Received: 20 April 2023 | Revised: 8 June 2023 | Accepted: 28 June 2023
DOI: 10.37917/ijeee.20.1.6 Vol. 20 | Issue 1 | June 2024

Open Access

Iraqi Journal for Electrical and Electronic Engineering
Original Article

IJEEE University of Basrah College of Engineering

Measuring Individuals Cybersecurity Awareness Based on Demographic Features

Idrees A. Zahid*[1], Samir Alaa Hussein[1], Shakir Mahmood Mahdi[2]
[1]Information Technology Center, University of Technology, Baghdad, Iraq
[2]Division of Graduate Studies, University of Technology, Baghdad, Iraq

Correspondance
*Idrees A. Zahid
University of Technology, Baghdad, Iraq
idrees.a.zahid@uotechnology.edu.iq

Abstract

Cybersecurity awareness has a huge impact on individuals and an even bigger impact on firms, universities, and institutes to those individuals belong. Consequently, it is essential to explore and asses the factors affecting the awareness level of cybersecurity. More specifically this research study examines the impact of demographic features of individuals on cybersecurity awareness. The Studied literature's limitations have been addressed and overcome in our research from the variability, and ambiguity aspects. A questionnaire was developed and responses were collected from 613 participants. Reliability and validity tests as well as correlations have been applied for the instruments and data employed in this study. Coefficients were calculated via multiple linear regression for the weights of each of the cybersecurity components. Data reliability test showed that Cronbach's Alpha value of 0.707 for the used data which is acceptable for research purposes. Results analysis showed r-value for each of the questions is greater than the r table which was 0.07992. Examining the proposed hypotheses showed that there is a difference as the null hypothesis is rejected for one of the demographic features being tested namely, gender. While there is no significant difference when it comes to the other two factors, education level, and age. Using the weight for each of the components, password security, technical behavior, and social influence could provide a solid base for decision-makers to focus on and implement the available resources for gender-specific developments to raise the cybersecurity awareness level..

Keywords

Cybersecurity Awareness, Cyberattacks, Demographic features, Multiple Linear Regression, Correlation.
At least four keywords or phrases in alphabetical order, separated by commas.

I. Introduction

Due to advances in technology and online services, the need for rising cybersecurity awareness is increased. Securing devices and protecting data is essential nowadays especially with the increased attacking tactics and techniques, like malware, ransomware, phishing, and others [1]. Institutions and firms' investment in cybersecurity protection requires an in-depth analysis. The urge for the factors affecting cybersecurity awareness is highly important for budget planners and decision-makers [2]. Protecting sensitive data and preventing attacks or breaches depends mainly on cybersecurity awareness factors. To increase the level of protection significantly, a strong password and updated software should be employed as well as avoiding phishing links and scams while serving and interacting online [3] [4]. Targeting passwords in an attempt to compromise an account and gain access is widely common. Using complex passwords and including a combination of numbers, letters, and special characters could highly reduce or even prevent guessing the used passwords. Creating a unique password for every account is an important procedure as well. Also avoid using common information like names, dates of birth as those are easily guessed [5]. Furthermore using an up to date software is essential and batching operating systems and any other used application with a security update is crucial as companies used to batch exposed security vulnerabilities if there is any [6]. Phishing scams are widely used tool by hackers. Practicing not opening documents or click on links from unknown senders, would increase the number of individuals as well as the institute's cybersecurity [7]. Besides the technical aspects of cybersecurity, considering the social and cultural dimensions of online cybersecurity is essential. Research has shown that women and men may have different experiences and concerns when it comes to cybersecurity. Organizations and individuals being aware of these gender-specific risks can help in taking steps to address them. This may include providing education and training on online safety, as well as creating policies and procedures to address and prevent online harassment. Considering the diverse experiences and needs of all users, creating a more inclusive and secure online environment for everyone is more robust [8] [9] [10]. Acknowledging that cybersecurity is not just a technical issue, but also a social and cultural one is fundamental [11]. It is not just about protecting computers and networks from attacks, but also about ensuring that all users practice and respond safely and with proper caution when online and in their day-to-day interactions. In addition to gender and cultural differences, education level can also play a role in cybersecurity awareness. People with different levels of education might react differently and be more aware of online threats and more likely to take steps to protect themselves. However, this does not mean that people with lower levels of education are necessarily more vulnerable to cyber threats [12]. Age is another feature that can influence cybersecurity awareness. Older individuals may be less familiar with technology and may not be as aware of the risks and best practices for online safety. They may be more likely to fall victim to phishing scams or to accidentally download malware, for example. On the contrary, older people might get well educated to protect their privacy and online activities against cybercrimes or attacks. The same paradox applies to younger individuals as they may be more involved in technology and able to securely navigate the online world. And they might also be more likely to take risks and be less cautious out of laziness or neglect. They may be more likely to use weak passwords, click on links from unknown sources, or share personal information online. Consequently, it is substantial for individuals of all ages to be aware of the risks and learn to protect themselves online and avoid attackers attempts. This may include seeking out resources and training on online safety, as well as staying up to date on the latest threats and best practices [13] [14] [15]. This research aims to:

