Computer Systems Science & Engineering
DOI:10.32604/csse.2022.019938
Article

Tech Science Press

Impact of Human Vulnerabilities on Cybersecurity

Maher Alsharif[1], Shailendra Mishra[2,*] and Mohammed AlShehri[1]

[1]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia
[2]Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Majmaah, 11952, Saudi Arabia
*Corresponding Author: Shailendra Mishra. Email: s.mishra@mu.edu.sa
Received: 02 May 2021; Accepted: 08 June 2021

Abstract: Today, security is a major challenge linked with computer network companies that cannot defend against cyber-attacks. Numerous vulnerable factors increase security risks and cyber-attacks, including viruses, the internet, communications, and hackers. Internets of Things (IoT) devices are more effective, and the number of devices connected to the internet is constantly increasing, and governments and businesses are also using these technologies to perform business activities effectively. However, the increasing uses of technologies also increase risks, such as password attacks, social engineering, and phishing attacks. Humans play a major role in the field of cybersecurity. It is observed that more than 39% of security risks are related to the human factor, and 95% of successful cyber-attacks are caused by human error, with most of them being insider threats. The major human factor issue in cybersecurity is a lack of user awareness of cyber threats. This study focuses on the human factor by surveying the vulnerabilities and reducing the risk by focusing on human nature and reacting to different situations. This study highlighted that most of the participants are not experienced with cybersecurity threats and how to protect their personal information. Moreover, the lack of awareness of the top three vulnerabilities related to the human factor in cybersecurity, such as phishing attacks, passwords, attacks, and social engineering, are major problems that need to be addressed and reduced through proper awareness and training.

Keywords: Cybersecurity; phishing attack; password attack; social engineering; cybersecurity awareness; security risk

1 Introduction

In today's world, the whole world is highly dependent on technology, leading to an excess of digital data formation. All the major sectors collect the larger datasets on the workstations and send them to other systems through the various networks. These devices have certain vulnerabilities that impact on organizational performance and effectiveness [1]. It can damage the performance and effectiveness of the company by

losing the trust of consumers and official representatives. Any critical data loss, such as the source files of copyright or trademark, can impact the organizational effectiveness and competitive advantage.

Moreover, a data breach due to improper security programs can affect a company's revenue [2]. Cybersecurity is a type of protection system that maintains the confidentiality, integrity, and accessibility of digital information. Cybersecurity consists of an evolving set of devices, risk management technologies, training approaches, and specific measures designed to protect the networks, programs, and data from any unauthorized access [3], with the tremendous development of the internet and its use in the delivery of services by the private sector to improve their services and reach more customers not only locally, but also globally. Government communities are also moving towards security controls and measures to provide effective services to individuals. Many factors affect the cybersecurity of the companies, such as software and networks, all of which are focused on, but one factor needs more attention: the human factor, and that's what we're going to address in this research. This research focuses on human errors and risk factors leading to security issues and develops effective solutions against security threats and attacks. Companies are now accessing websites and delivering services, customer relations, basic transactions, and purchases from these sites. To keep track of these transactions, users need to create a user account on these websites [4].

The Government of Saudi Arabia provided the opportunity to use the internet to drive the adoption of technology, data, and artificial intelligence to deliver government services to citizens, non-citizens, and the public and private sectors by using Absher as part of the vision of 2030 [5,6]. With these services, new risks such as hacking and identity theft are increasing for which security measures and policies are required to eliminate these risks, and with such assumptions, there are significant challenges to making it secure and trustworthy [7]. It is found that many users include simple passwords to protect computer systems and accounts, but hackers use malicious codes which are capable of hacking simple passwords easily, for which it is recommended that strong and complex passwords should be applied. Mainly, hackers access social media software to collect information about the victims through phishing or social engineering [8]. Therefore, it is an important task to educate users on how to protect themselves from such attacks.

Cybersecurity vulnerabilities are categorized into different areas, such as where the vulnerability may exist, why the vulnerability exists, or how the vulnerability can be abused. Cybersecurity is implementing systems or networks and various programs that protect the software and computer system from any digital attacks. These attacks aim to access, manipulate, dismantle sensitive information of companies, extort money from various interested parties, or penetrate a company's work. Moreover, the cybersecurity approach can be successfully implemented by providing multiple layers of protection deployed between computer systems, networks, or any data that needs to be kept secure [9]. If the computer systems, operations, and networks are connected with the secured systems and solution, then the performance and effectiveness of the business performance can be improved, and cyber-security can be managed [10]. With the coronavirus pandemic (COVID 19), the use of online services has increased, and many hackers take advantage of targeting victims by using either social engineering or phishing threats. Over time, various attempts have been made by malicious cyber attackers to penetrate the personal and confidential information of the targeted individual or a company. Cyber-attacks seem to be effective because they are cheaper and more convenient than physical attacks. Malware is the major attack that enables hackers to break the cybersecurity in the system. With every person using such technologies, the target spectrum has widened. Not every person is well versed with technological knowledge and is not updated and trained with the threats of cyber-attacks [11]. Employees in the organization tend to make unintentional mistakes that lead to data breaches, and the attackers exploit the corporate data [12].

