Intell. Law* **2019**, *27*, 117–139. [CrossRef]
7. Guarino, A.; Lettieri, N.; Malandrino, D.; Zaccagnino, R. A machine learning-based approach to identify unlawful practices in online terms of service: Analysis, implementation and evaluation. *Neural Comput. Appl.* **2021**, *33*, 17569–17587. [CrossRef]
8. Galinec, D.; Možnik, D.; Guberina, B. Cybersecurity and cyber defence: National level strategic approach. *Autom. Časopis Autom. Mjer. Elektron. Računarstvo Komun.* **2017**, *58*, 273–286. [CrossRef]
9. Oliver, D.; Randolph, A.B. Hacker definitions in information systems research. *J. Comput. Inf. Syst.* **2022**, *62*, 397–409. [CrossRef]
10. Craigen, D.; Diakun-Thibault, N.; Purse, R. Defining cybersecurity. *Technol. Innov. Manag. Rev.* **2014**, *4* . [CrossRef]
11. National Cybersecurity Authority, Saudi Arabia. 2017. Available online: https://nca.gov.sa/en/about (accessed on 10 January 2023) .
12. Saudi Federation for Cybersecurity, Programming & Drones. 2017. Available online: https://safcsp.org.sa/en/ (accessed on 10 February 2023).
13. Almudaires, F.; Rahman, M.H.; Almudaires, M. An Overview of Cybersecurity, Data Size and Cloud Computing in light of Saudi Arabia 2030 Vision. In Proceedings of the 2021 International Conference on Information Technology (ICIT),Amman, Jordan, 14–15 July 2021; IEEE: New York, NY, USA, 2021; pp. 268–273.
14. Alzubaidi, A. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon* **2021**, *7*, e06016. [CrossRef]
15. Cyberattacks Hit 95% of Saudi Businesses Last Years, Says Study. 2020. Available online: https://www.arabnews.com/node/1718596/saudi-arabia (accessed on 22 October 2022).
16. Nurse, J.R. Cybersecurity Awareness. *arXiv* **2021**, arXiv:2103.00474.
17. Majmaah University. 2023. Available online: https://www.mu.edu.sa/en (accessed on 15 March 2023).
18. Khader, M.; Karam, M.; Fares, H. Cybersecurity Awareness Framework for Academia. *Information* **2021**, *12*, 417. [CrossRef]
19. Capital Area Finance Authority. 2023. Available online: https://thecafa.org (accessed on 30 March 2023).
20. Nidup, Y. Awareness about the Online Security Threat and Ways to Secure the Youths. *J. Cybersecur.* **2021**, *3*, 133. [CrossRef]
21. Taherdoost, H. Determining sample size; how to calculate survey sample size. *Int. J. Econ. Manag. Syst.* **2017**, *2* .
22. Taha, N.; Dahabiyeh, L. College students information security awareness: A comparison between smartphones and computers. *Educ. Inf. Technol.* **2021**, *26*, 1721–1736. [CrossRef]
23. Alqahtani, M.A. Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis. *Comput. Intell. Neurosci.* **2022**, *2022*, 6775980 . [CrossRef]
24. Aldawood, H.; Skinner, G. Educating and raising awareness on cyber security social engineering: A literature review. In Proceedings of the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, Australia, 4–7 December 2018; IEEE: New York, NY, USA, 2018; pp. 62–68.
25. Khushali, V. A Review on Fileless Malware Analysis Techniques. *Int. J. Eng. Res. Technol. (IJERT)* **2020**, *9* , 46–49. [CrossRef]

26. Mogal, M.M.; Gonsalves, F. How Two Factor Authentication Helps in Cybersecurity. *Int. Res. J. Mod. Eng. Technol. Sci.* **2022**, *4*, 2390–2395.
27. Arefin, M.T.; Uddin, M.R.; Evan, N.A.; Alam, M.R. Enterprise network: Security enhancement and policy management using next-generation firewall (NGFW). In Proceedings of the Computer Networks, Big Data and IoT: Proceedings of ICCBI 2020, Madurai, India, 19–20 December 2018; Springer: Berlin/Heidelberg, Germany, 2021; pp. 753–769.
28. Armstrong, L.; Phillips, J.G.; Saling, L.L. Potential determinants of heavier internet usage. *Int. J. Hum.-Comput. Stud.* **2000**, *53*, 537–550. [CrossRef]
29. Sosanya, O.V. Beyond Cyber Security Tools: The Increasing Roles Of Human Factors Furthermore, Cyber Insurance in the Survival of Social Media Organisations. Available online: https://www.cybsafe.com/research/beyond-cyber-security-tools-the-increasing-roles-of-human-factors-and-cyber-insurance-in-the-survival-of-social-media-organisations/ (accessed on 16 March 2023).
30. Rasool, A.; Jalil, Z. A review of web browser forensic analysis tools and techniques. *Res. J. Comput.* **2020**, *1*, 15–21.
31. Eke, H.N.; Odoh, N.J. The use of social networking sites among the undergraduate students of University of Nigeria, Nsukka. *Libr. Philos. Pract.* **2014**, 1–11.
32. Allen, I.E.; Seaman, C.A. Likert scales and data analyses. *Qual. Prog.* **2007**, *40*, 64–65.
33. Khonji, M.; Iraqi, Y.; Jones, A. Phishing detection: A literature survey. *IEEE Commun. Surv. Tutorials* **2013**, *15*, 2091–2121. [CrossRef]
34. Monnappa, K. *Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware*; Packt Publishing Ltd.: Birmingham, UK, 2018.
35. Souppaya, M.; Scarfone, K. *Guide to Enterprise Patch Management Technologies*; NIST Special Publication: Washington, DC, USA, 2013; Volume 800, p. 40.
36. Turney, S. Chi-Square Tests: Types, Formula & Examples. 2022. Available online: www.scribbr.com/statistics/chi-square-tests/ (accessed on 26 October 2022).
37. Frick, R.W. Accepting the null hypothesis. *Mem. Cogn.* **1995**, *23*, 132–138. [CrossRef] [PubMed]
38. Samonas, S.; Coss, D. The CIA strikes back: Redefining confidentiality, integrity and availability in security. *J. Inf. Syst. Secur.* **2014**, *10* , 21–45.
39. Shen, L. The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer* **2014**, *10*, 16.
40. Facebook Mainpage. Available online: https://www.facebook.com/public/Main-Page (accessed on 18 February 2023).
41. Instgram. Available online: https://www.instagram.com (accessed on 18 February 2023).
42. Linkedin. Available online: https://www.linkedin.com (accessed on18 February 2023).
43. Snapchat. Available online: https://www.snapchat.com (accessed on18 February 2023).
44. Twitter. Available online: https://twitter.com (accessed on 18 February 2023).
45. YouTube. Available online: https://www.youtube.com (accessed on 18 February 2023).
46. WhatsApp. Available online: https://www.whatsapp.com (accessed on 18 February 2023).
47. Baskerville, R.; Rowe, F.; Wolff, F.C. Integration of information systems and cybersecurity countermeasures: an exposure to risk perspective. *ACM SIGMIS Database DATABASE Adv. Inf. Syst.* **2018**, *49*, 33–52. [CrossRef]
48. Kruger, H.; Steyn, T.; Dawn Medlin, B.; Drevin, L. An empirical assessment of factors impeding effective password management. *J. Inf. Priv. Secur.* **2008**, *4*, 45–59. [CrossRef]
49. Bonett, D.G.; Wright, T.A. Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *J. Organ. Behav.* **2015**, *36*, 3–15. [CrossRef]