JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

The role of the Public Security Directorate in reducing cybercrime on social media from the point of view of employees of the Cybercrime Combating Unit in Jordan

Dr :ANAS ADNAN ODIBAT

Dr Heba Tawfiqe Odah Abu Eyadah
University of Minnesota

The study aimed to identify the role of the Public Security Directorate to reduce cybercrime on social networking sites from the point of view of employees of the Cybercrime Combating Unit. It took a descriptive survey approach. A questionnaire was prepared in order to measure the role of the Public Security Directorate in curbing cybercrime. The questionnaire consisted of three areas, the first is the role of the Public Security Directorate in raising awareness of cybercrime, the second is the role of the General Mother Directorate in reducing cybercrime, and the third is the obstacles facing the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime. The questionnaire contained (28) paragraphs. The study population included all employees of the Cybercrime Combating Unit, and their number was (64) officers and individuals. The study sample was selected based on the purposeful sample method. The results related to this question showed that the role of the Public Security Directorate in raising awareness of cybercrime on social networking sites from the point of view of The employees of the Anti-Cybercrime Unit in Jordan were average, and the reason for this from the study's point of view was that the Public Security Directorate was concerned with raising awareness of the dangers of cybercrime, as the Anti-Cybercrime Department was constantly concerned with qualified administrative cadres and was keen to strive to improve work In the fight against crime of all kinds, especially cybercrime, because it has become a necessary requirement for the knowledge revolution This result can be explained by the fact that the Public Security Directorate is one of the institutions that achieve its goals through its officers and personnel, especially the Cybercrime Unit by combating electronic intrusions and working to spread culture and awareness in society of the dangers of cybercrime. In light of these results, the study recommends that the Public Security Directorate adopt in general, the Cybercrime Combating Unit plays its role in raising awareness of cybercrime, in order to enhance its capabilities and raise its level in combating crime, especially cybercrime.

Keywords: cybercrime, social networking sites, public security directorate.

Introduction:

The world has recently witnessed a new era of scientific progress and knowledge revolution, and this development has been accompanied by an unprecedented and rapid renaissance in all fields, perhaps the most prominent of which was in the information and communication sector, and this resulted in a human development revolution at all levels and levels, whether local or international, as it became a process The exchange of information and knowledge is easier and easier, and since the electronic environment has pioneers from different categories, as some criminals of Internet technologies and software have become accustomed to this digital environment fertile for carrying out electronic crimes in various forms and abuse on the international scene in the use of electronic means of communication that have appeared, which did not exist Inevitably, globalization and what it created of a massive technological revolution has put the social structures of societies in great shape to maintain their stability and traditionalism, and although this massive technological transformation had many developments and gains for humanity, it also created forms of deviations that humanity did not know. Before, crime no longer relied on its primitive form in traditional societies, as the assault was no longer psychological and financial. Rather, it has become targeting information, data, people, and communities remotely and without the direct presence of those responsible for it, and it is internationally called white-collar crimes, by committing the most serious abuses and the greatest harm quietly and safely without moving from the place or causing even bloodshed, so it is described as a soft crime. A single attack on a computer or smartphone is capable of causing destruction and destruction of the economies of major companies, as well as threatening the security and stability of individuals, their property, and societies, not limited to a country or a city, but rather a global scourge (Al-Anzi, 2019).

Countries and societies did not stand by and watch these societal problems created by cybercrime, but they have taken measures and laws that limit them and punish their perpetrators. However, the level of acceleration and development of this type of crime may exceed the legislative level that it is trying to track, in addition to the difficulty of proving this type of crime. Crimes and tracking down the perpetrators who establish themselves as fictitious personalities on that virtual society, which makes it difficult to track them down. A responsibility placed on the shoulder of one of the parties and handles its affairs to the extent that it should be the responsibility of society in all its social and civil institutions. If awareness spreads among individuals of the dangers of cybercrime, then individuals become the first line of defense for themselves and their society from exposure to this type of crime. From here the idea of the study sprouted. The current attempt to explore (Al-Aqil, 2022).

Study problem and questions:

The problem of the study is always raised through the application of reason and scientific logic in the problems that society is exposed to, and an attempt to identify the dimensions of these problems, the causes of their occurrence, the most prominent active factors affecting them and the resulting damages to society, in an attempt to reveal the ambiguity of these problems and try to devote efforts to confront them and limit their effects. on communities.

Despite the clear difference made by the technological revolution, which moved the world to huge and great developments, as it opened up areas for progress and prosperity for it and achieved a quality transfer that the world has not achieved throughout its long history, we cannot be certain that this technological revolution and the accompanying development at all levels Despite the countless benefits of this technological revolution, it also contained many risks and social diseases that society did not know before, and despite the great technological awareness of the dangers and threats it carries, which led some to illegally exploit it with the aim of Achieving private gains and harming society, both at the level of its individuals and institutions, as the forms of cybercrime varied, and there was a great professionalism in the improper exploitation of technology.

The rapid rise in the number of users of the World Wide Web reflects negatively on the increase in the number of perpetrators of cybercrime and an increase in its volume significantly. In 2021, the losses of global economic activities were estimated at more than $54 billion, and the number of victims of cybercrime reached 655 million, with 5.1 million victims in 2021. Today, at a rate of 81 victims per second, more than 4.232 million identity cards have been stolen (Cybercrime, 2016).

And regardless of the presence of bodies and institutions concerned with combating cybercrime, “however, these crimes are rapidly developing, which makes it difficult to combat and control them, so it is important for community institutions to focus on awareness and education to reduce cybercrime, and in light of the provision of facilities to enter the virtual world, including It contains positives and negatives. Young people will be subject to exploitation in all its forms, whether the victim is his thinking that attracts him to the negative direction and deviation to commit these crimes. Therefore, it was necessary for community institutions to raise awareness among young people of these crimes, especially educational institutions because they are responsible for preparing the future generation. A generation aware and educated.