- Evaluate and address cybersecurity awareness factors in order for the decision-makers to provide and asses the education, and training needed.

- To specify and target the level of cybersecurity awareness in order to provide the required education.

- For budget planning and capital investment purposes, as it is instrumental to be ahead planned and addressed.

- For sensitive positions recruitment, to give an insight for HR and employers to fill the position with the most appropriate individuals according to the provided demographic features.

This manuscript is organized as follows: the next section discusses the literature review. The methodology and work scenario adapted are explained in the material and methods section as well as the proposed hypotheses. The results section presents the outcome of the tests applied to each step to verify the reliability and validity as well as the correlation test results. The discussion section explains the analysis of the obtained results as well as the hypotheses outcomes. Finally, the conclusion section is presented with an overall conclusion based on the results deduced and the analysis of those results. Appendix A holds the correlation tables for each of the main component factors.

II. Literature review

Researchers in [16] explored the boosting of cyberattacks, specifically social engineering attacks which targets the end user mainly and the increasing level of cybersecurity awareness. Considering the end users as the main target for social engineering attacks, they hold the weakest link that composes the entire cybersecurity system for the firm, or institute they belong to. This weak target could be strengthened through cybersecurity awareness. A rise in the awareness level among employees and users could be achieved via educational programs.

Authors in [17] present in their study the level of understanding for cybersecurity attacks and the following consequences that Majmaah University students have. Their research found that via the questionnaire conducted to assess the level of understanding, found that an increase in cybersecurity awareness is a must among university students. Furthermore, traditional education methods should be combined with advanced ones, as well as videos and even games can be employed to provide students with the required awareness.

Determining the understanding level of threats that come from online activities and the prevention measures used for providing the youngest with online protection was the main aim of the study [18]. Survey outcomes, according to the collected data from random students' classes of age eleven and above, found that most of the children are unaware of online security and hidden risks.

The study [19] was conducted on developing countries students through a scientific questionnaire consisting of eleven items. Those questions tested the knowledge and understanding of the impact of software and email security. Although the questions did not cover all essential cybersecurity aspects, the study found that email security is mainly more beneficial to increase cybersecurity awareness than software security.
Authors in [13] researched the level of cybersecurity awareness in Saudi Arabia. The authors researched through an online questionnaire the level of awareness, cybersecurity practices, and incident reporting procedures. Analysis of the obtained results, the authors concluded to promote the level of awareness.
According to the literature studies discussed above, the necessity to assess the awareness of cybersecurity for induvial is essential to provide and complete the security measures from all aspects., considering that the end user is the main and weakest target. From this perspective, our research gains its importance to measure and assess individual cybersecurity awareness. Additionally, several limitations have been found in the literature and an overcome to those drawbacks in our research has been embraced as below.
In [17] authors assess the cybersecurity awareness among Majmaah University students, a lack of variability in samples limited their research study due to the nature of the samples representing university students only. Another limitation of this study is the limited understanding and ambiguity caused by the lengthy questions within the questionnaire.
Research [18] also presents a lack of variability limitation in the used samples due to its limitation to young people. Researchers in [19] also limited their samples to young people which results in a lack of variability, furthermore, the limited scope is used within this research that focuses only on email and software security.
In [20] and [21] samples lack of variability is also found. Samples from only employees from the industry are collected.
For [13] the drawback was in the lengthy subjects and unfamiliar concepts which results in unanswered questions that led to missing and incomplete samples. In our manuscript we overcome the lack of variability presented in [17], [20] and, [21] in which samples from only university students or industry are collected. A generalization in our sample collections is adopted from both academia and industry. We also overcome the drawbacks of [18],[19] were limited their samples to young people only. Variability is adopted from an age perspective to avoid homogeneity in our collected data.
Lengthy questions and subjects as well as ambiguity in questionnaire development in [17] and [13] are avoided in our research study.

