University of Benghazi … Faculty of Education

Journal of Faculty Education … The sixteen number December 2024

مجلة كلية التربية العلمية

Science Journal of Faculty of Education

THE REALITY AND PROSPECTS OF CYBERCRIMES AND THE EXTENT OF AWARENESS OF INTERNET USERS IN LIBYA

Aisha Saed Alatrash

Lecturer -Computer Department -Faculty of Education in Ajaylat

University of Zawia

واقع وآفاق الجريمة الإلكترونية ومدى وعي مستخدمي الإنترنت بها في ليبيا

عائشة سعيد الأطرش

محاضر –قسم الحاسوب –كلية التربية العجيلات– جامعة الزاوية

a.alatrash@zu.edu.ly

ABSTRACT

The use of the internet and information and communication technologies has been increasing significantly in Libya. Additionally, different social and economic activities are conducted online every day. As a result, this has led to critical concerns about the issue of cybercrime. Furthermore, the risks of cybercrimes vary and can cause economic and social harm, which can reach a high level. Therefore, this study aimed to introduce the reality of cybercrime in Libya and its prospects. As well as investigating the knowledge and awareness of internet users in Libya about this type of crime. The methodology used in this study was a questionnaire that targeted internet users in order to collect their knowledge about cybercrimes. There were 120 participants in the study. Additionally, the collected data were analyzed using SPSS (Statistical Package of Social Science). The results of this study showed that cybercrime exists in Libya. Although the discovered cybercrimes were not that dangerous, the potential of their spread and development is highly anticipated with the increasing involvement of technologies in all life activities. The results also showed that there are internet users in Libya who lack sufficient knowledge of the significant danger that cybercrimes could cause. Accordingly, the researcher presented some recommendations that could help eliminate the risk of cybercrime and protect internet users' data and privacy.

Keywords: cybercrime, cybercriminals, internet users, Libya, technology

الملخص

لقد تزايد استخدام الإنترنت وتكنولوجيا المعلومات والاتصالات بشكل كبير في ليبيا، بالإضافة إلى تزايد الأنشطة الاجتماعية والاقتصادية المختلفة عبر الإنترنت كل يوم، وبالتالي أدى ذلك إلى قلق كبير بشأن مسألة الجرائم الإلكترونية، حيث تتنوع مخاطر الجرائم الإلكترونية ويمكن أن تسبب أضرارًا اقتصادية واجتماعية قد تصل إلى مستوى عالٍ من الضرر، لذلك هدفت هذه الدراسة إلى التعريف بواقع وآفاق الجريمة الإلكترونية في ليبيا، كما هدفت إلى التعرف على مدى وعي وإدراك مستخدمي الإنترنت في ليبيا حول هذا النوع من الجرائم، كانت أداة الدراسة التي تم استخدامها عبارة عن استبيان استهدف مستخدمي الإنترنت من أجل جمع معرفتهم بالجرائم الإلكترونية، تكونت عينة الدراسة من 120 مشاركا، وتم تحليل البيانات التي تم جمعها باستخدام (الحزمة الإحصائية للعلوم الاجتماعية)، ولقد أظهرت نتائج هذه الدراسة وجود جرائم إلكترونية في ليبيا، وعلى الرغم من أن الجرائم المكتشفة لم تكن ذات خطر كبير، إلا أن إمكانية انتشارها وتطورها متوقع للغاية مع زيادة مشاركة التقنيات الحديثة في جميع أنشطة الحياة، كما أظهرت النتائج أيضًا أن هناك مستخدمين للإنترنت في ليبيا يفتقرون إلى المعرفة الكافية بالخطر الكبير الذي يمكن أن تسببه الجرائم الإلكترونية، وبناءً على ذلك قدمت الباحثة بعض التوصيات التي يمكن أن تساعد في القضاء على خطر الجرائم الإلكترونية وحماية مستخدمي الإنترنت وبياناتهم وخصوصيتهم.

الكلمات المفتاحية: الجرائم الإلكترونية، مرتكبو الجرائم الإلكترونية، مستخدمو الإنترنت، ليبيا،

التكنولوجيا

1. Introduction

Despite the importance of the internet and the advantages that information and communication technologies (ICT) provide for different life activities, the crimes registered daily through these technologies cannot be ignored. In addition, cybercrimes have been increasing and developing rapidly in developing countries due to the advancing development in ICT (Ksherti, 2010).