Hence the problem of the study came to try to identify the role of the Public Security Directorate in reducing cybercrime on social networking sites from the point of view of workers in the Anti-cybercrime Unit and school teachers in Jordan. The following sub-questions branch out from it:

Study questions:

1. What is the role of the Public Security Directorate in raising awareness of cybercrimes on social networking sites from the point of view of employees in the Anti-Cybercrime Unit in Jordan?
2. What is the role of the Public Security Directorate in reducing cybercrime on social networking sites from the point of view of the employees of the Anti-Crime Unit in Jordan?
3. What are the obstacles facing the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime?

Study objectives:

This study came to achieve a number of objectives, the most important of which are:

1. The importance of the study lies in trying to reach a set of scientific facts about the role of the Public Security Directorate in limiting the spread of cybercrime.
2. Disclosure of mechanisms to combat cybercrime by the Public Security Directorate in order to limit the spread of cybercrime.
3. Identifying the most important obstacles that hinder the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime.

Study Importance:

It is divided into two main aspects:

First: The theoretical aspect, which is:

1. A new addition to scientific research, especially to Arab studies related to combating cybercrime
2. An attempt to find some solutions to the problems faced by the Public Security Directorate in combating cybercrime.

Second: the applied side, which lies in its results:

1. Disclosure of the anti-cybercrime mechanism that must be taken by the Public Security Directorate to reduce cybercrime.

2. Providing workers in the Public Security Directorate and school teachers with the types of electronic crimes that the learner may be exposed to and how to combat such crimes.

The study Limitations:

This study was limited to the following determinants:

Temporal limitations: This study was implemented during the year 2022

Spatial limitations: The study was limited to workers in the cybercrime unit and school teachers in Jordan.

Human limitations: This study will be limited to workers in the cybercrime unit and school teachers in Jordan.

Objective limitations: This study was limited to the role of the Public Security Directorate in reducing cybercrime on social networking sites from the point of view of workers in the Anti-cybercrime Unit and school teachers in Jordan.

Determinants of its limitations: The results of the study will be generalized in the light of the psychometric characteristics of the study tool and the extent of its validity and reliability.

1. Theoretical framework and previous studies:

1.2 Study Terminology:

The Public Security Directorate (idiomatically): It is one of the agencies entrusted with maintaining internal security, and it consists of several departments, including the Department of Public Relations and Information (Al-Kasasbeh and Al-Hiyari, 9, 2022). A legal personality independent of the army and affiliated with the Ministry of the Interior to watch over and monitor deficiencies, maintain security in all its forms, continuously search for and arrest those responsible for any deficiencies, and provide mechanisms and devices to facilitate work.

Public Security Directorate (procedurally): It is a security agency whose mission is to maintain security.

Cybercrime (idiomatically): It is defined as those criminal practices that are carried out through smart electronic devices, as it focuses on four types, including: crimes related to computer technology, information electronic crimes, financial crimes, and electronic shopping crimes (Al-Aqil, 2022, 49). Whereas, Essat and Bouazza (129 2022) defined it as taking an action or refraining from preparing and planning to use digital devices to commit a crime or act contrary to the law of the state, hacking them with the intention of sabotaging, distorting, disabling, or erasing data via the Internet.

Qasimi and Dughmush (2022, 221) defined it as every action that is done by information systems with the intention of harming others. And the Public Security Directorate defines it as every act that is criminalized by laws that may attack material and/or moral conditions resulting directly or indirectly from the interference of technology and is punishable by law.

Cybercrime (procedural): such as forms of illegal, social, and intentional behavior committed using electronic devices linked to the Internet by individuals who are fully aware of technology techniques, to cause material and moral damage to devices and individuals, as well as harm to society, its security and stability. Characteristics of cybercrime

Social networking sites (idiomatically): Web pages that facilitate active interaction between subscribers of Internet sites, with the aim of providing tools of interest, that help interaction and sharing among them (Abu Ayada and Al-Khatib, 2022). It was defined as a social networking site available on the Internet that enables the exchange of information, ideas, and confiscation at any time and any place, and the formation of virtual communities with the aim of strengthening the culture of dialogue (Diab, 2021). It is a group of websites that provide communication between individuals in a virtual community that is divided into groups according to Interests or affiliations (and the exchange of files, news, and media (Qasimi and Daghmosh, 226, 2022).

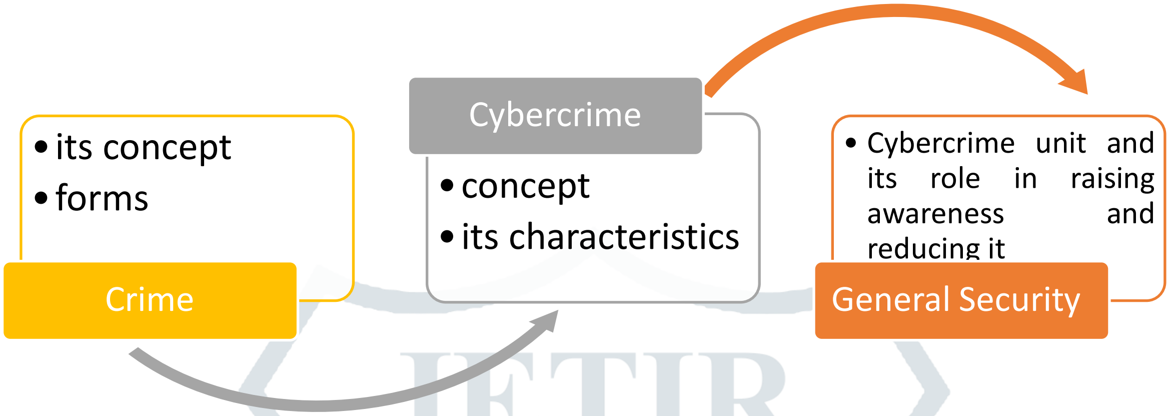
Social networking sites (procedurally): Social networks address the minds of individuals and work to transfer information and intellectual and behavioral cultures in a new way. These are interactive sites that enable users to open up to the world and create virtual communities that allow them to meet and gather online and exchange information. They also allow people to make their voices heard, to express their opinions, and to participate in political life. and local by default.

