big data and cognitive computing

MDPI

Article

Assessment of Cybersecurity Awareness among Students of Majmaah University

Talal Alharbi [1,*] and Asifa Tassaddiq [2]

[1] Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majmaah 11952, Saudi Arabia
[2] Department of Basic Sciences and Humanities, College of Computer and Information Sciences, Majmaah University, Al Majmaah 11952, Saudi Arabia; a.tassaddiq@mu.edu.sa
* Correspondence: talal@mu.edu.sa; Tel.: +966-164-046-730

Abstract: Information exchange has become increasingly faster and efficient through the use of recent technological advances, such as instant messaging and social media platforms. Consequently, access to information has become easier. However, new types of cybersecurity threats that typically result in data loss and information misuse have emerged simultaneously. Therefore, maintaining data privacy in complex systems is important and necessary, particularly in organizations where the vast majority of individuals interacting with these systems is students. In most cases, students engage in data breaches and digital misconduct due to the lack of knowledge and awareness of cybersecurity and the consequences of cybercrime. The aim of this study was to investigate and evaluate the level of cybersecurity awareness and user compliance among undergraduate students at Majmaah University using a scientific questionnaire based on several safety factors for the use of the Internet. We quantitatively evaluated the knowledge of cybercrime and protection among students to show the need for user education, training, and awareness. In this study, we used a quantitative research methodology and conducted different statistical tests, such as ANOVA, Kaiser–Meyer–Olkin (KMO), and Bartlett's tests, to evaluate and analyze the hypotheses. Safety concerns for electronic emails, computer viruses, phishing, forged ads, popup windows, and supplementary outbreaks on the Internet were well-examined in this study. Finally, we present recommendations based on the collected data to deal with this common problem.

Keywords: cybersecurity; security awareness; information security; statistical analysis

Citation: Alharbi, T.; Tassaddiq, A. Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data Cogn. Comput.* **2021**, *5*, 23. https://doi.org/10.3390/bdcc5020023

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

Received: 24 March 2021
Accepted: 6 May 2021
Published: 10 May 2021

1. Introduction

The exponential growth in modern technologies has revolutionized our lives, particularly the communication channels used to widely disseminate information and to interact with others in real time. Various communication techniques have been developed worldwide. Consequently, public and private sectors have begun to offer more services and adopt new technologies to provide access to information anytime and anywhere upon request from customers. The key reason behind automating services and adopting new technologies is to support and satisfy a wide range of customers, whose number has been increasing rapidly owing to the increase in the usage of the Internet [1].

In response, the number of hackers and organized cybercrime groups has grown exponentially. These cybercriminals have been adopting new methods to carry out cybercrime. The primary motivation for hacking is the financial gain obtained by stealing sensitive information and holding it for ransom. Hackers can also earn money by selling secret data to competitors on the dark web, which makes cyberspace unsafe and poses considerable risks to organizations and their customers. Thus, cybersecurity breaches have become a serious threat to global security and the economy, targeting critical infrastructure and having a considerable financial impact on business performance and results in a significant loss of intellectual property [2].

Cybersecurity should be prioritized across an organization, not just in the IT department [3]. The worldwide increase in cybersecurity incidents is mainly because most people do not strictly follow the exact security rules and instructions provided at the workplace. A top security threat that renders organizational assets vulnerable to external and internal actors is the people of an organization; that is, they are the weakest link [4]. In most cases, hackers gain unauthorized access to critical systems hosted in a secure environment through human mistakes [5,6]. Therefore, employing active cybersecurity measures is essential, particularly in developed countries, such as the Kingdom of Saudi Arabia, where the Internet is an integral part of people's lives. The percentage of computer users increased substantially from 43% to 51% during 2007–2009. By 2018, the percentage of Internet users was approximately 19% [7–11].

According to the Telecommunications Act of June 2001, the Kingdom of Saudi Arabia has increasingly invested in strengthening its security posture and thinks that developing and regulating the telecommunications sector is vital [12]. Therefore, the Communications and Information Technology Commission (CITC) was established to regulate the Internet and monitor incoming and outgoing network traffic. This helps protect cyberspace and reduce cybersecurity threats across countries. In 2006, the Computer Emergency Response Team (CERT) was formed with the aim of imparting institutions with the skills and competencies to be able to detect and prevent cyberattacks through educational and training functions [13]. The rank of the Kingdom in the domain of technology innovation has dramatically accelerated among developed countries owing to the inclusion of cybersecurity in Saudi Vision 2030 [14].

Given the rapid growth in cyberthreats and cybercrime, cybersecurity awareness in the Kingdom has neither received sufficient attention nor has the importance of security been investigated among college students [15]. Due to the higher recurrence of hacking assaults on the data frameworks in schools and colleges, it is vital that students be aware of the consequences and challenges of cybersecurity and cybercrime. There is an urgent need to establish a comprehensive training program to increase awareness regarding the dangers of loss of sensitive information, as it may result in reducing the confidence of students and in undermining the reliability of schools [16–19]. Accordingly, we performed an empirical assessment of cybersecurity awareness and practices among students, focusing on the most common security issues threatening the entire environment. Our key contributions are as follows:

- We assessed and explored the cybersecurity awareness level among college students at Majmaah University by concentrating on several safety factors for the use of the Internet.
- We investigated and analyzed the security knowledge and skills of students regarding information security and cybercrime using multiple statistical tests.
- We theoretically constructed approaches to enhance cybersecurity awareness among students and enlighten students about the hazards and challenges prevailing in computer networks.
- We suggest the best security measures and procedures based on the gap observed in the current state-of-the-art methods to handle incidents correctly and efficiently and embed security culture into the college environment.

