applied sciences

MDPI

Article

Factors Affecting Cybersecurity Awareness among University Students

Mohammed A. Alqahtani

Department of Computer Information Systems, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; maqhtani@iau.edu.sa; Tel.: +966-50-584-8693

Abstract: One of the essential stages in increasing cyber security is implementing an effective security awareness program. This work studies the present level of security knowledge among Imam Abdulrahman Bin Faisal University college students. A module was created to assist the students in becoming more informed. The main contribution of this work is an assessment of cybersecurity awareness among the university students based on three essential aspects: password security, browser security, and social media. Numerous questions were designed and sent to them to evaluate their awareness. The current survey received as many as 450 responses with their answers. Various statistical analyses were applied to the responses, including the validity and reliability test, feasibility test of a variable, correlation test, multicollinearity test, multiple regression, and heteroskedasticity test, carried out using SPSS. Furthermore, a multiple linear regression model and coefficient of determination, a hypothesis test, ANOVA test, and a partial test using ANOVA were also carried out. The hypothesis investigated here concerns password security, browser security, and social media. The results of partial hypothesis testing using a *t*-test showed that the password security variable significantly affects cybersecurity awareness (*p*-value = 0.0001). The regression coefficient of the password security variable in the multiple linear regression model was found to have a beta value of 0.147. In addition, the browser security variable significantly affects awareness, with a *p*-value = 0.0001. The regression coefficient of the password security variable had a beta value of 0.188. The social media activities variable significantly affects cybersecurity awareness (*p*-value = 0.0001). The regression coefficient of the social media activities variable had a beta value of 0.241. Based on the research conducted, it is concluded that knowledge of password security, browser security, and social media activities significantly influences cybersecurity awareness in students. Overall, students have realized the importance of cybersecurity awareness.

Keywords: cybersecurity; password security; browser security; social media; ANOVA; SPSS

check for updates

Citation: Alqahtani, M.A. Factors Affecting Cybersecurity Awareness among University Students. *Appl. Sci.* **2022**, *12*, 2589. https://doi.org/10.3390/app12052589

Academic Editor: Suhuai Luo

Received: 14 January 2022
Accepted: 24 February 2022
Published: 2 March 2022

1. Introduction

The rapid advancement of contemporary technology has altered our life, particularly the methods of communication utilized to provide information and interact with people. Everywhere in the world, several networking techniques have been developed. In response, both the social and commercial spheres have begun to offer additional services and embrace new technologies to give customers data access anywhere at any time and from any place. The primary motivation for automation operations and innovation is to help the diverse variety of customers, fast-expanding due to increased Internet usage [1].

As a result, the number of hackers and organized cybercrime gangs has skyrocketed. These cybercriminals have been exploring new ways to carry out cyber-attacks. The primary motivation for cyber criminals seems to be the personal benefit gained by acquiring sensitive information and retaining it for blackmail. Hackers may also benefit by supplying private information to competition on the dark web, making cyberspace insecure and presenting significant threats to businesses and customers. As a result, cyber security breaches have become a severe danger to world security and the economy, compromising essential infrastructure and wreaking havoc on company performance, resulting in significant cognitive property loss [2].

Cyber security should be emphasized throughout a business, not only in IT [3,4]. The global trend in cyber security issues is primarily due to the fact that most personnel do not adequately adhere to the specific security regulations and instructions supplied in the workplace. People represent a significant security vulnerability that exposes organizational assets to external and internal attackers; they are the weakest link [5,6]. The human factor is the most common way for hackers to get unauthorized access to vital systems in a protected environment [7,8]. As a result, implementing proactive cyber security measures is essential, particularly in developed nations where the Internet is a fundamental part of everyone's life, such as Saudi Arabia. During 2007–2009, the ratio of Internet users improved significantly, rising from 43 percent to 51 percent. By 2018, the rate of Internet users was around 19% [9–13].

The Kingdom of Saudi Arabia has expanded its investment in boosting its security infrastructure, according to the Telecommunications Act of June 2001. Therefore, it is vital to strengthen and manage the telecommunications industry [14]. It was for this purpose that the Communications and Information Technology Commission (CITC) was established to supervise Internet regulation and network traffic. In addition, the Computer Emergency Response Team (CERT) was established in 2006 to provide organizations with the knowledge and skills needed to identify and prevent cyber-attacks through teaching and training activities [14]. As a result of the incorporation of cyber security in Saudi Vision 2030, the Kingdom's standing in the sphere of technological advancement has rapidly increased in industrialized nations [15].

Cyber security awareness has received insufficient attention given the fast rise in cyber dangers and cybercrime in the Kingdom. The importance of security has not been examined among college students [16]. Since hacking attacks of data systems in schools and colleges are becoming more widespread, students must understand the implications and problems of cyber security and cybercrime. There is an urgent need to design a comprehensive training program to raise awareness of the consequences of personal information loss, which may undermine student confidence and institutional credibility [17–20].

It is the most basic and widely used safeguarding system. The first stage in obtaining safe access is to provide the user's login and passcode. The main issue with passcodes is that we can forget them. As a result, we frequently search for ways to remember them, such as writing them in a notebook, using toolkits to organize and save passcodes (passcode managers or passcode keepers), or by using "Cookies", which keep the user ID and passcode (hashed) to access the website. Another disadvantage of this method is that passcodes could be stolen or decrypted [21–23].

Increased Web Browser Attack—The services supplied by developing technologies are often delivered through web pages. Web browsers are undoubtedly the most widely adopted apps, allowing consumers to undertake a wide range of tasks that attach them to an outside world. As a result, Internet browsers are becoming an immensely crucial tool for millions of Internet users nowadays. Unfortunately, like every piece of software, Internet browsers have a variety of flaws [24,25]. The hackers use such defects to gain control of the user's computer, hack the customer's data, delete files and use the stolen machine to target other systems. According to an Osterman Research report [26], 11 million virus variants had been detected by 2008, with 90 percent of these viruses originating from covert downloads from prominent and often credible locations. If Internet browser consumers do not identify a rogue website, they risk disclosing personal details to a potentially hazardous party. Our survey focuses on active security indicators since active security measures are directly tied to automatic hacking identification in Internet browsers.

Social media are electronic connections (such as social networking websites and microblogging platforms) wherein people build online groups to exchange information, thoughts, or private messages. Privacy is defined as "independence from unapproved access" and the capacity to govern one's data since only those whom the possessor desires to have access to them are permitted to use them. This encompasses both authorities with respect to what material is visible on social media and who may see it. Social media use is widespread across general culture and on school campuses. The growing reputation of social media websites has given rise to a new range of concerns and problems that now confront us in the twenty-first century. Since digital networks are their primary modes of communication, modern college youth are at a higher risk of image injury or loss of money than previous generations. As a result, we conducted an experimental evaluation of students' cyber security understanding and activities, concentrating on the most frequent security vulnerabilities facing the overall ecosystem. Some of the key contributions are listed below:

- A cybersecurity awareness assessment was carried out with the college students of Imam Abdulrahman Bin Faisal University based on a few key issues, such as password security, browser security, and social media;
- An investigation was conducted to analyze the students' level of knowledge about security concerns, especially cybercrime;
- Statistical analysis was performed and, based on numerous tests, the results were estimated;
- The data was collected through the survey questionnaires and, based on the responses, SPSS and ANOVA tools were utilized to make the analysis.

The remainder of this paper is organized as follows: Section 2 contains a literature review, Section 3 discusses the research methodology, Section 4 presents the results which were subject to many tests, and Section 5 consists of a discussion of the results, after which the paper is concluded.

2. Literature Review

This section highlights previous findings undertaken to measure individual cyber security awareness levels. It should be noted, however, that only a few studies have aimed to determine the level of cyber security awareness among students and the associated significant challenges.

2.1. Cybersecurity Awareness

Cyber security awareness and training programs might be an element of national security and they should be well-structured to provide people with a basic grasp of cyber security. Al-Janabi and Al-Shourbaji [27] studied Middle Eastern security awareness, concentrating on school environments and examining cyber security within teaching faculties, among researchers and students. The authors revealed that participants in the Middle East do not have a basic understanding of the importance of cyber security. As a result, all users and administrators should be given safety awareness and training as part of an overall safety management strategy. Ahmed et al. [28] investigated cyber security recognition in the Bangladeshi population and evaluated the acquired data using Pearson's chi-squared test [29]. According to these findings, governments fail to offer the necessary guidelines and awareness initiatives. As a result, most individuals are uninformed about cybercrime and cyber security risks.

Most academic organizations' business strategies do not incorporate active cyber security awareness and training initiatives. Slusky and Partow-Navid [30] examined the results of security testing for a group of pupils at California State University, Los Angeles, USA, College of Business and Economics. They discovered that the main issue with cyber security awareness is not a lack of essential knowledge, as one might think; instead, it is the methods pupils use when coping with these issues in real-world situations. The results were meant to aid the institution in developing its curriculum, which included extra information security training.

2.2. Students' Knowledge

Alotaibi et al. [31] investigated the level of cyber security knowledge among college students. Their investigation revealed that cyber security awareness in Saudi university students is poor since most students were unaware of their data protection. Correspondingly, Senthilkumar and Easwaramoorthy [32] studied university students in Tamil Nadu's key towns to examine their attentiveness to cyber security. They concentrated on particular cyber security risks, such as malware-infected websites, phishing, and the theft of personal information. According to their findings, students' awareness of cyber security and related threat problems was above average, with 70% of respondents having a basic understanding of cyber security dangers. As a result, the authors proposed that security awareness and training programs be launched at a higher level to guarantee that learners can protect their data from cyber-attacks.