Libya is one of the developing countries where the internet quality and services were improved a few years ago, and therefore, the use of information and communication technologies, mainly social media networks, has increased. Furthermore, many activities started being conducted online, and numerous organizations, such as banks and shops, started providing their services via these technologies. Consequently, that may lead to occurring cybercrimes, as it has been cited that the growth of economic and social activities on the internet contributes to the cybercrime's spread and development (Lagazio et al. 2014; Mshangi et al. 2014; Ksherti 2010).

Therefore, internet users must be acquainted with these kinds of crimes and the danger they cause, be aware of unreliable online activities, and have sufficient knowledge of how to avoid being a victim of these crimes. Hence, the purpose of this paper is to present the reality of cybercrime in Libya by capturing the experiences and information provided by the research participants, in addition to investigating the awareness of internet users about cybercrimes, and then illustrating recommendations in order to eliminate them and prevent their future expansion and development.

1.1. Relevance of the Research

The topic of cybercrime has been considered an important area of research and this study contributes to expanding the literature review on this topic.

Furthermore, based on the realisation of the danger of cybercrime, as it is no less important than a crime on the ground, this study aimed to investigate the reality of cybercrime's existence in Libya and the extent of internet users' awareness of it. Furthermore, it clarified the importance of the awareness of cybercrime danger and its future spread in Libya.

1.2. Research Problem and Questions

As a result of the spread of using the internet in different social and economic activities in Libya, as well as the danger of cybercrimes that is globally recognised, this study concerned Libyan internet users' awareness of these crimes. Consequently, this study aimed to answer the following questions:

Q1- To what extent are internet users in Libya aware of cybercrimes?

Q2- What are the reality and prospects of cybercrimes in Libya?

2. Literature Review

In the era of the spread of information technology, everyone is more likely to fall victim to cybercrime. The spread of technology and modern means of communication is a double-edged sword (Lagazio et al. 2014). They can be used to facilitate communications around the world, and they are one of the most important means of transmission of different cultures around the world in order to bring the distances between countries and different civilizations closer. However, they can also be used to cause serious harm to specific individuals or entire institutions in order to serve personal goals (Wall, 2001). In addition, the growing advancement of information and communication technology portends the development of cybercrime tools and methods in a more complex or more harmful way than before (Chawki et al. 2015). Moreover, one of the reasons for cybercrime increase is the growing use of modern technologies with no or poor security awareness as well as the absence of regulations (El-Guindy, 2008). As a result, countries are obliged to develop mechanisms to combat these crimes, enact laws, educate people about the developments of these crimes, and encourage them to report them.

The risk of cybercrime is no less significant than a physical crime. There are similarities and differences between them (Dashora 2011; Chen & Davis 2006). The key difference is that cybercrime boundaries cannot be outlined as they may expand to different cities, countries, or even continents (Katos & Bednar, 2008). For example, a virus can affect many computers connected to the Internet from different places. Additionally, the identity of cybercriminals is difficult to recognize as they may use a faraway server, which is miles away from their physical location, to host illegal material or to attack victims (Katos & Bednar, 2008).

As comprehensive knowledge of cybercrime is necessary for cybercrime investigation (Chen & Davis, 2006), the following section clarifies the concept, types, tools, and characteristics of cybercrime. It also defines cybercrime perpetrators and their motives for perpetrating cybercrime. Moreover, possible methods discussed in previous studies that combat cybercrime and limit its spread are demonstrated.

2.1. Concept of Cybercrime

The notion of cybercrime does not completely differ from the notion of physical crime, as both include conducting acts that cause law-breaking (Dashora, 2011). Cybercrime is defined as every illegal behavior that is carried out using electronic devices (Clancy et al. 2007). Besides, it is described as criminal activities executed on the internet using computers (Chawki et al. 2015; Dashora 2011) and causes serious harm to individuals, groups, and institutions. In contrast to physical crimes, cybercrime occurs without the presence of the person who committed the crime at the crime scene, as it is conducted through computers and modern means of information and communication technology (Chawki et al. 2015).

Furthermore, cybercrime may perhaps aim to steal information and use it for self-benefit or to cause serious psychological (Dashora, 2011) and material harm to the victim. Additionally, it may seek to reveal important security secrets belonging to important institutions in the country or data of individuals (Wall, 2001) with the aim of blackmailing them and tarnishing their reputation to achieve material gains or serve political goals (Chen & Davis, 2006).

Cybercrime also includes the use of information without permission and privacy violations (Setiawan et al. 2018; Wall 2001), in addition to computer hacking, credit card fraud, cyberterrorism, hate speech, internet pornography, child sex abuse, and the danger of surveillance (Chawki et al. 2015; Broadhurst 2006; Wall 2001). The methods of cybercrime are almost unlimited, but many of them, in general, pursue the basic steps of scouting, getting access, and deception (Chen & Davis, 2006).

