Journal of Positive School Psychology http://journalppw.com
2023, Vol. 7, No. 10, 59-76

Awareness Of Cybercrime Risks And Its Relationship To Attitude Toward The Internet Use Among University Students

Dr. Huda R. Alsaeed[1] , Dr. Walid A. Elsayad[2] , Dr. Rehab Tharwat Abd El Ghani Abo Bakr[3] , Dr. Maher A. Hassan[4]

[1, 2, 3 , 4] *Imam Abdulrahman Bin Faisal University, Kingdom of Saudi Arabia.*

ABSTRACT

The current study aimed at identifying the level of awareness of cybercrime risks and the attitude reality toward the Internet among Abdulrahman Bin Faisal University students and the relationship between them. The study used a descriptive survey method. A questionnaire was prepared to measure awareness of the cybercrime risks, and a scale of attitude toward the Internet. They were applied to a sample of (288) in the Faculties of Education and Applied Studies at Imam Abdulrahman Bin Faisal University; selected in a stratified random method. The study found out a high level of awareness of the cybercrime risks and the attitude toward the Internet among students. It also found out a weak direct correlation between the attitude toward the Internet in its overall score with awareness of the cybercrime risks in its overall score and its various dimensions. In addition, the results indicated that there were no differences in the score of awareness of the cybercrime risks due to the gender variable, while differences were found out between the duration of Internet use in favor of the most used, except for the first dimension (Electronic Crimes against Persons). There were differences in the attitude toward using the Internet due to the gender variable in favor of females, while there were no differences for the variable of attitude toward the Internet in its various dimensions (psychomotor and affective) and its total score according to the variable of duration of Internet use, except for the cognitive dimension. The current study recommended the necessity of spreading awareness of the cybercrime risks and targeting it in university courses.

Keywords: Cybercrime Risks, Attitude toward the Internet Use.

1. Introduction:

The world today is experiencing an unprecedented scientific and technological revolution, which has resulted in the emergence of many modern technologies; the most notably is the Internet. It has saved man a lot of time and effort in facilitating the performance of his work and meeting his daily needs. Despite the various positive aspects that the Internet has achieved, it has led to the spread of many risks and negative behaviors, most notably cybercrime, which is considered one of the most dangerous crimes due to its characteristics that represent a major challenge to local and international laws.

These crimes have begun to expand and spread until they have become organized crimes that pose a real threat to individuals, societies, and their institutions alike. This threat even extends to countries, their autonomy, and their economies, and destroys their social structure (Al-Mutawa, 2020). The Internet has no longer only become a means of getting to know each other, socializing, and facilitating doing business. Rather, it has become a new means of luring people, defrauding them,

violating and hacking their personal information, publishing and promoting pornographic materials, and exploiting youth and children and recruiting them against society.

Many studies have confirmed the spread of electronic crimes to which young people are exposed via the Internet. The study by Nasi et al., (2015) showed that 6.5% of the participants in the study were victims, and that threats and violence were the most common forms, as confirmed by Mubaraki (2017). It stated that 37.1% of the study sample had their personal accounts burned, 77.1% were subjected to defamation and slander, 19.3% were subjected to blackmail and threats, and 22.6% had fake accounts created in their names. A study by Broadhurst et al. (2018) indicated that (138) individuals from the study participants were recruited within a week in the form of fake e-mail or phishing attacks. The study by Qaisi and Al-Gharib (2010) also indicated the presence of 63% of major electronic crimes directed towards Internet users, which come in order: sexual crimes, hacking, destabilizing intellectual security, electronic terrorism, hacking private websites, and financial crimes.

Cybercrimes clearly affect the social, economic and security aspects, threatening the structure and stability of society on the one hand, and the private lives of individuals on the other hand, as they are among the new crimes in the Saudi regime that have begun to appear prominently in recent years, which necessitated the necessity of combating them and overcoming their negative effects (Al Aqeel, 2022). This matter prompted the Council of Ministers of the Kingdom of Saudi Arabia (2007) to approve the system for combating cybercrimes; this is to avoid these risks, achieve information security, preserve the rights resulting from the legitimate use of computers and the information network, and protect the public interest, morals, public morals, and the national economy. In addition, The security, legislative, judicial and educational institutions in the Kingdom of Saudi Arabia have developed their methods and means to confront these cybercrimes with an advanced scientific method and an effective strategy (Al Zahrani, 2019).

Educational institutions, led by universities, also play a major role in spreading social awareness to protect students from the electronic risks and threats they face, especially those related to the cultural and information aspects that have become prevalent in this era. The resulting crimes and deviations that may befall them while dealing with these applications. In this regard, the study of Al Otaibi (2015) indicated that there is a general positive attitude among students toward using the Internet at its all levels: cognitive, affective, and psychomotor. The study by Al Gharib and Al Amir (2017) indicated that knowledge of the penal code for cybercrimes has a major role in combating cybercrimes. The studies conducted by Conway & Hadlington (2021) and Moallem (2018) indicated that some students were aware of the potential consequences of providing personally identifiable information, such as identity theft and stalking, but they readily provided it when requested. As for the study of Al Zein and Al Kharabsha (2020), it indicated that university students had knowledge of their rights and duties when using electronic devices in order to avoid getting into problems that exposed them to legal accountability. Almrezeq (2021) indicated that there was a significant increase in awareness of cybersecurity among students. A study by Salem et al. (2021) indicated that users who had a higher level of knowledge, training, and use of security awareness behaved in a more professional

manner toward cyber threats. As for Al Habib study (2022), it indicated that students had a high degree of awareness of cybersecurity concepts and applications. Despite this, there are many studies that confirmed the students' weak awareness of cybercrimes. In Saudi universities; such as the studies of: Al Zahrani, 2019; Al Anazi, 2019; Mahjoub & Abdul Qader, 2020; and Al Mutawa, 2020, which indicated that the role of universities in the Kingdom of Saudi Arabia in educating their students about the danger of electronic crimes (national, social, economic) was with a moderate degree.