III. Materials And Methods Used

The materials employed and methodology followed in this study are structured and explained in this section alongside the proposed hypotheses.

A. Questionnaire Development

This sub-section describes the process used to develop the questionnaire, including the selection of items, pilot testing, and revisions. In order to provide a theoretical foundation, we prepared a questionnaire that covered a number of questions designed to assess the subjects' global familiarity with cybersecurity concerns as well as their awareness of cybersecurity dangers. The survey was conducted and distributed in diverse ways to ensure that responses from various sets of male and female participants were collected swiftly and accurately. The survey contained 17 questions covering all facets of cybersecurity, including three demographic questions. These queries and questions were given and distributed to undergraduate and graduate students, who responded with a total of 613 responses. Again, these replies were classified in accordance with the hypothesis and analysis. The following question components are present: Passwords, technological behavior, and social influence-based questions. Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree were the options for the Likert scale-based multiple-choice responses to these questions.
The following questions were drafted in the online survey used in this research:

- Section 1 (Password Security related questions):
  Q1: Do you set a password for your phone?
  Q2: Do you set a password for your computer?
  Q3: Do you use a complex password?
  Q4: Do you change your password periodically?
  Q5: Do you use one password for all your accounts?
  Q6: Do you reuse your old password?
- Section 2 (Technical Behavioral related questions):
  Q7: Do you lock your phone when unattended?
  Q8: Do you lock your computer when unattended?
  Q9: Do you login to your account using public machines?
  Q10: Do you install applications on your phones via advertising links?
  Q11: Do you install licensed products on your computer?
  Q12: Do you open attachments from an unknown sender?
  Q13: Have you activated two factor authentication?
- Section 3 (Social Influence related questions):
  Q14: Do you apply cybersecurity advice and procedures when at home as well?
  Q15: Do you educate and advise your family and

friends regarding cybersecurity tips and protection procedures?
Q16: Do you follow your institute policies when using online services?
Q17: Have you attended cybersecurity awareness workshops or seminars?.

Questions numbered 5,6,9,10, and 12 are marked as reversed questions meaning that their coding in the Likert system is reversed so 5 as a value is given for the Strongly Disagree option, and 1 is given for Strongly Agree. Each of the grouped questions above, i.e., each section will compose an independent variable will be denoted as $x1, x2, x3$, representing section 1, section 2, and section 3 respectively. All independent variables will be utilized towards the composition of the cybersecurity awareness denoted by (y) which represents the dependent variable.

B. Data Collection

This sub-section describes the method used to collect data, such as online surveys, mail surveys, or face-to-face interviews. It also includes details on any incentives offered to participants, the response rate, and any missing data.
Three demographic features, including age, gender, and education level, were collected from respondents as an online survey was constructed and distributed to answer 17 questions pertaining to cybersecurity awareness. We used a Likert scale to rate the responses. A total of 613 responses were collected, with no missing data as we designed the online survey to have all the answers to be collected mandatory otherwise no response will be sent. A total of 324 responders were males which constitutes about 52% of the total responses while 289 of the responses were female and which was about 48% of the total population. Regarding the taxonomy of the education level; 435 of the respondents hold or during a bachelor's degree that which is about 71% and 125 with a master's degree, which is about 20%, and 53 with a Ph.D. degree which is about 9%. For the age statistics, 307 participants were between 18 and 25 years old, whereas 174 responses come from participants aged 25 to 35 years old, and a total of 132 responses comes from 35 years old or older. Figure 1 provides a graphical representation for the samples of the data collected based on demographic features.

C. Tools Employed

To test the research hypotheses and apply the validity and reliability tests to the instruments and data collected we used R programming language version 4.2.2 with SPSS version 26 to do statistical computing. Figure 2 presents the method employed in this research graphically. As shown in Figure 2 the process includes developing a questionnaire and collecting data from targeted users. A validity test is applied for the developed questionnaire, while a reliability test is applied for the collected data.
A correlation test is performed for the assigned factors. Awareness factors along with the collected data are used to calculate cybersecurity awareness using multiple linear regression. Employing the output of the overall process to validate the research hypotheses.