2.2. Types of Cybercrime

The common types of cybercrime conducted by attackers are highlighted in this section. First, cybercrime targets individuals to obtain their important and confidential information (Neufeld 2010; Mshangi et al. 2014). This includes identity theft (IC3 2020; Clancy et al. 2007; Chawki & Abdel-Wahab 2006), such as the theft of others' personal information, their e-mail addresses, or their account information. After that, the stolen information may be used to impersonate victims to conceal the identity of criminals (Chawki & Abdel-Wahab, 2006), defame the reputation of certain people, or spoil work relationships or social ones. This type of cybercrime also threatens individuals by hacking and stealing their very private information and then blackmailing them in order to earn money (Goodman & Brenner, 2002) and incite them to commit illegal acts.

Moreover, defamation is another type of cybercrime against individuals (Dashora, 2011) when a criminal uses stolen information, adds some false information, and then sends it through social media with the purpose of discrediting the victim and psychologically destroying them.

What's more, credit card fraud is a type of cybercrime (IC3 2020; El-Guindy 2008; Broadhurst 2006) that is committed by using credit card information (Dashora, 2011; Goodman & Brenner 2002; Wall 2001) for illegal payments or transactions.

Furthermore, harassment (Clancy et al., 2007), hate speech (Wall, 2001), and stalking (Dashora, 2011) conducted through the Internet and directed at specific people are types of cybercrime (Goodman and Brenner, 2002). Moreover, the spread of child pornography, sexual exploitation, and other offenses against internet users, especially children, are considered cybercrimes (Chawki et al. 2015; Mshangi et al. 2014; Dashora 2011; Wolak et al. 2008; Broadhurst 2006; Goodman & Brenner 2002; Wall 2001).

Other types of cybercrime are conducted against property (Neufeld, 2010), such as unauthorized access to computer systems (Dashora 2011; Clancy et al. 2007; Goodman & Brenner 2002) and the transfer of malicious software hidden in some applications and programs with the aim of damaging computers, electronic devices, or files of organizations, companies, or individuals.

There are also cybercrimes committed against organizations (Mshangi et al. 2014), including attacking official websites and government networking systems at the local and international levels. For instance, terrorist attacks on the Internet usually focus on destroying infrastructure and attacking computer networks that are against their position (El-Guindy, 2008) and often have a political goal (Dashora, 2011).

In addition, online terrorism and violent acts (Broadhurst, 2006) that aim to create fear are usually crimes committed for a political (Shinder & Tittel, 2002, cited at Chen & Davis, 2006), religious, or intellectual goal.

Furthermore, cybercrime does not necessarily include attacking specific targets; destructive programs such as viruses, worms, spyware, Trojan horses, and spam are instances of large-scale attacks directed toward as many systems as possible (Dashora 2011; Chen and Davis 2006; Goodman & Brenner 2002) and allow the swindling of a huge number of victims located around the world with less effort. What's more, phishing and spam are serious crimes (IC3 2020; Chawki et al. 2015), in which perpetrators use fake websites and deceitful emails to ask victims to change their passwords, verify their accounts (Stair & Reynolds, 2016), or send their private information (Chawki & Abdel-Wahab, 2006). Additionally, Trojan horses deceive the user to run it as it appears in the form of a useful and safe program, and its operation leads to disabling the infected computer (Chawki et al. 2015; Dashora 2011). Moreover, spyware gathers information from computers without the knowledge of its owners (Chawki & Abdel-Wahab, 2006). As well, viruses use executable files to spread into electronic devices and damage them, while worms infect electronic devices without the need for any action as they use system flaws to carry out their attacks (Dashora, 2011).

2.3. Characteristics of Cybercrime

- Cybercrimes are implemented with less effort compared to traditional crimes because they are executed via electronic devices from anywhere (Zhang et al. 2012).
- The ease of committing cybercrime away from security oversight (Chawki et al. 2015), as it is committed via a computer without anyone seeing criminals.
- The difficulty of detecting cybercrime and determining the extent of the damage caused by it (Zhang et al. 2012).

- Cybercrime is a cross-border crime as it can be conducted from anywhere and at any time (Sarre et al. 2018; Chawki et al. 2015) (i.e., both a criminal and a victim can be from different countries, and the time between them can differ).