The remainder of this paper is organized as follows: Section 2 discusses the related works, and Section 3 presents the methodology used to assess the cybersecurity awareness level. Section 4 describes the analysis results based on the dataset collected in this study. Section 5 presents the findings of the statistical tests performed in this study, and Section 6 concludes the paper.

2. Related Work

This section summarizes the related prior studies conducted in the area of measurement of the individual awareness level of cybersecurity. However, only a few studies

focused on the cybersecurity awareness level among college students and the relevant key problems.

Cybersecurity awareness and training programs can be part of national security and should be well-structured to provide people with the basic knowledge of cybersecurity. Al-Janabi and Al-Shourbaji [20] presented a survey on security awareness in the Middle East, focusing on educational settings and analyzing security awareness among academic staff, researchers, and students. The authors observed that the contributors in the Middle East do not have the essential awareness of the significance of cybersecurity. Therefore, the overall security management plan should include security awareness and training for all administrators and users. Ahmed et al. [21] studied the awareness of cybersecurity among a population in Bangladesh and analyzed the collected data based on Pearson's chi-squared test [22]. These studies indicated that the proper guidelines and awareness programs that should to be provided by governments are missing. Consequently, most people are unaware of cybercrime and cybersecurity issues.

Most academic institutions do not include active cybersecurity awareness and training programs in their strategic plans. Slusky and Partow-Navid [23] briefly analyzed the outcomes of security assessment for a group of students at the College of Business and Economics at California State University, Los Angeles, USA. They observed that the key problem related to cybersecurity awareness is not the absence of required information, as might be expected; instead, it is the approach used by students while dealing with this information in practical circumstances. The findings were intended to help the college design its syllabus, which included additional information security training.

Alotaibi et al. [24] discussed the cybersecurity awareness level among college students. Their analysis showed that the cybersecurity knowledge among the students in Saudi universities is insufficient, as most students were not conscious of the safety of their information. Similarly, Senthilkumar and Easwaramoorthy [25] conducted a survey of college students in the main towns of Tamil Nadu, India, to assess their responsiveness toward cybersecurity. They specifically focused on different cybersecurity threats, such as websites infected with malware, phishing, and stealing personal information. Their analysis showed that the awareness level of the students in terms of cybersecurity and related threat issues was above average, that is, 70% of the respondents had a basic knowledge of cybersecurity threats. Therefore, the authors suggested that security awareness and training programs should be initiated at a higher level to ensure that students are able to ensure the safety of their information from cyberattacks.

Moallem [26] examined students' attitudes toward cybersecurity in the Silicon Valley in California, USA. The author focused on evaluating the cybersecurity level among students in the most advanced technological environment in the world because their behavior is tremendously diverse. College students were not conscious of the safety of their information, even though they were aware that their activities were observed and monitored, and their data were not securely transmitted across the university networks. Therefore, universities should regularly conduct training to change the behavior of students and improve their understanding of the fundamentals of cybersecurity and cyberthreats [27].

Moallem [28] discussed the understanding of the state of privacy awareness and theft mindfulness. The author observed that criminals do not always use the same attack vectors. Instead, they shift between email phishing, network traffic, etc., aiming at deception. Thus, it is necessary to formalize a plan of action to increase cybersecurity awareness and learn to protect sensitive information. Zwilling et al. [29] focused on the correlation among cybersecurity mindfulness, understanding, and activities using protection tools, based on users in Turkey, Israel, Poland, and Slovenia. The results demonstrated that common users had satisfactory cybersecurity knowledge, but it was rarely employed in practice. The initial outcomes of studies at Nigerian universities showed that students possessed elementary cybersecurity knowledge, but were unaware of how to protect their information [30]. Aljeaid et al. [31] attempted to assess the end-user knowledge related to phishing attacks, focusing on the assessment of the understanding of and responsiveness

toward cybersecurity threats. Several authors have experimentally shown that users with insufficient knowledge can be easily deceived [32–34].

3. Methodology

3.1. Research Tools

The survey technique was used to achieve the objectives of the study and collect qualitative information about the level of cybersecurity knowledge among the students of Majmaah University. The survey was conducted online to obtain a large sample of male and female students in an efficient and ethical manner. The questionnaire consisted of 50 questions to cover different aspects of cybersecurity, including demographics (5 questions); Internet usage (10 questions); the use of security tools, such as anti-virus and firewall (7 questions); phishing awareness (5 questions); cryptology (8 questions); browser security (5 questions); social networking (4 questions); and cybersecurity knowledge (6 questions). The survey questions were selected based on instruments developed by other researchers on cybersecurity [35].

The questions included in the Internet usage section aimed to explore the behavior of students when they are connected to the Internet. The questions regarding the use of security tools aimed to analyze the current security practices among the students of Majmaah University. The questions regarding phishing awareness were aimed to evaluate their knowledge of phishing and viruses. The browser security section was aimed to evaluate the students' understanding of security of the browser usually used by them. The social networking and cybersecurity knowledge sections assessed the awareness levels of the students on the risk of using different social network platforms and on how to respond to an incident of cybercrime. Thus, we investigated the cybersecurity knowledge, skills, behavior and attitudes, and self-perception of the students.