Cybercrime Unit: An official documented website on the Internet and Facebook belonging to the Criminal Investigation Unit in Public Security, with the aim of spreading awareness, guidance and protection for citizens from falling victim to technology criminals (Al-Dahla and Erekat, 2018, 7).

Cybercrime Unit (procedurally): A unit affiliated with the General Security dedicated to following up the perpetrator via the Internet and its software and applications, as well as punishing and prosecuting the perpetrators.

2.2. Theoretical framework and previous studies:

Theoretical literature will be presented according to the scheme shown in Figure (1):



Source: Researchers 2022

It is clear from Figure (1) how theoretical literature is dealt with in the study, where crime will be discussed in terms of the concept and forms of crime, and then talk about cybercrime, in terms of concept and characteristics, and also talk about public security by talking about the cybercrime unit and its role in raising awareness and reducing the crime.

The concept of crime:

The word crime is linguistically derived from the triple root of the verb (germ), meaning cutting off, that is, cutting off, materially or morally, and the origin of the word crime means earning and cutting off. Ibn Manzoor says: offense: transgression (Suleiman, et al., 2018). It causes harm to our society and is punishable according to the law. It is defined as the social phenomenon of psychological complexes, emotional disorders, tendencies and trends affected by a corrupt environment.

Also, the school of sociology believes that social factors are the main factor in the occurrence of crime. It has confirmed that the criminal is nothing but an accumulation of society, and the product of a group of social factors that man is exposed to. Some of them saw it as a natural phenomenon in any society, including Durkheim, who described it as a natural phenomenon. which is paid by a society and its effects are borne by its members" (Abdullah, 2011).

Cybercrime:

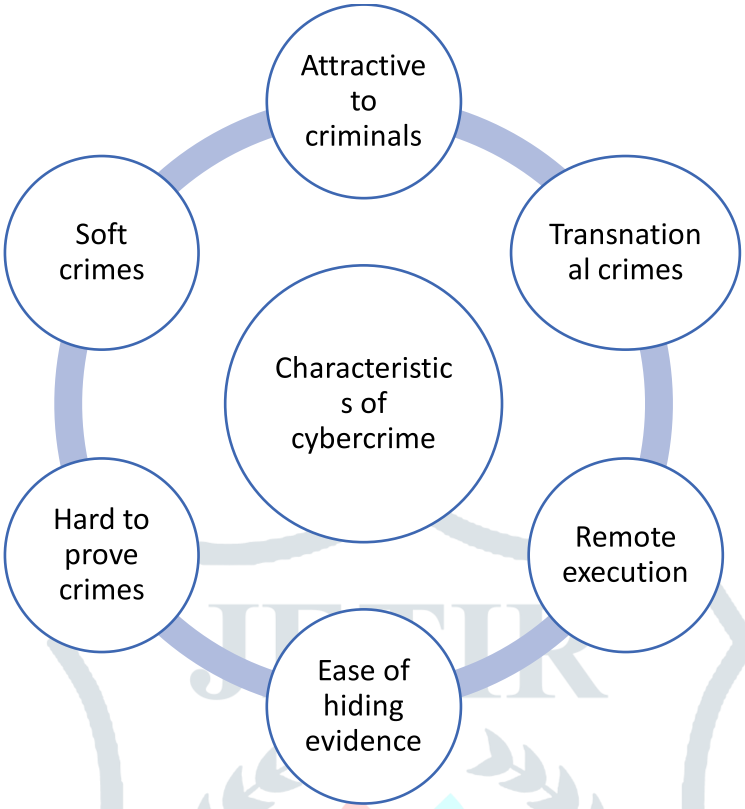
The researchers did not agree on a single definition of cybercrime. Van der Hulst & Neve stated that there is a reference absence of a general and reference concept, and mostly virtual, electronic and digital terms are used, not a consensus or a single concept (Al-Zabin, 2020).

Characteristics of cybercrime:

After presenting the concepts of cybercrime according to the above, it can be said that cybercrime is characterized by a number of features that differ from what was characterized by traditional crimes, and it was important to address those characteristics that distinguish them and that make them a great threat to society, and among the most important characteristics as mentioned by Essat and Bouazza (2022), Qasimi and Daghmosh (2022), and Al-Aqeel (2022), as follows:

1. Transnational crimes, as they are committed globally, as they are not confined to a specific country, category, or region, but rather they are crimes that have become committed in most parts of the world, even if we do not say all of them, even poor countries have become full of fraudsters through the information network, just as the network Covering the entire world, crime is almost committed in every place where this network is found, as it is found wherever there is the Internet.
2. Remote execution, criminals were able to carry out the crime in a country far from its location by hacking into a concerned network, intercepting a financial transfer, stealing important data, or carrying out sabotage.
3. Crimes that are difficult to prove, in which the perpetrator uses complex technical means in a few seconds, with the ease of concealing any evidence and tampering with information. Therefore, the difficulty of proof emerges in front of all of this in computer crimes, especially due to the lack of evidence.
4. Soft crimes, as they are characterized by not requiring any violence, effort, clash or shooting, merely transferring data from one place to another or electronic theft of a bank account.
5. Attractive crimes for criminals, for the speed of their implementation, only one click on a remote smart device, with huge benefits and gains without any effort.