2.4. Cybercrime Perpetrators

A cybercrime perpetrator is a person with technical skills specialized in information crimes who exploits their knowledge and skills in penetrating networks and security systems, luring others, and breaking passwords to obtain all the precious and valuable information. Besides, they can be divided into the following:

1. Hackers: Those can be amateur hackers or professional hackers (crackers) (Chawki et al. 2015; Chen & Davis 2006). Amateur hackers mean young adults who are fascinated by informatics and computers. They usually target unauthorized access to computer systems, breaking security barriers with the aim of expertise or curiosity (Dashora, 2011). Whereas, professional hackers (crackers) are specialists in the field of technology (Dashora, 2011) and are more dangerous and usually work in groups.

2: Haters: They are also called the Avengers, who inflict harm in return for injustice and damage. Additionally, most of their activities are carried out using viruses and malware to damage and destroy information systems. For instance, depressed employees who have been dismissed from employment or are unsatisfied with their employer or the place in which they work or used to work, and therefore, to take revenge, hack the system of their work (Chawki et al. 2015; Dashora 2011).

3: Extremists: An extremist in this field is defined as a person who uses the internet to publish and broadcast intellectual materials that feed intellectual extremism, in addition to creating websites that facilitate their transfer and promotion. Extremists also include terrorist groups that use social media networks to plan their activities, publish their thoughts, and encourage others to follow them (El-Guindy, 2008). These people usually communicate through the Internet and use all websites that seek to achieve propaganda purposes in their favor (El-Guindy, 2008).

4: Spies: They target information systems to acquire secret information about an organization or individual to achieve self-benefit, sell it, or send it to competitors (Nykodym et al. 2005).

2.5. Motivations for Perpetrating Cybercrime

- Money motivation of the desire to achieve wealth is considered one of the main factors in perpetrating cybercrimes (Li 2017; El-Guindy 2008).
- Personal motivation when perpetrators devote their time to learning how to hack banned websites and security systems (Li, 2017).
- Motivation for revenge (Sabillon et al. 2016; Shinder & Tittel, 2002, cited at Chen and Davis, 2006) is one of the most dangerous motivations that can benefit a person who has abundant information about the institution or company in which he/she works or used to work (Li, 2017).
- Amusement and fame motivation is committing a crime for the purpose of entertainment or fame and not intending to cause harm (Sabillon et al., 2016; Shinder & Tittel, 2002, cited at Chen & Davis, 2006).
- Political motivation often takes place on anti-government political websites that distribute fabricated news and information about officials (Chen & Davis, 2006). This is among the most prominent attempts to overthrow officials or their governments in various countries around the world (Li, 2017).
- Terrorist motivation is to use the internet for many terrorist activities such as recruitment, financial support, and psychological war (El-Guindy, 2008).

2.6. Methods of Combating Cybercrime and Limiting its Spread

Cybercrimes are difficult to completely prevent even through the implementation of legislation; therefore, the likely step to reduce cybercrimes is to educate people and raise their awareness of cybercrimes when they use their devices (Dashora, 2011). Additionally, anyone can avoid being a victim if he or she avoids certain wrong activities and behaviors on the internet (Goodman & Brenner, 2002, cited at Chawki et al. 2015). The following steps can protect people from being victims:

- It is necessary to verify the address of any email that requires private information (Cropf & Bagwell, 2016), such as a credit card or a bank account.
- Avoid opening any emails from unknown sources (Cropf & Bagwell, 2016) that may lead to hacking computers and stealing all personal information, accounts, and passwords stored in them.
- Passwords should not be disclosed to anyone or any website (Dashora, 2011), and they should be unfamiliar and changed frequently to ensure not to fall into the wrong hands (Johansen, 2020).
- Do not save personal photos on the computer (Chaib, 2022) and other electronic devices, especially those that are connected to the Internet.
- Avoid posting personal photos or personal information publicly on social networking sites or any other sites so that they are not exposed to theft by cybercriminals (Johansen 2020; Dashora 2011).
- Not to download any file or program from unknown resources (Chaib, 2022), and avoid using any unreliable software in order to save devices and personal accounts from being hacked.
- Ensuring that operating systems and security systems are updated and installing security programs such as antivirus and antimalware programs limit electronic intrusion, viruses, and other malware and maintain the safety of users' devices and the confidentiality of their information (Johansen 2020; Dashora 2011).
- Governments and relative organizations should track cybercrimes and develop strict legislation to combat them, as cybercriminals will remain unafraid if related laws are not clear or strictly executed (Aboud, 2012).
- Educating people about cybercrimes, as it was stated that people’s knowledge of data security is essential (Whitman & Mattord, 2004, cited at Aboud, 2012). Aboud (2012) added that people will discover more cybercrimes if they have enough knowledge about data security.
- Cybercrimes should be reported to the authorities, because when they remain ignored and unreported, the perpetrators will continue repeating cybercrimes (Aboud, 2012).
- Always be careful of what your children access on the Internet to protect them from any kind of stalking, exploitation, or harassment (Johansen 2020; Dashora 2011).

