Knowing the Level of Information Security Awareness in the Usage of Social Media Among Female Secondary School Students in Eastern Makkah Al-Mukarramah- Saudi Arabia

Magdah Ezat Gharieb

Faculty of Arts and Humanities, King Abdulaziz University,
Jeddah, Saudi Arabia omary57@hotmail.com
E-mail: mgharib@kau.edu.sa

Abstract

This study aims at knowing both the level of information security awareness in the use of social media among female secondary school students in Makkah Al-Mukarramah, and the procedures that students follow when exposed to hacking or other security problems. The study relied on the descriptive survey approach. The results showed a high percentage of social media use among the study sample, and the most used applications by the students are snapchat and Instagram applications successively. In fact, 48% of the study sample have awareness of information security, the majority of the students memorize the password in the devices, most of them do not change them, and they have knowledge of fake gates and social engineering. However, their knowledge of electronic hacking is weak, and students do not share passwords with anyone at a rate of 67%. At the same time, they do not update passwords. Moreover, most of the procedures followed by students when exposed to theft and hacking is to change the e-mail data and the password, and the results varied apart from that, which reflects the weak awareness of the students and the weakness of procedures related to information security. The study recommends the necessity to raise awareness and education of the importance of information security and safety, especially in light of what the world faces from data electronic attacks and hackings of electronic applications.

Keywords:
information security, cybercrime, social networks, high school students, electronic applications

1. Introduction

"People think information security is about technology, but it's really about educating people, and about 90% of all breaches are human," says Patricia Patria, vice president of information technology at Baker College. In this context, a staff member at a major research university reported that about 100,000 people daily access the university network using two or three devices, and 75% of incoming emails are spam, and there are more than a thousand attempts to hack the university campus network every minute.

Modern societies have become captive to methods of deception and misinformation because of the development of computers and information technology. This development coincided with the flow of correct and misleading information at the same time, focused on the minds of users through social networks, and the security of information and data on networks became extremely important. Henceforth, information security is of great interest in all countries and in every organization regardless to its size. Moreover, maintaining data integrity and privacy is a task for which every official in any sector bears responsibility. Information security is not limited to organizations, but to individuals as well. Each person bears all responsibility in preserving his data from loss, theft or violation of privacy.

However, how does an individual protect his internet data from intended and unintended threats? Do individuals have sufficient awareness of the importance of information security? Moreover, how do students in educational institutions face these risks and threats in an era when the internet is at hand all the time and available to all age groups? In addition, and since social networking applications are synchronized with the developments in the use of means of communication and the Internet that share information and data between individual users, which increases the exchange of personal information, preserves it, and makes it available more quickly and easily in circulation, a report issued by the United Nations Development Program in 1999 titled " Globalization with a Human Face" asserted that although globalization offers tremendous opportunities for human progress in all fields due to the rapid transfer of information and knowledge and the free movement of goods and services, it poses, in turn, risks to human security in the twenty-first century. Security means protecting a person, organization or country against threats and crimes from foreign countries. Information security means the totality of measures to be taken by the concerned agencies to maintain the confidentiality of information and ensure that it reaches only the concerned authorities in a timely manner, and ensures that it does not fall into the hands of enemies or friends alike. Thus, the security of information imposed itself through the raising care of securing and protecting the information used over the Internet from risks and hacking, and storing it to avoid tamper or loss. It has become necessary to spread awareness of information security when using social media, which is fraught with many risks due to its frequent use and the circulation of various information through it, including personal data. Besides, social media applications are the language of the current era and of the electronic communication between individuals. This communication takes several forms

including sharing photos, written messages, videos and many expressive formulas provided by the used applications. Henceforth, each person is responsible for the information he shares. Indeed, each application has its own policy and the user's lack of awareness of this policy makes him an easy target for hackers and impersonators to gain access to his information, blackmail them, steal them, or just threaten them for the purpose of entertainment, gain fame, financial extortion and other reasons as mentioned by Al-Ghathbar (2011). All this requires educating all members of society, especially the young category, on ways to preserve information and raise awareness of information security and warning them from forms of hacking, impersonators and other types of cybercrime, as they are one of the most targeted categories by hackers, as mentioned by Abdul Majid (2018). In addition, this category represents the basis of future societies and contributes to their development and progress. Thus, the correct founding of this generation, keeping them out of dangers, and making them properly aware of these dangers leads to building an impenetrable fortress for the security of the state against the attacks of intruders in the future (Al-Omari, 2004).