The study summarizes these characteristics in Figure (2):



Source: Researchers, 2022

Through the previous figure, the characteristics of cybercrimes that were previously reviewed are summarized

Types of cybercrime:

With the spread of technology and its development, many types of cybercrime have been developed, which in their entirety work to threaten society in its security and safety, and many classifications of these crimes have been monitored according to the point of view. Mobaideen, Al-Sheikh, and Mashaqbeh (2022), Al-Aqeel (2022), Eissat and Bouazza (2022), and Al-Iraqi (2022). There are several classifications of electronic crimes that exist in the academic community. The study summarizes them as follows:

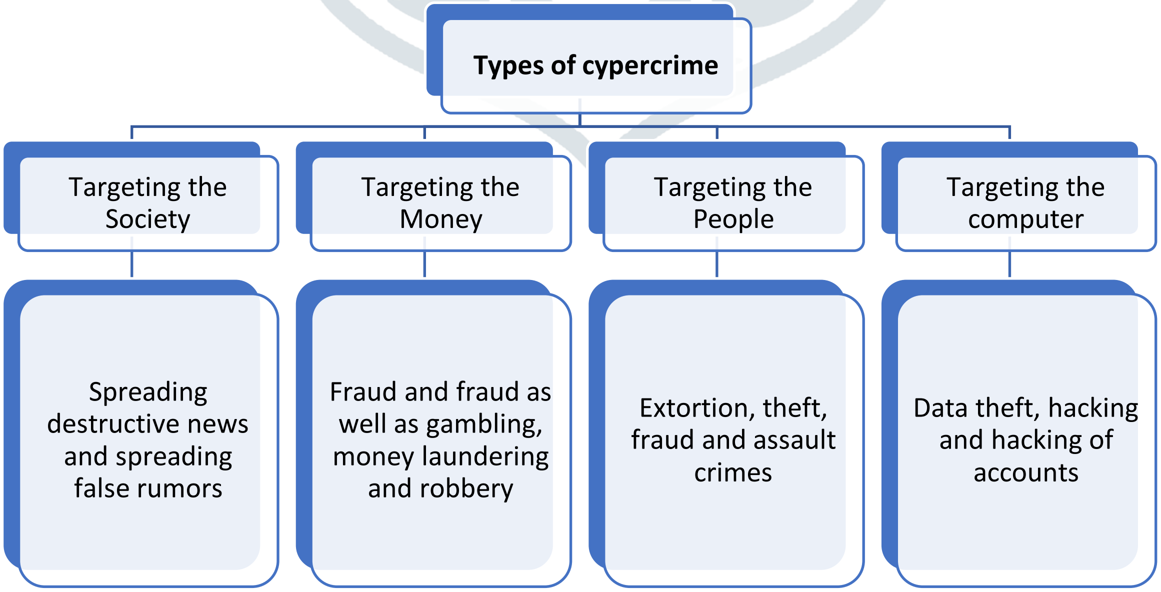
1. **Crimes targeting the personal computer:** The personal computer here does not mean the computer only, but all devices connected to the Internet have become vulnerable to these types of crimes, including personal communication devices, and this type of crime includes everything that would harm data and operating systems such as data theft and hacking. Hacking personal accounts, personal emails, official websites, spreading viruses, and all acts that damage devices and their operating activities. Crimes committed against persons: This

type of crime includes everything that may harm individuals, whether materially or morally. Examples of such crimes include data theft.

2. **Crimes against persons:** This type of crime includes everything that may harm individuals, whether materially or morally. Examples of such crimes include data theft, crimes that harm data and operating systems, such as data theft, hacking, hacking of personal accounts, personal emails and official websites, and publishing Viruses, and all acts that may damage the devices and their operating activities. Personality, exposure to extortion, theft, fraud, and assault crimes, including insult, slander, defamation, and broadcasting news and rumors that are morally or morally harmful to individuals or entities.
3. **Crimes involving money:** including fraud and fraud, as well as gambling, money laundering, bank robbery, trade and promotion of narcotic substances, as well as burglary of credit card numbers and illegal electronic transfer of funds (Muhammad Ali, 2017).
4. **Sexual crimes:** Exploiting minors and inciting them to engage in immoral sexual activities, seducing them to commit them, publishing their data, photographing or showing their sexual charms, threatening them with them, and increasing the broadcast of sexual content and pornographic clips and sending them to personal accounts.
5. **Crimes targeting society:** This new type of crime is represented in electronic practices that affect the security of society and threaten its safety, by spreading destructive news, promoting extremist ideology and spreading false rumors, the aim of which is to destabilize societies and threaten their stability.

The researchers summarize these characteristics in Figure (3):

Figure 3: Types of cybercrime


Types of cypercrime
Targeting the Society
Targeting the Money
Targeting the People
Targeting the computer
Spreading destructive news and spreading false rumors
Fraud and fraud as well as gambling, money laundering and robbery
Extortion, theft, fraud and assault crimes
Data theft, hacking and hacking of accounts

Source:

Researchers, 2022

Through the previous figure, the researchers summarize the types of electronic crimes that were reviewed previously.