2.7. Cybercrimes in Libya

In many developing countries, cybercrimes are not reported mostly because of the lack of cybercrime regulations, the lack of citizens’ awareness about cybercrime and data security (Aboud, 2012), and organizations’ fears of losing customers (Mshangi et al. 2014) and reputation (Aboud, 2012). In Libya, although cybercrime exists, no official record of the number of crimes conducted online was found. The reasons behind this may be the same reasons mentioned above or due to the low rates of cybercrime in this country.

The existence of cybercrimes in Libya can be noticed on social media networks, such as abusive activities including defamation, harassment, hate speech, promoting destructive and harmful ideas to society, and illegal impersonation of others, especially officials. Additionally, it has been cited that electronic blackmail cases have increased recently in Libya, and the Libyan authority announced the arrest of people who lured girls on social media sites and blackmailed them for money (Osama Ali, 2024). The authority called on citizens to report any electronic threat or blackmail attempts they are exposed to through social media, warning them against dealing with untrustworthy or unknown people to avoid falling victim to such crimes (Ibid.).

Moreover, the Libyan House of Representatives officially published the Anti-Cybercrime Law on 27 September 2022 (The Law Society of Libya, 2022). The law stresses the need to protect electronic transactions and aims to reduce the occurrence of cybercrimes by identifying these crimes and enacting deterrent penalties for them in a way that helps achieve justice and information security and protects the system and public morals (Ibid.). However, the Defender Center for Human Rights (DCHR) and 18 human rights groups argued the Libyan House of Representatives to immediately repeal cybercrime law because it threatens freedom of expression (Defender Center, 2022). Human Rights Watch (2023) has also urged the repeal of the “repressive” cybercrime law, arguing that it restricts freedom of opinion and criminalizes peaceful expression as the law includes vague and overly broad definitions, which could lead to prosecutions for nonviolent expressions and punishment with up to 15 years in prison and significant fines.

3. Research Methodology

This study applied the quantitative approach. Data from the literature review was used to construct the items of the research instrument. The collected data were analysed using a statistical package for social sciences (SPSS).

3.1. Research Instrument

A questionnaire was used to collect data relative to the study. The questionnaire was designed using Google Forms. It contained three parts, each consisting of simple statements and questions so that participants of different ages and educational levels could answer them. The first part of the questionnaire asked about demographic information. Besides, in order to answer the first research question, the second part consisted of 10 statements with a three-point Likert scale measuring participants’ attitudes toward the use of ICT and the Internet. The scale was rated as 1 for no, 2 for sometimes, and 3 for yes. Furthermore, the third part contained ten items of criminal cases selected from the literature review. In this part, a multiple-choice question form was used to enable participants to select each case they experienced while using the Internet. This part helped investigate the existence and reality of cybercrimes in Libya. Finally, the questionnaire ended with an open-ended question asking participants if they would like to add additional information or notices related to the study.

3.1.1. Reliability of the Questionnaire

To ensure the validity of the questionnaire, specialists in the field of this study were invited to revise the questionnaire and provide comments to improve it. Furthermore, in order to test the internal consistency of the questionnaire, the Alpha Cronbach value was measured and applied to a pilot sample of 30. As shown in Table 1 below, the value of Cronbach’s alpha was 0.810, indicating a good level of reliability. Therefore, the questionnaire was ready to be conducted.

Table 1: The result of the reliability test of the questionnaire

Cronbach's Alpha	N of Items
.810	10

3.2. Research Participants

The questionnaire link was shared with Libyan internet users on social media groups and was also sent via email. There were 120 responses from different demographic characteristics, which are shown in the following charts:

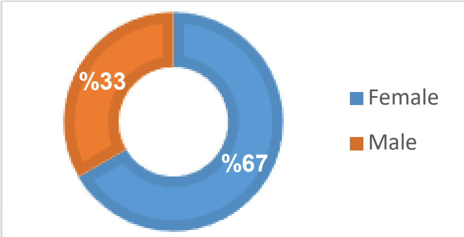

Fig. 1: Gender of the participants

It is noticeable from Fig. 1 that the majority of research participants were females (67%) while just 33% of them were males

.

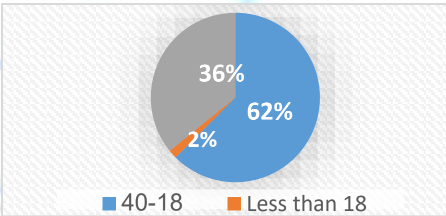

Fig. 2: Age groups of the participants

As shown in Fig. 2, the participants varied in age and most of them (62%) were in the 18–40 age group. while 36% of them were in the age group of more than 40 years old and only 2% of them were under 18 years old.