Hence, the need emerged to enhance awareness among university students to protect them from falling into, being exposed to, or participating in cybercrimes, adopting appropriate educational and ethical measures to raise their awareness in order to achieve the optimal use of modern technologies and their dealings with the Internet (Al Mutawa, 2020).Thus, a study by Mohammed (2020) stressed the importance of introducing an electronic culture subject to raise awareness of the legal and legislative aspects of cybercrimes. Also, Alharbi& Tassaddiq (2021) indicated the necessity of including a cybersecurity awareness and training program for students in the security awareness plan and promoting it strongly by universities.

Based on the previous introduction, it is found out that cybercrimes have negatively affected university students on the one hand and society on the other hand; exposing them to many risks and threats, such as hacking their personal accounts, stealing their information, and impersonating their identities, in addition to the economic and social damage to society. This imposes on universities the need to educate their students and provide them with a culture of information security to protect them from these risks. Hence, this study is carried out to identify the extent of students' awareness of the cybercrime risks and its relationship to the attitude toward using the Internet among university students. **The problem of the current study is determined in the following questions:**

1. What is the reality of awareness of cybercrime risks and the attitude toward using the Internet among students at Imam Abdulrahman Bin Faisal University?

2. What is the relationship between awareness of cybercrime risks and the attitude toward using the Internet among students at Imam Abdulrahman Bin Faisal University?

3. Are there statistically significant differences between the mean scores of students in the extent of their awareness of cybercrime risks and the attitude toward using the Internet according to the variables: gender and duration of Internet use?

This study may benefit officials in the Ministry of Education, Saudi universities, and all sectors of society in identifying the extent of university students' awareness of cybercrime risks and its relationship to their attitude toward using the Internet, in order to protect them from electronic risks and threats to which they are exposed while using the Internet.

In the end, the current study aims at identifying awareness of the cybercrime risks and the attitude toward using the Internet among students at Imam Abdulrahman Bin Faisal University and the relationship between them.

2. Conceptual Framework of the Study:

2. 1. Definition of Cybercrime:

The phenomenon of using the Internet has spread to all countries of the world, as well as the Arab world, to a large extent, and this has resulted in differences in attitudes toward using the Internet and the applications it provides, whether positive or negative.

It also resulted from misuse and poor awareness of cybercrimes, which varied and had different types, threatening individuals, groups, and even societies. The first information crime was committed by computer in 1988 in one of the financial institutions of the United States of America. These crimes quickly expanded, their methods varied, and their losses and risks increased. They have become a source of threat to the national security of countries (Al Bishri, 2020; Rustum, 2012).

There have been many names given to cybercrimes. Some have called them Computer-Related Economic Crimes, which refers to crimes that target business sectors, or those that target confidentiality, integrity of content, and the availability of information. There are those who call them Cyber Crimes; crimes that occur via the Internet or the virtual world (Mohammed, 2020).

Ahmed (2009) defined it as performing an illegal act or intentionally abstaining from performing an obligatory act through the illegal use of any electronic means, the results of which include violating a right, whether this right is material or moral. Maabad (2013) defines it as any harmful act carried out by an individual through his use of electronic media such as computers, mobile devices, telephone communications networks, information transmission networks, the Internet, and illegal uses of computer or electronic data.

Matar (2015) defines it as a criminal activity that takes place via the Internet, and this can include stealing intellectual property and bank accounts, spreading harmful viruses on other computers, and disseminating confidential information. As for Al Bashri (2020), he defines it as a group of illegal acts. Computers and the information network are the means of committing them and they cause many risks at all levels.

Hence, cybercrime includes all forms of illegal behavior committed using technological devices, which negatively affects the individual and society.

2.2. Characteristics of Cybercrimes:

The characteristics of cybercrimes are as follows (Al Anazi, 2019):

- A transnational crime: it does not recognize the elements of place and time, as it is characterized by geographical distance.
- Soft crimes: carried out by transferring data from one computer to another.
- Crimes that are difficult to prove: they use complex technical means.
- Ease of implementation: It is implemented with minimal effort.
- Crimes that are attractive to criminals: They highlight the large gains that can be achieved by committing these crimes.
- Difficulty controlling the extent of damage caused by it compared to traditional crimes.

Al Badaina, 2014; Al Bashri, 2020; Al Jarrahi, 2015; and Kemp et al., 2021 believed that the forms and manifestations of cybercrime are many and varied in: sabotage and misuse of information, which includes theft and sale of technical, military, and industrial information, violation of privacy, eavesdropping,

espionage, defamation, spreading rumors, exchanging encrypted messages between members of criminal gangs.