Previous studies

Al-Zabin (2020) conducted a study to identify cybercrime and the level of awareness of its seriousness from the point of view of Jordanian university youth at Al-Balqa Applied University, Princess Rahma University College, and to identify the habits and patterns of Internet use among young people, and to determine if there are differences attributed to gender, specialization, and year. In order to achieve the objectives of the study, a questionnaire was prepared consisting of (34) items. The research used the descriptive method, the social survey method, in the sample method. The study sample consisted of (212) male and female students. The study was conducted in November of 2012. The random sample was used, and descriptive statistics (percentages) and the (t) test were used, and the one-way variance test for variables. The results of the study revealed that the rate of students’ exposure to cybercrime came at a low level. The results of the study also showed that 13.42% spend from two hours to less than four hours on The Internet, while the most used site is Facebook with a rate of 14.32%, and 31.34% access the sites for the purpose of entertainment and entertainment. Spend their time using the Internet to develop their skills, activate sports, cultural and entertainment activities, to attract young people to reduce addiction to social networking sites, and hold lectures to raise awareness of the dangers of cybercrime.

Jaafar bin Shaflot (2018) study entitled: The Role of Saudi Universities in Combating Cybercrime from the Viewpoint of University Students: A Case Study of Prince Nayef University for Security Sciences The study aimed to identify the role of Saudi universities in combating cybercrime from the perspective of university students, and it may be a society The study was conducted by students at the Naif Arab University for Security Sciences, and the sample was chosen by the intentional random method, and its size was 472 individuals. And that the most important of these reasons, according to the point of view of the study sample, is the low cost of the Internet and the increase in the number of its users, while the results indicated that the least important reason for the spread of cybercrime is the spread of banking institutions in the Kingdom. The role of education, community service and scientific research in Saudi universities positively affects the fight against crime.

Conducted by Schlach and Qureshi (2017). A study entitled "The spread of electronic crime affecting people in the Algerian environment" The study aimed to identify the patterns and habits of people using the Internet in the Algerian environment and to identify the most important images and forms of electronic crime against people. The study sample consisted of (64) Internet users from various cafes in the state of Massila The study found results that people are exposed to crime and the porn industry to a moderate degree, and that the crimes of impersonation, deception and solicitation target this type of crime in a large number of young people and people in general in order to deceive and pressure them.

Gharib, and Al-Amir (2017) also conducted a study entitled "The extent of awareness among the young age group of the Saudi information crime penal system," and the number of respondents reached "214" boys and girls. The study reached results, the most important of which is that 70% of the respondents are familiar with the term cybercrime, and the study also showed that the vast majority have no intention of practicing the hobby of electronic penetration of any automatic device, and this is evidence of the spread of awareness among young people.

Mubaraki (2017) conducted a study entitled "Forms of Electronic Crime Committed via Facebook". The study aimed to identify electronic crimes committed via Facebook to which young users of websites in Algeria were subjected. The sample survey method was relied upon. The results of the study showed that 0.57% exposed their account. 0.77% were subjected to defamation and slander, 5.0% were subjected to blackmail and threats through Facebook, 2.00% of them created a fake account in their names, and 20% received sexual pornography via Facebook.

Commenting on previous studies.

Through the previous presentation of some studies that dealt with cybercrime, it becomes clear to us the following:

1- The studies that dealt with the subject of cybercrime were mostly descriptive studies that attempt to shed light on the reality of cybercrime and the extent of individuals' vulnerability to it.

2- Despite the different geographical regions and countries in which studies are conducted, most of the studies have agreed on a great similarity in the type of crimes in most countries, due to the fact that cybercrime is global in nature and is not linked to a place where it can be carried out from anywhere. place in the world, so it is not bound by specific geographical borders.

3- The studies agree with the current study in the way of handling and data collection tools, as the majority of previous studies depend on the descriptive method in dealing with and on the questionnaire as a tool for data collection.

Study Approach

The study used the descriptive survey method and the field survey method due to its suitability to its objectives, nature and importance.

3.1 Study population:

The study population consisted of all workers in the Criminal Investigation Department in the Public Security Directorate (2021/2022), whose number is (316) officers and individuals. The purposeful sampling method was adopted in the crime unit, combating cybercrime, numbering (65) officers and individuals for their suitability in answering the study questions. . Table No. (1) shows the division of the study sample.

Table (1): Description of the characteristics of the study sample

Variables	Category	Number	Percentage
Sex	**Male**	**34**	**%52.3**
	Female	**31**	**%47.6**
Experience	**Less than 10 years**	**40**	**%61.1**
	More than 10 years	**25**	**%38.46**
Total		**65**	**100.0**

3.2 Study limitations:

The study was conducted and implemented in the light of the following limits and determinants: Objective limits:

The role of the Public Security Directorate in reducing cybercrime on social media from the point of view of employees in the Cybercrime Combating Unit. Human boundaries: officers and personnel of the Cybercrime Combating Unit in the Public Security Directorate. Spatial boundaries: the Cybercrime Control Unit. Temporal boundaries: the year 2021/ 2022.

3.3 Study tool:

To achieve the aim of the study, a questionnaire was used as a tool for collecting sample data.

First: Steps for designing the study tool:

It was built according to a set of steps as follows:

1- Examination of previous studies and literature related to the subject of the study, such as studies: Jaafar bin Shaflot (2018), as these articles contribute to giving an initial idea of how to measure the role of the Public Security Directorate in reducing cybercrime, and the paragraphs that the study reached were reformulated after international literature review in the form of measurable paragraphs in terms of taking into account the ease and clarity of paragraph construction.

2- The questionnaire was based on three areas: first, the role of the Public Security Directorate in raising awareness of cybercrimes, the second is the role of the Public Security Directorate in reducing electronic crimes, and the third is the obstacles facing the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime.

3.4 Validate the tool:

The indications of the validity of the questionnaire were verified by presenting it to (10) expert arbitrators in the field of cybercrime, and their directions and suggestions were taken to add new appropriate paragraphs, place the paragraphs in the field to which they belong, and delete some inappropriate paragraphs based on the agreement of (80%) of the opinions of the arbitrators. on it.