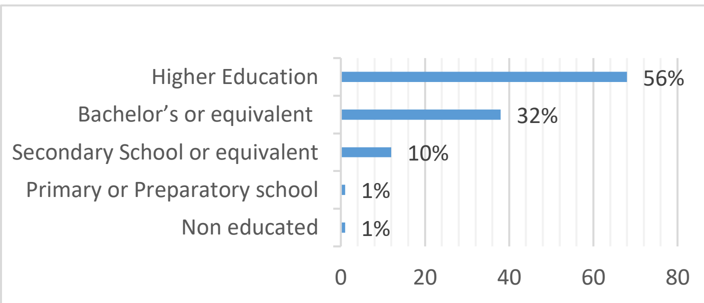

Fig. 3: Education level of the participants

Regarding the educational level of participants, Fig. 3 above demonstrates that nearly all participants were educated (56% higher education, 32% bachelor's degree or equivalent, 10%

secondary school or equivalent, 1% still in primary or preparatory school), while 1% were uneducated.

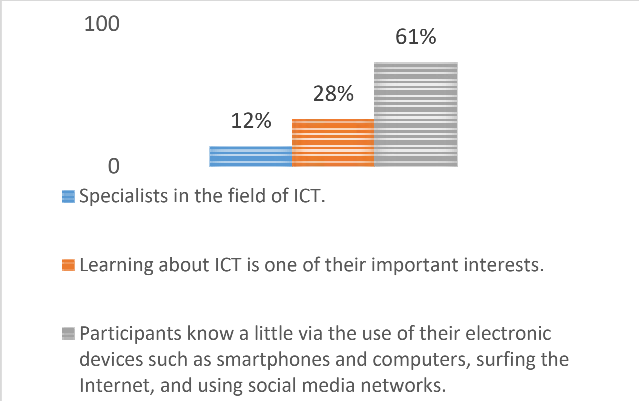

Fig. 4: Participants' knowledge about ICT

On the subject of participants' knowledge of information and communication technology (ICT), Fig. 4 above illustrates that 61% of the participants have little knowledge of using their electronic devices such as smartphones and computers, surfing the Internet, and using social media networks. While 28% of them stated that learning about ICT is one of their interests and 12% of them were specialised in the field of ICT.

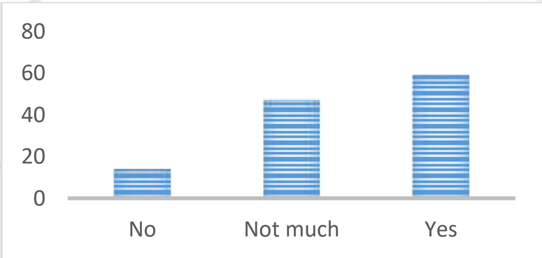

Fig. 5: Participants' understanding of the cybercrime concept

In addition, fig. 5 demonstrates that 49% of participants understood the concept of cybercrime, its seriousness, and the possibility of being a victim, 39% of them had little understanding of it, while 12% had no understanding at all.

3.3. Data Analysis

The collected data were analysed using SPSS. Descriptive statistics (frequencies, percentages, means, and standard deviation) were used to answer the research questions.

4. Results and Discussion

4.1. Participant's Behaviour on the Internet

This section discusses the behavior of participants on the Internet in order to answer the first research question: "To what extent are Internet users in Libya aware of cybercrimes?" The results of participants' behavior in this study were divided into three parts: participants' behavior while using the Internet, participants' behavior while using electronic accounts, and participants' behavior on social media networks, each of which is summarized in the following tables along with their related statistics.

Table 2: Participants' behaviour during using the Internet

Items	No	Sometimes	Yes	Mean	Std. d.
Participants save their private photos and information on their smart devices that connected to the Internet.	31	27	62	2.2583	0.8451
	25.8 %	22.5%	51.7%		
Participants download files from any website regardless its reliability and safety.	60	37	23	1.6917	0.7756
	50%	30.8%	19.2%		
Participants click on pop-up ads when they surf the Internet.	80	25	15	1.4583	0.7088
	66.7%	20.8%	12.5%		
Participants use the auto saving features of their password on all websites that they visit regardless their security level.	50	42	28	1.8167	0.7884
	41.7%	35%	23.3%		

Table 2 above shows that approximately half of the participants (51.7%) save their private photos and information on their smart devices connected to the Internet. As a result, this behavior could expose their private information to being stolen and used illegally. Moreover, 50% of participants do not download programs and files from any website, while 30.8% of them do that sometimes and 19.2% do that without taking into consideration the reliability and safety of these websites. Besides, 66.7% of participants do not click on pop-up ads that suddenly appear when they surf the Internet, while the rest of them click always (12.5% of participants) and sometimes (20.8% of participants). The key danger of pop-up ads represents redirecting users to other unsafe or bad content websites or trying to force them to download unsafe or bad materials. What's more, 41.7% of the respondents do not auto-save their password on all websites they visit when they are not sure about their safety, whereas the rest 35% of them do that sometimes and 23.3% of them always do.