2. The Research Problem

The language of electronic applications has become the language of young people who have been associated with them as a result of the use of mobile phones and laptops and the multiplicity of social media and its forms ranging from making images, words and videos available using private messages and personal data of the users. The awareness of the importance of information security will have a positive and effective impact in instilling the basics of information security in the minds of students, as educational institutions contain the young generation who can understand these basics and apply them in their practical and future lives, especially in light of the electronic attack on data and websites hacking. Female students often practice their activities through social networking sites such as Facebook, Twitter, Instagram, Snapchat and e-mail programs. In fact, these programs are fertile ground for such hackers who target the category of female students to lure them and set ambushes for them to get what they want from them, such as sending fake links to them to download malicious programs or buying from unreal fake websites.

Since the young groups are the most social media using groups as mentioned by Al-Jathami (2017) on the one hand, and being one of the most exposed groups to electronic risks on the other hand (Abdul Majeed, 2018), it is necessary to know the extent to which the young category is familiar with information security when using the social media, specifically female secondary school students, whose ages range between 15 and 18 years. Accordingly, the idea of the study came to examine the level of awareness of

information security and what are the precautionary measures that this category uses to preserve their personal information and not to be vulnerable to hacking or cybercrimes. The problem of the study can be expressed by the following question:

What is the level of awareness of information security in the use of social media among female secondary school students in Makkah? And, what are the procedures that the students follow in case their accounts are hacked or they are exposed to security problems?

3. The Related Works

There were many previous studies related to information security. The selected studies are those close to the subject of the current study, which are summarized in the following studies, from the most recent to the oldest:

Al-Zubaidi's study (2021) entitled "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia" focused on measuring the current level of cyber-security awareness in Saudi Arabia, in terms of cybersecurity practices, level of awareness, and incident reporting, based on an online questionnaire of 1230 participants. The results of the study showed that 31.7% used public Wi-Fi to access the Internet, 51% used their personal information to create their passwords, 32.5% had no idea about phishing attacks, 21.7% were a victim of cybercrime while only 29.2% among them reported the crime, which reflects their levels of consciousness. It turns out that to reduce the rapidly increasing number of cyber-attacks, the level of cybersecurity awareness of ordinary people should be raised significantly. It is important to reinforce this knowledge through specially designed programs that could be created to further educate people, in order to reduce their probabilities of becoming a victim of such attacks.

The study of (Al-Moaiqel, 2018) entitled "the educational security requirements for society in social media" came to reveal these requirements in the intellectual, social and health fields and to follow up the statistically significant differences in the answers according to the following variables (faculty members, general education teachers, and guardians). The study used the descriptive survey method on a stratified random sample of 537 from the study population in the city of Riyadh. The questionnaire was used as a tool for the study. The study reached many results namely that the sample members agreed largely on the requirements of achieving educational security in the use of social media in its three fields, In addition to relying on the religious side in promoting self-censorship among individuals. The study recommended the need to raise awareness of the harms of addiction to interaction in social media and to clarify the harms of that in all fields.

The study of Al-Jathami (2017) entitled "the level of awareness of information security issues among secondary school students in government schools in Riyadh" aimed at

knowing the level of awareness of security issues. The number of samples from female students reached 429. The study used the descriptive survey method and the questionnaire as its study tool. It reached a set of results including the fact that the large percentage of the female students, amounting to 41%, was very familiar with information security issues. The study also showed that 85% of the students were aware of the need to use passwords on their devices to protect them from hacks. The researcher recommended the need to raise the level of awareness of information security issues in a general way focusing in particular on the category of female high school students, in addition to the need to develop effective training awareness programs on information security issues.