3.5 Statistical standard

A five-point Likert scale was adopted to correct the study tools, by giving each of its paragraphs one degree out of its five degrees (strongly agree, agree, neutral, disagree, strongly disagree) and it is represented numerically (5, 4, 3, 2, 1) on ranking, and the following scale has been adopted for the purposes of analyzing the results:

Table 2: Study scale

From 1.00 to 2.33	From 2.34 to 3.67	From 3.68 to 5.00
Small	Average	Large

The scale was calculated using the following equation:

(The upper limit of the scale (5) - the lower limit of the scale (1))/ the number of required categories (3) = (5-1)/3 = 1.33, and then adding the answer (1.33) to the end of each category.

3.6 The stability of the reduction of electronic crimes

To ensure the stability of the study tool, it was verified by the test-retest method by applying the scale, and re-applying it after two weeks on a group from outside the study sample consisting of (20), and then the Pearson correlation coefficient was calculated between their estimates in the two times.

The stability coefficient was also calculated using the internal consistency method according to the Cronbach alpha equation, and Table No. (2) shows the internal consistency coefficient according to the Cronbach alpha equation and the repetition stability for the domains and the overall level. These values were considered appropriate for the purposes of this study.

Table (3)

Cronbach's alpha internal consistency coefficient for domains and total score

Fields	Internal consistency
The role of the Public Security Directorate in raising awareness of cybercrime	0.84
The role of the General Mother Directorate in reducing cybercrime	0.80
Obstacles facing the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime	0.85

4. Study results and discussion:

4.1 Results of the first question, which reads: What is the role of the Public Security Directorate in raising awareness of cybercrimes on social media from the point of view of workers in the Anti-Cybercrime Unit in Jordan?

To answer this question, the arithmetic means and standard deviations were extracted. The role of the Public Security Directorate in raising awareness of cybercrime on social networking sites from the point of view of workers in the Anti-Cybercrime Unit in Jordan, and Table (4) illustrates this.

Table (4)

Arithmetic averages and standard deviations of the role of the Public Security Directorate in raising awareness of cybercrime on social networking sites from the point of view of employees of the Cybercrime Combating Unit in Jordan ranked in descending order according to the arithmetic averages

Rank	NO.	Item	Arithmetic Mean	Standard Deviation	Level
1	6	The Public Security Directorate works in continuous coordination with local community institutions in order to raise security awareness in combating cybercrime	3.52	1.501	Average
2	2	The Public Security Directorate is keen to host specialists in the field of cybercrime to benefit from their experience in raising awareness	3.48	1.480	Average
3	4	The Public Security Directorate is conducting awareness campaigns through its official pages in order to reduce cybercrime	3.38	1.578	Average

Rank	NO.	Item	Arithmetic Mean	Standard Deviation	Level
4	5	The Security Directorate is holding awareness sessions on how to use security social media in order to raise awareness of how to deal with it	3.31	1.590	Average
5	3	The Public Security Directorate publishes awareness flyers posters to reduce the dangers of cybercrime	3.23	1.529	Average
6	7	The Public Security Directorate prepares media materials (actual videos and plays) directed at the community to raise awareness of cybercrimes	3.14	1.456	Average
7	1	The Public Security Directorate is keen to hold awareness seminars on the topic of cybercrime for the local community	3.11	1.621	Average
		The role of the Public Security Directorate in raising awareness of cybercrime	3.31	1.381	Average

Table (4) shows that the arithmetic averages ranged between (3.11-3.52), where Paragraph No. (6) which states “The Public Security Directorate works in continuous coordination with local community institutions in order to raise security awareness in combating cybercrime” ranked first With an arithmetic mean of (3.52), while Paragraph No. (1) which reads “The Public Security Directorate is keen to hold awareness seminars on the topic of cybercrime for the local community” ranked last, with a mean of (3.11). The arithmetic average of the role of the Public Security Directorate in raising awareness of cybercrimes on social media from the point of view of the employees of the Anti-Cybercrime Unit in Jordan as a whole was (3.31). The results related to this question showed that the role of the Public Security Directorate in raising awareness of cybercrimes on social networking sites from the point of view of the workers in the Anti-cybercrime Unit in Jordan was medium, and the reason for this is from the point of view of the study that the Public Security Directorate was concerned with raising awareness of cybercrime The dangers of cybercrime, as the Department of Cybercrime Control has continuously paid attention to qualified administrative cadres and is keen to strive to advance work in combating crime of all kinds, especially cybercrime, because it has become a necessary requirement for the knowledge and technological revolution. This result can be explained by the fact that the Public Security Directorate is one of the institutions that achieve Its objectives through its officers and personnel, as the Criminal Investigation Department, in particular the Anti-Cybercrime Unit, combats electronic intrusions and works to spread culture and awareness in society of the dangers of electronic crimes. These results agreed with the study of Al-Zabin (2020).

4.2 The results of the second question, which reads: What is the role of the Public Security Directorate in reducing cybercrime on social networking sites from the point of view of workers in the Anti-Crime Unit in Jordan?

To answer this question, the arithmetic means and standard deviations were extracted for the role of the Public Security Directorate in reducing cybercrime on social networking sites from the viewpoint of the employees of the Anti-Crime Unit in Jordan, and the table below illustrates this.