Table 3: Participants' behaviour during using electronic accounts

Items	No	Sometimes	Yes	Mean	Std. d.
Participants do not change their password and security setting, in case someone helps them create any of their electronic accounts.	86	16	18	1.4333	0.7417
	71.7%	13.3%	15%		
Participants do not make sure whether they want to select the option of auto backup all files or not, when they create an account such as Gmail or iCloud.	42	40	38	1.9667	0.8192
	35%	33.3%	31.7%		
Participants share with others the use of their electronic accounts such as Gmail or iCloud, especially in smartphones.	98	16	6	1.2333	0.5303
	81.7%	13.3%	5%		
Participants open links and attachments they receive regardless they know the sender or not.	61	45	14	1.6083	0.6896
	50.8%	37.5%	11.7%		

The participants' behaviour while using their electronic accounts is illustrated in Table 3 above. It can be noticed that the majority of participants (71.7%) change their password and security settings, in case someone helped them create their electronic accounts such as social media accounts, Gmail, and iCloud. While the rest of them do not change their passwords and are exposed to leaking their private information, which could include some sensitive information that criminals can exploit to threaten or blackmail them.

Additionally, the table shows that 34% of participants make sure to check or uncheck the automatic backup option for their data when they create an account such as Gmail, 31.7% of them are not sure whether to check it or not, and 33.3% of them are sometimes not sure to check this option. The reason why people do not care about this important option is that they usually do not care of such details in addition to their lack of awareness of cybercrimes. Furthermore, this option could help criminals reach private information backed up on accounts they have accessed without permission.

Moreover, the major participants (81.7%) do not share the use of their electronic accounts with others (family and friends), which helps protect their information from being reached, especially when they select the option to back up information on their accounts. While the rest of the participants who share the use of their electronic accounts with others are likely to be exposed to this danger.

Finally, most of the participants (50.8%) are cautious about opening links and attachments received in their mailboxes when they do not know the senders. While some of them (37.5%) open them sometimes, and the rest (11.7%) open them all the time. Opening links and attachments sent from unknown senders will expose receivers to being redirected to other unreliable and bad content websites, as well as their information will be in danger in case they type it into unknown linked websites, which may imitate an official organisation such as a bank website.

Table 4. Participants' behaviour on social media networks

Items	No	Sometimes	Yes	Mean	Std. d.
Participants post many of their information and personal photos publically on social media networks	91	21	8	1.4250	0.6567
	75.8%	17.5%	6.7%		
Participants add or confirm all friends' requests on social media networks even from strangers.	80	29	11	1.3083	0.5911
	66.7%	24.2%	9.2%		

Regarding the participants' behavior on social media networks, Table 4 above shows that 75.8% of the sample do not post much of their personal information and photos publically on social media networks, whereas 6.7% of them post much of their information, and 17.5% of them do so sometimes. Avoiding posting personal information will protect users from being impersonated. .

What's more, 66.7% of the participants were cautious about not adding or confirming all friend requests on social media networks, while 9.2% of them accept all friend requests even from strangers, and 24.2% of them do so sometimes. Adding strangers to a user's social media account will allow them to know everything the user posts, as well as monitor their behavior on social media networks, which will help cybercriminals use their information or impersonate them.

4.2. Participant's Experience Online

This section discusses participants' online experience in order to answer the second research question: "What is the reality and prospects of cybercrime in Libya?" The key results of this section are summarized as follows:

- Malware infection was the most common attack, with 26.7% of participants responding that one of their electronic devices had been exposed to malicious software.
- 7% of participants were subjected to defamation and denigration.
- 3% of them were exposed to impersonation on the Internet for some reason (to gain self-benefit, to tarnish their reputation by publishing immoral content or spreading rumors, or to attack others for the purpose of sedition).
- 25% of participants received anonymous content that was immoral, called for religious extremism, followed political trends, incited illegal acts, or otherwise.
- 2% of respondents answered that their photos and private information had been posted online without their permission.
- 3% of them were threatened or blackmailed by publishing their private information, such as photos, to force them to do illegal or immoral acts or to get money from them.
- 2% of them had their electronic devices or accounts hacked or subjected to hacking attempts.
- 7% of the sample fell victim to online fraud or lost money.
- 5% of the respondents were exposed to suspicious or criminal situations other than those mentioned above.
- More than half of the respondents (57.5%) had not experienced any suspicious or criminal situation while using the Internet.