This study discusses the causes of human errors and proposes effective security measures and controls to reduce and handle cyber-attacks. Hacking personal details of the companies and users can be done by the

attackers using malicious codes and cyber-attacks, for which it is important to secure internal networks and communication channels. The human factor is the primary cause of security, and companies are not focusing on insider risks due to which they can suffer from the cyber-attacks and lack awareness about cyber-security employees cannot defend against cyber-threats vulnerabilities. Traditional security methods and employee training are not enough to protect classified data from sophisticated cyber-attacks based on human vulnerabilities. Traditional technologies such as sandboxes, antivirus controls, secure email, and others were designed to fend off attacks that directly target the network. Different strategies are needed to deal with the new phishing attacks that target vulnerable employees [13].

A combination of cyber-attack awareness training, secured email addresses, URL filtering, and the newly developed instant identification of phishing sites to catch unknown attackers must be implemented to protect systems from these phishing attacks [14]. Blocking phishing attempts from the beginning of the chain is important to prevent any damage or injury. Some other policies can be used to protect the system from malicious cyber-attacks. Updating the security policies should be the first step in the organizations by setting the security rules and policies to protect confidential data from attackers [15]. Employee monitoring tools are another development that needs to be implemented in organizations to monitor user activities. This research explores and exploits human vulnerabilities and their impact on the organization;

- This research examines human vulnerabilities and their measures by using qualitative and quantitative techniques.
- Focus on human vulnerabilities and reduce the risk by focusing on human nature and responding to different situations.
- The research aims to promote an approach that would significantly influence the fight against cybersecurity issues like social engineering, phishing, and password attacks.
- Reduce human vulnerabilities by measuring the current status and providing a suitable solution to close the gap between the current user's awareness and the target level to improve security and reduce user vulnerabilities.

The remainder of this paper is organized as follows. Related work in social engineering, phishing, password attacks, and countermeasures is discussed in section two. Research Methodology is discussed in section three. A detailed discussion of the implementation and result analysis is discussed in section four. The paper is concluded in section five.

2 Related Work

In the context of cyber-attacks, human vulnerability is a major problem in business communities where insider risks and threats can be posed by hackers easily. Even if many layers of protection are implemented in the security stack or employees are educated about phishing and its risks, malicious criminals develop various sophisticated tricks to exploit the vulnerabilities of the human mind with broad tactics. There are several ways in which human vulnerabilities can be exploited. Some of them are described below:

Social engineering is a cyber-attack used to exploit a person in a psychological way to make him divulge his secret information [16]. Criminals use social engineering methods because the human tendency to trust is easier to exploit than other hacking software. Nearly 95% of web attacks are due to social engineering tricks. A malicious perpetrator first studies the targeted victim to compile background information for the cyber-attack. The criminal then attempts to gain the victim's trust and persuade them to take further actions that eventually lead to breaching security, such as revealing sensitive personal information or granting access to personal profiles [17].

Phishing is a cybercrime that uses fraudulent websites, text messages, or emails to steal personal or company information [18]. Attackers who mainly use these phishing tactics have an easy time as they

cleverly hide behind the intended victim's emails and websites. Phishing is one of the common examples of social engineering in cyberattacks [19]. There are different types of phishing attacks, such as spearfishing, whaling, or clone phishing. There are a few very common mistakes made by employees that lead to cyber-attacks by criminals. Miss delivery is one of the major mistakes. Miss delivery is sending confidential information to another person using the wrong email address [20]. This is an act of carelessness, or sometimes, when automatically suggested email addresses are displayed, employees use the suggested email address without checking if it is the required email address. Another such common mistake is using simple passwords for their profiles. Simple passwords can be easily cracked by cyber attackers, making the user and their data accessible to the attacker [21].

In [22], the authors discussed that computer systems and networks are increasing quickly, enabling hackers to easily perform phishing and malware attacks. They used a mixed method to survey victims and non-victims of cybercrime. In this research, using some devices to log on to the internet can pose a risk, and they suggest using policies when using the free internet. In [23], the authors conducted interviews with 35 experts and non-experts and some individual users. The results show the theoretical possibilities as a function of time and how they affect different security behaviours. In [24], the authors discuss social engineering and provide technical and non-technical solutions such as policy, education and training, Network Guidance, auditing, technical and physical measures.