2.3. Types of Cybercrimes:

Cybercrimes are among the most important causes of cyberterrorism, as the idea of cyberterrorism is linked to developments that have occurred in the field of information. Cyberterrorism groups focus on inflaming emotions and arousing the emotions of young people. **The types of cybercrimes are as follows:**

1. Cybercrimes targeting the self and honor: crimes such as (murder, battery, abortion, indecent assault or rape, slander and insults, and revealing secrets).
2. Electronic crimes targeting money: These include crimes (electronic begging, seizing electronic payment cards, forging an electronic signature, forging securities, money laundering, and financial extortion) (Ahmed, 2009).
3. Cybercrimes targeting the interests of the state and the security of society: These include crimes (spreading extremist ideas, spreading false rumors, creating anti-social websites, drug trafficking, and hacking government websites) (Al Zahrani, 2019).
4. Electronic crimes targeting computers and information technology: They include crimes (penetrating and destroying information networks, damaging and distorting computer programs, transmitting viruses and malicious programs, espionage, hacking and piracy, blocking and hacking website services) (Ahmed, 2019; Gamal and Sera'a, 2018).

2.4. Reasons for the Spread of Cybercrime:

There are many reasons and factors that led to the spread of cybercrimes, including: deficiencies in security awareness programs, weak deterrent laws, an increase in the Internet user base, economic factors and the spread of unemployment, weak religious faith, and family problems (Al Zahrani, 2019).

The negative effects of cybercrime are many and varied. From an economic standpoint, it costs countries a lot of money. From a scientific and technological perspective, the gap between developed and developing countries increases (Abdul Karim, 2007). From a moral and educational perspective, it affects the role of universities in achieving their goals and affects the university in terms of its developmental and competitive projects (Mohammed, 2020).

3. Study Methodology:

3.1. Study Method: The descriptive survey method was used as it was suitable for the current study.

3.2.Study Sample:

The study sample consisted of (288) students from Imam Abdulrahman Bin Faisal University in Dammam, the Kingdom of Saudi Arabia, divided into (56) males; at a rate of 20% and (232) females; at a rate of approximately 80%. The participants also consisted of (109) from students who use the Internet for less than 10 years, at a rate of approximately 38%, and (179) for students who use the Internet for more than 10 years, at a rate of approximately 62%.

3.3.Study Instruments:

To achieve the aims of the study, the following two instruments were designed:

3.3.1. Awareness Questionnaire of the Cybercrime Risks:

A questionnaire was designed to measure awareness of the cybercrime risks, after reviewing a set of instruments for measuring awareness of cybercrime in a study (Al Jaabari et al., 2020; Gharib and Al Amir, 2017; Qaisi and Al Gharib, 2010; Al Mansouri, 2020; Moallem, 2018). The questionnaire consists of 22 items distributed over four main pivots: cybercrimes (against persons (5 items), against society (5 items), financial (6 items), and information technology (6 items)), on a five-point Likert scale (strongly agree, agree, neutral, disagree, strongly disagree) and give a rating of (5, 4, 3, 2, 1).

Validity:

The validity of the questionnaire was calculated by presenting it to a group of jury members in the field of study, namely (educational techniques, educational psychology, and education), who were seven members. They recommended amending some of the wordings, and they were amended, and the agreement exceeded more than 85%.

After administering the questionnaire to a pilot sample of university students consisting of (35 male and female students), the internal consistency of the questionnaire was calculated between the statement s and sub-dimensions and was as follows: The degree of correlation of the statement s of the first dimension with its total score ranged between (0.852 - 0.955), and the degree of correlation of the statement s ranged The second dimension's total score ranged between (0.768 - 0.968), the degree of correlation of the third dimension's statement s with its total score ranged between (0.868 - 0.965), and the degree of correlation of the fourth dimension's statement s with its total score ranged between (0.788 - 0.948). The correlation coefficient of the dimensions with the total score was also calculated. For the questionnaire, they were as follows: (0.942, 0.956, 0.952, 0.949), all of which have high consistency coefficients that are significant at a significance level of (0.01), which means the significance of the questionnaire results.

Reliability:

The reliability of the questionnaire was calculated using Cronbach's alpha coefficient, and the reliability coefficient of the questionnaire as a whole was (0.976), which is a highly significant reliability coefficient at a significance level of (0.01); which means the significance of the questionnaire results.

3.3.2.A Scale of the Attitude toward the Internet:

The scale of attitude toward the Internet was designed after reviewing and analyzing a number of scales and examining their various dimensions (cognitive, psychomotor, and affective), such as the Zhang Scale, which was translated into Arabic by Mahmoud Musa (2011) and Al Otaibi (2015). The scale consists of 24 items distributed equally on three main pivots, which are the dimension (cognitive, psychomotor, and affective), respectively, on a five-point Likert scale (strongly agree, agree, neutral, disagree, strongly disagree) and is given a rating of (5, 4, 3, 2, 1) except for the inverse statement s, which are: (4, 14, 16, 20, 21) are corrected in reverse.

Validity:

The validity of the scale was calculated by presenting it to a group of jury members in the field of study, namely (educational techniques, educational psychology, and education), who were seven members. They recommended modifying some of the wordings, which were modified, and the agreement was more than 85%.

After administering the scale to a pilot sample of university students consisting of

(35 male and female students), the internal consistency of the questionnaire was calculated between the dimensions and the total score of the scale, and it was, respectively, as follows: (0.750, 0.887, 0.892), all of which are high consistency coefficients and significant at a significance level of (0.01); which means the significance of the scale results.

Reliability:

The reliability of the scale was calculated using Cronbach's alpha coefficient, and the reliability coefficient of the scale as a whole was (0.900), which is a highly significant reliability coefficient at a significance level of (0.01); which means the significance of the scale results.