The study of Omar (2015) entitled "The importance of information security in Combating Cybercrime: A Case Study of the Sudanese Center for Information Security", aimed at introducing information security and spreading a culture of information protection and awareness of the risks and challenges it faces. The researcher addressed two aspects. The first is related to information security and its related issues. The second is a description of the experience of the Sudanese Center for Information Security and an evaluation of its tasks, duties and services. The study relied on the descriptive approach and the case study. It reached several results namely the need to pay attention to the for information security education both for individuals and society about the importance and necessity of establishing centers similar to the Sudanese Center for Information Security.

4. Study Community and Research Method

Study Community: The study community consisted of female high school students in eastern Makkah Al-Mukarramah whose total number reached 6206 in 2019, as stated by the Education Department statistics on its website. East Makkah schools consist of five government schools whose names are as follows:

1- 17th Secondary School
2- 33rd Secondary School
3- 41st Secondary School
4- 45th Secondary School
5- 56th Secondary School

Study Methodology: The descriptive survey method was used in the study, as it is one of the most appropriate methods for studying social phenomena.

Data collection tool and measuring the validity of the tool: The researcher used the online questionnaire as a tool for the study. The questionnaire was distributed to the east of Makkah schools by the Education Department after approving the conduct of the study. Only 85 questionnaires were filled out. They were previously refereed by two

faculty members at King Abdul-Aziz University. the questionnaire was also tested on a group of 56 high school students to measure the clarity of the questionnaire, and it was modified according to the notes suggested by the students.

Application framework:
The following is a review of the results that were reached after obtaining the data back from the study sample. Some illustrations were used to present the results:

1- Social media usage rate:
The percentage of social media use was very high among female students, as it represented 98% of the study sample, equivalent to 83 students.
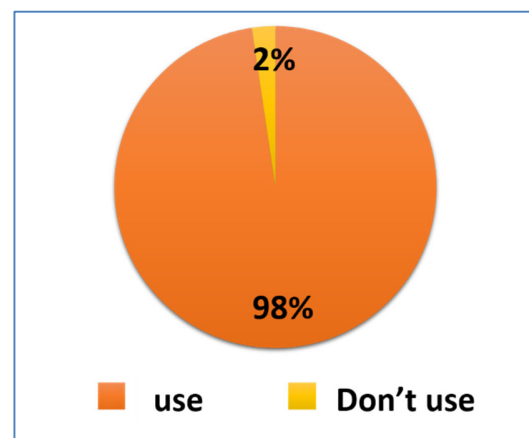

Figure 1: Social media usage rate

2- Types of the used applications:
The results show through the bar chart that the most used application by female students is the snapchat application by 81%, followed by the Instagram application by 80% of female students, and then email with only 18%. On the other hand, the statistics indicated a weak use of the Facebook application.
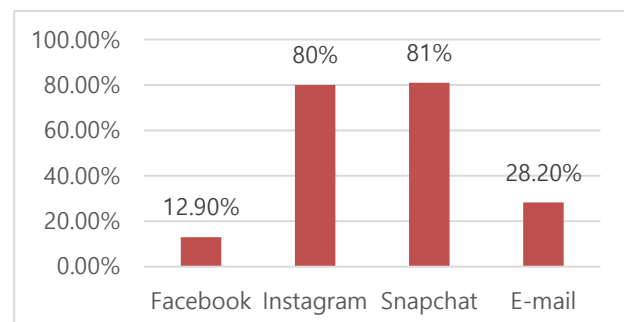

Figure 2: Types of the used applications

3- Types of information exchanged on social media:

Figure (3) shows that the majority of female students exchange personal photos on social media in the snapchat application, with an average rate of 58%, which is one of the most used applications for publishing personal photos, while the rest of the applications are used to publish photos in a very weak percentage, ranging from 2% to 13%. The results also show the students' interest in publishing public photos in a large way in social media as students use the Instagram application by 60%, which indicates the majority of use, followed by the snapchat application at a medium rate. Finally, the use of public photos in face book and e-mail, which ranges between weak and very weak, and students use advertising and trade in applications at very low rates.
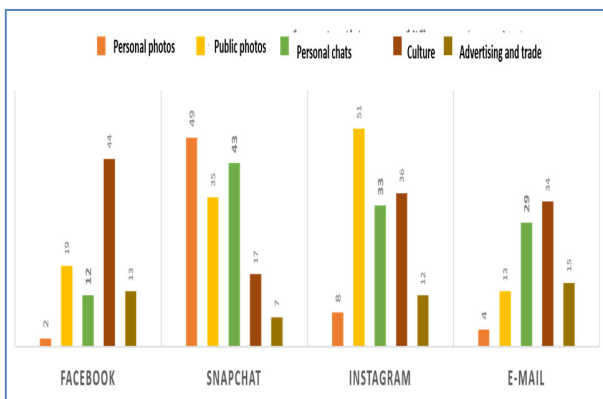
Figure 3: Types of information exchanged in social media