In [25], the authors discussed the behaviour of individual decision styles that affect cybersecurity compliance. In [26], authors discussed human activities by performing assessment, quantification, and reporting to identify the risk, and they proposed to revise the standard BS ISO/IEC 27002:2013 to adapt it to the human factor. The researchers [27] discussed the relationship between cybersecurity risk-related behaviours in a business environment and Internet addiction in the UK by using an online questionnaire that included cybersecurity attitudes and analyzed the responses. Cybersecurity awareness, training, and educating users about cybersecurity and the questions need to be asked to find out the cybersecurity issues [28]. All the studies offered various training that is capable of reducing human vulnerabilities by measuring the current level and providing an appropriate solution to close the gap between the current awareness of the users and the target level to improve the security and reduce the vulnerabilities of the users.

3 Research Methodology

In this research, mixed data collection methods were included that contained qualitative interviews and quantitative online questionnaires to measure information security awareness [29]. The first phase (Fig. 1) is related to the policy and procedures in the organization, and the second phase (Fig. 2) is related to the users and the training plan. It is found that qualitative research focuses on hypothetical and theoretical data. Qualitative research provides insights and obtains a practical understanding of the problem, primarily based on observations, anticipations, and interpretations.

The description of inquiry objectives in qualitative research is to understand, describe, discover and make theoretical approaches and hypothetical information. Qualitative is flexible in structure. It can be modified according to the facts collected. Data collection in qualitative researcher is the main instrument for collecting and processing the data. This qualitative data can be obtained from various sources, such as conducting interviews with relevant people in the field, focus groups to analyze and explore the research topics based on their findings and observations. It is difficult to assess and ensure the validity and quality of qualitative research because it is so diverse. They also explained the ontology that deals with the questions. Also, epistemology deals with the theories of knowledge.

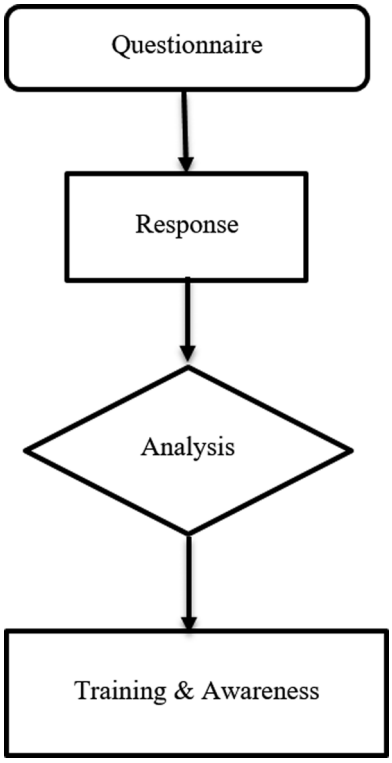

Figure 1: Step1(Phase I)

In this study, all users were categorized by gender and age and divided into three categories of information users (youth, adults, and seniors). As a research methodology, five (5) sequential steps were followed in data collection to ensure the accuracy of the data collected. The study's findings revealed the strengths and weaknesses among all the targeted users where more focus should be given to improving all the weaknesses.

The questionnaire prepared for this study attracted 333 participants as the participants answered all the questions. A questionnaire will be used to collect information about users related to the main topics of this research, namely passwords, social media, social engineering, and phishing. Also, the questionnaire provides information about what makes users become victims of phishing or social engineering. The participants were divided into three categories according to their age: Adolescents, Adults, and Older Information Users, as described below:

-Category 1: Adolescents (male & female) (18 years or younger).
-Category 2: Adults (male & female) (from 19 to 45 years old).
-Category 3: Seniors (male & female) (older than 45 years).

These categories were mainly selected to differentiate the level of awareness of passwords, social media, social engineering, and phishing among different generations, which will help the concerned organizations in the kingdom of Saudi Arabia to increase the level of awareness of information users and fill any gaps based on the identified weaknesses resulting from this survey. Five sequential steps were followed to collect the data effectively while distributing the questionnaires using the two research methods (qualitative interviews and quantitative questionnaires). The first step in this study focuses on the main human vulnerabilities such as passwords (weak passwords, obvious passwords, writing passwords on paper),

social engineering, and phishing, and then assesses the current environment and controls related to these cybersecurity vulnerabilities by creating a questionnaire. Based on the results, we will know the awareness level of users and answer these questions:

-How to avoid password issues?
-How do hackers use social engineering and phishing?
-How to protect users from social engineering and phishing?