4. Results:

4. 1. To answer the first question: What is the reality of awareness of cybercrime risks and the attitude toward using the Internet among students at Imam Abdulrahman Bin Faisal University? Means and standard deviations were used to begin ranking the basic dimensions and then to rank the statements within the dimensions; Table (1) shows the results regarding the extent of awareness of the cybercrime risks, and tables (2-5) show the sub-dimensions.

Table (1) The Mean Score and Standard Deviation of the Extent to which Male and Female Students are Aware of the Cybercrime Risks

No.	Dimension	M	S. D	Rank
1	Awareness of Crimes against Persons	4.04	1.24	1
2	Awareness of Crimes against Society	3.77	1.32	3
3	Awareness of Financial Crimes	3.62	1.31	4
4	Awareness of Information Crimes	3.78	1.31	2
Awareness of cybercrime risks as a whole		3.80	1.23	

It is clear from **Table (1)** that the mean score of awareness ragrding cybercrimes risks as a whole reached (M = 3.80) and (SD = 1.23). The responses of the study sample were **(agree)** in all dimensions of awareness of the cybercrime risks; as it was limited between (3.62-4.04), and the standard deviation was between (1.24-1.32), which confirms the presence of convergence in the opinions of male and female students. The component with the highest mean score is awareness of crimes against persons, (M = 4.04), ranked first, followed by awareness of information crimes (M = 3.78), in the second place, then awareness of crimes against society. In the third stage, (M=3.77), and finally, awareness of financial crimes ranked last, (M=3.62).

Table (2) The Mean Score and Standard Deviation of the Extent of Awareness of the Cybercrime Risks against Persons

No.	Statements	M	S.D	Rank
1	Impersonation by falsifying data	4.03	1.32	3
2	Harming others through social media	4.18	1.29	1
3	Infringing on private life by misusing modern technologies	3.99	1.27	4
4	Blackmail and material and moral threats	4.06	1.39	2

5	Electronic fraud through eavesdropping or hacking into personal accounts	3.94	1.36	5
Awareness of cybercrime risks against persons as a whole		3.58	0.98	

It is clear from **Table (2)** that the mean score of awareness of risks against people as a whole is between (3.94 and 4.18), and the responses of the study sample were **(agree)**, and the standard deviation was limited between (1.27-1.36). These values show a convergence in the opinions of the study sample regarding the extent of awareness of the cybercrime risks against people at Imam Abdulrahman Bin Faisal University. The two statements (2, 4) which are: "Harming others through social media" and "Blackmail and material and moral threats" obtained the highest mean score: (4.18, 4.06); respectively. They ranked first and second, while the statement (5), which is: "Electronic fraud through eavesdropping or hacking into personal accounts," received the lowest mean score (3.94) and ranked last.

Table (3) The Mean Score and Standard Deviation of the Extent of Awareness of the Cybercrime Risks against Society

No.	Statements	M	S.D	Rank
6	Websites that traffic in human sexuality	3.71	1.43	3
7	Websites that aim to harm public order	3.94	1.38	1
8	Websites that spread extremist ideas in society	3.94	1.40	1
9	Drug trafficking websites	3.61	1.47	5
10	Hacking government authorities' websites	3.63	1.52	4
Total awareness of cybercrime risks against society		3.77	1.31	

It is clear from **Table (3)** that the mean score of statements of awareness regarding the cybercrime risks against society is limited to (3.61-3.94). The responses of the study sample were **(agree)**, and the standard deviation was limited to (1.38-1.52). These values show a convergence in the opinions of the study sample regarding the extent of awareness of the cybercrime risks against society, and that the statements (7, 8) which are: "Hacking websites that aim to harm public order" and "Websites that spread extremist ideas in society" ranked first with a mean score of (3.94), while the two statements (10, 9) which are : "Hacking government authorities' websites" and "Drug trafficking websites" received the lowest mean score (3.63, 3.61); respectively, and occupied the last two places.

Table (4) The Mean Score and Standard Deviation of the Extent of Awareness of the Risks of Information Crimes

No.	Statements	M	S.D	Rank
11	Malware that aims to destroy data	3.79	1.45	2
12	Spying and hacking to obtain private information	3.81	1.43	1
13	Hacking and blocking website services	3.79	1.38	2
14	Violation of intellectual property rights	3.78	1.41	4
15	Creating fake web pages	3.75	1.44	6

16	Email hacking	3.78	1.43	4
Total awareness of the Risks of Information Crimes		3.78	1.31	

It is clear from (**Table 4**) that the mean score of the statements regarding awareness of risks of information crimes against society is limited between (3.75 - 3.81). The responses of the study sample were **(agree)**, and the standard deviation was limited between (1.38 - 1.45). These values show a convergence in the opinions of the study sample regarding the extent of awareness of the risks of cybercrimes. Statement (12), which is: "Spying and hacking to obtain private information" ranked first with a mean of (3.81), while statement (15), which is: "Creating fake web pages," got the lowest mean of (3.75) and came in the last place.