D. Research Hypotheses

This sub-section describes the statistical methods used to analyze the data, such as descriptive statistics, reliability analysis, or internal analysis. Two main hypotheses will be proposed in this research; these are the null hypothesis and the alternative hypothesis.
According to the demographic features collected alongside the responses, for each of those demographic variables, the two hypotheses will be applied and tested as below:

1. Gender feature:
   - Null hypothesis: There is no difference in cybersecurity awareness being measured in this research between male and female.
   - Alternative hypothesis: There is a difference in cybersecurity awareness being measured between males and females.
2. Age feature:
   - Null hypothesis: There is no difference in cybersecurity awareness according to the age of the respondents.
   - Alternative hypothesis: There is a difference in cybersecurity awareness according to the age of respondents.
3. Education Level feature:
   - Null hypothesis: There is no difference in cybersecurity awareness according to the level of education of the participants.
   - Alternative hypothesis: There is a difference in cybersecurity awareness according to the level of education of the participants.

E. Cybersecurity Awareness as Dependent Variable

The scoring methodology is used to determine the participants' cybersecurity awareness level in order to analyze the grouping factors and demographic features on that level. As the number of questionnaire items utilized in this study is $N = 17$, and the Likert system is employed with a maximum value of 5 and a minimum value of $1, 17$ reflects the lowest possible score according to the scoring technique. To classify participant scores, the Department of National Education (2006) criteria

TABLE I. Cybersecurity Awareness Classification

Number	Score	Classification
1	71 - 85	Very High Awareness
2	58 - 71	High Awareness
3	44 - 58	Medium Awareness
4	30 - 44	Low Awareness
5	17 - 30	Very Low Awareness

are proposed in this study. The scoring classification is as follows:
The level of cybersecurity awareness is measured according to the levels provided in Table I. Five classification levels have been listed with the range score of each. The bigger the scoring is, the highest the level of awareness will be.

IV. Results Analysis

This section includes the results outcome of the reliability test as well as the validity test. It also presents correlation tests, multiple linear regression, and results of the tested proposed hypotheses.

A. Reliability and Validity

In data collecting, the instrument's validity and reliability are vital. Therefore, the quality of the research outcomes will be determined by the reliability of the data. Whether or not the data is accurate, depends heavily on whether or not the study instrument is reliable. Cronbach's alpha is a regularly employed statistic for evaluating the reliability of measurement equipment. It is a measurement of the internal consistency of a test or the extent to which various test items measure the same underlying construct. Questions employed within the questionnaire should be tested for validity as well to ensure the appropriate outcomes and a measured valid result. Data reliability test results will be discussed next followed by questions validity test results. Finally, a correlation test result is drawn for the internal items and for the independent variable.

1)Data Reliability

The Cronbach's alpha coefficient is derived from the correlations between the test items. A high Cronbach's alpha coefficient shows that test items are closely correlated, indicating that they measure the same underlying construct. A low Cronbach's alpha coefficient shows that the test items are not as highly associated, indicating that they may not be assessing the same underlying construct. The Cronbach's alpha coefficient that's typically 0.7 or higher is generally considered to be acceptable for research purposes. As we have implemented Cronbach's alpha test on our data we obtain a 0.707 value for that factor, which indicates that our data has passed the reliability test. With the number of items N in the study equals 17 to provide results of the reliability tests that are reliable enough, namely the Cronbach's Alpha value of 0.707. Cronbach's Alpha value is between 0.7–0.8. This shows that each statement utilized in the variable is sufficiently dependable; hence, all questions or statement items implemented or used in this study are appropriate for further study.

2) Questions Validity

The findings of testing the validity of each item, based on the 613 respondents that were analyzed, are presented in Table II. According to the findings of the validity test, all of the questions pertaining to the independent variables, such as password security $(X1)$, technical behavior $(X2)$, and social influence $(X3)$. A correlation value (r-value) that is greater than the r table (0.079920). The r value of the table is obtained based on the degree of freedom df, which is assigned for the number of items and respondents in our research study. The value of (r table) is $N-2$ – the degrees of freedom (df) for the Pearson correlation coefficient. In our research data, $N = 613$ so the df is 611. This suggests that each of the questions can be answered correctly. Therefore, it is possible to draw the conclusion that all of the questions that were utilized in this study are appropriate for more research.