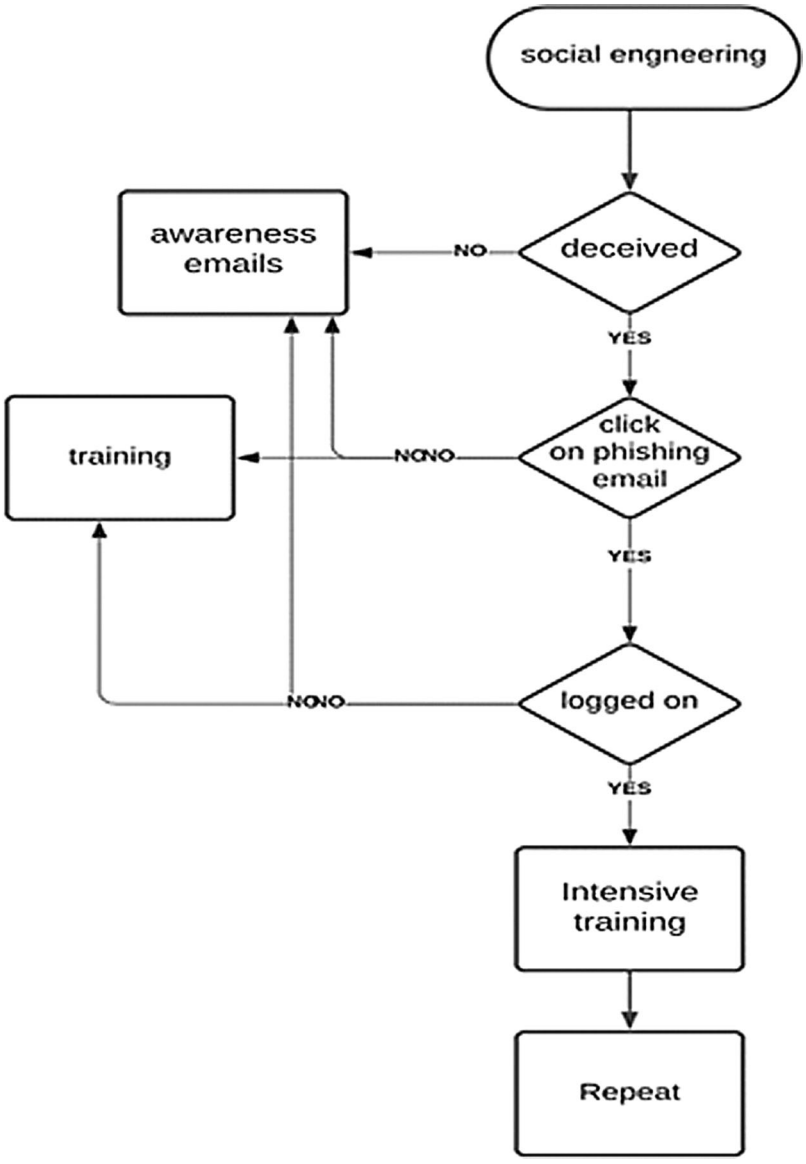

Figure 2: Step 2–Phase II

Usually, users use simple passwords like their children's names and birthdays or simple passwords that are easy to remember. The problem with this is that the password is easily cracked by hackers or social engineering. Therefore, the policy of using complex passwords should be done as follows:

-A complex password contains a capital letter, a small letter, a number, and a special character.
-8 or more characters.
-Expiration date for the password, for example, three months.
-Password history.

This policy may be good, but it has several weaknesses because changing the password every period with the application of complexity, length, and history can make it too difficult for users to remember, and that is why most users write their passwords on a piece of paper or choose a password that is associated with their life, such as their birthday or their children's name. Mainly, people use social media networks to perform data communication, where hackers perform social engineering attacks to get suspicious information and guess the password from social networks. Social engineering sometimes comes from unexpected parties, such as someone the employee meets in training or hiring websites. It is essential to educate users about social engineering and provide effective recommendations and security guidelines. According to Trend Micro, 94% of malware comes from phishing emails [30]. Hackers take advantage of people's greed to get them to click on the link in the phishing email by offering rewards or sweepstakes. Educate employees about phishing and spot it, and set strict email policies for the company to avoid it.

4 Result and Analysis

4.1 Awareness Related to Information and Cybersecurity-Related Questions

Participants were selected from all regions of Saudi Arabia, where 74% of men and 26% of women participated in this study. The age of the respondents, 59.8%, ranged from 19 to 45 years, 18.2% were younger than 16.5 years, while the remaining 19.7% were over 45 years old. 30.9% of the men were students, 60.6% were employed, while the remaining 8.4% did not fall under either employed or students. The response to social engineering, phishing emails, and passwords is tabulated in Tabs. 1–3. Fig. 3 shows the comparison of lack of top vulnerabilities related to humans in the cybersecurity awareness level between males and females.