Table (5)

Arithmetic averages and standard deviations of the role of the Public Security Directorate in reducing cybercrime on social networking sites from the point of view of the employees of the crime control unit in Jordan arranged in descending order according to the arithmetic averages

Rank	NO.	Item	Arithmetic Mean	Standard Deviation	Level Average
1	17	The security services respond as quickly as possible to complaints about cybercrime	3.57	1.541	Average
2	9	There is continuous follow-up of complaints filed regarding cybercrime	3.55	1.426	Average
3	18	Encouraging citizens to report cybercrime	3.45	1.531	Average
4	13	Directing legislation and laws in line with knowledge and technological development in order to reduce cybercrime	3.42	1.379	Average
5	16	The Public Security Directorate works to provide guarantees and protection to whistleblowers of cybercrime	3.37	1.557	Average
6	11	You use specialists to monitor websites and track abusers	3.35	1.430	Average
6	15	The Public Security Directorate activates the latest technology in order to track the perpetrators of cybercrime	3.35	1.504	Average
8	10	It uses an advanced media system to reduce the spread of cybercrime	3.23	1.423	Average
9	14	The Public Security Directorate introduces and trains teachers and students on how to exploit hackers. (hacking) them over the Internet	3.12	1.463	Average

10	12	The Internet links the institutions with the Anti-Cybercrime Unit in the Public Security Directorate	3.03	1.380	Average
11	8	There are deterrent policies (legislation and procedures) against perpetrators of cybercrimes	2.98	1.431	Average
		The role of the General Mother Directorate in reducing cybercrime	3.31	1.276	Average

Table (5) shows that the arithmetic averages ranged between (2.98-3.57), where Paragraph No. (17), which states that "the security services respond as quickly as possible to complaints regarding cybercrime," ranked first, with an arithmetic mean of (3.57). Paragraph No. (8), which reads: "There are effective deterrent policies (legislations and procedures) against perpetrators of cybercrime," ranked last, with an arithmetic mean of (2.98). The arithmetic average of the role of the Public Security Directorate in reducing cybercrime on social networking sites from the point of view of the employees of the Anti-Crime Unit in Jordan as a whole was (3.31).

The results related to this question showed that the role of the Public Security Directorate in reducing cybercrime on social networking sites from the point of view of the employees of the Anti-Crime Unit in Jordan was medium. This is due to the expansion of the technological space and the emergence of the problem of breaches and cybercrimes that require the Public Security Agency to intensify efforts to reduce electronic crimes. This result can be explained by the fact that the Public Security Directorate, and in particular the Anti-Cybercrime Unit, seeks to combat crime of all kinds and that it seeks to reduce the spread of crimes of all kinds, especially electronic crimes. These results agreed with the study of Jaafar Bin Shaflot (2018).

4.3 The results of the third question, which reads: What are the obstacles facing the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime?

To answer this question, the arithmetic means and standard deviations were extracted for the obstacles facing the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime, and Table (6) illustrates this.

Table (6)

Arithmetic averages and standard deviations of the obstacles facing the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime, arranged in descending order according to the arithmetic averages

Rank	NO.	Item	Arithmetic Mean	Standard Deviation	Level Average
1	26	Citizens' lack of awareness of the seriousness of cybercrimes	3.38	1.444	Average
2	28	Lack of material and human resources in the cybercrime unit	3.20	1.492	Average
3	22	The high financial cost of preparing the electronic crime awareness material.	3.15	1.406	Average
4	24	Ease of erasing evidence in electronic crimes	3.12	1.495	Average
5	20	Not employing technology in raising awareness is one of its drawbacks	3.02	1.505	Average
6	23	Society's culture and its lack of acceptance of the existence of cybercrime and citizens' reluctance to report cybercrime	2.91	1.411	Average
7	25	Absence of traditional visual evidence at the crime scene	2.89	1.491	Average
8	21	Institutions and companies focus on the primary role of work and not think about the negatives of social media	2.80	1.337	Average
9	19	Lack of cooperation between the Public Security Directorate and civil society organizations in conducting campaigns to educate society about cybercrimes	2.54	1.426	Average
10	27	Lack of technical and specialized skill of the employees of the cybercrime unit in dealing with cybercrimes	2.42	1.446	Average
		Obstacles facing the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime		1.146	Average

Table (6) shows that the arithmetic averages ranged between (2.42-3.38), where Paragraph No. (26), which stipulates "citizens' lack of awareness of the seriousness of cybercrime," ranked first with an arithmetic average of (3.38), while it came Paragraph No. (27), which reads: “Lack of technical and specialized skill among employees of the cybercrime unit in dealing with cybercrimes,” ranked last, with an arithmetic average of (2.42). The arithmetic average of the obstacles facing the Public Security Directorate in carrying out its role in raising awareness of the dangers of cybercrime as a whole was (2.94). The Public Security Directorate is striving to mitigate the obstacles facing the Anti-Cybercrime Unit in order to carry out its work to the fullest and in the best way. This result can be explained by the fact that the Public Security Directorate, and in particular the Anti-Cybercrime Unit, is making every effort, whether on the material, human or technical levels, to mitigate the obstacles and difficulties they face. In combating crime, especially electronic crimes, which have become the most prominent crimes of the era, these results agreed with the study of Jaafar Bin Shaflot (2018).

Conclusion:

In this research, I have dealt with the role of the Public Security Directorate in raising awareness of cybercrime on social networking sites from the point of view of employees in the Anti-Cybercrime Unit in Jordan. This result can be explained by the fact that the officers and personnel of the Public Security Directorate, especially the Cybercrime Unit, seek to combat all types of crime in order to maintain the security and stability of society in light of the technological revolution.

5. Recommendations and suggestions

In light of the findings of the study, we propose the following recommendations:

1- The study found that the level of the Public Security Directorate's role in raising awareness of cybercrime on social networking sites from the point of view of the employees of the Anti-Cybercrime Unit in Jordan was at a medium level; Therefore, work must be done to increase this potential by holding training courses and field workshops to activate the role of the Public Security Directorate in combating crime.