3) Correlations

To results of correlation, tests represent how the tested data are correlated or not. In this subsection, two main correlation tests have been made. The first represents the correlation of the questions, i.e., items in each of the factors compromising

TABLE II. Validity test for the 17 questions

Variable	Question Item	r-Value	r-Table
Password Security	Q1	0.532	0.079920
	Q2	0.616	0.079920
	Q3	0.592	0.079920
	Q4	0.624	0.079920
	Q5	0.464	0.079920
	Q6	0.527	0.079920
Technical Behavioural	Q1	0.515	0.079920
	Q2	0.503	0.079920
	Q3	0.411	0.079920
	Q4	0.481	0.079920
	Q5	0.464	0.079920
	Q6	0.464	0.079920
	Q7	0.494	0.079920
Social Influence	Q1	0.799	0.079920
	Q2	0.757	0.079920
	Q3	0.556	0.079920
	Q4	0.706	0.079920

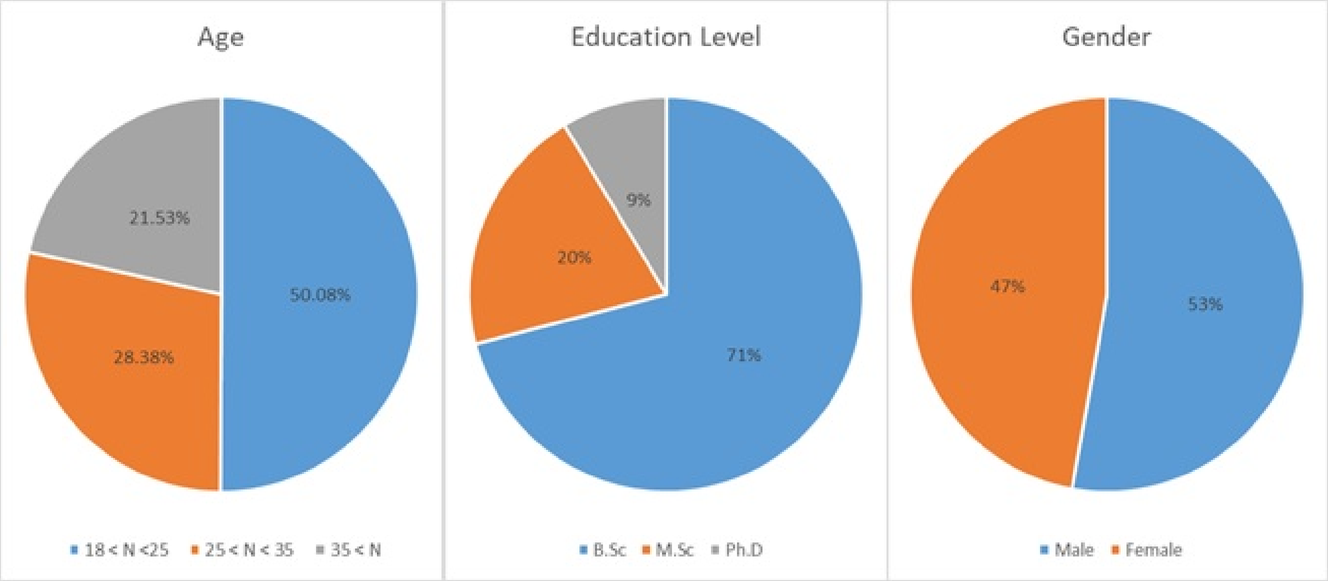

Fig. 1. Graphical Statistics for the distribution of the participants demographics