Table 1: Response related to social engineering

Social engineering & Social media	Answers	Male		Female		Average	Total lack of awareness
Do you use your real name	Yes **P**	186	75%	64	74%	**75%**	**47%**
	No	63	25%	20	26%	26%	
Do you use your personal information on the password " birthday, father name, son name	Yes **P**	187	75%	59	70%	**73%**	
	No	62	25%	25	30%	28%	
Do you use your accurate information's in social apps " your birthday, city	Yes **P**	49	20%	10	12%	**17%**	
	No	87	35%	32	38%	37%	
	Sometime **P**	113	45%	42	50%	**48%**	
Did you share your information's with others through those apps	Yes **P**	29	12%	48	57%	**35%**	
	No	145	58%	29	8%	33%	
	Sometime **P**	75	30%	7	35%	**33%**	

Table 2: Response related to phishing emails

Phishing emails	Answers	Male		Female		Average	Total lack of awareness
Do you know what phishing means	Yes	97	39%	22	26%	33%	**33%**
	No **P**	124	50%	49	58%	**54%**	
	Maybe **P**	28	11%	13	16%	**14%**	
Do you use unknown websites to purchase	Yes **P**	26	10%	10	12%	**11%**	
	No	191	77%	68	81%	79%	
	Maybe **P**	32	13%	6	7%	**10%**	
Do you open any email that comes to your mailbox	Yes **P**	38	15%	15	18%	**16%**	
	No	154	62%	44	52%	57%	
	Sometime **P**	57	23%	25	30%	**48%**	
Did you sing-out from your email after finish	Yes	104	42%	15	19%	35%	
	No **P**	108	43%	49	64%	**33%**	
	Sometime **P**	37	15%	13	17%	**33%**	
Do you use anti-spam	Yes	75	30%	15	19%	25%	
	No **P**	174	70%	62	81%	**75%**	

Table 3: Response related to passwords

Password	Answers	Male		Female		Average	Total lack of awareness
Do you use a different password for your accounts	Yes	174	70%	53	69%	70%	**38%**
	No **P**	75	30%	24	31%	**30%**	
Do you change your password frequently?	Yes	49	20%	16	21%	**21%**	
	No **P**	100	40%	30	39%	39%	
	Sometime **P**	100	40%	31	40%	**40%**	
Do you use two-factor authentications while unlocking the device or the programs?	Yes	149	60%	39	51%	56%	
	No **P**	100	40%	38	49%	**44%**	
Do you use easy or complicated password	Easy **P**	84	34%	39	51%	43%	
	Complicated	165	66%	38	49%	**57%**	

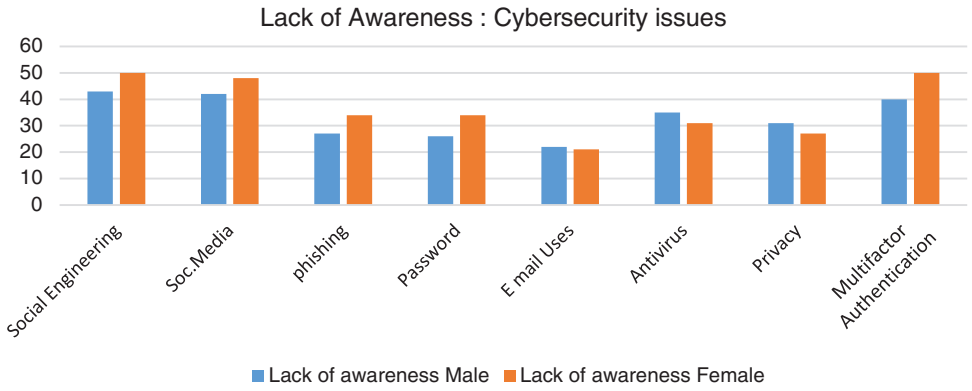

Figure 3: Lack of awareness level

The overall results showed that the level of awareness related to cybersecurity and information security (61%) had been achieved, which is an alarmingly low level that requires it to be increased to the maximum extent. The results show that the awareness of social engineering (53%), social media (55%), phishing (70%), passwords (70%), email usage (78%), antivirus (67%), and data protection (71%) is high.

4.2 Hypothesis Testing

Hypothesis testing is used to make statistical decisions using experimental data and validating the test results [31,32]. The important steps in hypothesis testing are establishing the research hypothesis as a null and alternative hypothesis, collecting data in a way that will be used to test the hypothesis, conducting an appropriate statistical test, and deciding whether the null hypothesis is supported or refuted. The purpose of a hypothesis test is to see if the null hypothesis (there is no difference, no effect) can be rejected or confirmed. If the null hypothesis is rejected, then the research hypothesis can be accepted. If the null hypothesis is accepted, then the research hypothesis is rejected.