3.2. Study Setting and Participants

The survey was originally designed in English and then translated into Arabic to make it clear to the participants and to obtain accurate answers. The preliminary version was reviewed by seven native Arabic speakers who were fluent in English and experts in translation to ensure the accuracy of the translation and the linguistic equivalence. We conducted two pilot tests to evaluate the feasibility of the techniques and to ensure the validity of the questions. Then, we analyzed the feedback received from the participants and restructured the survey to obtain the final version of the survey. The first pilot study aimed to ensure that the questions included in the survey were suitable for students from different educational backgrounds and that they could be answered in a timely manner. Therefore, we distributed hard copies of the survey to 10 students from different colleges. The first five students were selected randomly from the College of Computer and Information Sciences, which consisted of two departments, namely, computer science and information technology. The remaining five students were selected from five colleges belonging to different fields. The participants of the first pilot test strongly recommended shortening the survey and clarifying some technical terms. Accordingly, the final version of the survey was reduced to 50 precise questions, providing extensive descriptions and definitions of some cybersecurity technical terms for the benefit of those who did not hail from an IT background. Next, we uploaded the updated questionnaire to Google Forms and made it accessible only to the target respondents. The purpose of the study was clearly stated on the first page. The survey link was sent to the Deans of all colleges via their official Majmaah email, seeking their help to distribute and share the questionnaire with the departments of their concerned colleges. The snowball sampling technique was adopted to increase the sample size; consequently, 576 students of Majmaah University completed the online survey questionnaire.

3.3. Inclusion and Exclusion Criteria

The participants had to be 18 years old and above. Participants under the age of 18 were excluded because the focus of this study was on the cybersecurity awareness level among adult students.

3.4. Research Strategy

In this study, a multilevel survey process was undertaken to enhance the quality of the questionnaire and ensure that the questions included in the survey were clear and accurate. After editing the entire survey based on the feedback, the final version was posted online to collect data about the level of cybersecurity awareness among the students of Majmaah University. Based on the survey results, measures were developed to strengthen the cybersecurity knowledge and promote security awareness among the students of Majmaah University.

3.5. Respondents' Impression

In the questionnaire, we asked the respondents about their impressions on how excited they were to fill out the survey questionnaire. The respondents were given five options: strongly agree, agree, neutral, disagree, and strongly disagree (that filling out the survey was exciting).

As shown in Figure 1, the majority of the respondents felt that the survey was exciting, whereas only a few felt that it was not exciting to participate in the survey. As 75% of the respondents felt excited about participating in the survey, this indicated that the survey was well-designed.

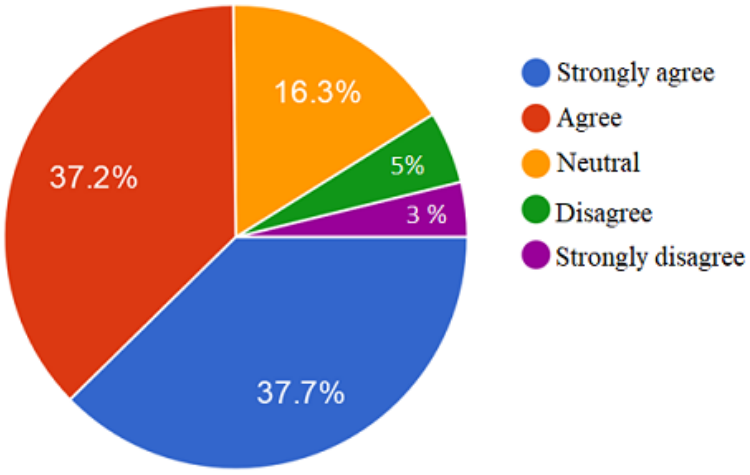

Figure 1. Respondents' impression about answering the survey.

4. Results

We intended to analyze the entire group of students defined as the population, and the respondents were the sample selected as a subset of the population. We aimed to conduct a survey for the majority of students of Majmaah University as a population, focusing on the awareness and attitudes of students toward multiple cybersecurity concerns, such as viruses, phishing, forged flyers, pop-ups, and patching. To achieve these research objectives, we used the research distribution and students' knowledge of the main cybersecurity concepts, countermeasures, password management, browser security, and social network platforms.

4.1. Research Distribution

One of the research objectives was to measure the influence of the life cycle demographics of the students on the adoption of cybersecurity measures. Therefore, demographic variables, such as sex, age, the college currently attended by the participants, the year

of study, and the devices used on a daily basis, were selected. Table 1 summarizes the demographic information of the participants of the study in more detail.

Table 1. Demographic information of research respondents.

Variables		Number #	Percentage %
Sex	Male	353	61.3
	Female	223	38.7
Age (years)	18–25	536	93.1
	26–34	28	4.9
	Above 34	12	2.1
Type of College	College of Computer and Information Sciences (Number of IT/Cybersecurity = 7)	89	15.4
	College of Science (Number of IT/Cybersecurity = 3)	39	6.8
	College of Science and Humanities (Number of IT/Cybersecurity = 1)	94	16.3
	College of Business Administration (Number of IT/Cybersecurity = 1)	46	8
	College of Applied Medical Sciences (Number of IT/Cybersecurity = 1)	58	10.1
	College of Medicine (Number of IT/Cybersecurity = 1)	37	6.4
	College of Dentistry (Number of IT/Cybersecurity = 1)	47	8.1
	College of Engineering (Number of IT/Cybersecurity = 1)	39	6.8
	College of Education (Number of IT/Cybersecurity = 0)	73	12.7
	Community College (Number of IT/Cybersecurity = 0)	54	9.4
Year of Study	1st year	70	12.2
	2nd year	124	21.5
	3rd year	143	24.8
	4th year	112	19.5
	5th year	77	13.4
	Internship year	49	8.5
Daily Used Device	Smart phone	435	75.5
	Tablet	92	16
	Desktop	12	2.1
	Laptop	37	4.2

As presented in Table 1, most of the respondents were between 18 and 25 years of age (93.1%), as the target of the study was college students. There were more male participants (61.3%) than female participants (38.7%). The key indicator of the respondents' background was the college they attended. With regard to the devices used regularly, most of the participants (75.5%) used smartphones, followed by those who used tablets (16%).