4- Knowledge of the term "information security":

The results of the study in the pie chart below show that the percentage of female students' awareness of information security reaches 40%. On the other hand, the percentage of female students who are not aware of information security is 12%, while the female students who are not sure of the term of information security represent 48%. This percentage shows the students' lack of knowledge of the general concept of protecting themselves when using these applications.
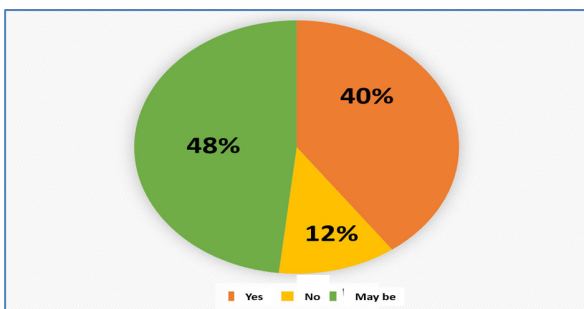

Figure 4: Familiarity with the term "information security"

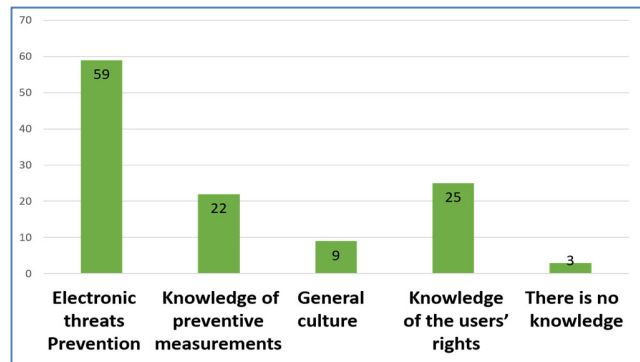### 5- The importance of information security:

Figure 5: The importance of information security

The answers to this question confirm the conclusion reached from the question preceding it. Although most of the students are not aware of the term of information security, the results indicated how important information security is from the point of view of the students, who believe by a large percentage that information security is important for the prevention of electronic dangers by 69%. The ratio converges in relation to knowledge of preventive measures and the users' rights in a similar way to the importance of information security from the point of view of the female students. Some female students considered it as just a general culture with a very weak rate of up to 10%. While only three of the female students are not aware of the importance of information security. This disparity requires preparing and presenting a course to educate and make students aware about this concept and the implications of using different applications.

6- Types of cybercrimes:

The results in Figure (6) showed that the female students' knowledge of the currently prevalent electronic crimes is intermediate between social engineering and the fake portal. As for hacks, the percentage of knowledge about them is very low. Four of the students nominated other crimes that are among the currently recognized electronic crimes such as phishing, espionage and impersonation, which is a type of social engineering. Another student mentioned the term false promotion as a type of cybercrime. On the other hand, some female students stated that they did not know any of the types of cybercrime mentioned in the questionnaire at a rate of 8%.
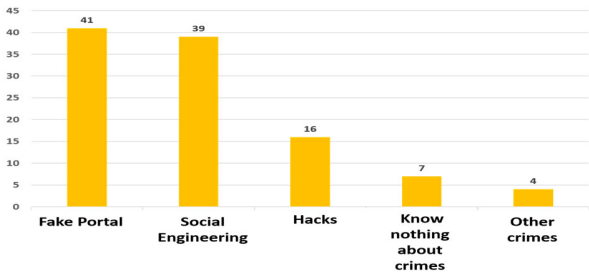
Figure 6: Types of cybercrime

7- Are passwords saved in devices?