Table (5) The Mean Score and Standard Deviation of the Extent of Awareness of the Financial Cybercrime Risks

No.	Statements	M	S.D	Rank
17	Electronic fraud to seize money or bonds	3.91	1.42	2
18	Information breach of bank data	3.96	1.41	1
19	Money laundering sites	3.31	1.52	6
20	E-commerce fraud sites	3.65	1.48	3
21	Electronic transfer of illicit funds	3.54	1.50	4
22	Online gambling sites	3.36	1.45	5
Total awareness of financial crime risks		3.62	1.31	

It is clear from (**Table 5)** that the mean score for statements about the extent of awareness regarding risks of financial crimes is limited to (3.31-3.96), and the responses of the study sample are limited to (Agree - Neutral), and the standard deviation is limited between (1.41-1.52). These values show convergence in the opinion of the study sample regarding the extent of awareness regarding risks of financial crimes, the two statements (18, 17) which are: "Information breach of bank data" and "Electronic fraud to seize money or bonds" ranked first and second with a mean score, respectively (3.96, 3.91). As for the two statements (19, 22), which are: "Online gambling sites" and "Money laundering sites," they received the lowest mean scores, respectively (3.36, 3.31), and occupied the last two places, as the responses of the study sample were "neutral".

The following table shows the reality of university students' use of the Internet in its total score and various dimensions:

Table (6) Mean and Standard Deviation of Attitude toward Using the Internet

No.	Dimension	M	S.D	Rank
1	Cognitive Level	4.15	0.59	1
2	Psychomotor Level	3.91	0.68	2
3	Affective Level	3.70	0.64	3
The attitude scale as a whole		3.92	0.55	

It is clear from **Table (6**) that the mean score for the total dimensions of the attitude scale toward using the Internet reached (M = 3.92) and the standard deviation (SD = 0.55). The responses of the study sample were **(agree)** in all dimensions of the scale as the mean score was limited between (3.70-4.15), and the standard deviation was between (0.59-0.68), which confirms the presence of convergence in the opinions of male and female students. The level with the highest mean score is the cognitive level (M = 4.15) and ranked first, followed by the psychomotor level (M = 3.91) in second place, and finally the affective level (M = 3.70) in the third place; however, the total score of the attitude scale was at a high level among the study sample.

4.2. To answer the second question: What is the relationship between awareness of cybercrime risks and the attitude toward using the Internet among students at Imam Abdulrahman Bin Faisal University? To answer this question, the Pearson correlation coefficient was used to determine the degree of correlation between the attitude toward using the Internet in its total score of awareness of the cybercrime risks in its various dimensions and its overall score.**This is shown in Table (7):**

Table (7) Correlation Coefficient between Awareness of the Cybercrime Risks and the Attitude to Use the Internet

	Cybercrimes against Persons	**Cybercrimes against Society**	**Financial Cybercrimes**	**Information Cybercrimes**	**Total Score of Awareness of Electronic Risks**	**The attitude scale as a whole**
Cybercrimes against Persons	1.000					
Cybercrimes against Society	.888	1.000				
Financial Cybercrimes	.834	.897	1.000			
Information Cybercrimes	.861	.873	.922	1.000		
Total Score of Awareness of Cybercrime Risks	.938	.959	.958	.959	1.000	
The attitude scale as a whole	.252	.274	.298	.274	.288	1.000

It is clear from **Table (7)** that the correlation coefficients between awareness of cybercrimes with its various dimensions and its total score are high and positive and

range between (0.834-0.959), which indicates the presence of a high direct correlation between these various dimensions and the total score, while there is a weak and insignificant correlation ranging between (0.252 - 0.298) between awareness of the risks of cybercrime with its various dimensions and its total score with the attitude toward using the Internet, which indicates a weak correlation between the two variables of the study.

4.3To answer the third question: 3. Are there statistically significant differences between the mean scores of students in the extent of their awareness of cybercrime risks and the attitude toward using the Internet according to the variables: gender and duration of Internet use?

To calculate the differences between the two study groups according to the variables of gender and duration of Internet use, a t-test was used for two separate groups. This is shown in **Table (8) and Table (9)**.

Table (8) Significance of Differences in Awareness of the Cybercrime Risks and the Attitude toward Using the Internet according to the Gender Variable

Variable	Gender	N	M	S. D	t	df	sig
Cybercrimes against Persons	Male	56	3.9893	1.06202	-.333	286	.739
	Female	232	4.0509	1.28150			
Cybercrimes against Society	Male	56	3.6929	1.17177	-.480	286	.631
	Female	232	3.7871	1.34917			
Financial Cybercrimes	Male	56	3.5714	1.09722	-.311	286	.756
	Female	232	3.6322	1.35694			
Information Cybercrimes	Male	56	3.7976	1.09023	.082	286	.935
	Female	232	3.7816	1.36143			
Total Score of Awareness of Cybercrime Risks	Male	56	3.7628	1.02815	-.272	286	.786
	Female	232	3.8129	1.28067			
Cognitive Level Psychomotor Level	Male	56	3.9397	.66572	-2.914	286	.004
	Female	232	4.1950	.56856			
Affective Level Cognitive Level	Male	56	3.6652	.71673	-3.091	286	.002
	Female	232	3.9752	.66291			
Psychomotor Level	Male	56	3.4576	.66156	-3.200	286	.002
	Female	232	3.7586	.62467			
The attitude scale as a whole	Male	56	3.6875	.59972	-3.613	286	.000
	Female	232	3.9763	.52077			

It is clear from the previous **Table (8)** that the (t) value is not significant for the variable of awareness of cybercrimes with its total score and its various dimensions according to the gender variable. This indicates accepting the null hypothesis. While there were statistically significant differences of the attitude variable toward using the Internet with its various dimensions and its total score according to the gender variable in favor of females; this indicates rejection of the null hypothesis and acceptance of the alternative hypothesis.