4.2. Knowledge of Main Cybersecurity Concepts

The fundamental concepts of cybersecurity are confidentiality, integrity, and availability, that is, the CIA triad. These aspects can be achieved by applying particular processes and techniques to systems and services connected directly to the Internet. Academic institutions should take measures to protect their sensitive data and networks from ever-increasing cyberattacks because hackers are using increasingly sophisticated approaches [36]. Students are the most vulnerable assets in universities; therefore, we investigated students' knowledge of the fundamental concepts of cybersecurity.

Table 2 indicates that 40.1% of the students applied updates automatically, leaving the responsibility for updating outdated software to the device, whereas 42.4% of the students applied updates manually. However, 17.6% of them either neglected updates or did not update at all, making their devices vulnerable and easy to attack and compromise.

Table 2. Result of "How do you update your device?"

Variable	Frequency	Percentage (%)
Automatic update (No intervention from the user)	231	40.1
Manual update (User disables automatic update and updates outdated software when it is needed)	244	42.4
No update (User does not apply required updates)	32	5.6
Neglect update (User does not care about updates at all)	69	12

Adults nowadays spend a considerable amount of time on their cellphones and computers, as we observed through this survey. On average, the students spent four to eight hours per day on cellphones and computers, even when they were busy. However, we think that this time may drastically increase when they have free time. Figure 2 shows the most commonly used social networks among the college students.

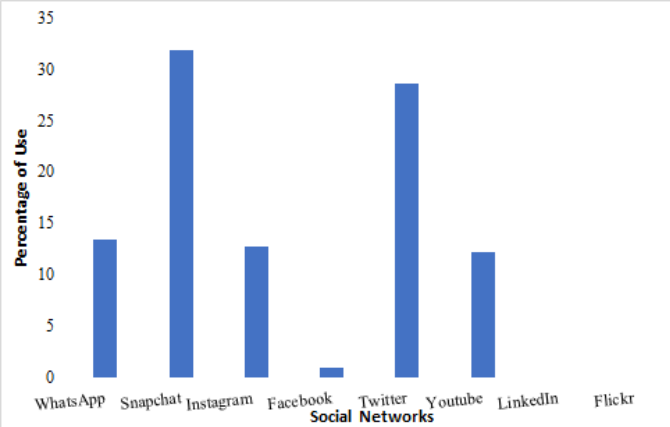

Figure 2. Most-used social networks.

4.3. Knowledge of Cybersecurity Countermeasures

The architecture of a computer includes built-in protection mechanisms to enforce security policies and combat cyberattacks. Antivirus software, more broadly referred to as antimalware software, is mainly designed to protect users when they are tricked into downloading malicious attachments or clicking malicious links. The software tracks the patterns of usage and distinguishes between normal and abnormal patterns based on the definitions and signatures obtained from its database [37].

Therefore, students should understand the basic principles of antivirus software and the application of its functions to protect their systems and services. We expected that the majority of the students would have antivirus software installed on their personal computers. However, we observed that more than 30% of them had not installed any antivirus software on their systems. They believed that there was no need for protection, and no one could access their computers if their username and password were strong and kept private. These participants were unaware of firewalls and did not know that they help keep their devices safe. Specifically, they did not know whether the firewall was enabled on their devices or not.

We also observed that approximately 21% of the respondents were unaware of the dangers of installing free software from unreliable and unknown sources. This number is quite high and unexpected because the Deanship of IT at Majmaah University frequently sends text messages and emails advising against this practice. Most surprisingly, 41% of the students could not recognize situations where their computers were infected with malware or controlled by hackers.

Only 22% of the students were unaware of two-factor authentication and did not know how it added an extra layer of security. Apparently, they had not enabled this mechanism on their accounts when it became available, which is consistent with the findings discussed

in a recently published paper [38]. Some people do not adopt the two-factor authentication mechanism because they believe it is annoying to use and difficult to deal with [39].

The students were also unaware of how to use their emails safely and securely. We observed that 75% of them often checked their emails regularly from public Wi-Fi without using a virtual private network (VPN) or attempting to make the connection secure. The same participants answered "Yes" to the question of whether they would open an email received from an unknown or strange sender. This indicated that the security awareness program and security training seminar usually conducted by the university are not well-designed and do not cover this aspect.

4.4. Knowledge of Password Management

The password is considered a basic and important security aspect that protects data and information and provides access to authenticated systems. The recommended characteristics of a strong password include the following: the password should be at least 12 characters long, including alpha and numeric characters, and a mix of both uppercase and lowercase letters with at least one symbol, that is, a special character [40]. Therefore, we explored the students' knowledge of the core principles of password security and examined how they manage their passwords.

Table 3 indicates that 42.7% of the students used strong passwords all the time and believed that the password must be changed periodically. However, 60.7% of them felt that having a strong and long password was annoying; hence, they used the same password for all websites and accounts, assuming that this is sufficient to secure their accounts and is the best security practice. Unfortunately, in this case, if an attacker compromises one account and discovers the password, the attacker will attempt to use the same password for other accounts.

Table 3. Password security questions.

Variable	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
All my passwords include: 12 upper and lower characters, numbers, and symbols	42.7%	30.4%	14.1%	9.7%	3.1%
I must change my password periodically	19.4%	24.3%	27.3%	18.4%	10.6%
I can use previously used passwords	13.5%	26.4%	22.4%	23.8%	13.9%
I use one strong password for across different websites and accounts	17.4%	30.7%	19.4%	18.6%	13.9%
It is annoying to have a long and strong password for each website and account	34.5%	26.2%	19.4%	10.1%	9.7%
I often share my passwords with others	4.5%	5%	6.3%	19.8%	64.4%

4.5. Knowledge of Browser Security

Users must know how to protect networked data from breaches, which usually occur because of the vulnerabilities of the browser. Thus, it is important to train users on the security features that will significantly enhance the overall browser security for safe online browsing to combat most security exploits [41]. Accordingly, we evaluated the students' knowledge of important web browser security mechanisms because malware can be implemented as a browser extension.