Moallem [33] investigated students' opinions regarding cyber security in California's Silicon Valley. Since learners' behavior is variable, the author assessed the cyber security level in the largest and most influential technology environment. Even when they were aware that their actions were being seen and tracked, college students were unaware that their data was not safely transported across university systems. As a result, institutions should offer training regularly to influence students' behavior and increase their awareness of the basics of cyber security and cyber threats [34]. In addition, Moallem [35] discussed the level of security awareness and theft mindfulness. Fraudsters may not always utilize the same cyber-attacks, according to the author.

Instead, they switch between phishing scams, network traffic, and other methods of deceit. As a result, it is vital to develop a plan to raise cyber security awareness and secure critical data. Zwilling et al. [36] investigated the relationship between cyber security awareness, comprehension, and activity with protection product users in Turkey, Israel, Poland, and Slovenia. The findings showed that although familiar users possessed adequate cyber security awareness, it was seldom used in practice. Preliminary research results at Nigerian institutions revealed that students possessed basic cyber security knowledge but were unsure how to secure their information [37]. Al said et al. [38] aimed to measure end-user awareness of phishing attempts, emphasizing understanding and reactions to cyber security risks. Several writers have demonstrated experimentally that consumers with limited information may be readily duped [39–41].

2.3. Password Security

As a result of the increasing number of passcodes to recall, users either choose simple but default passcodes [42] or reprocess their possibly strong passcode [43–45], occasionally with slight adjustments or merely by pursuing predetermined building activities [46]. According to one survey, 80% of users retained their existing passcodes wherever feasible whereas 16% changed them to one of the passcodes they had been using on some other website, while 4% used passcodes that were more or less fresh [47]. One of the most severe security issues caused by passcode repetition arises in the context of data theft. Consumers are warned that when a website they use is hacked by the European Union's General Data Protection Regulation (GDPR), they are strongly advised to change their passcodes. Even if the user accomplishes this, however, other identities secured with the same credentials are also vulnerable. It has been claimed that about eight billion records were released in different data thefts in the first nine months of 2019 alone [48], possibly opening the gates to many more companies, some of which are vital for the user or the community. According to an American study of users of various backgrounds and ages [49], consumers have a skewed knowledge of safety features. According to the findings of this study, respondents overvalued the safety enhancement provided by adding digits to their passcodes while underestimating the reliability of employing keyboard rhythms and frequent terms. In a poll conducted by [50], individuals not only overvalued the enhanced safety of attaching characters or numbers at the end of passcodes but often reused passcodes or portions of passcodes. Another prevalent occurrence is the incorporation of private details into user-chosen passcodes.

In research by [51], which examined over 20 million chunks of information from Chinese users, it was discovered that experts used passcodes with a standard size of 8–11 characters, whereas pupils used shorter passcodes. In terms of passcode protection, they found that more than half of consumers had passcodes that merely consisted of numbers and less than a third contained a mix of special typescripts. The research also indicated that more than 12 percent of corporate users utilize their birthdays and cell phone numbers in their passcodes, while 11.5 percent use their username and e-mail to generate their passcodes. Another study of Chinese passcodes [52] found that the usage of Chinese characters, alone or in conjunction with dates and numerals, accounted for 26% of the whole, suggesting that the use of English alphabets is prevalent. It was also noted that genuine Chinese character logins were created using only two to four Chinese characters.

2.4. Social Media

"Users' comprehension of dangers and how to defend themselves against computer hackers is consequently crucial in modern existence", writes [31]. As per a Pew Research Centre [53] study, 69 percent of US people use Facebook and 73 percent use YouTube. Instagram, Pinterest, Snapchat, LinkedIn, Twitter, Reddit, and WhatsApp have much smaller percentages of users. Eighty percent of people aged 18–24 use at least one social networking site. Specifically, 94% use YouTube, 81% use Facebook, 78% use Snapchat, 71% use Instagram, and 45% use Twitter. In Richardson's [54] (2017) study, 90 percent of respondents used Facebook and Snapchat, while 70 percent used Instagram. Most users check their profiles many times every day [53] (Pew Research Center, 2019). Knight-McCord [55] (2016) researched which social networking sites were most popular among students. They administered a survey to 363 pupils online and in person. Previous research discovered that Instagram was the most popular site, with Snapchat and Facebook second. LinkedIn and Pinterest, on the other hand, were less popular. According to Sharma, Jain, and Tiwari [56], 84 percent of students believe that posting personal information on social networking sites (SNS) is harmful. Moallem [33] (2018) researched cyber security knowledge among students at two California State universities in Silicon Valley.

3. Materials and Methods

A survey approach was utilized to meet the study's goals and collect qualitative data on the degree of cyber security awareness among Imam Abdulrahman Bin Faisal University students. The study was carried out online to ensure that a mixed group of male and female pupils' responses were collected quickly and responsibly. There were 20 items in the survey covering all aspects of cyber security, including five demographic items.

The questions in the Internet use section were designed to elicit information about students' online behavior. The questions about the usage of security technologies were designed to assess current security practices in IAU University students. The browser security component was designed to evaluate students' comprehension of the security of the browsers they often use. Finally, the networking sites and cyber security knowledge portions examined students' understanding of the risks of utilizing various social networking platforms and how to respond to a cybercrime occurrence. As a result, we investigated the students' cyber security awareness, abilities, behavior and attitudes, and self-perceptions. These questions were distributed to undergraduate and post-graduate students, and a total of 450 responses were received. These responses were again categorized according to the hypothesis and analysis. The following are the categories of questions: Questions based on password, browser, and social media activities. The responses to these questions were multiple-choice answers, with the following choices: Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree.

The following are the questions drafted:

Q1. Passwords are made up of 12 letters and a combination of letters, digits, or signs.

Q2. Change password periodically.
Q3. Use previously used passwords whenever needed to create a password.
Q4. Use a single secure passcode for all web pages and logins.
Q5. It is inconvenient to have a different long and solid passcode for every webpage and account.
Q6. I do not mind sharing my passwords with my friends.

The questions related to browser security are as follows:

Q7. The web browser should be updated regularly.
Q8. Avoid installing extensions from third-party websites.
Q9. Examine the web browser's privacy controls and parameters regularly.
Q10. Examine browsing history for any unusual activity.

The questions related to social media activities are as follows:

Q11. It is OK to publish private photographs on social networking sites.
Q12. Accepting invitations from outsiders seems OK.
Q13. There is no concern with openly posting one's present location on social networking sites.
Q14. No problem with adding all personal information to social media.
Q15. Learn how to submit any danger or questionable conduct on social networks.

The passcode is an essential security element that protects data and information while allowing access to authenticated systems. A passcode should be at least 12 characters, including letters and numerals, capital and lowercase letters, and at least one symbol or unique character [43]. Given this, we investigated the students' understanding of the fundamental concepts of password security and how they handle their passwords.

4. Results

4.1. Demographic Data

Demographic data in this research is in the form of respondent data: gender, age, education level, computer skills, and how often respondents make online purchases. The distribution of demographic data can be seen in Table 1.

Table 1. Distribution of research respondent demographic data (n = 450).

Variable	Category	Number	Percentage (%)
Gender	Male	238	52.8%
	Female	212	47.2%
Age	<20	178	39.5%
	20–35	240	53.3%
	36–49	28	6.2%
	50–65	4	1%
Education	Diploma	16	3.6%
	Bachelor's Degree	417	92.6%
	Master's Degree	10	2.2%
	PhD	7	1.6%
Computer Skill	Beginner	67	14.9%
	Intermediate	237	52.7%
	Advance	146	32.4%
Purchase Online	Rarely	132	30%
	Frequently	318	70%

In Table 1, it can be seen that the number of female respondents (52.8%) is greater than that of male respondents. Most of the respondents were aged 20–35 years (53.3%), followed by respondents aged less than 20 years (39.5%). A large number of respondents were in this age group because the main target of this research is students, the level of education attained by most of the students in this study being a bachelor's degree (92.6%). Based on computer skills, most respondents have skills in using computers at an intermediate level (52.7%), followed by respondents who are proficient in using computers (32.4%). In the field of online purchasing, it can be seen that most of the respondents often purchase online (70%).

4.2. Description of the Independent Variable (X) Used

4.2.1. Password Security (X_1)

A password is a secret set of characters or words used to authenticate access to digital systems and computer systems. A password is one of the most critical factors in protecting data and information, but it is also hazardous because it is vulnerable to attack [55]. In good computer security practice, passwords must be between 8 (eight) and 24 (twenty-four) characters long and include at least one uppercase letter, one number, and one unique character [57]. These are usually formed from frequently used words, although this is not recommended as they are easier to guess or decipher.

From the information in Table 2, it is known that as many as 32% of students agree and 29% even strongly agree that one ought to use a strong password. However, most students (41%) disagree that passwords should be changed periodically; most students (39%) use their old passwords to create new passwords. Most students (30%) are also more likely to use one password for all websites/accounts and consider using long passwords very inconvenient. However, students are not willing to tell or share their passwords with friends. Based on these results, students still lack awareness of password security.