When asked about one of the preventive measures in the use of applications when dealing with saving passwords in the devices, the female students reported that the majority of them save the passwords in the devices automatically, with a percentage of up to 59%, and their number is 50 students out of 85 students.
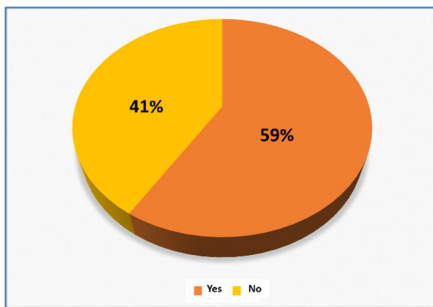

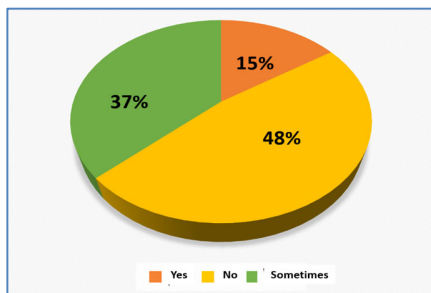**Figure 7: Passwords Auto save**

8- Change passwords regularly:

Figure 8: Changing Passwords periodically

The results showed that only 15% of the students who are keen to change passwords for regularly used applications, while the study shows that 48% do not change passwords regularly, and many female students mediated by 37% in the average password change rate. This behavior confirms

the extent to which the students need to be aware of the importance of changing passwords.

9- Sharing passwords:

Figure (9) showed that the percentage of female students who do not share passwords with anyone is 67%, as their number reaches 65 students, which is a high percentage that reflects the students' keenness to protect their information. The percentage varies between female students who share accounts passwords and those who believe that they may share passwords with someone at very weak rates.
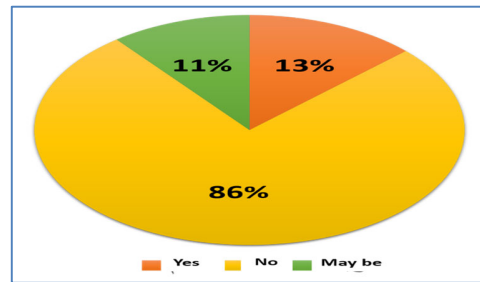

Figure 9: Sharing passwords

10- Type of used symbols:

Figure (10) shows that the percentage of female students who use letters and numbers is the highest, as the percentage reaches 61%, followed by numbers, letters and symbols at a lower percentage, and finally the rest of the types of symbols with low percentages.
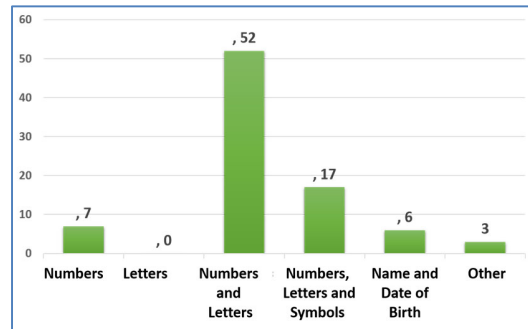

Figure 10: Type of symbols used

11- Update data in social media:

Figure (11) shows that the majority of female students do not update data in social media applications with a high rate of 66%, while female students who do update data reached 34%.
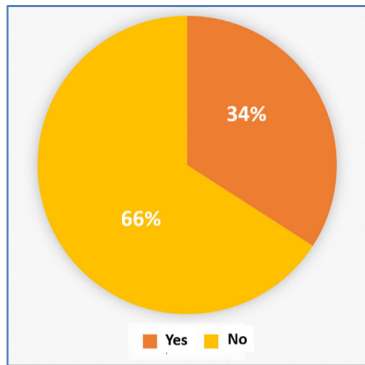
Figure 11: Periodical data update

12. Modification of privacy and security data:

Figure (12) shows that the rates are equal in both answers. The number of female students who modify privacy settings is 53%, and their number is 45. As for the female students who are not keen to modify privacy and security data, their number is 40, at a rate of 47%.
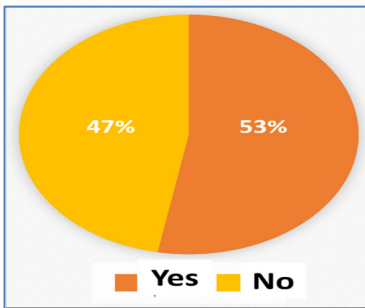