Table 4 indicates that more than 80% of the students regularly updated their web browser, which is a great practice for patching zero-day vulnerability and preventing malware attacks. They also appeared to be aware of the risks involved in installing extensions from third-party websites and unknown resources. Approximately 60% of them checked the security settings and configurations of the web browser regularly and knew how to find suspicious activities from the browser history. This indicates that they could protect their systems against common attacks that bypass built-in security mechanisms and web browser protection, such as website tracking, zombie cookies, and adware.

Table 4. Browser security questions.

Variable	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The web browser should be updated regularly	41%	38.2%	17.5%	2.3%	1%
I should avoid installing extensions from third-party websites	31.6%	37.7%	25.5%	2.8%	2.4%
I must check the security settings and configurations of the web browser periodically	29.9%	29.5%	27.1%	10.2%	3.3%
I must check the browser history and find suspicious activities	35.2%	37.7%	18.4%	6.4%	2.3%

4.6. Knowledge of Social Network Platforms

Hackers obtain users' personal data through social engineering techniques that can easily lure users to reveal confidential information with minimal hacking skills. It is known that most students are active on social media and sometimes post sensitive information [42]. Therefore, we thought that it was critical to perform an exploratory study on how college students behave on social media.

Table 5 indicates that most of the students shared personal pictures on public social media accounts with no hesitation. This can inadvertently leak sensitive and confidential information, such as personal identifiable information (PII) [43]. Notably, 56% of the students kept their location private and never shared it publicly on social media. It is complicated to report harmful and abusive violations on social media; however, in this survey, more than 70% of the respondents knew how to report any threat they faced.

Table 5. Social network platform questions.

Variable	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
It is acceptable to post personal pictures on social media	15.6%	21.9%	26.7%	18.8%	17%
It is ok to accept friend requests from strangers	14.4%	21.2%	30.2%	22.7%	14.4%
There is no problem with sharing my current location publicly on social media	8.5%	12%	23.3%	26.9%	29.3%
There is no problem with adding all personal information like data of birth, current job, etc.	9.7%	14.4%	23.4%	24.3%	28.1%
I know how to report any threat or suspicious activity on social media	33.5%	38.5%	15.5%	9%	3.5%

5. Discussion and Findings of Tests

To the best of our knowledge, this study is the first to examine students' knowledge of cybersecurity. The findings presented reveal the cybersecurity awareness level among college students and motivate new research directions in this area to develop efficient tools and techniques to measure the improvement in students' knowledge and understanding of cybersecurity. Most of the participants in the survey were unaware of the fundamental concept of cybersecurity and did not know how to manage their data, even though 92% of them had attended a formal security awareness program. Phishing attacks are increasing daily, targeting users who have little or no knowledge of cybersecurity. In this section, we measure the validity and reliability of the method used in this study to ensure the consistency of the inter-variables with the study constructs.

5.1. Study Limitations

Although the findings presented in this paper provide important points for developing cybersecurity awareness program, several limitations need to be highlighted, which we plan to improve in the future. The questions covered in the survey should be checked by cybersecurity experts. The preliminary data produced valuable results; however, further research needs be carried out on different student populations and different universities. The sample size must be increased, which may improve the findings.

5.2. Reliability Test

Table 6 indicates the value of Cronbach's alpha for the reliability of the scale used in this study. The standard value for this test to be acceptable in the social sciences is a minimum of 0.70 [44]. In our study, the alpha value was calculated as 0.811, which is

significant and acceptable for further research. Thus, any inference drawn based on these findings is reliable.

Table 6. Reliability statistics.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. Items
0.795	0.811	50

5.3. Factor Analysis

Factor analysis is a statistical technique generally used to observe a set of variables and determine the interrelationships among correlated variables, aiming to convert a large number of correlated variables to a lower number of factors for either confirmatory or exploratory purposes [45]. In this study, we used factor analysis for confirmatory purposes and data summary. Therefore, we adopted Kaiser–Meyer–Olkin (KMO) and Bartlett's tests to evaluate the collected data and determine whether they were suitable for the factor analysis.

Table 7 highlights the sampling adequacy used to evaluate the relationship among the data within the constructs we analyzed [46]. Overall, the questionnaire assessed the constructs, such as the use of security tools, phishing, cryptology, browser security, social networking, and cybersecurity knowledge, with the dependent variable of cybersecurity awareness. The result of this test was 0.795, which is relatively close to 0.8, which denotes a meritorious level of data adequacy [47]. The internal correlations of the possible constructs also showed a significance value (P = 0.000); thus, we concluded that the data collected were sufficient to continue the evaluation of possible factor outcomes and draw inferences from the study. This test also provided the constructs we analyzed.

Table 7. KMO and Bartlett's test of sampling adequacy.

KMO and Bartlett's Test (This Test Is Based on Correlations)		
Kaiser–Meyer–Olkin measure of sampling adequacy		0.795
Bartlett's test of sphericity	Approx. chi-square	7.565×10^3
	df	946
	Sig.	0.000

Table 8 illustrates the component correlation matrix, which shows the internal correlations of each component examined in this study. The r values of the constructs between themselves are mostly positive, which indicates that each component is positively associated with cybersecurity awareness, except encryption whose r value is −0.081. This inverse correlation value explains the inverse relationship between our password habit component and the level of cybersecurity awareness. In reality, this finding is contrary to the normal tendency of the existence of relationships; consequently, we re-evaluated our data composition. As presented in Table 1, only 89 respondents hailed from an IT background, which constitutes approximately 15.4% of the total respondents, whereas the remaining 84.6% of the respondents belonged to a non-IT field. Therefore, it is possible that 84.6% of the respondents did not have sufficient knowledge about this aspect.