Table 2. The questions about the password security variable.

Question	Totally Disagree	Disagree	Neutral	Agree	Totally Agree
Passwords are made up of 12 letters and a combination of letters, digits, or signs.	4%	17%	18%	32%	29%
Change password periodically.	18%	41%	20%	14%	7%
Use previously used passwords whenever needed to create a password.	10%	18%	17%	39%	16%
Use a single secure passcode for all web pages and logins.	10%	23%	19%	30%	18%
It is inconvenient to have a different long and solid passcode for every webpage and account.	10%	11%	13%	34%	32%
I do not mind sharing my passwords with my friends.	54%	23%	12%	8%	4%

4.2.2. Browser Security (X_2)

Browser Security is essential for securing user data and information. The browser is considered to be the main door in conducting online activities, so the browser is the main target for hackers or cyber thieves to access sensitive information [58]. Keeping up-to-date with the latest version is one of the most effective ways to help secure your browser or another system.

From the results in Table 3, it is known that as many as 40% of students agree and 39% even strongly agree that the web browser must be updated regularly. As many as 38% of students strongly agree that installing extensions from third-party websites should be avoided. Most of the students (35%) agreed that the security settings and configurations of the web browser should be checked periodically, and as many as 36% of students studied browser history to find any suspicious activity. Based on these results, it is shown that students have a good level of awareness of browser security.

4.2.3. Social Media Activities (X_3)

In the era of increasingly advanced use of technology, surfing on social media has become a part of our daily life. People can access information in various fields, share their daily activities, and have non-face-to-face interactions through social media.

Table 3. The questions about the browser security variable.

Question	Totally Disagree	Disagree	Neutral	Agree	Totally Agree
The web browser should be updated regularly.	1%	5%	15%	40%	39%
Avoid installing extensions from third-party websites	2%	8%	18%	34%	38%
Examine the web browser's privacy controls and parameters regularly.	4%	12%	22%	35%	27%
Examine the browsing history for any unusual activity.	6%	11%	20%	36%	27%

From the results in Table 4, it can be seen that most students disagree (25%) or strongly disagree (23%) to upload personal photos on social media. Meanwhile, most students are neutral about accepting friendships from strangers on social media. However, some students strongly disagreed that one ought to share one's current social media location and disagreed that one ought to add all one's personal information on one's social media pages. As many as 68% of students already know how to report suspicious activity on social media.

Table 4. The questions about the social media activities variable.

Question	Totally Disagree	Disagree	Neutral	Agree	Totally Agree
It is OK to publish private photographs on social networking sites.	23%	25%	25%	21%	6%
Accepting invitations from outsiders seems OK	21%	26%	28%	21%	4%
There is no concern with openly posting one's present location on social networking sites.	49%	28%	12%	8%	3%
No problem with adding all personal information to social media.	33%	22%	22%	18%	5%
Learn how to submit any danger or questionable conduct on social networks.	4%	14%	14%	37%	31%

Figure 1 shows the most used social media by people around the world. For example, it can be seen that Facebook is the most used social media application with almost 2700 million or 2.7 billion active users every month in 2021.

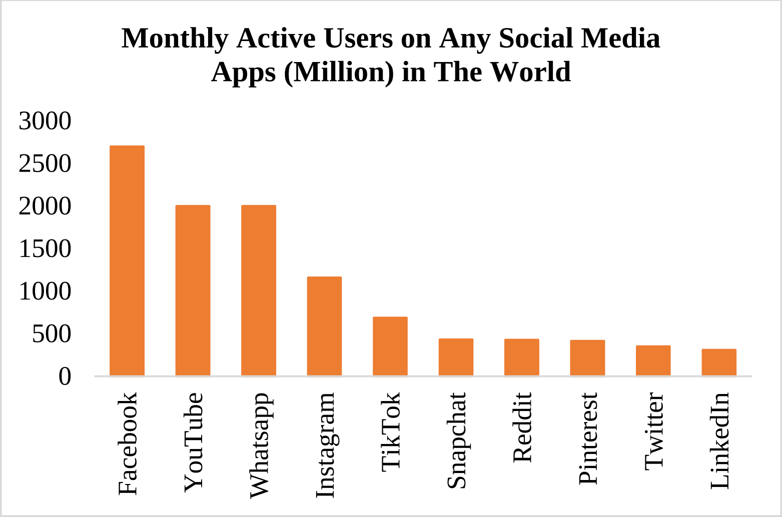


Figure 1. The most used social media in the world.

4.2.4. Data Analysis

Validity and Reliability Test

The validity test [57–59] results for each item from 450 respondents in this study are presented in Table 5.

Table 5. Validity test results.

Variable	Question Item	r-Value	r-Table
Password Security (X_1)	Q1	0.334	0.092
	Q2	0.183	
	Q3	0.509	
	Q4	0.596	
	Q5	0.481	
	Q6	0.513	
Browser Security (X_2)	Q1	0.552	
	Q2	0.605	
	Q3	0.826	
	Q4	0.791	
Social Media Activities (X_3)	Q1	0.683	
	Q2	0.692	
	Q3	0.717	
	Q4	0.740	
	Q5	0.298	
Cybersecurity Awareness (Y)	Q1	0.590	
	Q2	0.657	
	Q3	0.339	
	Q4	0.598	

Table 5 shows the results of testing the validity of each item from the 450 respondents studied. The results of the validity test show that all questions about the independent variables, namely, password security (X_1), browser security (X_2), social media activities (X_3), and also the dependent variable, namely, cybersecurity awareness (Y), have a correlation value (r-value) > r table (0.092). This indicates that each question is valid. So, it can be concluded that all questions used in this study are suitable for further research. After obtaining the results on the validity, the reliability test was carried out to determine the reliability of each statement presented in Table 6.

Table 6. Reliability Test Results.

Cronbach's Alpha	Number of Items	Description
0.596	19	Reliable enough

Table 6 shows the reliability testing results, namely, the Cronbach's Alpha value of 0.596. Cronbach's Alpha value is between 0.5–0.6. This indicates that every statement used in the variable is reliable enough, with the result that all statement items used in this study are suitable for further research.

Feasibility Test of a Variable

This stage tested the correlation between variables using Bartlett's test and the Kaiser–Meyer–Olkin (KMO) test. This test is carried out to assess the feasibility of a variable analyzed using factor analysis [60].

Table 7 shows that the significance value of Bartlett's test of sphericity is 0.000, the p-value (0.000) < α (0.05), which means that there is a correlation between variables. Furthermore, it can be seen that if the KMO value is 0.783, the KMO value is between the values 0.5–1, which means that the variables are homogeneous. Both tests have been met so that the variables can be predicted and further analysis can be carried out.

Table 7. KMO and Bartlett's Test.

Kaiser–Meyer–Olkin Measure of Sampling Adequacy		0.783
Bartlett's Test of Sphericity	Approximate Chi-Square	1795.927
	Df	171
	Sig	0.000

Correlation Test

A Correlation test [61] is a process to test the independent and dependent variables to determine the level of closeness of the relationship between two variables.

Table 8 shows the correlation component matrix containing the correlation values between the variables used in the study. The main focus of this test is to determine the relationship level between each independent variable—password security (X_1), browser security (X_2), and social media activities (X_3)—and cybersecurity awareness (Y). To make it easier to interpret the strength of the relationship between the two variables, the authors provide the following criteria (Sarwono, 2006).

Table 8. Correlation component matrix.

Variable	Password Security	Browser Security	Social Media Activities	Level of Awareness
Password Security	1			
Browser Security	0.023	1		
Social Media Activities	0.298	−0.074	1	
Level of Awareness	0.277	0.184	0.366	1

Based on Table 8, Password Security is positively related to cybersecurity awareness (r = 0.277). However, the correlation value is between 0.25–0.5, indicating a moderate level of relationship between password security and cybersecurity awareness. Browser Security is positively related to cybersecurity awareness (r = 0.184). The correlation value is between 0–0.25, indicating a low relationship between browser security and cybersecurity awareness. Social media activities positively relate to cybersecurity awareness (r = 0.366). The correlation value is between 0.25–0.5, indicating a moderate relationship between social media activities and cybersecurity awareness Table 9.

Table 9. Guidelines for providing an interpretation of correlation coefficients.

Correlation Value (r)	Interpretation
0	No correlation
>0–0.25	Low Correlation
>0.25–0.5	Moderate Correlation
>0.5–0.75	High Correlation
>0.75–0.99	Very High Correlation
1	Perfect Correlation

4.2.5. Multiple Tests

Assumptions Test

The residuals are assumed to be generally distributed in multivariate normality–multiple regression. However, no multiple regression presupposes that the independent variables are not substantially connected. The variance inflation factor (VIF) values are used to test this assumption [62].

Normality Test

The normality assumption is related to the residual distributions. This is considered customarily distributed, and the regression line is fitted to the data so that the mean of the residuals is zero.

The normality test [63] results using the normal p-plot with 450 respondents can be seen in Figure 2. The normal p-plot shows that all data points are spread around the line. This indicates that the data has met the assumption of normality.