Table (9) Significance of Differences in Awareness of the Cybercrime Risks and the Attitude toward Using the Internet according to the Internet Use Duration

Variable	Type	N	M	S. D	t	df	sig
Cybercrimes against Persons	**Less than 10 years**	109	3.869	1.306	-1.813	286	.071
	Older than 10 years	179	4.141	1.190			
Cybercrimes against Society	**Less than 10 years**	109	3.493	1.350	-2.804	286	.005
	Older than 10 years	179	3.936	1.268			
Financial Cybercrimes	**Less than 10 years**	109	3.408	1.322	-2.160	286	.032
	Older than 10 years	179	3.749	1.287			
Information Cybercrimes	**Less than 10 years**	109	3.567	1.307	-2.211	286	.028
	Older than 10 years	179	3.917	1.299			
Total Score of Awareness of Cybercrime Risks	**Less than 10 years**	109	3.584	1.262	-2.363	286	.019
	Older than 10 years	179	3.936	1.201			
Cognitive Level Psychomotor Level	**Less than 10 years**	109	4.055	.662	-2.018	286	.045
	Older than 10 years	179	4.200	.546			
Affective Level Cognitive Level	**Less than 10 years**	109	3.864	.737	-.973	286	.331
	Older than 10 years	179	3.945	.648			
Psychomotor Level	**Less than 10 years**	109	3.690	.691	-.200	286	.842
	Older than 10 years	179	3.706	.611			
The attitude scale as a whole	**Less than 10 years**	109	3.870	.615	-1.212	286	.227
	Older than 10 years	179	3.950	.501			

It is clear from **(Table 9)** that (t) value is significant for the variable of awareness of cybercrime risks in its total score and the dimensions of cybercrime (against society, financial, information) according to the variable of the Internet use duration for the benefit of Internet users for a period of more than 10 years, except for the first dimension, which is cybercrimes against persons; there is no statistical significance between the two groups. While there are no statistically significant differences for the

attitude variable toward using the Internet in its two dimensions (psychomotor - affective) and its total score according to the variable of duration of Internet use, except for the cognitive dimension; there are significant differences in favor of Internet users for a period of more than 10 years.

5. Discussion and Results Interpretation:

5.1. **Regarding awareness of the cybercrime risks as a whole:** The results showed that awareness of the cybercrime risks exists to a large degree among male and female students (M = 3.80). According to these results, it is found out that they are compatible and congruent with the efforts exerted by Saudi Universities with the Ministry of Communications and Information Technology to educate students about the cybercrime risks and cybersecurity, and to introduce them to the cybercrime risks with various types, whether the crimes concern individuals or society, or information or financial aspects. This result is consistent with the findings of a study by Al Habib (2022), which confirmed that students have a high degree of awareness with the concepts and applications of cybersecurity knowledge. Other studies indicated that there has been a significant increase in cybersecurity awareness among university students (Almrezeq, 2021; Alzubaidi, 2021).

5.1.1. **Regarding awareness of the cybercrime risks against persons:** It ranked first (M=4.03), and this confirms students' awareness of the cybercrime risks against persons such as impersonation, harming others through social media, infringing on private life, blackmail and material and moral threats, and electronic fraud. This is consistent with the university's advertisements, awareness lectures, and seminars to introduce students to information cybercrimes and their risks. This is consistent with the study of Moallem (2018), which indicated students' knowledge of the risks of disclosing personal information via websites.

5. 1. 2 Regarding awareness of the cybercrime risks: It ranked second (M=3.78), and this confirms students' awareness of the cybercrime risks, such as malicious programs that aim to destroy data, files, and devices, espionage, hacking, obtaining private information, blocking website services, hacking them, violating intellectual property rights, and creating fake web pages. This is consistent with the university's advertisements, awareness lectures, and seminars to introduce students to information crimes and their dangers. This result is consistent with the findings of Almrezeq's study (2021), which indicated the presence of awareness among university students of digital crimes related to technology and the Internet. Another study by Moallem (2018) indicated that some students are aware of the potential consequences of providing personally identifiable information, such as identity theft and stalking, but feel comfortable providing it.

5. 1. 3 **Regarding awareness of the cybercrime risks against society:** It ranked third (M=3.77(. This confirms students' awareness of the cybercrime risks that target society, its security and stability, such as hacking the websites of government agencies and leaking data that affects national security, and websites that target violating public order or public morals, spreading false rumors, or spreading extremist ideas in society. This is consistent with the campaigns carried out by the university and government media to educate students about the cybercrime risks on society. This result differs from the findings of a study by Al Mutawa (2020) about students' low awareness of the social and national risks of cybercrime.

5. 1. 4. Regarding awareness of the financial cybercrime risks: It ranked last (M=3.62(. This confirms students' awareness of the financial cybercrimes risks such as seizing money and bonds through electronic fraud, hacking credit cards and bank data, money laundering, and fraud. E-commerce and online gambling sites. This is consistent with the campaigns carried out by the university, media institutions and banks to raise students' awareness of financial cybercrimes. This result differs from what was indicated by the study of Qaisi and Al Gharib (2010) that many Internet users are exposed to financial cybercrimes due to their low awareness with their risks.