Table 8. Component correlation matrix (extraction method: principal component analysis. Dependent variable: cybersecurity awareness. Rotation method: oblimin with Kaiser normalization).

Component	Use of Security Tools	Phishing	Cryptology	Browser Security	Social Networking	Cybersecurity Knowledge	Cybersecurity Awareness
Use of security tools	1						
Phishing	0.041	1					
Cryptology	0.135	−0.097	1				
Browser security	0.203	0.032	0.115	1			
Social networking	0.296	−0.147	0.049	0.211	1		
Cybersecurity knowledge	0.093	0.106	0.091	0.112	0.028	1	
Cybersecurity awareness	0.094	0.034	−0.081	0.095	0.076	0.09	1

Table 9 presents the results of the analysis of variance (ANOVA) used to determine the standard deviation and variability for each question used in this study and for each extracted component collectively. The overall value of significance was acceptable (0.05% level of significance). However, the sum of squares and mean squares were significantly high, indicating that the variability in the constructs led to an acceptance of the result. Thus, we concluded that the constructs analyzed in this study were reliable for evaluating the cybersecurity awareness level of the respondents.

Table 9. ANOVA (dependent variable: level of awareness and predictors (constant): use of security tools, phishing, cryptology, browser security, social networking, and cybersecurity knowledge).

	Model	Sum of Squares	df	Mean Square	F	Sig.
1	**Regression**	93.152	6	15.525	117.158	0.000
	Residual	74.341	561	0.133		
	Total	167.493		567		

Table 10 presents a model summary of the extent of influence of all the components on cybersecurity awareness. The R^2 value determined the overall rate of change in this study. We inferred that all the components (use of security tools, phishing, cryptology, browser security, social networking, and cybersecurity knowledge) resulted in a 55% change in the level of awareness of the respondents. These findings indicated that the respondents' level of cybersecurity awareness fell within the average level. A higher R^2 value would indicate that the respondents were at a good level of awareness in keeping their systems and services secure and safe. The *p*-value (0.000) indicated that these findings are significant and reliable to be projected further and can be used for any future decisions.

Table 10. Model summary (predictors: (constant), use of security tools, phishing, encryption, browser safety, social networking, and enhancing related knowledge).

Model	R	R Square	Adjusted R-Square	Standard Error of the Estimate	Change Statistics				
					R-Square Change	F Change	df1	df2	Sig. F Change
1	0.746	0.556	0.551	0.36403	0.556	117.158	6	561	0.000

Table 11 highlights the coefficient values to estimate the impact of each component used in this study. This table provides an analysis of each component individually to observe its relationship with the level of awareness and is different from Table 10, which indicates the overall level of awareness. The beta values and significance levels are now considered. The beta value of security tools was 0.286, with a significant p-value = 0.000. This relationship indicates that the use of security tools enhanced cybersecurity awareness by 28.6%. This is evident as the majority of the respondents appeared to be aware of firewalls and antivirus software, that is, the basic concepts of cybersecurity, as discussed earlier. The second component is phishing, which has a beta value of 0.581 and a significant p-value = 0.000. This indicates that phishing positively influenced the awareness level of the respondents about cyberthreats. Notably, the respondents were aware of phishing attacks. The third component is cryptology, which has a beta value of 0.196 with a significance p-value = 0.000. This indicates that cryptology raised the awareness level among the respondents by 19.6%. This level of response was apparent, as these types of arrangements are usually made at the backend; hence, the respondents appeared to not be fully aware of these security arrangements made by the service providers. The next component is social networking, which has a beta value of 0.142 with a significant p-value = 0.000. This indicates that social networking enriched the cybersecurity awareness level by 14.2%. It was also observed that only 14.2% of the respondents were aware of the cybersecurity issues encountered through social networking. The remaining two components, browser security and cybersecurity knowledge, appear to be insignificant, with the p-values of 0.007 and 0.643, respectively. This indicates that the respondents were not fully aware of the security issues related to web browsers. It also appears that the students lacked the essential knowledge of cybersecurity [48].

Our results were compared with similar research conducted in multiple countries. For example, the p-value for different components of cybersecurity awareness was $p = 0.002$ in Bangladesh [21]. A similar survey was administered in India and the p-value was 0.003934 based on the responses to cybersecurity awareness among college students [25]. Further, the study [29] conducted in Turkey found a significant and positive connection to cybersecurity awareness with $\beta = 2.654$ and $p < 0.01$, but Israel ($\beta = -0.139$; $p < 0.01$) and Poland ($\beta = -0.315$; $p < 0.01$) were negatively associated with cybersecurity awareness. This demonstrates that the level of cybersecurity awareness in Israel and Poland was lower compared with that in other countries. Our study revealed a significant p-value ($p < 0.001$) for different associated components. This indicates that students at Majmaah University were aware of security tools, phishing, encryption, browser safety, social networking and other related knowledge. However, several reasons may have affected the results. For example, our sample was only students mostly aged 18–25 years. The younger generation is becoming more aware of security and related concerns. More than 60% of the respondents in our research were men, and as found in [24], the male population in the Kingdom of Saudi Arabia is more aware of security and related issues than women. In [27], t-values showed the same type of measures with t = 2.234; 10.87; 3.194; $p < 0.05$. According to the high level of comparison with published papers [24–34], it was found that the data collected even in tech-savvy surroundings [26] had approximately the same statistical measures as in California, USA. Hence, in view of this comparison, we assessed that the behavior of people even in the presence of a good level of awareness is the main obstacle to overcome in managing cybersecurity threats and challenges. They are aware but they do not take the necessary precautions.