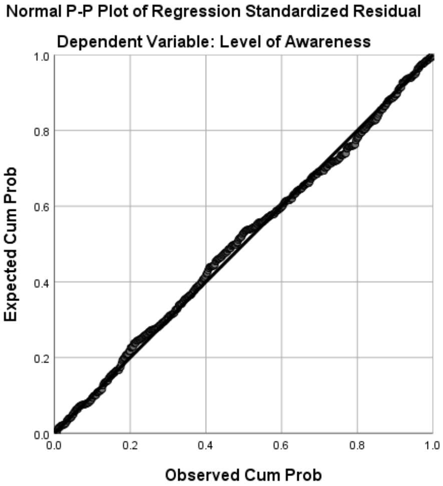


Figure 2. Normality test.

Multicollinearity Test

The results of the multicollinearity test using the VIF (variance inflation factor) value can be seen in Table 10.

Table 10. Multicollinearity Test.

Variable	VIF Value
Password Security (X_1)	1.100
Browser Security (X_2)	1.008
Social Media Activities (Y)	1.105

The VIF value in Table 10 shows that the VIF value of the three variables is less than 10 (VIF < 10), so it can be concluded that all the independent variables used in this study do not experience multicollinearity.

Heteroskedasticity Test

This study detects the occurrence of heteroskedasticity [64] by looking at the pattern of data points on the scatter-plot graph. Figure 3 shows that the observation points spread randomly and do not form a design or line. The plot also indicates whether the data distribution is around the zero point. This suggests that the regression model is free from heteroskedasticity problems, and the heteroskedasticity assumption has been fulfilled.

Multiple Linear Regression Model and Coefficient of Determination (R2)

All classical assumption tests have been fulfilled; the next step is to build multiple linear regression model equations. The regression model equation that is produced can be used to analyze the effect of password security, browser security, and social media activities on cybersecurity awareness. The regression coefficient values are shown in Table 11.

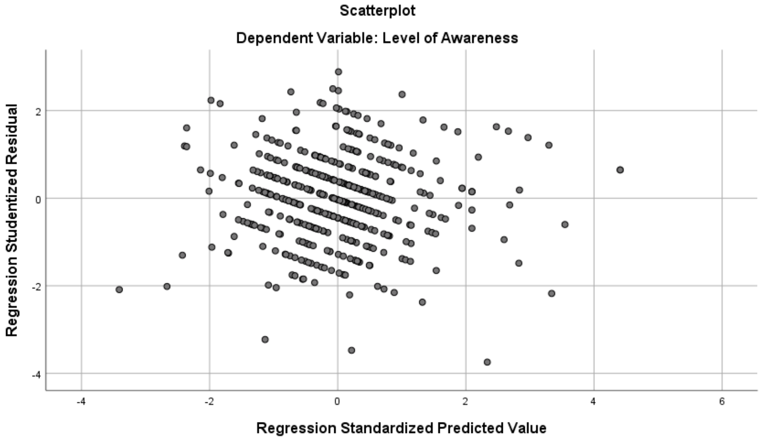


Figure 3. Heteroskedasticity Test.

Table 11. Multiple linear regression coefficient.

Variable	Regression Coefficient (β)
Intercept	4.301
Password Security (X_1)	0.147
Browser Security (X_2)	0.188
Media Social Activities (X_3)	0.241

The multiple linear regression model formed based on the regression coefficients in Table 11 is as follows:

$$\text{Cybersecurity Awareness} = 4.301 + (0.147)\ X_1 + (0.188)\ X_2 + (0.241)\ X_3$$

The regression coefficient value above can be explained such that if the level of student knowledge of password security increases by 1%, then the level of cybersecurity awareness will increase by 14.7%. Likewise, if the level of student knowledge of browser security rises by 1%, then cybersecurity awareness will increase by 18.8%. Finally, if student knowledge of social media activities increases by 1%, then cybersecurity awareness will increase by 24.1%.

The coefficient of determination is the value used to measure how much the ability of the independent variable included in the model can explain the variation of the dependent variable. Based on Table 12, the coefficient of determination (R2) is 0.206, meaning that password security, browser security, and social media activities contribute to the influence of cybersecurity awareness by 20.6%, while the residual value of 79.4% (100% − 20.6%) indicates that other factors that affect cybersecurity awareness are not included in the model.

Table 12. Correlation Coefficient and Determination.

Model	R	R^2	Adjusted R^2
Regression	0.454	0.206	0.201

4.2.6. Hypothesis Test

ANOVA Test (F-Test)

The following is an F-test to see whether the independent variable has a simultaneous effect on the dependent variable [65]. The hypothesis in this test is as follows:

Hypothesis 0.

1: *Password Security (X_1), Browser Security (X_2), and Social Media Activities (X_3) together are not significantly related to Cybersecurity Awareness (Y).*

2: *Password Security (X_1), Browser Security (X_2), and Social Media Activities (X_3) together are significantly related to Cybersecurity Awareness (Y).*

Table 13 shows the results of the p-value (0.000) < 0.05, so it can be concluded that Password Security (X_1), Browser Security (X_2), and Social Media Activities (X_3) together have a significant effect on Cybersecurity Awareness (Y).

Table 13. F-test Results.

Model	F	Sig (p-Value)
Regression	38.666	0.000

Partial Test (t-Test)

A partial test [66] using the t-test is used to determine the significant effect of each independent variable on the dependent variable. The hypothesis in the partial test is as follows:

Hypothesis 1.

1: *Password Security (X_1) is not significantly related to Cybersecurity Awareness (Y).*
2: *Password Security (X_1) is significantly related to Cybersecurity Awareness (Y).*

Hypothesis 2.

1: *Browser Security (X_2) is not significantly related to Cybersecurity Awareness (Y).*
2: *Browser Security is (X_2) is significantly related to Cybersecurity Awareness (Y).*

Hypothesis 3.

1: *Social Media Activities (X_3) is not significantly related to the Cybersecurity Awareness (Y).*
2: *Social Media Activities (X_3) is significantly related to Cybersecurity Awareness (Y).*

Table 14 shows the results of partial hypothesis testing (t-test). Based on these results, the conclusions are:

(1) The Password Security variable (X_1) has a p-value (0.0001) < (0.05), so it can be concluded that Password Security (X_1) has a significant effect on Cybersecurity Awareness (Y).
(2) The Browser Security variable (X_2) has a p-value (0.0001) < (0.05), so it can be concluded that Browser Security (X_2) has a significant effect on Cybersecurity Awareness (Y).
(3) The Social Media Activities (X_3) variable has a p-value (0.0001) < (0.05), so it can be concluded that Social Media Activities (X_3) have a significant effect on Cybersecurity Awareness (Y).

Table 14. Results of t-test.

Variable	t-Value	Sig (p-Value)
Password Security (X_1)	3.931	0.0001
Browser Security (X_2)	4.839	0.0001
Social Media Activities (X_3)	7.428	0.0001

5. Discussion

The results of partial hypothesis testing using the t-test (Table 14) show that the password security variable significantly affects cybersecurity awareness (p-value = 0.0001). The regression coefficient of the password security variable in the multiple linear regression model (Table 11) shows the beta value of 0.147. Therefore, it can be concluded that password security has a positive and significant effect on cybersecurity awareness. The positive impact shows that using passwords will increase cybersecurity awareness by 14.7%. The browser security variable significantly affects cybersecurity awareness (p-value = 0.0001). The regression coefficient of the password security variable shows a beta value of 0.188. Therefore, it can be concluded that browser security has a positive and significant effect on cybersecurity awareness. The positive impact shows that knowledge of browser security will increase cybersecurity awareness by 18.8%. The social media activities variable significantly impacts cybersecurity awareness (p-value = 0.0001). The regression coefficient of the social media activities variable shows a beta value of 0.241. Therefore, it can be concluded that social media activities positively and significantly affect cybersecurity awareness. The positive effect shows that using social media will increase cybersecurity awareness by 24.1%.

The results of simultaneous hypothesis testing using the F-test (Table 13) show that password security, browser security, and social media activities have simultaneously significant effects on cybersecurity awareness (p-value < 0.05). The magnitude of the influence of the two variables can be seen based on the value of the coefficient of determination (R2) obtained in this study, which is 0.206, indicating that password security, browser security, and social media activities contribute to the influence of cybersecurity awareness by 20.6%. Meanwhile, the residual value of 79.4% indicates that other factors that affect cybersecurity awareness are not included in the model. It should be emphasized that not all models with a low R2 are bad models. According to [67] (2019), regression models with R2 values below 50% can be accepted in several fields, such as the social field and the study of human behavior. Suppose the value of R2 is low but the independent variable has a significant effect. In that case, the model can still provide conclusions about the relationship of the independent variable to the dependent variable.

The p-value (p-value < 0.05) indicates that the respondents in this study already have an awareness of cybersecurity awareness, but it is still low; this is because they do not take more or actual actions to implement cybersecurity in their daily life (R2 = 0.206). Several reasons were thought to affect the results, probably because most respondents in this study (53%) were women. According to (Alotaibi et al., 2017), men have a higher awareness of cybersecurity than women. The research that supports the results of this study is research conducted by Alharbi and Tassaddiq (2021) among students at Majmaah University, Saudi Arabia, which included 60% male respondents and stated that students at Majmaah University already have a high level of awareness of cybersecurity awareness. It is proven by the high R2 value reaching 55% (R2 = 0.55) and the variables used, such as security tools, browser safety, social networking, and other cybersecurity knowledge, have a positive effect (p-value < 0.05).