To test the validity of the data in this study, our hypothesis is:

- Null hypothesis: there is no relationship between cybersecurity analysis in men and women.
- Alternative hypothesis: there is a relationship between cybersecurity analysis in men and women.

The hypothesis is tested using the chi-square test. Tab. 4 shows the relationship between gender and whether they check the email or the sender's name. It can be seen that the majority of the respondents answered in the affirmative to the cybersecurity question and checked the sender's name and email address. Without the percentages in the cross-tabulation section, we rely on the chi-square to determine the existence of the relationship. The interest in the chi-square test, which has a p-value of 0.515, is greater than 0.05. Here we cannot reject the null hypothesis (Tab. 4). We conclude that there is no relationship between how the male and female gender deal with cybersecurity by checking the names and email addresses of those who send them an email.

Tab. 5 depicts the relationship between gender and whether or not they sign out of email after using it. The interest in the chi-square test has a p-value of 0.002, which is less than 0.05. Here we reject the null hypothesis.

Table 4: The relationship between gender and whether they check the email and the sender's name

		Do you check the sender's name and email address			Total
		Sometimes	No	Yes	
Gender	Female	16	20	41	77
	Male	50	44	155	249
	Prefer not to say	1	2	4	7
Total		67	66	200	333
Chi-square tests					
	Value	Df	Asymptotic significance (2-sided)		
Pearson chi-square	3.261	4	.515		
Likelihood ratio	3.153	4	.533		
N of valid cases	333				

Table 5: The relationship between gender and whether they sign-out from email after use

		Do you share your email address with everyone?		Total
		No	Yes	
Gender	Female	59	18	77
	Male	181	68	249
	Prefer not to say	5	2	7
Total		245	88	333
Chi-square tests				
	Value	Df	Asymptotic significance (2-sided)	
Pearson chi-square	.485[a]	2	.785	
Likelihood ratio	.494	2	.781	
N of valid cases	333			

Note: [a]The key result in the Chi-Square Tests is the Pearson Chi-Square. The value of the test statistic is .485, 6.027 and 8. 811.The footnote (a) for this statistic pertains to the expected cell count assumption (i.e., expected cell counts are all greater than 0.05): no cells had an expected count less than 0.05, so this assumption was met.

Tab. 6 shows the relationship between gender and whether they use two-factor authentication while unlocking their devices. The interest in the chi-square test has a p-value of 0.277, which is greater than 0.05. Here we fail to reject the null hypothesis.

Tab. 7 shows the relationship between gender and whether they use easy or complicated passwords. The interest in the chi-square test has a p-value of 0.012, which is less than 0.05. Here we reject the null hypothesis.

Table 6: The relationship between gender and whether they use two-factor authentication while

		Do you know what does phishing email means?			Total
		Maybe	No	Yes	
Gender	Female	11	45	21	77
	Male	28	124	97	249
	Prefer not to say	2	4	1	7
Total		41	173	119	333
Chi-square tests					
	Value	Df	Asymptotic significance (2-sided)		
Pearson chi-square	6.027[a]	4	.197		
Likelihood ratio	5.973	4	.201		
N of valid cases	333				

Note: [a]The key result in the Chi-Square Tests is the Pearson Chi-Square. The value of the test statistic is .485, 6.027 and 8. 811.The footnote (a) for this statistic pertains to the expected cell count assumption (i.e., expected cell counts are all greater than 0.05): no cells had an expected count less than 0.05, so this assumption was met.

Table 7: The relationship between gender and whether they use easy or complicated passwords

		Do you use easy or complicated passwords?		Total
		Easy	Complicated	
Gender	Female	39	38	77
	Male	84	165	249
	Prefer not to say -	1	6	7
Total		124	209	333
Chi-square tests				
	Value	Df	Asymptotic significance (2-sided)	
Pearson chi-square	8.811[a]	2	.012	
Likelihood ratio	8.872	2	.012	
N of valid cases	333			

Note: [a]The key result in the Chi-Square Tests is the Pearson Chi-Square. The value of the test statistic is .485, 6.027 and 8. 811.The footnote (a) for this statistic pertains to the expected cell count assumption (i.e., expected cell counts are all greater than 0.05): no cells had an expected count less than 0.05, so this assumption was met.