2- That the Public Security Directorate in general / the Anti-Cybercrime Unit adopt its role in raising awareness of cybercrime, in order to enhance its capabilities and raise its level in combating crime, especially cybercrime.

References:

Abu Ayada, Heba, and Al-Khatib, Maha (2022). Suggested educational ways to activate the role of social networks in developing cultural awareness among Jordanian university students after the Covid-19 pandemic**. Al-Zaytoonah University Journal for Human and Social Studies**. 3(1), 142-162.

Al-Anazi, Ibrahim (2019). The role of educational institutions in raising awareness of the dangers of cybercrime: a study of a sample of educational institutions for the secondary and university levels in Riyadh. **Journal of Security Research**, 28 (79). 79-13.

Al-Aqeel, Saleh (2022). Social awareness and cybercrime: a field study on a sample of individuals in the city of Buraidah in the Qassim region. **Journal of Humanities and Administrative Sciences**, 26(1), 44-68.

Al-Badaina, Diab (2014). Cybercrime: Concept and Causes, **Scientific Forum**, New Crimes in Light of Regional and International Changes and Transformations, College of Strategic Sciences, 4 (2).

Al-Dahla, Mahmoud, and Erekat, Ahmed (2018). **The role of the cybercrime unit page on Facebook in security awareness:** an analytical study, an unpublished master's thesis. Middle East University, Amman.

Al-Iraqi, Khaled (2022). Rumors and cyber crimes in the United Arab Emirates. **Journal of Fiqh and Legal Research**, 38(1), 155-208.

Al-Zabin, Ghadir (2020). Electronic crimes and the level of awareness of their seriousness - a field study on a sample of university youth**, Journal of the Islamic University of Islamic Studies,** 29 (2), 230-248.

Al-Zaher, Hanan and Al-Saleh, Ibtisam and Al-Taj, Ahmed (2022). The extent to which the element of publicity is achieved in the crime of the publicly indecent act through social networking sites. **Journal of Fiqh and Legal Research,** 37 (1), 1673-1702.

Bounaara, Yasmina (2015). Cybercrime, **Standard Journal**, Faculty of Fundamentals of Religion, Emir Abdelkader University of Islamic Sciences, Algeria, 39 (1), 31-50.

Chellach, Latifa, and Ibrahim, Qureshi (2017) “Suicide in cybercrime against persons in the Algerian environment”, **master’s thesis**. University of Mohamed Boudiaf, Algeria.

Cybercrime in Gulf society and how to confront it (2016), prepared by the Research and Studies Complex, **Sultan Qaboos Academy for Police Sciences**, Gulf Cooperation Council, General Secretariat, 14.

Diab, Maged (2021). The role of social networks in strengthening the culture of dialogue among Sudanese graphic designers. **Journal of Arts**, Literature, Humanities, and Sociology. 65(1), 232-255.

Dibs, Hani (2022). The relationship of cybersecurity management to reducing cybercrime from the viewpoint of employees of the Cybersecurity Center, the National Information Directorate for Information Security and Network Incidents. **Al-Mishkat Journal of Humanities and Social Sciences**, 9(2), 415-451.

Dughmush, Jihad Nizar. (2022). Cybercrimes committed through social networking sites. **Researcher Journal of Legal and Judicial Studies**, 39(1), 216-241.

Haimi, Sir (2022). Obstacles to the criminal investigation of electronic crimes. **Academic Journal of Legal and Political Research**, 6(1), 1734-1752.

Shaflout, Jaafar (2018). The Role of Saudi Universities in Combating Cybercrime from the Viewpoint of University Students: A Case Study of Naif Arab University for Security Sciences, **Journal of the College of Arts**, Port Said University, 12 (1), 4-20.

Eissat, Al-Omari, and Bouazza, Abdel-Raouf (2022). Cybercrime among adolescents: motives of turnout and mechanisms of social control. **Journal of Human and Society Sciences**, 11(1), 125-145.

Al-Ghadian, Suleiman (2018). Pictures of electronic blackmail crimes, their motives, and the psychological effects of it from the point of view of teachers, officials, and psychological counsellors, **Security Research Journal**, King Fahd Security College, Center for Research and Studies, 27 (69), p. 168.

Gharib, Magda, and Prince, Hassan (2017.) The extent of awareness among the young age group of the Saudi information crime penal system. **International Arab Journal of Informatics**: 3 (9) 07-50.

El Gheiri, Adam (2009). The concept of crime using the international information network, **Al-Rafidain Journal of Law**, University of Mosul, 20 (1), 332-333.

Mubaraki, Manal (2017) "Forms of Cybercrime Committed Through Facebook", **Master Thesis**. Larbi Ben Mahdi University - Umm El Bouaghi, Algeria.

Mobaideen, Dina and Al-Sheikh, Hanan and Al-Mashaqba, Saddam (2022). The impact of the proposed cybercrime law on media freedoms from the point of view of those in charge of media in Jordan. **Journal of the Association of Arab Universities for Research in Higher Education**, 42(2), 13-27.

Muhammad Ali, Muhammad Hussain (2017). The injustice of the method of organizing society in reducing the dangers of cybercrime among university youth: a study on the Youth Welfare Office, Al-Azhar University for Boys - Assiut, **Journal of Social Work**, 58 (1), 385.

Nouri, Saadoun (2011). Social factors influencing the commission of crime: a field study of the impact of social factors that lead to the commission of crime in the city of Ramadi, **Journal of Anbar University for Human Sciences**, 1 (1), 135

Hani, Deif Allah (2022**). The relationship of cybersecurity management to reducing cybercrime from the viewpoint of employees of the Cybersecurity Center**, the National Information Directorate for Information Security and Network Incidents. Al-Mishkat Journal of Humanities and Social Sciences, 9(2), 415-451