Table 11. Coefficients (dependent variable: level of awareness).

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95% Confidence Interval for B	
		B	Standard Error	Beta			Lower Bound	Upper Bound
1	(Constant)	1.754	0.015		114.803	0.000	1.724	1.784
	Use of security tools	0.155	0.016	0.286	9.493	0.000	0.123	0.187
	Phishing	0.316	0.016	0.581	19.507	0.000	0.284	0.347
	Cryptology	0.107	0.016	0.196	6.700	0.000	0.075	0.138
	Browser security	0.044	0.016	0.081	2.729	0.007	0.012	0.076
	Social networking	0.077	0.016	0.142	4.674	0.000	0.045	0.109
	Cybersecurity knowledge	0.007	0.016	0.013	0.464	0.643	-0.023	0.038

6. Conclusions and Recommendations

Information security is essential for academic institutions, where most users have no knowledge of the basic concepts of cybersecurity or of the best practices on how to protect their devices from malware, viruses, and scams. In this study, we evaluated cybersecurity knowledge among college students at Majmaah University, located in Saudi Arabia, via a quantitative research approach. Overall, we mathematically demonstrated that a cybersecurity awareness and training program for students should be included in the security management plan and strongly promoted by top executives and managers. Academic institutions need to hold comprehensive security awareness and training sessions regularly to ensure that all users know how to recognize the most common cybersecurity threats and vulnerabilities. Based on the analysis results, we recommend the following:

- Majmaah University should promote knowledge on common cybersecurity factors, including vulnerabilities, attacks, and incidents, to their students to strengthen their security position.
- Passive awareness methods, such as email, oral presentation, newsletters, and SMS messages, are insufficient for educating users. There is a need to integrate more proactive methods, such as training and interviews. A combination of both methods is more effective and highly recommended.
- The delivery methods for cybersecurity awareness and training programs can be video-based, text-based, or game-based, as the target here is adult students. Security awareness must be taught at an early age to develop a sustainable cybersecurity behavior among users.
- Different datasets should be obtained from different universities and the findings should be systematically compared with those presented in this paper. Further questions should be added to cover all the important aspects of cybersecurity behavior.

Author Contributions: Conceptualization, T.A.; methodology, T.A. and A.T.; validation, A.T.; formal analysis, T.A. and A.T.; investigation, T.A. and A.T. ; writing—original draft preparation, T.A. and A.T.; writing—review and editing, T.A. Both authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Acknowledgments: The authors would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work.

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

References

1. Gamreklidze, E. Cyber security in developing countries, a digital divide issue: The case of Georgia. *J. Int. Commun.* **2014**, *20*, 200–217. [CrossRef]
2. Garg, A.; Curtis, J.; Halper, H. Quantifying the financial impact of IT security breaches. *Inf. Manag. Comput. Secur.* **2003**, *11*, 74–83. [CrossRef]
3. Green, M.J.S. *Cyber Security: An Introduction for Non-Technical Managers*; Ashgate Publishing, Ltd.: Farnham, UK, 2015.
4. Whitman, M.E.; Mattord, H.J. *Principles of Information Security*; Cengage Learning: Boston, MA, USA, 2011.
5. Willard, N.E. *Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn to Use the Internet Safely and Responsibly*; John Wiley & Sons: Hoboken, NJ, USA, 2007.
6. Simsim, M.T. Internet usage and user preferences in Saudi Arabia. *J. King Saud Univ. Eng. Sci.* **2011**, *23*, 101–107. [CrossRef]
7. Internet Usage in the Kingdom of Saudi Arabia. Available online: www.citc.gov.sa/en/reportsandstudies/studies/Pages/Computer-and-Internet-Usage-in-KSA-Study.aspx (accessed on 20 February 2021).
8. Aboul Enein, S. Cybersecurity Challenges in the Middle East. Available online: https://www.gcsp.ch/publications/cybersecurity-challenges-middle-east (accessed on 30 April 2021).
9. Sait, S.M.; Al-Tawil, K.M.; Ali, S.; Hussain, A. Use and effect of Internet in Saudi Arabia. 2003. Available online: https://core.ac.uk/download/pdf/242401013.pdf (accessed on 30 April 2021).
10. Katz, F.H. The effect of a university information security survey on instruction methods in information security. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, 23–24 September 2005; pp. 43–48.
11. Alshankity, Z.; Alshawi, A. Gender differences in internet usage among faculty members: The case of Saudi Arabia. In Proceedings of the 2008 Conference on Human System Interactions, Krakow, Poland, 25–27 May 2008.
12. CITC Roles and Responsibilities. Available online: www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/default.aspx (accessed on 20 February 2021).
13. Hathaway, M.; Spidalieri, F.; Alsowailm, F. *Kingdom of Saudi Arabia Cyber Readiness at a Glance*; Potomac Institute for Policy Studies: Arlington, VA, USA, 2017.
14. Nurunnabi, M. Transformation from an oil-based economy to a knowledge-based economy in Saudi Arabia: the Direction of Saudi Vision 2030. *J. Knowl. Econ.* **2017**, *8*, 536–564. [CrossRef]
15. ALArifi, A.; Tootell, H.; Hyland, P. Information Security Awareness in Saudi Arabia. In Proceedings of the CONF-IRM, Vienna, Austria, 21–23 May 2012; Volume 57, pp. 1–11.
16. Aloul, F.A. The need for effective information security awareness. *J. Adv. Inf. Technol.* **2012**, *3*, 176–183. [CrossRef]
17. Boneh, D.; Lynn, B.; Shacham, H. Short signatures from the Weil pairing. In *International Conference on the Theory and Application of Cryptology and Information Security*; Springer: Berlin/Heidelberg, Germany, 2001; pp. 514–532.
18. Liu, X.; Zhang, Y.; Wang, B.; Yan, J. Mona: Secure multi-owner data sharing for dynamic groups in the cloud. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *24*, 1182–1191. [CrossRef]
19. Kamara, S.; Lauter, K. Cryptographic cloud storage. In *International Conference on Financial Cryptography and Data Security*; Springer: Berlin/Heidelberg, Germany, 2010, pp. 136–149.
20. Al-Janabi, S.; Al-Shourbaji, I. A study of cyber security awareness in educational environment in the middle east. *J. Inf. Knowl. Manag.* **2016**, *15*, 1650007. [CrossRef]
21. Ahmed, N.; Kulsum, U.; Azad, I.B.; Momtaz, A.Z.; Haque, M.E.; Rahman, M.S. Cybersecurity awareness survey: An analysis from Bangladesh perspective. In Proceedings of the 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Dhaka, Bangladesh, 21–23 December 2017.
22. Plackett, R.L. Karl Pearson and the chi-squared test. *Int. Stat. Rev. Int. Stat.* **1983**, *51*, 59–72. [CrossRef]
23. Slusky, L.; Partow-Navid, P. Students information security practices and awareness. *J. Inf. Priv. Secur.* **2012**, *8*, 3–26. [CrossRef]
24. Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. A survey of cyber-security awareness in Saudi Arabia. In Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016.
25. Senthilkumar, K.; Easwaramoorthy, S. A Survey on Cyber Security awareness among college students in Tamil Nadu. In *IOP Conference Series: Materials Science and Engineering*; IOP Publishing: Bristol, UK, 2017; Volume 263, p. 042043.
26. Moallem, A. Cyber Security Awareness Among College Students. In *International Conference on Applied Human Factors and Ergonomics*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 79–87.
27. Taha, N.; Dahabiyeh, L. College students information security awareness: a comparison between smartphones and computers. *Educ. Inf. Technol.* **2020**, *26*, 1–16. [CrossRef]
28. Moallem, A. *Cybersecurity Awareness Among Students and Faculty*; CRC Press: Boca Raton, FL, USA, 2019.
29. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2020**. [CrossRef]
30. Garba, A.; Sirat, M.B.; Hajar, S.; Dauda, I.B. Cyber Security Awareness Among University Students: A Case Study. *Sci. Proc. Ser.* **2020**, *2*, 82–86. [CrossRef]
31. Aljeaid, D.; Alzhrani, A.; Alrougi, M.; Almalki, O. Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. *Information* **2020**, *11*, 547. [CrossRef]