Based on the three variables used, the password security variable has the lowest coefficient value (β = 0.147), implying that students still lack awareness of password security. It can be seen that most students (41%) disagree that passwords must be changed periodically; most students (30%) are more likely to use 1 password for all websites/accounts and think that using long passwords is very inconvenient. According to [68], users may have difficulty in remembering a long and complex password. Yildirim (2019) [69] said that instead of requiring users to follow strict password policy rules, motivating and directing them to create solid, easy-to-remember passwords seem to be a more efficient and helpful way. Users can also use strong passwords only if the system or account requires a high level of security [70].

6. Conclusions

Based on the research conducted, it can be concluded that knowledge of password security, browser security, and social media activities significantly influence cybersecurity awareness in students. Overall, students have realized the importance of cybersecurity awareness. However, in practice, students' levels of cybersecurity awareness are still lacking, especially when it comes to password security. Students usually do not pay much attention to using good and correct passwords to protect their accounts or websites. Based on the research results explained in the previous chapter, the summary is obtained as follows: Password Security variable (X_1) has a significant and positive effect on Cybersecurity Awareness (p-value = 0.0001, = 0.143). This shows that a good knowledge about password security could increase awareness because passwords are the main means of accessing and maintaining accounts or other systems. The knowledge about student password security in this study is still deficient. Students usually do not pay much attention to using good and correct passwords to protect their accounts or websites. Browser Security variable (X_2) has a significant and positive effect on Cybersecurity Awareness (p-value = 0.0001, = 0.188).

This shows that good knowledge about browser security can increase awareness. The level of knowledge about student browser security in this study is good; it can be seen from the number of students who always update their browsers regularly and tend to pay attention to the security of the browsers they use. The Social Media Activities (X_3) variable has a significant and positive effect on Cybersecurity Awareness (p-value = 0.0001, = 0.241). This shows that proper and correct social media activities can increase awareness. The activity of using social media by students in this study was good and can be seen from the number of students who prefer to keep their personal information from being too widely spread through social media. The students also know how to report suspicious threats on social media. Password Security (X_1), Browser Security (X_2), and Social Media Activities (X_3) variables simultaneously have a significant effect on Cybersecurity Awareness (p-value = 0.000), with a correlation coefficient of 20.6% (R2 = 0.206). This shows that the independent variable used can explain the level of cybersecurity awareness of 20.6%. All the SPSS analysis tables are listed in the Appendix A.

7. Limitations of the Work

Based on these results, several things can be done to increase cybersecurity awareness in students by means of socialization and campaigns related to cybersecurity. It should be noted that this research still has several limitations, such as the level of question reliability, which is still not decent, and limited use of the independent variables. This research, also, did not always represent another more comprehensive cybersecurity topic. In future research, it is recommended to add more variables that might affect cybersecurity awareness.

8. Comparative Analysis

There are several works in the literature wherein a similar methodology is applied to assess student's awareness for cybersecurity, as discussed in the literature review section. The following are the works sharing this perspective: Senthilkumar and Easwaramoorthy [32] studied university students in Tamil Nadu's key towns to examine their attentiveness to cyber security. They concentrated on particular cyber security risks, such as malware-infected websites, phishing, and the theft of personal information. According to their findings, students' awareness of cyber security and related threat problems was above average, with 70% of respondents having a basic understanding of cyber security dangers. Another work conducted by Moallem [33] investigated students' opinions regarding cyber security in California's Silicon Valley.

Similarly, Knight-McCord [53] (2016) researched which social networking sites were most popular with students. They administered a survey to 363 pupils online and in person. Previous research discovered that Instagram was the most popular site, followed by Snapchat and Facebook. LinkedIn and Pinterest, on the other hand, were less popular. According to Sharma, Jain, and Tiwari [54], 84 percent of students believe that posting personal information on social networking sites (SNS) is harmful. Finally, Moallem [33] (2018) researched cyber security knowledge in students at two California State universities in Silicon Valley.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable for studies not involving humans or animals.

Informed Consent Statement: Not applicable.

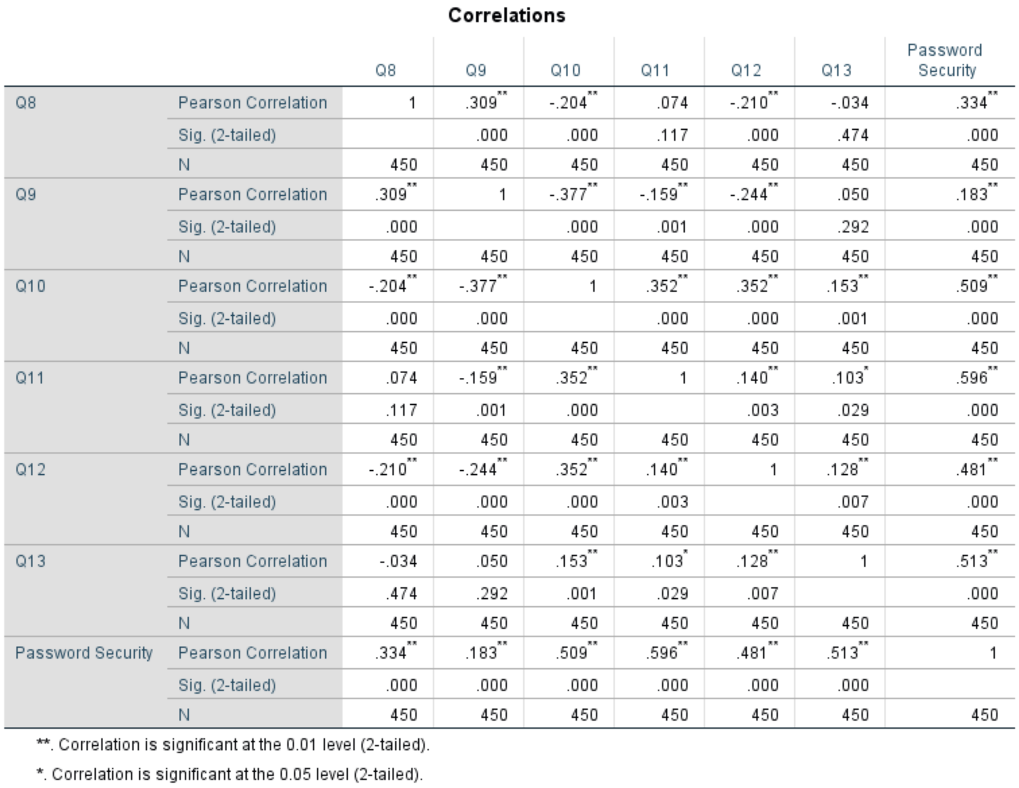
Data Availability Statement: The data used in this study is based on the survey for the questions distributed among the students of the university.

Acknowledgments: The author would like to thank the Dean of College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A

1. Validity Test

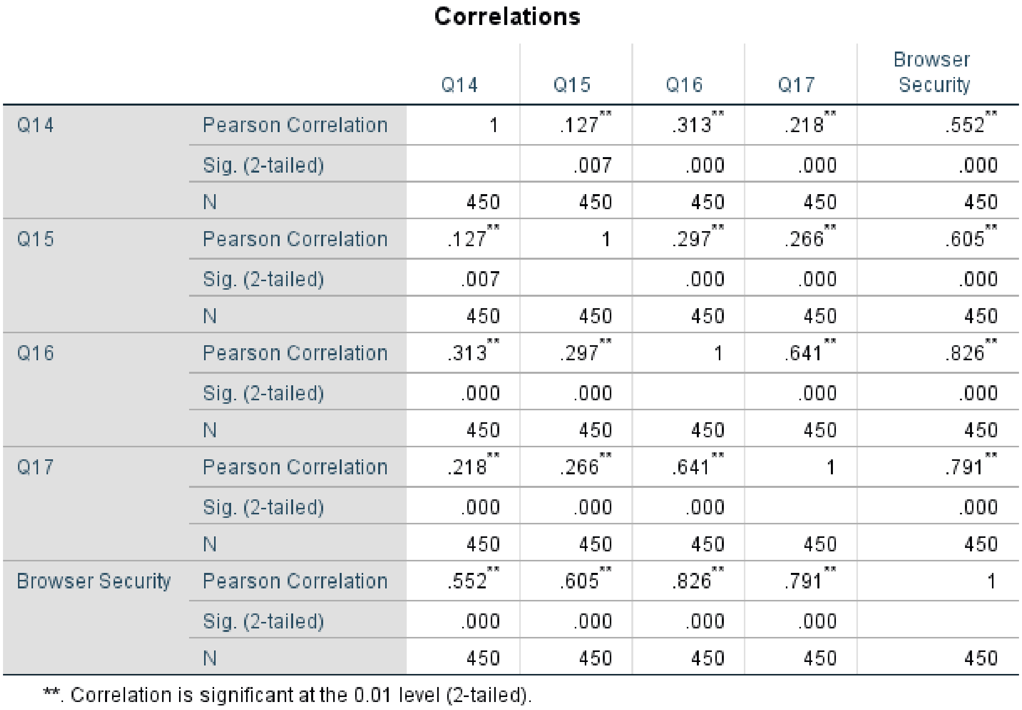


Correlations

		Q8	Q9	Q10	Q11	Q12	Q13	Password Security
Q8	Pearson Correlation	1	.309**	-.204**	.074	-.210**	-.034	.334**
	Sig. (2-tailed)		.000	.000	.117	.000	.474	.000
	N	450	450	450	450	450	450	450
Q9	Pearson Correlation	.309**	1	-.377**	-.159**	-.244**	.050	.183**
	Sig. (2-tailed)	.000		.000	.001	.000	.292	.000
	N	450	450	450	450	450	450	450
Q10	Pearson Correlation	-.204**	-.377**	1	.352**	.352**	.153**	.509**
	Sig. (2-tailed)	.000	.000		.000	.000	.001	.000
	N	450	450	450	450	450	450	450
Q11	Pearson Correlation	.074	-.159**	.352**	1	.140**	.103*	.596**
	Sig. (2-tailed)	.117	.001	.000		.003	.029	.000
	N	450	450	450	450	450	450	450
Q12	Pearson Correlation	-.210**	-.244**	.352**	.140**	1	.128**	.481**
	Sig. (2-tailed)	.000	.000	.000	.003		.007	.000
	N	450	450	450	450	450	450	450
Q13	Pearson Correlation	-.034	.050	.153**	.103*	.128**	1	.513**
	Sig. (2-tailed)	.474	.292	.001	.029	.007		.000
	N	450	450	450	450	450	450	450
Password Security	Pearson Correlation	.334**	.183**	.509**	.596**	.481**	.513**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	
	N	450	450	450	450	450	450	450