Figure 12: Modifying the privacy data

13- Accessibility of the location by applications:

Chart (13) indicates that 50% of the female students allow the geographical location when using the snapchat application. The researcher has assumed this percentage by referring to the number of female students who use the application in Figure (5). The percentage of availability varies in other applications very weakly, but most of the students are keen to close the sharing of the site through the applications, except for the snapchat application, as shown in Figure (16), and the study shows that some students provide the service only when needed, by varying rates.
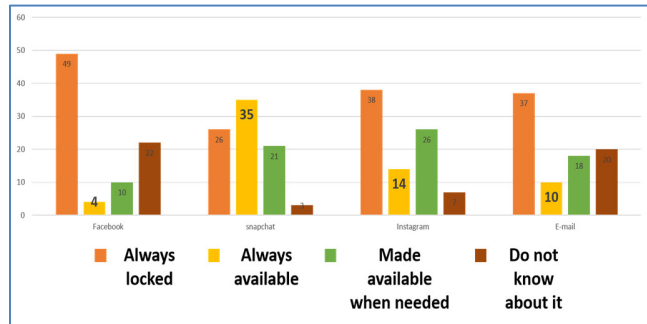

Figure 13: Location Accessibility

14- Protection programs on devices:

When asked about protection programs on devices to ensure the protection of information, 52% of the students agreed that their devices contain protection programs, while 29% were not sure that their devices contain protection programs, while 19 % of female students confirmed that their devices do not have security software.
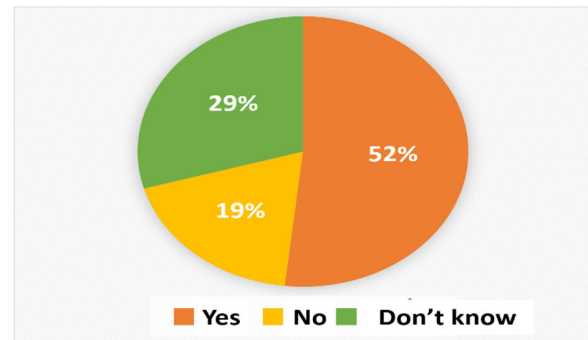

Figure 14: Protection software on devices

15- Activate 2-Step Verification in applications:

Activating the two-step verification is one of the important steps to protect the users' information that was provided by the developers of the applications. The results show that the rate of activation of this procedure is 55% by female students when using the applications. This rate constitutes an average use rate for this procedure.
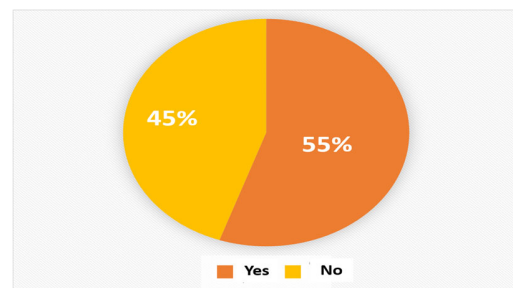

Figure 15: Activating 2-Step Verification

16- Permanently Deleting messages from the account or unwanted e-mails:

igure (16) shows that only 35% of the female students were keen to permanently delete e-mails from the server, and the percentage that varies from care to negligence amounted to 40%, while the study indicated that 25% of the students do not delete messages permanently, and it was the lowest category.
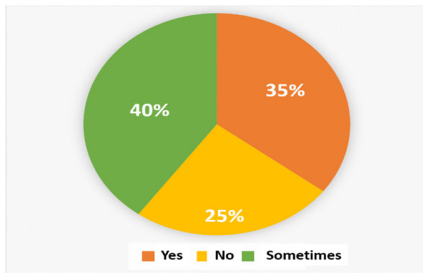

Figure 16: Deleting unwanted messages from the mail

17- Verifying the receiving account:

The results showed that the students verify the receiving account before publishing, and the answers of the majority approved with a rate of 59%, while the hesitation responses of some sample members ranged from sometimes checking by 20% of the receiving account, and the rest neglected this verification by up to 21%.
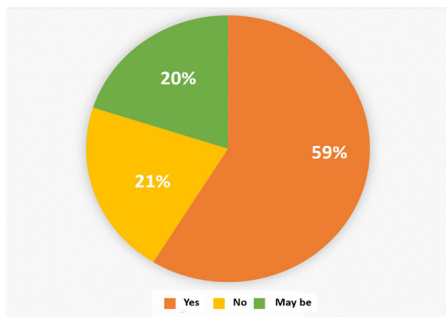

Figure 17: Verifying the receiving account

18- How to verify the receiving account of the transmitted information:

The results in Figure (18) showed that most of the female students rely on ensuring the security of the site when sending data to the application or the site. However, the percentage is equal for the female students who talk to the receiver when using the application to transfer information or verify the link of the two sites. The students do not use the authentication words between them except in very weak percentages, and the results showed that the female students who do not check the receiving account constitute a weak percentage of the total number of female students.
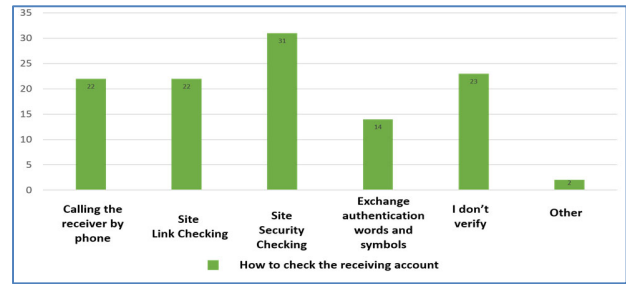

Figure 18: How to verify the receiving account

19- Protection measures when exposed to theft:

Figure (19) indicates that the most frequently followed procedures by female students when exposed to theft and hacking is to change the e-mail data and the password at a very high rate. Apart from this, the results varied, reflecting the weak awareness of the students and the weakness of the procedures related to information security in this question.

Figure 19: Measurements when exposed to theft

Results:

The following table was used to measure the level of awareness of information security, the measurements used for protection or when exposed to hacks, depending on the sample size that responded to the questionnaire.

Table 1: Study Results Ranking

Level	Female students' number
Very low	0 – 16
Low	17 – 33
Medium	34 – 50
High	51 – 67
Very high	68 - 85

5. Conclusion, Recommendation & Suggestion

The study reached several results, including: The results indicated that there was no clear picture of information security in the minds of the female students. The rate of using social media applications is very high, as it constituted 98% of the study sample. It was also found that there is a lack of female students' awareness of the term of "information security", as the largest percentage varied between female students who did not have a background about this term and female students who were not confident of knowing this term. The results showed that the students are aware of the importance of information security and awareness of cybercrime. The actions taken by the students to protect their information varied, which reflects the weak awareness of information security procedures. When the account is stolen, most of the students depend on changing the e-mail data and the password, and this procedure is weak, as most of the hackers are keen first to change this data after hacking.

Recommendations:

1. Providing a course that provides the necessary skills to spread awareness of information security.
2. Providing awareness-training courses in schools by the Education Department on information security in the use of social media for female teachers, students and parents.
3. Periodically publishing the statistics related to information crimes through social media by the competent authorities.
4. Direction towards the use of strong passwords with symbols, letters and numbers and the adoption of the study of Al-Salloum (2013), which depends in setting passwords on the geographical coordinates of a specific area chosen by the user, in addition to activating the security features of the applications used.
5. Permanent guidance to parents and teachers, and their making aware of information security and the risks arising from wrong use and supervision of children.

Suggestions:

1. Carrying out a proposed study to clarify the rights and duties in the use and dissemination of information through social media.
2. Comparing the results of the study with the level of awareness of information security among female students in different cities in the Kingdom of Saudi Arabia.

References

[1] Alzubaidi,Abduaziz(2021)."Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia". Heliyon ,Vol. 7, Issue 1. Available from: https://www.sciencedirect.com/science/article/pii/S2352340921002493

[2] Ahmed, Ashraf (2014). Information Security Strategy. Egypt: Arab Thought House.