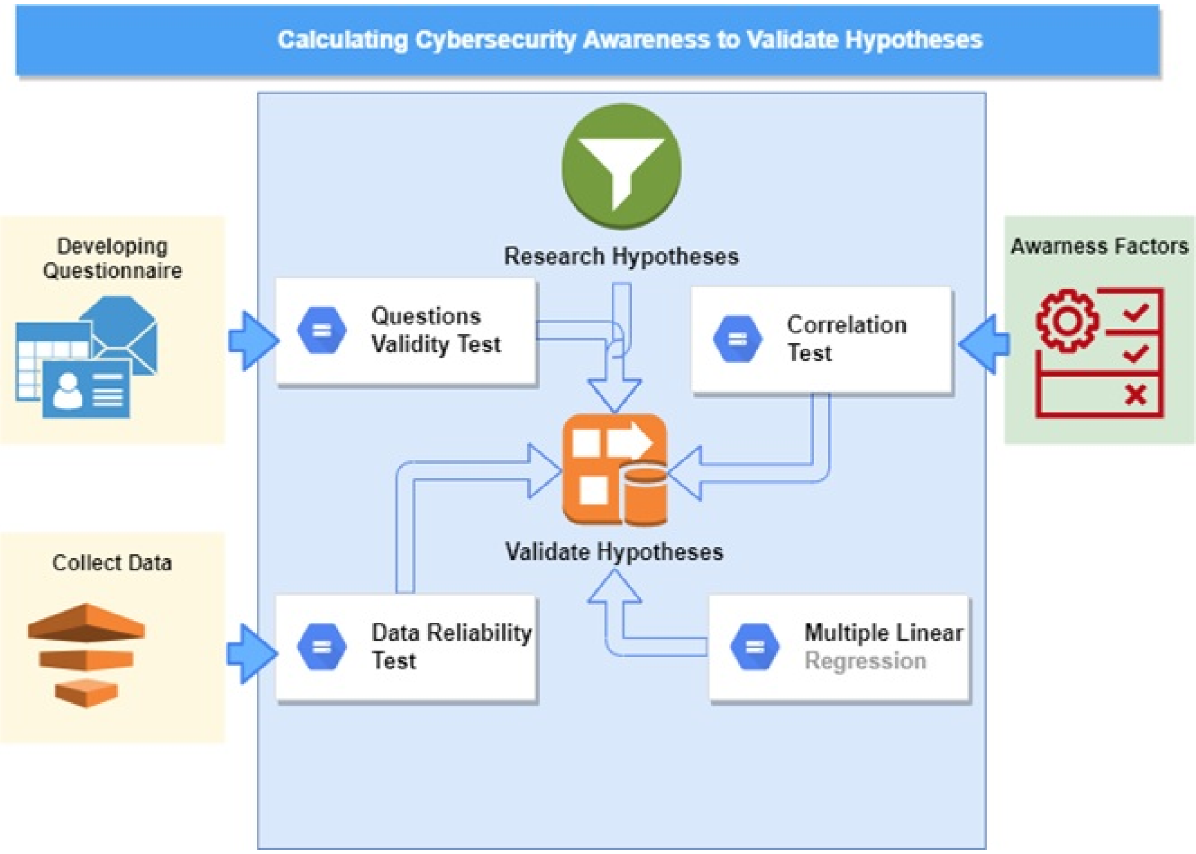

Fig. 2. Cybersecurity awareness to validate hypothesis

TABLE III. Independent Variables Correlations

Variable	Password Security	Technical Behavioral	Social Influence	Cybersecurity Awareness
Password Security	1			
Technical Behavioral	0.445	1		
Social Influence	0.240	0.274	1	
Cybersecurity Awareness	0.729	0.660	0.563	1

cybersecurity awareness. The second test is the correlation of the three main components that compose cybersecurity awareness as independent variables. The results of both of those correlation tests are presented in the following two subsections:

- Internal Items Correlation for Each Main Factor:
  The matrix is a table where the rows and columns represent the variables, and the cells contain the correlation coefficients between the variables. The correlation coefficient is a measure of the strength and direction of the relationship between two variables. A positive coefficient indicates a positive relationship, meaning that as one variable increases, the other variable also tends to increase. A negative coefficient indicates a negative relationship, meaning that as one variable increases, the other variable tends to decrease. The magnitude of the coefficient indicates the strength of the relationship; the closer the coefficient is to 1 or -1, the stronger the relationship. Correlation for the questions related to password security, questions related to technical behavior as well as correlation related to social influence is presented in Appendix A. The three mentioned factors correlations showed positive correlations representing that each of the questions categorized in that specific main factor is positively correlated towards its main category or factor. As presented in Appendix A, all questions showed a positive correlation for each question, and no negative or near-zero correlation results have been found.
- Independent Variable Correlation:
  As part of the validity test of the categorized input factors as independent variables namely Password Security, Technical Behavioral, and Social Influence towards measuring cybersecurity awareness, a correlation test has been applied to those factors with correspond to cybersecurity awareness. The results of these correlations are presented in Table III.
  Table 3 clearly presents the positive correlation between the independent variables and cybersecurity awareness as well as a positive correlation between each of the independent variables themselves. Password Security factor gives us the highest correlation with cybersecurity awareness with a 0.729 value, Technical behavioral Table III shows that its correlation with the dependent variable is 0.66 while Social Influence presents 0.563.