**. Correlation is significant at the 0.01 level (2-tailed).

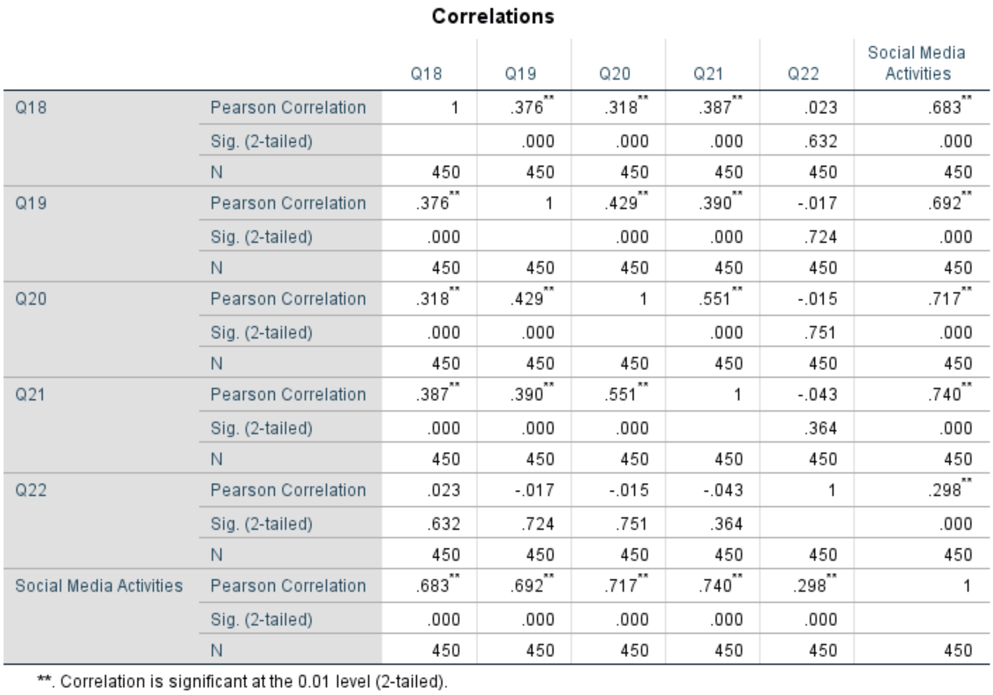
*. Correlation is significant at the 0.05 level (2-tailed).



Correlations

		Q14	Q15	Q16	Q17	Browser Security
Q14	Pearson Correlation	1	.127**	.313**	.218**	.552**
	Sig. (2-tailed)		.007	.000	.000	.000
	N	450	450	450	450	450
Q15	Pearson Correlation	.127**	1	.297**	.266**	.605**
	Sig. (2-tailed)	.007		.000	.000	.000
	N	450	450	450	450	450
Q16	Pearson Correlation	.313**	.297**	1	.641**	.826**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	450	450	450	450	450
Q17	Pearson Correlation	.218**	.266**	.641**	1	.791**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	450	450	450	450	450
Browser Security	Pearson Correlation	.552**	.605**	.826**	.791**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	450	450	450	450	450

**. Correlation is significant at the 0.01 level (2-tailed).

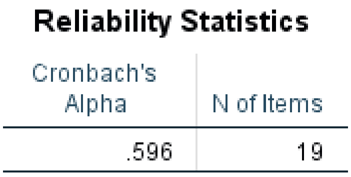


Correlations

		Q18	Q19	Q20	Q21	Q22	Social Media Activities
Q18	Pearson Correlation	1	.376**	.318**	.387**	.023	.683**
	Sig. (2-tailed)		.000	.000	.000	.632	.000
	N	450	450	450	450	450	450
Q19	Pearson Correlation	.376**	1	.429**	.390**	-.017	.692**
	Sig. (2-tailed)	.000		.000	.000	.724	.000
	N	450	450	450	450	450	450
Q20	Pearson Correlation	.318**	.429**	1	.551**	-.015	.717**
	Sig. (2-tailed)	.000	.000		.000	.751	.000
	N	450	450	450	450	450	450
Q21	Pearson Correlation	.387**	.390**	.551**	1	-.043	.740**
	Sig. (2-tailed)	.000	.000	.000		.364	.000
	N	450	450	450	450	450	450
Q22	Pearson Correlation	.023	-.017	-.015	-.043	1	.298**
	Sig. (2-tailed)	.632	.724	.751	.364		.000
	N	450	450	450	450	450	450
Social Media Activities	Pearson Correlation	.683**	.692**	.717**	.740**	.298**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	
	N	450	450	450	450	450	450

**. Correlation is significant at the 0.01 level (2-tailed).

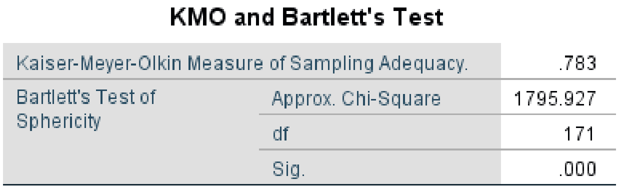
2. Reliability Test



Reliability Statistics

Cronbach's Alpha	N of Items
.596	19

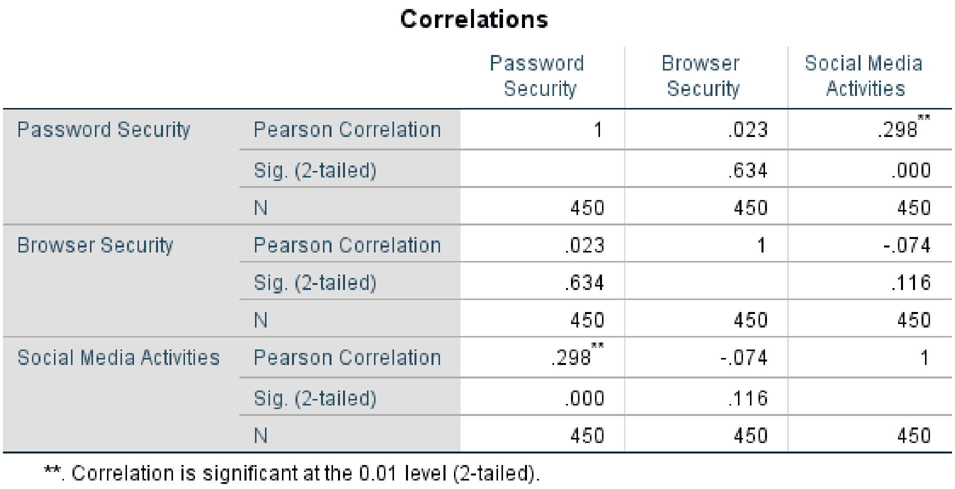
3. Feasibility test of a variable



KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.783
Bartlett's Test of Sphericity	Approx. Chi-Square	1795.927
	df	171
	Sig.	.000

4. Correlation Test

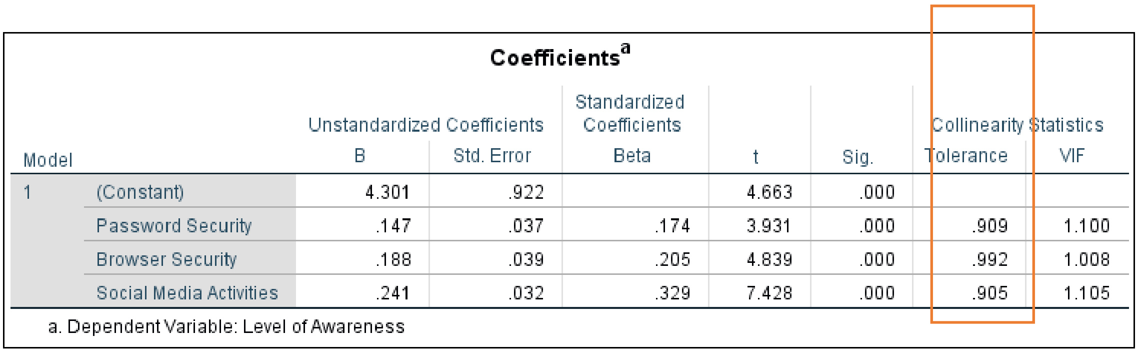


Correlations

		Password Security	Browser Security	Social Media Activities
Password Security	Pearson Correlation	1	.023	.298**
	Sig. (2-tailed)		.634	.000
	N	450	450	450
Browser Security	Pearson Correlation	.023	1	-.074
	Sig. (2-tailed)	.634		.116
	N	450	450	450
Social Media Activities	Pearson Correlation	.298**	-.074	1
	Sig. (2-tailed)	.000	.116	
	N	450	450	450