[3] Al-Khatami, Maha Bint Dakhil Allah (2017). The level of awareness of information security issues among secondary school students in government schools in Riyadh. Journal of Humanities and Social Sciences: Imam Muhammad bin Saud Islamic University - Deanship of Scientific Research, v. 47, 355-400. Retrieved from http://search.mandumah.com/Record/852688

[4] Al-Arabi, Ahmed Obada (2013). International standards for information security policies: An analytical study of the standards of the International Organization for Standardization (ISO/IEC 27002) and the extent of their application in Arab universities. Journal of King Fahd National Library: King Fahd National Library, Vol. 19, Vol. 2.- pp. 157-210 Retrieved from http://search.mandumah.com/Record/483528

[5] El-Sayed, Hamdi Abolnour (2017). The right to privacy under social media monitoring. Journal of Legal and Economic Research: Menoufia University. vol. 27, pp.-46.- pp. 123-239. retrieved fromhttp://search.mandumah.com/Record/900013

[6] Ghathbar, Khalid bin Suleiman and Al-Sabeeh, Amal Nasser. (2011). An Analytical Study of Saudi Hackers: Hackers, Saudis, Hacking, Digital War, Study = Hacker, Saudi, Hacking, Cyberwar, Study. Journal of Information Studies: The Saudi Library and Information Association, p. 10 .- pp. 243 - 270 retrieved from http://search.mandumah.com/Record/95019

[7] Al-Muaqil, Abdullah bin Abdulaziz.. (2018). Educational security requirements for society in social media. Journal of Educational Sciences: Imam Muhammad bin Saud Islamic University. P. 16.- pg. 11-100. retrieved from http://search.mandumah.com/Record/929507

[8] Al-Yousef, Abdullah bin Mohammed (2015). Information crimes and criminal evidence: names, characteristics and social, security and health dimensions. The First International Conference on Combating Information Crimes - ICACC: Imam Muhammad Ibn Saud Islamic University - College of Computer and Information Sciences, Kingdom of Saudi Arabia. Riyadh: Imam Muhammad bin Saud Islamic University. College of Computer and Information Sciences - p. 95 - 113. Retrieved from http://search.mandumah.com/Record/690611

[9] Ansari, Asaad Azami (2017). Social media and the recklessness of users. Sawt al-Ummah: The Salafi University - House of Authorship and Translation, Vol. 49, v8.- pg. 3-8. retrieved from http://search.mandumah.com/Record/825382

[10] Hussein, Freja. (2011). Cybercrime and the Internet. Informatics Magazine: Ministry of Education - Agency for Development and Planning, vol. 1-9, 36. retrieved from http://search.mandumah.com/Record/122156

[11] Score, Iman. (2017). Teens' use of social networking sites. Al-Hikma Journal for Media and Communication Studies: Treasures of Wisdom Foundation for Publishing and Distribution, p. 12.- pp. 187-196. retrieved from http://search.mandumah.com/Record/869217

[12] Abdel Hakim, Moulay Ibrahim (2015). Electronic crimes. Journal of Law and Human Sciences: Zayan Ashour University in Djelfa, pp. 23.- pp. 211-244. retrieved from http://search.mandumah.com/Record/705832

[13] Abdul Majeed, Nabih Tariq (2018). Cyber security is an urgent necessity for the security of societies: the safe family proposal for educating the Arab Gulf community in information security for both students and parents. The Arab International Journal of Informatics: Association of Arab Universities - Association of Faculties of Computers and Information, Vol. 6, p. 11. - pp. 1 - 26 retrieved from http://search.mandumah.com/Record/902383

[14] Omar, Muawiya Mustafa. (2015). The importance of information security in combating cybercrime: a case study of the Sudanese Center for Information Security. Bahri University Journal of Arts and Humanities: University of Bahri, Vol. 4, p. 7. - pp. 231-251. Retrieved from http://search.mandumah.com/Record/759142

[15] Muhammad, Malik. (2017). Information and security: a strategic bet and new tools for conflict. Journal of Communication in the Humanities and Social: Enaya University, p. 50.- pp. 73-93. retrieved from http://search.mandumah.com/Record/863710