B. Multiple Linear Regression

In data collecting, the instrument's validity and reliability are vital. Therefore, the quality of the research outcomes will be determined by the reliability of the data. Whether or not the data is accurate depends heavily on whether or not the study instrument is reliable. Cronbach's alpha is a regularly employed statistic for evaluating the reliability of measurement equipment. It is a measurement of the internal consistency of a test or the extent to which various test items measure the same underlying construct. As we have several factors representing independent variables towards measuring the dependent variables defined by cybersecurity awareness a multiple linear regression is employed using R programming language for the data collected, regression coefficients are obtained and presented in Table V.

Employing the equation of multiple linear regression to analyze the impact of each factor using equation 1:

$$y = c + b1x1 + b2x2 + ... + bnxn \tag{1}$$

Equation 1 generally describes the connection between several independent variables or predictor variables and one dependent variable. A dependent variable is modeled as a function of multiple independent variables with coefficients and a constant term. Multiple regression is so-called because it involves two or more predictor variables. Denoting (y) in equation 1 as the dependent variable that represents cybersecurity awareness and assigning the constant value to (c) in equation 1 to represent the intercept value of -0.8264. While regression coefficients that represent: Password Security, Technical Behavioral, and Social Influence, with values: 0.5147, 0.469, and 0.3017 respectively will substitute b1, b2, and b3 for the independent variables to form our cybersecurity awareness formula as in equation 2:

$$\begin{aligned} CybersecurityAwareness = & -0.8264 + (0.5147)X1 \\ & + (0.469)X2 + (0.3017)X3 \end{aligned} \tag{2}$$

C. Research Hypotheses Results

For the research hypotheses proposed a test was utilized to measure the acceptance of each. For each of the tested demographic features collected two hypotheses were proposed as follows:

- Null Hypothesis: in which the correlation coefficient between populations is not substantially different from zero. There is no linear association or correlation between x and y in the sample population.
- Alternative Hypothesis: The population correlation coefficient is a considerable distance from zero. There is a significant or considerable linear relationship in the population between x and y.

Test results are presented in Table IV the significant value (Sig). If the significant value of the specific variable is less than alpha where alpha $a = 0.05$ then the null hypothesis is rejected and the alternative hypothesis is accepted.
According to the values obtained in Table 7 for the significant value regarding each of the demographic features then:

1. Gender Factor: Null hypothesis is rejected and the alternative hypothesis is accepted.
2. Education Factor: Null hypothesis is accepted and the alternative hypothesis is rejected.
3. Age Factor: Null hypothesis is accepted and the alternative hypothesis is rejected.

V. Discussion

This section discusses the results main sections as connected to the main hypotheses and proposition in this manuscript.

A. *Correlation Results Analysis*

Correlation test results show a noticeable positive indication that each group of questions items is all correlated towards their grouping factor. Besides that, the grouped factors show also a positive correlation towards the dependent variable, i.e., cybersecurity awareness. This indication provides a solid base for the proposition and discussion of the research hypotheses.

B. *Hypotheses Results Discussion*

Examining the results of the research hypotheses and the significant values obtained from the tests provides a powerful impact on the research study. As the demographic features have been tested towards the awareness of cybersecurity, the results obtained to the proposed hypotheses for the three studied factors; namely: 1) Gender, 2) Education Level, and 3) Age, have shown that:

1. For the Gender factor: as the null hypothesis has been rejected and the alternative one has been accepted, there is a difference in cybersecurity awareness between males and females.
2. For the Education Level factor: the null hypothesis has been accepted, indicating that there is no difference in cybersecurity awareness based on the level of education.
3. For the Age factor: the null hypothesis has been accepted as well, indicating that the age factor does not show any related difference in cybersecurity awareness.

TABLE IV. Hypotheses Test Results

Variable	Sig
Gender	0.000
Education Level	0.608
Age	0.514

TABLE V. Regression Coefficients

Intercept	Regression Coefficients
Password Security	-0.8264
Technical Behavioral	0.5147
Social Influence	0.469
Cybersecurity Awareness	0.3017

C. *Multiple Linear Regression Analysis*

Exploring multiple linear regression and equation 1 obtained from the analysis of the multiple linear regression as the coefficients concluded. We can see the impact of each component of the independent variables $x1, x2$, and $x3$ representing password security, technical behavioral, and social influence respectively, towards the dependent variable (y), i.e., the cybersecurity awareness. The greatest impact is held by the password security independent variable with a coefficient value of 0.514 followed by a coefficient value of 0.469 for the technical behavioral, and the social influence independent variable constitutes the lesser impact towards cybersecurity awareness with a coefficient value of 0.3017.