32. Ahram, T.Z.; Nicholson, D. Advances in Human Factors in Cybersecurity. In Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, Orlando, FL, USA, 21–25 July 2018; Springer: Berlin/Heidelberg, Germany, 2018.
33. Al-Khater, W.A.; Al-Maadeed, S.; Ahmed, A.A.; Sadiq, A.S.; Khan, M.K. Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access* **2020**, *8*, 137293–137311. [CrossRef]
34. Garba, A.A.; Siraj, M.M.; Othman, S.H.; Musa, M. A Study on Cybersecurity Awareness among Students in Yobe State University, Nigeria: A Quantitative Approach. Available online: https://www.researchgate.net/publication/343600853_A_Study_on_Cybersecurity_Awareness_Among_Students_in_Yobe_A_Quantitative_Approach (accessed on 30 April 2021).
35. 2015 Cyber Security Survey: Major Australian Business. Available online: www.cyber-securityhub.gov.za/cyberawareness/images/pdfs/2015-ACSC-Cyber-Security-Survey-Major-Australian-Businesses.pdf/ (accessed on 20 February 2021).
36. Shen, L. The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer* **2014**, *10*, 16.
37. 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]
38. Colnago, J.; Devlin, S.; Oates, M.; Swoopes, C.; Bauer, L.; Cranor, L.; Christin, N. "It's not actually that horrible" Exploring Adoption of Two-Factor Authentication at a University. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018; pp. 1–11.
39. Fennell, C.; Wash, R. Do Stories Help People Adopt Two-Factor Authentication? Available online: https://www.rickwash.com/papers/SOUPS2019_LBW_Submission.pdf (accessed on 30 April 2021).
40. 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]
41. Ter Louw, M.; Lim, J.S.; Venkatakrishnan, V.N. Enhancing web browser security against malware extensions. *J. Comput. Virol.* **2008**, *4*, 179–195. [CrossRef]
42. Alwagait, E.; Shahzad, B.; Alim, S. Impact of social media usage on students academic performance in Saudi Arabia. *Comput. Hum. Behav.* **2015**, *51*, 1092–1097. [CrossRef]
43. Mesch, G.S. Is online trust and trust in social institutions associated with online disclosure of identifiable information online? *Comput. Hum. Behav.* **2012**, *28*, 1471–1477. [CrossRef]
44. Taber, K.S. The use of Cronbach's alpha when developing and reporting research instruments in science education. *Res. Sci. Educ.* **2018**, *48*, 1273–1296. [CrossRef]
45. Cavana, R.; Delahaye, B.; Sekeran, U. *Applied Business Research: Qualitative and Quantitative Methods*; John Wiley & Sons: Hoboken, NJ, USA, 2001.
46. Cerny, B.A.; Kaiser, H.F. A study of a measure of sampling adequacy for factor-analytic correlation matrices. *Multivar. Behav. Res.* **1977**, *12*, 43–47. [CrossRef] [PubMed]
47. Kaiser, H.F.; Rice, J. Little jiffy, mark IV. *Educ. Psychol. Meas.* **1974**, *34*, 111–117. [CrossRef]
48. Abawajy, J. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.* **2014**, *33*, 237–248. [CrossRef]