**. Correlation is significant at the 0.01 level (2-tailed).

5. Multicollinearity Test

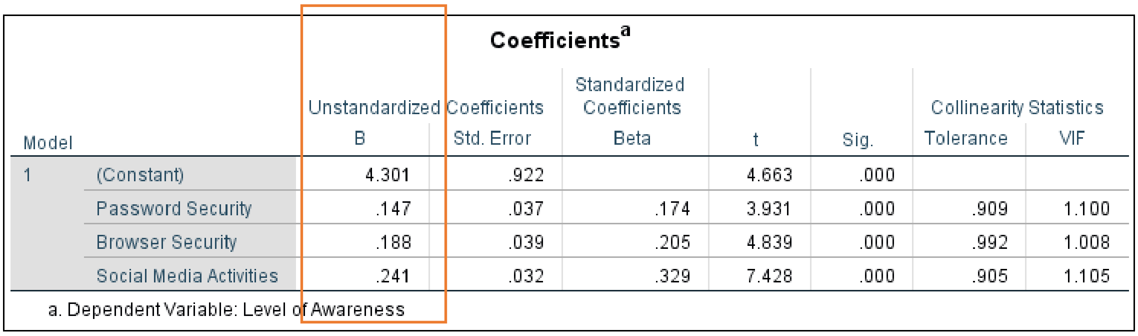


Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	4.301	.922		4.663	.000		
	Password Security	.147	.037	.174	3.931	.000	.909	1.100
	Browser Security	.188	.039	.205	4.839	.000	.992	1.008
	Social Media Activities	.241	.032	.329	7.428	.000	.905	1.105

a. Dependent Variable: Level of Awareness

6. Regression

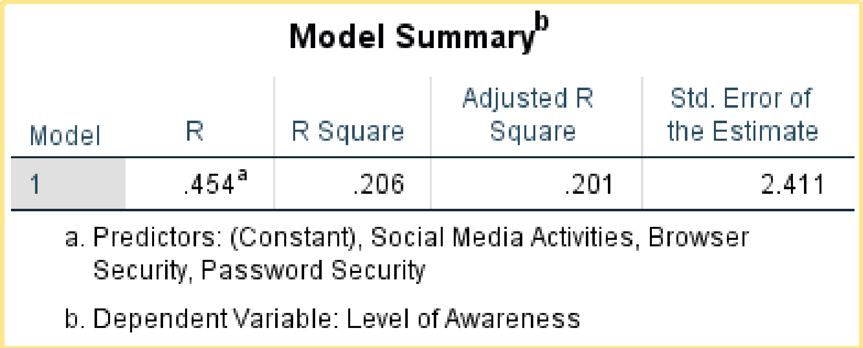


Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	4.301	.922		4.663	.000		
	Password Security	.147	.037	.174	3.931	.000	.909	1.100
	Browser Security	.188	.039	.205	4.839	.000	.992	1.008
	Social Media Activities	.241	.032	.329	7.428	.000	.905	1.105

a. Dependent Variable: Level of Awareness

7. R^2



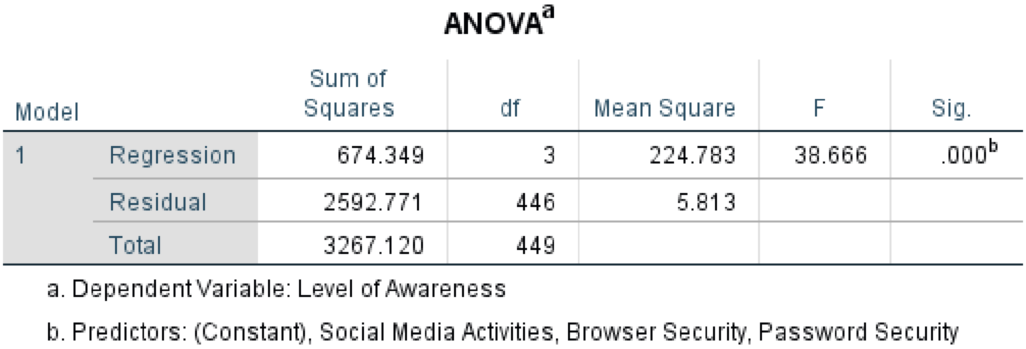
Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.454[a]	.206	.201	2.411

a. Predictors: (Constant), Social Media Activities, Browser Security, Password Security

b. Dependent Variable: Level of Awareness

8. ANOVA Test (F-Test)



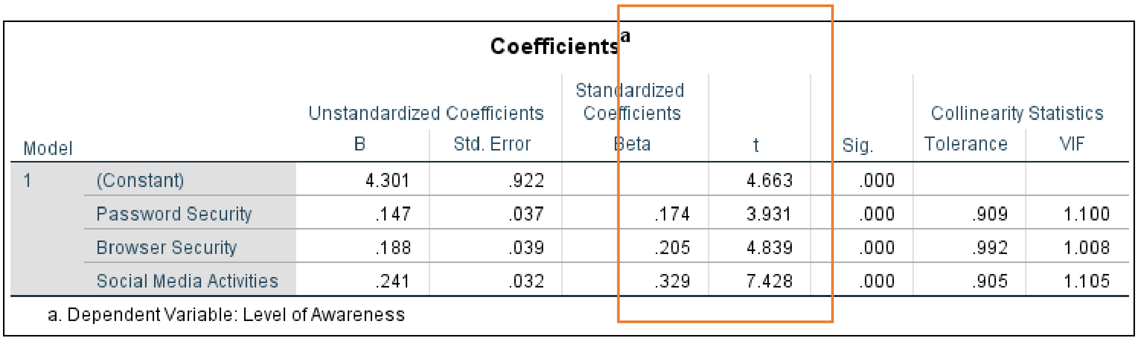
ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	674.349	3	224.783	38.666	.000[b]
	Residual	2592.771	446	5.813		
	Total	3267.120	449			

a. Dependent Variable: Level of Awareness

b. Predictors: (Constant), Social Media Activities, Browser Security, Password Security

9. *t*-Test



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	4.301	.922		4.663	.000		
	Password Security	.147	.037	.174	3.931	.000	.909	1.100
	Browser Security	.188	.039	.205	4.839	.000	.992	1.008
	Social Media Activities	.241	.032	.329	7.428	.000	.905	1.105

a. Dependent Variable: Level of Awareness

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, J.S. *Cyber Security: An Introduction for Non-Technical Managers*, 1st ed.; Routledge: London, UK, 2016; pp. 1–264.
4. Shaukat, K.; Luo, S.; Varadharajan, V.; Hameed, I.A.; Xu, M. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access* **2020**, *8*, 222310–222354. [CrossRef]
5. Whitman, M.E.; Mattord, H.J. *Principles of Information Security*; Receiv. US Pat. Pers. Identif. device. 2005; Cengage Learning: Boston, MA, USA, 2011; p. 1.
6. Shaukat, K.; Luo, S.; Chen, S.; Liu, D. Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. In Proceedings of the 2020 International Conference on Cyber Warfare and Security (ICCWS), Albany, NY, USA, 17–18 March 2022.
7. 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.
8. Simsim, M.T. Internet usage and user preferences in Saudi Arabia. *J. King Saud Univ.-Eng. Sci.* **2011**, *23*, 101–107. [CrossRef]
9. 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).
10. 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).
11. Sait, S.M.; Al-Tawil, K.M.; Ali, S.; Hussain, A. *Use and effect of Internet in Saudi Arabia*; KFUPM: Dhahran, Saudi Arabia, 2003.
12. 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, New York, NY, USA, 23–24 September 2005.
13. 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.
14. Hathaway, M.; Spidalieri, F.; Alsowailm, F. *Kingdom of Saudi Arabia Cyber Readiness at a Glance*; Potomac Institute for Policy Studies: Arlington, VA, USA, 2017.
15. 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]
16. ALArifi, A.; Tootell, H.; Hyland, P. Information Security Awareness in Saudi Arabia. In Proceedings of the CONF-IRM 2012, Vienna, Austria, 21–23 May 2012.
17. Aloul, F.A. The Need for Effective Information Security Awareness. *J. Adv. Inf. Technol.* **2012**, *3*, 176–183. [CrossRef]
18. Boneh, D.; Lynn, B.; Shacham, H. Short Signatures from the Weil Pairing. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, QLD, Australia, 9–13 December 2001.
19. 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.* **2013**, *24*, 1182–1191. [CrossRef]
20. Kamara, S.; Lauter, K. Cryptographic Cloud Storage. In Proceedings of the International Conference on Financial Cryptography and Data Security, Tenerife, Spain, 25–28 January 2010.
21. Pfleeger, C.P.; Pfleeger, S.L.R. *Security in Computing*, 4th ed.; Prentice Hall: Hoboken, NJ, USA, 2006.
22. Egan, M.; Mather, T. *The Executive Guide to Information Security: Threats, Challenges, and Solutions*, 1st ed.; Addison-Wesley Professional: Boston, MA, USA, 2004.
23. Stolfo, S.J.; Bellovin, S.M.; Hershkop, S.; Keromytis, A.D.; Sinclair, S.; Smith, S.W. *Insider Attack and Cyber Security: Beyond the Hacker*, 1st ed.; Springer: Boston, MA, USA, 2008.
24. Soghoian, C. A Remote Vulnerability in Firefox Extensions. Available online: http://paranoia.dubfire.net/2007/05/remote-vulnerability-in-firefox.html (accessed on 12 June 2013).