Tabs. 4–7 show a correlation between cybersecurity analysis among men and women, as indicated by the survey data presented in Tabs. 1–3. The test results show that there is no relationship between cybersecurity analysis between men and women. The study was analyzed using the chi-square procedure, which helps establish relationships between variables by examining the nature of p-values. If the p-value is less than 0.05, the null hypothesis is rejected, while if the p-value is greater than 0.05, it is accepted. In the above cases, the p-value is greater than 0.05, which leads us not to reject the null hypothesis, i.e., how males deal with cybersecurity is different from how females deal with it.

The use of two-factor authentication to unlock devices is significantly different between the two genders, implying that one gender is more likely to use two-factor authentication than the other. The uses of anti-spam features in emails are also significantly different between genders. This is indicated by the p-value being greater than 0.05, suggesting the acceptance of the null hypothesis. The importance of phishing emails is also significantly different between genders, with the p-value greater than 0.05. However, some factors show a strong relationship between the two genders. The uses of complicated or simple passwords related to genders. This was shown by a relationship with a p-value of less than 0.05. Thus, the null hypothesis is rejected and the conclusion is that there is a relationship between the use of cybersecurity by males and females. Another variable that showed a strong relationship was the issue of unsubscribing from emails after finishing work. It also had a p-value of less than 0.05. Users tend to use their personal information on social media, making them victims of phishing and social engineering and making it easier for hackers to find out their passwords.

5 Conclusions

There are different security vulnerabilities and security flaws in applications that interact over the internet. The overall results highlighted that the level of awareness related to cybersecurity issues (61%) had been achieved, which is an alarmingly low level that requires it to be increased to the maximum extent. The results show the lack of awareness of social engineering (37%), social media (35%), phishing (30%), passwords (30%), email usage (22%), antivirus (33%), and data protection (29%). This study found that the sample has a high lack of awareness about the top three vulnerabilities related to cybersecurity, and the major problem needs to be addressed and reduced through proper awareness and training. The study was analyzed using chi-square, which helps identify relationships between variables by examining the nature of p-values. If the p-value is less than 0.05, the null hypothesis is rejected, while if the p-value is greater than 0.05, it is accepted. From the above examples, the p-value is greater than 0.05, which leads us not to reject the null hypothesis.

Therefore, the way males deal with cybersecurity is different from the way females do the same. The use of two-factor authentication to unlock devices differs significantly in both genders, implying that one gender uses two-factor authentication more than the other. The use of anti-spam features in emails is also significantly different between genders. This is indicated by the p-value being greater than 0.05, suggesting the acceptance of the null hypothesis. The importance of phishing emails is also significantly different between genders, with the p-value also greater than 0.05. Thus, the null hypothesis is rejected and the conclusion is that there is a relationship between the use of cybersecurity by males and females. Another variable that showed a strong relationship was the issue of unsubscribing from emails after finishing work.

Hacking personal details of the companies and users can be done by the attackers using malicious codes and cyber-attacks, for which it is important to secure internal networks and communication channels. The human factor is the primary cause of security, and companies are not focusing on insider risks due to which they can suffer from the cyber-attacks and due to lack of awareness about cyber-security employees are not able to defend against cyber-threats and vulnerabilities. to encouraging compensation that helps the organization educate users. This step takes at least 9 to 10 months between phishing, gathering information, and creating appropriate training paths. Future work is required to conduct other comprehensive surveys among educational, governmental, medical, and industrial institutions to measure information security awareness among their employees and provide various statistical results to help them identify and address all weaknesses.

Acknowledgement: The authors sincerely acknowledge the support from Majmaah University, Saudi Arabia, for this research.

Funding Statement: The authors would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project Number No -R-14xx-4x.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Wang, F. D. Maio and E. Zio, "Considering the human operator cognitive process for the interpretation of diagnostic outcomes related to component failures and cybersecurity attacks," *Reliability Engineering & System Safety*, vol. 202, pp. 1–14, 2020.

[2] T. A. Hemphill and P. Longstreet, "Financial data breaches in the US retail economy: Restoring confidence in information technology security standards," *Technology in Society*, vol. 44, pp. 30–38, 2016.

[3] A. Corallo, M. Lazoi and M. Lezzi, "Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts," *Computers in Industry*, vol. 114, pp. 1–15, 2020.

[4] S. Milivojevic and E. M. Radulski "The 'future internet' and crime: Towards a criminology of the internet of things," *Current Issues in Criminal Justice*, vol. 32, no. 2, pp. 193–207, 2020.

[5] Vision 2030 KSA, 2016. [Online]. Available: https://www.vision2030.gov.sa/.

[6] Absher KSA, 2012. [Online]. Available: Absherhttps://www.absher.sa.

[7] I. Arend, A. Shabtai, T. Idan, R. Keinan and Y. B. Meyer, "Passive-and not active-risk tendencies predict cyber security behavior," *Computers & Security*, vol. 97, pp. 1–7, 2020.