5. 1. 5. Attitude toward using the Internet: The results showed that there is a strong attitude among students toward using the Internet (M = 3.92), at its three levels: cognitive, psychomotor, and Affective. According to these results, it is found out that they were compatible and congruent with reality. This age group (university students) is the group that uses the Internet the most and browses its websites. This result is consistent with what was found in the study of Al Otaibi (2015) regarding the presence of a general positive attitude toward using the Internet at all its cognitive, affective, and psychomotor levels among students.

5.2. **The relationship between awareness of the cybercrime risks with its various dimensions and the attitude toward using the Internet:** The results showed that there is a relationship between the dimensions of awareness of the cybercrime risks with each other and with the total score of awareness of cybercrime. They are all strong direct correlations, while the results showed that there is a weak direct correlation between the attitude toward using the Internet with awareness of the cybercrime risks in their overall score and various dimensions. Focusing on these results, it is found out that they were compatible and consistent with reality, as this age group (university students) is the group that uses the Internet the most and browses its sites. Despite this, they have awareness of the cybercrime risks. This is consistent with the findings of Salem et al. study (2021), which confirmed that users who have a higher level of knowledge, training, and usage in security awareness behaved in a more professional manner toward cyber threats than those who do not have this knowledge, while this result differs with Al Barashdi study (2019), which indicated that 70% of participants believed that there is a relationship between cybercrimes and social media users on an ongoing basis. Another study, by Qaisi and Al Gharib (2010), showed the presence of major cybercrimes directed against Internet users.

5.3. **Differences between the mean scores of students in awareness of the cybercrime risks and the attitude toward using the Internet according to the gender variable:** The results showed acceptance of the null hypothesis, which indicates that there are no differences in awareness of the cybercrime risks in its total score and various dimensions according to the gender variable. This indicates that males and females have approximately the same amount of awareness of the cybercrime risks. It also indicates that social media and media in Saudi society and the university and its various institutions warn a lot against cybercrime, which has spread as a result of the use of smart devices and the ease of hacking them. This is consistent with the study of Al Zein and Al Kharabsha (2020), which indicated that there are no differences between the level of awareness of Jordanian youth about cybercrimes due to the variable of gender. It differs with a study carried out by Lembrechts (2012) and

Marcum et al. (2012), which found out that there are similar predictions of cyberbullying between both genders, and that females are more likely to spread rumors than males. However, results indicated that there are statistically significant differences for the variable of the attitude toward using the Internet in its various dimensions and its overall score according to the gender variable in favor of females. This indicates the rejection of the null hypothesis and the acceptance of the alternative one. This may be due to some customs of Saudi society, which tends to leave greater freedom of exit and movement to males than to females. That leads to a greater attitude for females toward using electronic devices at home and of course the ease of obtaining information via the Internet. This differs from the study of Al Zein and Al Kharabsheh (2020), which indicated that there are no differences between the level of awareness of Jordanian youth about cybercrimes due to the variable of gender. This is due to similar levels of awareness between males and females .

5.4. **Differences between the mean scores of students in awareness of the cybercrime risks and the attitude toward using the Internet according to the variable of duration of Internet use:** The results showed that there are statistically significant differences for the variable of awareness of cybercrime risks, in its total score and its various dimensions, according to the duration of Internet use, in favor of Internet users for a longer period. From 10 years, except for the first dimension, which is cybercrimes against persons, there is no statistical significance between the two groups. This may be due to what is linked to the advantage of females in using the Internet, and most of the study sample is female. The period of using the Internet for more than 10 years has a significant impact on knowledge and vulnerability to cybercrimes in its various dimensions. However, there are no statistically significant differences for the variable of the attitude toward using the Internet in its various dimensions (psychomotor - affective) and its overall score according to the variable of duration of Internet use, in order to increase the interest of students and society toward electronic transformation, except for the cognitive dimension; there are differences in favor of Internet users for a period of time older than 10 years. These results indicated that the attitude toward the Internet increases as the duration of Internet use increases. This is consistent with the study of Al Otaibi (2015) and the study of Moallem (2018), which indicated a positive attitude toward using the Internet.

Recommendations and Suggestions:

1- Increasing the interest of universities and research centers in educating students about the risks of cybercrimes.
2- Universities' interest in teaching a course on cybersecurity for the various specializations.
3- Concluding cooperation and partnership agreements between universities and the Ministry of Communications to educate students about the risks of cybercrimes.

References

1. Abdul Karim, S. (2007). Ethics of the information society in the Internet age. King Fahd National Magazine, 13(1), 286-305.
2. Ahmed, E. (2009). Methods of combating cybercrime in Egypt and the role of the Ministry of Interior. Arab Manager Magazine, (187). 22-39.
3. Al Aqeel, S. (2022). Social awareness and electronic crimes: A field study on a sample of individuals in the city of Buraidah in the Qassim

region. Journal of Humanities and Administrative Sciences, (26), 44-68.