25. Reis, C.; Barth, A.; Pizano, C. Browser Security: Lessons from Google Chrome: Google Chrome developers focused on three key problems to shield the browser from attacks. *Queue* **2009**, *7*, 3–8. [CrossRef]
26. Osterman Research. Available online: http://www.ostermanresearch.com/ (accessed on 15 June 2013).
27. 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]
28. Ahmed, N.; Kulsum, U.; Bin Azad, I.; Momtaz, A.S.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.
29. Plackett, R.L. Karl Pearson and the Chi-Squared Test. *Int. Stat. Rev. Int. Stat.* **1983**, *51*, 59–72. [CrossRef]
30. Slusky, L.; Partow-Navid, P. Students Information Security Practices and Awareness. *J. Inf. Priv. Secur.* **2012**, *8*, 3–26. [CrossRef]
31. 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.
32. Senthilkumar, K.; Easwaramoorthy, S. A Survey on Cyber Security awareness among college students in Tamil Nadu. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Vellore, India, 2–3 May 2017.
33. Moallem, A. Cyber Security Awareness among College Students. In Proceeding of the International Conference on Applied Human Factors and Ergonomics, Orlando, FL, USA, 21–25 July 2018.
34. Taha, N.; Dahabiyeh, L. College students information security awareness: A comparison between smartphones and computers. *Educ. Inf. Technol.* **2021**, *26*, 1721–1736. [CrossRef]
35. Moallem, A. *Cybersecurity Awareness among Students and Faculty*; CRC Press: Boca Raton, FL, USA, 2019.
36. 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**, *62*, 82–97. [CrossRef]
37. Garba, A.; Sirat, M.B.; Hajar, S.; Dauda, I.B. Cyber Security Awareness among University Students: A Case Study. *J. Crit. Rev.* **2020**, *7*, 16. [CrossRef]
38. 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]
39. Al-Khater, W.A.; Al-Ma'Adeed, S.; Ahmed, A.A.; Sadiq, A.S.; Khan, M.K. Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access* **2020**, *8*, 137293–137311. [CrossRef]
40. Garba, A.A.; Siraj, M.M.; Othman, S.H.; Musa, M.A. A Study on Cybersecurity Awareness among Students in Yobe State University, Nigeria: A Quantitative Approach. *Int. J. Emerg. Technol.* **2020**, *11*, 41–49.
41. Shaukat, K.; Suhuai, L.; Vijay, V.; Hameed, I.A.; Shan, C.; Dongxi, L.; Jiaming, L. Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies* **2020**, *13*, 2509. [CrossRef]
42. Florencio, D.; Herley, C. A Large-Scale Study of Web Password Habits. In Proceedings of the 16th International Conference on World Wide Web, Banff, AB, Canada, 8–12 May 2007.
43. Stobert, E.; Biddle, R. The Password Life Cycle: User Behaviour in Managing Passwords. In Proceedings of the 10th Symposium on Usable Privacy and Security, MP, Canada, 9–11 July 2014.
44. Wash, R.; Rader, E.; Berman, R.; Wellmer, Z. Understanding Password Choices: How Frequently Entered Passwords Are Re-Used across Websites. In Proceedings of the Twelfth Symposium on Usable Privacy and Security, Denver, CO, USA, 22–24 July 2016.
45. Shaukat, K.; Rubab, A.; Shehzadi, I.; Iqbal, R. A socio-technological analysis of cyber crime and cyber security in Pakistan. *Transylv. Rev.* **2017**, *1*, 84.
46. Haque, S.T.; Wright, M.; Scielzo, S. Hierarchy of users' web passwords: Perceptions, practices and susceptibilities. *Int. J. Human-Comput. Stud.* **2014**, *72*, 860–874. [CrossRef]
47. Bang, Y.; Lee, D.-J.; Bae, Y.-S.; Ahn, J.-H. Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. *Int. J. Inf. Manag.* **2012**, *32*, 409–418. [CrossRef]
48. 2020 Data Breaches. Available online: https://www.identityforce.com/blog/2020-data-breaches (accessed on 2 September 2021).
49. Ur, B.; Bees, J.; Segreti, S.M.; Bauer, L.; Christin, N.; Cranor, L.F. Do Users' Perceptions of Password Security Match Reality? In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 7–12 May 2016.
50. Ur, B.; Fumiko, N.; Jonathan, B.; Segreti, S.M.; Richard, S.; Lujo, B.; Nicolas, C.; Cranor, L.F. I Added'!'at the End to Make It Secure': Observing Password Creation in the Lab. In Proceedings of the Eleventh Symposium on Usable Privacy and Security, Ottowa, ON, Canada, 22–24 July 2015.
51. Liu, Z.; Hong, Y.; Pi, D. A Large-Scale Study of Web Password Habits of Chinese Network Users. *J. Softw.* **2014**, *9*, 293–297. [CrossRef]
52. Han, G.; Yu, Y.; Li, X.; Chen, K.; Li, H. Characterizing the semantics of passwords: The role of Pinyin for Chinese Netizens. *Comput. Stand. Interfaces* **2017**, *54*, 20–28. [CrossRef]
53. Pew Research Center. Social Networking Fact Sheet. 2019. Available online: https://www.pewinternet.org/2018/03/01/social-media-use-in-2018/ (accessed on 2 September 2021).
54. Richardson, C. Student Perceptions of the Impact of Social Media on College Student Engagement. Available online: https://scholarcommons.sc.edu/etd/4417/ (accessed on 2 September 2021).
55. Knight-McCord, J.; Cleary, D.; Grant, N.; Herron, A.; Lacey, T.; Livingston, T.; Emanuel, R. What social media sites do college students use most. *J. Undergrad. Ethn. Minor. Psychol* **2016**, *2*, 21–26.

56. Sharma, B.K.; Jain, M.; Tiwari, D. Students perception towards social media—With special reference to Management Students of Bhopal Madhya Pradesh. *Int. J. Eng. Appl. Sci.* **2015**, *2*, 30–34.
57. Shay, R.; Komanduri, S.; Patrick, G.; Kelley, P.; Giovanni, L.; Mazurek, M.L.; Lujo, B.; Nicolas, C.; Lorrie, F.C. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA, USA, 14–16 July 2010.
58. Carstens, D.S.; McCauley-Bell, P.R.; Malone, L.C.; DeMara, R.F. Evaluation of the human impact of password authentication practices on information security. *Inf. Sci. J.* **2004**, *7*, 1–19.
59. Heale, R.; Twycross, A. Validity and reliability in quantitative studies. *Évid. Based Nurs.* **2015**, *18*, 66–67. [CrossRef]
60. Koepp, G.A.; Snedden, B.J.; Flynn, L.; Puccinelli, D.; Huntsman, B.; Levine, J.A. Feasibility Analysis of Standing Desks for Sixth Graders. *ICAN Infant, Child, Adolesc. Nutr.* **2012**, *4*, 89–92. [CrossRef]
61. Piaw, C.Y. *Mastering Research Statistics*; Malaysia; McGraw Hill Education: New York, NY, USA, 2013.
62. Finch, H. Comparison of the Performance of Nonparametric and Parametric MANOVA Test Statistics when Assumptions Are Violated. *Methodology* **2005**, *1*, 27–38. [CrossRef]
63. Shapiro, S.S.; Francia, R.S. An approximate analysis of variance test for normality. *J. Am. Stat. Assoc.* **1972**, *67*, 215–216. [CrossRef]
64. Schwert, G.W.; Paul, J.S. Heteroskedasticity in stock returns. *J. Financ.* **1990**, *45*, 1129–1155. [CrossRef]
65. Wilcox, R.R.; Ventura, L.C.; Karen, L.T. New monte carlo results on the robustness of the anova f, w and f statistics. *Commun. Stat. Simul. Comput.* **1986**, *15*, 933–943. [CrossRef]
66. Kierepka, E.M.; Latch, E.K. Performance of partial statistics in individual-based landscape genetics. *Mol. Ecol. Resour.* **2014**, *15*, 512–525. [CrossRef] [PubMed]
67. Frost, J. *Regression Analysis: An Intuitive Guide for Using and Interpreting Linear Models*; Statisics by Jim Publishing: State College, PA, USA, 2019.
68. Keith, M.; Shao, B.; Steinbart, P.J. The usability of passphrases for authentication: An empirical field study. *Int. J. Human-Comput. Stud.* **2007**, *65*, 17–28. [CrossRef]
69. Yıldırım, M.; Mackie, I. Encouraging users to improve password security and memorability. *Int. J. Inf. Secur.* **2019**, *18*, 741–759. [CrossRef]
70. Florêncio, D.; Herley, C.; Van Oorschot, P.C. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. In Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, 20–22 August 2014.