[8] M. Grobler, M. A. P. Chamikara, J. Abbott, J. J. Jeong, S. Nepal *et al.*, "The importance of social identity on password formulations," in *Personal and Ubiquitous Computing*, vol. 24, pp. 1–15, 2020.

[9] D. Upadhyay and S. Sampalli, "SCADA (Supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations," *Computers & Security*, vol. 89, pp. 1–18, 2020.

[10] M. H. Uddin, M. H. Ali and M. K. Hassan, "Cybersecurity hazards and financial system vulnerability: A synthesis of literature," *Risk Management*, vol. 22, no. 4, pp. 239–309, 2020.

[11] H. S. Lallie, L. A. Shepherd, J. R. Nurse, A. Erola, G. Epiphaniou *et al.*, "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers & Security*, vol. 105, pp. 1–20, 2021.

[12] M. Jartelius, "The 2020 "Data breach investigations report–a CSO's perspective," *Network Security*, vol. 2020, no. 7, pp. 9–12, 2020.

[13] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, pp. 1–14, 2020.

[14] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future Internet*, vol. 12, no. 10, pp. 1–39, 2020.

[15] S. Mishra, S. K. Sharma and M. A. Alowaidi, "Analysis of security issues of cloud-based web applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, pp. 1–12, 2020.

[16] K. Krombholz, H. Hobel, M. Huber and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015.

[17] N. Y. Conteh and P. J. Schmick, "Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks," *International Journal of Advanced Computer Research*, vol. 6, no. 23, pp. 31, 2016.

[18] B. B. Gupta, N. A. Arachchilage and K. E. Psannis, "Defending against phishing attacks: Taxonomy of methods, current issues and future directions, *Telecommunication Systems*, vol. 67, no. 2, pp. 247–267, 2018.

[19] S. R. Curtis, P. Rajivan, D. N. Jones and C. Gonzalez, "Phishing attempts among the dark triad: Patterns of attack and vulnerability," *Computers in Human Behavior*, vol. 87, pp. 174–182, 2018.

[20] D. Rashkovski, V. Naumovski and G. Naumovski, "Cybercrime tendencies and legislation in the Republic of Macedonia," *European Journal on Criminal Policy and Research*, vol. 22, no. 1, pp. 127–151, 2016.

[21] M. Yıldırım and I. Mackie, "Encouraging users to improve password security and memorability, *International Journal of Information Security*, vol. 18, no. 6, pp. 741–759, 2019.

[22] N. Akdemir and C. J. Lawless, "Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach," *Internet Research*, vol. 30, no. 6, pp. 1665–1687, 2020.

[23] N. H. Chowdhury, M. T. Adam and T. Teubner, "Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures," *Computers & Security*, vol. 97, pp. 101931, 2020.

[24] L. Hadlington, "The "human factor" in cybersecurity: Exploring the accidental insider," in *Research Anthology on Artificial Intelligence Applications in Security*, Edition 1. 701 E. Chocolate Ave. Hershey, PA 17033, USA: IGI, Chapter 87., Page No. 1960–-1977, 2021. [Online]. https://www.igi-global.com/chapter/the-human-factor-in-cybersecurity/270680

[25] C. Donalds and K. M. O. Bryson, "Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents," *International Journal of Information Management*, vol. 51, pp. 1–16, 2020.

[26] M. Evans, L. A. Maglaras, Y. He and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Security and Communication Networks*, vol. 9, no. 17, pp. 4667–4679, 2016.

[27] L. Hadlington, "Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, vol. 3, no. 7, pp. 1–18, 2017.

[28] H. Alqahtani and M. K. Thorne, "Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR)," *Information*, vol. 11, no. 2, pp. 121, 2020.

[29] X. Cheng, T. Hou and J. Mou, "Investigating perceived risks and benefits of information privacy disclosure in IT-enabled ride-sharing," in *Information & Management*, vol. 58, no. 7, pp. 1–15, 2021.

[30] J. Zhao, Q. Yan, J. Li, M. Shao, Z. He *et al.*, "TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data," *Computers & Security*, vol. 95, pp. 1–14, 2020.

[31] S. Mishra and M. Singh, "A conceptual framework for effective M-governance," *Journal of Engineering Science and Technology*, vol. 14, no. 6, pp. 3514–3535, 2019.

[32] A. Mpatziakas, S. Papadopoulos, A. Drosou and D. Tzovaras, "A hypothesis testing tool for the comparison of different cyber-security mitigation strategies in IoT," in *2021 IEEE Int. IOT, Electronics and Mechatronics Conf. (IEMTRONICS)*, Toronto, ON, Canada, pp. 1–7, 2021.