4. Al Anzi, I. (2019). The role of educational institutions in raising awareness of the risks of cybercrime: a study of a sample of educational institutions for the university and secondary levels in the city of Riyadh. Journal of Security Research, 28(74), 13-79.
5. Al Badaina, Dh. (2014). Cybercrime concept and causes. Published working paper, Scientific Forum, New Crimes in Light of Regional and International Changes and Transformations, Amman, Hashemite Kingdom of Jordan.
6. Al Barashdi, H. (2019). Facebook and cybercrime in Oman: Is there a relationship? Journal of Information and Technology Studies, 2(2), 1-11.
7. Al Bishri, H. (2020). Cybercrime and how to deal with it from the point of view of university youth. Scientific Journal of the College of Arts, (38), 633-664.
8. Al Jarrahi, M. (2015). The role of Saudi universities in developing youth awareness of the seriousness of cybercrimes to support issues of combating cyberterrorism. The First International Conference on Combating Information Crimes, ACC, Kingdom of Saudi Arabia. Riyadh: Imam Mohammed Bin Saud Islamic University, 75-80.
9. Al Gharib, M. &Al Amir, H. (2017). The extent of awareness among the young age group of the Saudi cybercrime penal system. International Arab Journal of Informatics, 5(9), 17-32.
10. Al Habib, M. (2022). The degree of awareness of cybersecurity among male and female postgraduate students at the College of Education at Imam Mohammed Bin Saud Islamic University and ways to enhance it from their point of view. Journal of Educational Sciences, (30), 269-320
11. Al Jabari, M &Amr, B. (2020). The effectiveness of technical and legal awareness programs in confronting cybercrime from the perspective of university students. Hebron University Journal of Research, Hebron University, 9, 129-156.
12. Al Mansouri, S. (2020). Cybercrimes against persons. Moroccan Law Journal, 43, 27-42.
13. Al Mutawa, A. (2020). The level of awareness among students of the College of Education in Shaqra at Shaqra University and the system for combating information crimes and educational measures. Journal of Educational Sciences, (24), 290-373.
14. Al Otaibi, Kh. (2015). The attitude toward using the Internet and its relationship to dimensions of alienation and some other variables among a sample of university students. Scientific Journal of King Faisal University - Humanities and Administrative Sciences, 16(1), 65-97.
15. Al Zahrani, H. (2019). The role of Islamic universities in the Kingdom of Saudi Arabia in educating their students about the danger of cybercrime and ways to prevent it. Journal of the Islamic University of Arabic Language and Social Sciences, 2(3), 385-468.
16. Al Zein, Gh. & Al Kharabsha, A. (2021). Electronic crimes and the level of awareness of their danger: A field study on a sample of Jordanian university youth. Islamic University Journal for Human Studies, 29(2), 230-248.
17. Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of

Majmaah University. Big Data and Cognitive Computing, 5(2) 1-23.

18. Almrezeq, N. (2021). Exploratory study to measure awareness of cybercrime in Saudi Arabia. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2992-2999.
19. Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1), e06016.
20. Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018). Phishing and cybercrime risks in a university student community. Available at SSRN 3176319.
21. Cabinet (2007). Resolution No. (79) dated 3/27/2007 approving the system for combating cybercrimes. Kingdom of Saudi Arabia.
22. Conway, G., & Hadlington, L. (2021). How do undergraduate students construct their view of cybercrime? Exploring definitions of cybercrime, perceptions of online risk and victimization. Policing: A Journal of Policy and Practice, 15(1), 119-129.
23. Gamal, Q& Sera'a, K. (2018). Economic dimensions of cybercrime. Journal of Marketing Studies and Business Administration, 2(1), 45-53.
24. Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. Journal of Contemporary Criminal Justice, 37(4), 480-501.
25. Lembrechts, L. (2012). "Digital Image Bullying Among School Students in Belgium :An Exploration of the Characteristics of Bullies and their Victims". International Journal of Cyber Criminology. 6(2): 968-983.
26. Maabad, E. (2013). Cybercrime in foreign drama. Childhood Studies, 16(60), 86-96.
27. Mahjoub, E.& Abdel Qader, R. (2020). The reality of the role of Imam Mohammed Bin Saud Islamic University in confronting electronic crimes in light of the objectives of preventive education. Journal of Educational and Psychological Sciences, 14(1), 32-68.
28. Marcum, C.; Higgins, G.; Freiburger, T.& Ricketts, M. (2012). "Battle of the sexes: An Examination of Male and Female Cyber Bullying". International Journal of Cyber Criminology. 6(1), 904- 911.
29. Matar, H. (2015). The Comprehensive Dictionary of Social Sciences and Humanities Terms. Dar Al-Hamid for Publishing and Distribution.
30. Moallem, A. (2018). Cyber Security Awareness Among College Students. International Conference on Applied Human Factors and Ergonomics. 782, Orlando, Florida: Springer, 79 - 87.
31. Mohammed, M. (2020). A future study of the role of Egyptian universities in confronting cybercrime among students. Academic Journal of Educational and Psychological Sciences, (58), 28-71
32. Mubaraki, M. (2016). Forms of cybercrime committed via Facebook. Not Published Master's Thesis. Larbi Ben Mahdi University - Oum El Bouaghi, Algeria.
33. Nasi, Matti , Oksanen, atte, Keipi,Teo & Rasanen, Pekke.(2015). Cybercrime victimization among young people: a multi-nation study. Journal of Scandinavian Studies in Criminology and Crime Prevention, 16(2), 203-210.
34. Qaisi, N. & Al Gharib, A. (2010). Cybercrimes directed at Internet users: A survey of some Internet

users in the Kingdom of Saudi Arabia. Not Published Master's Thesis. Imam Mohammad Bin Saud University in Riyadh.

35. Rostom, H. (2012). Thefts and computers. Symposium on New Economic Crimes, Cairo, National Center for Social and Criminological Research, 278-279.
36. Salem, Y., Moreb, M., & Rabayah, K. S. (2021, July). Evaluation of Information Security Awareness among Palestinian Learners. International, Conference on Information Technology (ICIT) ,.21-26.