VI. Conclusion

In conclusion, this study provides evidence that there is a difference in cybersecurity awareness based on gender between men and women. As the data was collected from the participants through the validated items within the questionnaire, the r-value for each of the questions is greater than the r table which was 0.079920. This indicates that each of the questions could be answered correctly and is valid for the questionnaire. Data reliability test results showed that Cronbach's Alpha value is 0.707 which is considered to be acceptable for research purposes. The results suggest that the gender factor has a difference in cybersecurity awareness while education level and age factors do not provide any differences in the awareness level. These findings have important implications for organizations and individuals, as understanding the factors that impact cybersecurity awareness can help to improve cybersecurity strategies and reduce the risk of cyber-attacks. Also, the factors' coefficients compromising the cybersecurity awareness level provide a clear indication of the weight of each component. The need for raising awareness can be well categorized according to the studied factors and features. For future work, considering the available resources and the required amount needed to improve the awareness level for the targeted individuals, the regression coefficient could be a great start to building the improvement strategies.

Conflict of Interest

The authors have no conflict of relevant interest to this article.

References

[1] S. Venkatesha, K. R. Reddy, and B. Chandavarkar, "Social engineering attacks during the covid-19 pandemic," *SN computer science*, vol. 2, pp. 1–9, 2021.

[2] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, "Information security awareness in educational institution: An analysis of students' individual factors," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 352–359, IEEE, 2015.

[3] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[4] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2157–2177, 2021.

[5] S. M. Kennison, I. T. Jones, V. H. Spooner, and D. E. Chan-Tin, "Who creates strong passwords when nudging fails," *Computers in Human Behavior Reports*, vol. 4, p. 100132, 2021.

[6] I. Mugarza, J. L. Flores, and J. L. Montero, "Security issues and software updates management in the industrial internet of things (iiot) era," *Sensors*, vol. 20, no. 24, p. 7160, 2020.

[7] F. L. Greitzer, W. Li, K. B. Laskey, J. Lee, and J. Purl, "Experimental investigation of technical and human factors related to phishing susceptibility," *ACM Transactions on Social Computing*, vol. 4, no. 2, pp. 1–48, 2021.

[8] I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as "the three r's"," *Heliyon*, vol. 5, no. 12, 2019.

[9] S. Wolf, A. C. Burrows, M. Borowczak, M. Johnson, R. Cooley, and K. Mogenson, "Integrated outreach: Increasing engagement in computer science and cybersecurity," *Education Sciences*, vol. 10, no. 12, p. 353, 2020.

[10] A. Withanaarachchi and N. Vithana, "Female underrepresentation in the cybersecurity workforce–a study on cybersecurity professionals in sri lanka," *Information & Computer Security*, vol. 30, no. 3, pp. 402–421, 2022.

[11] D. Van Der Linden, O. A. Michalec, and A. Zamansky, "Cybersecurity for smart farming: socio-cultural context matters," *IEEE Technology and Society Magazine*, vol. 39, no. 4, pp. 28–35, 2020.

[12] R. Van Bavel, N. Rodríguez-Priego, J. Vila, and P. Briggs, "Using protection motivation theory in the design of nudges to improve online security behavior," *International Journal of Human-Computer Studies*, vol. 123, pp. 29–39, 2019.

[13] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in saudi arabia," *Heliyon*, vol. 7, no. 1, 2021.

[14] L. Zhang-Kennedy and S. Chiasson, "A systematic review of multimedia tools for cybersecurity awareness and education," *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1–39, 2021.

[15] S. Tirumala, M. R. Valluri, and G. Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures," in *2019 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–6, IEEE, 2019.

[16] H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: A literature review," in *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)*, pp. 62–68, IEEE, 2018.

[17] T. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among students of majmaah university," *Big Data and Cognitive Computing*, vol. 5, no. 2, p. 23, 2021.

[18] Y. Nidup, "Awareness about the online security threat and ways to secure the youths," *Journal of Cybersecurity*, vol. 3, no. 3, p. 133, 2021.

[19] M. A. Alqahtani *et al.*, “Cybersecurity awareness based on software and e-mail security with statistical analysis,” *Computational Intelligence and Neuroscience*, vol. 2022, 2022.

[20] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness,” *MIS quarterly*, pp. 523–548, 2010.

[21] W. R. Flores and M. Ekstedt, “Shaping intention to resist social engineering through transformational leadership, information security culture and awareness,” *Computers & security*, vol. 59, pp. 26–44, 2016.