Regarding the open-ended question at the end of the questionnaire that asked participants whether they would like to add any experience, information, or notices related to the research topic, the following answers were received:

- Internet users should strengthen their security settings and not share their privacy.
- Conducting lectures and seminars to raise Internet users' awareness of the extent of the dangers related to cybercrimes.
- There must be security management and specialist organizations that follow cybercrimes, catch criminals, and punish them.
- There should be an official website or application that simulates the electronic police and allows receiving reports, determining and accessing the location of criminals, and protecting victims.
- Hacking emails via fake links is one of the most common cybercrimes in Libya.
- Cybercriminals sometimes lure victims to immoral websites via fake links to educational websites.

5. Conclusion

The study results revealed the existence of some cases of cybercrime in Libya, which are likely to continue and develop in the near future. In addition, there is no doubt that new cybercrimes will appear with the continuous advancement of technology, and therefore, information security software must always be updated to recognize and prevent them. Internet users in Libya should learn from others and from experiences around the world and prepare themselves for the possible increasing development of cybercrime in the country.

Furthermore, the key finding of this study showed that some Internet users in Libya do not have enough knowledge about cybercrimes and are not aware of the dangers they may cause. They are also unaware of the types of cybercrimes they may face while using the Internet. In addition, some of them have never heard about cybercrimes, which may not be highly dangerous at present, but their danger will increase and develop with the advance of technological development. What's more, as cybercrime is still unfamiliar behavior to many people, victims can be lured easily. As a result, the Libyan government must play a role in eliminating cybercrimes and preventing their spread. Likewise, organizations should be established with the aim of educating people about the dangers of cybercrimes, how to confront them, and how to prevent falling victim to them. Finally, security in cyberspace is essential, as if cyberspace is not secure, it will affect the lives of Internet users and therefore the entire society.

6. Recommendations

Everyone is responsible for contributing to combating and confronting cybercrimes, so it is recommended to follow the methods of combating cybercrimes mentioned in the literature review. Likewise, organizations must make efforts to eliminate this kind of crime and prevent its development; therefore, the researcher recommended the following:

- Conducting further studies related to cybercrime in Libya. In addition, educational institutes and related organizations should conduct regular surveys to measure users' awareness of cybercrimes and accordingly prepare lectures, workshops, and symposiums with up-to-date and useful content. Besides, regular surveys help in reporting any new type of cybercrime and thus help in monitoring the progress of cybercrime development in Libya.
- It is important to provide internet users with sufficient knowledge about the risks of cybercrimes and how to avoid becoming a victim of them. In addition, using the media to raise people's awareness of the seriousness of cybercrimes will play a key role.
- The government and related organizations should develop ways and means to track cybercrime in the country accurately. They should also consider enacting relevant penal laws for cybercriminals and amending them regularly or as required to reduce the risks of cybercrimes and limit their spread.
- Everyone should be careful when dealing with foreign people or unknown companies online.
- Firewalls should always be activated and updated to protect people online.

7. References

Aboud, S.J (2012) An overview of cybercrime in Iraq. The Research Bulletin of Jordan ACM, 2(2), pp 31- 34.

Broadhurst, R. (2006) Developments in the global law enforcement of cyber-crime. An International Journal of Police Strategies and Management, 29(2), pp. 408-433.

Chaib, N. (2022) Strategic mechanism of combating cybercrime under the new environment of digital communication. Law and Political Science Journal, 8(2), pp. 710-718.

Chawki, M. et al. (2015) Cybercrime, Digital Forensics and Jurisdiction. Switzerland: Springer International Publishing.

Chawki, M. and Abdel-Wahab, M. (2006) Identity theft in cyberspace: issues and solutions. Lex Electronica, 11(1).

Chen, T. and Davis, C. (2006) An overview of electronic attacks. In: KANELLIS, P. (ed.) Digital Crime and Forensic Science in Cyberspace. London: Idea Group Pub, pp. 1–26.

Clancy, T.K. et al. (2007) Combating Cybercrime: Essential Tools and Effective Organisational Structures, A guide for Policy Makers and Managers. National Center for Justice and the Rule of Law: The University of Mississippi School of Law.

Cropf, R.A and Bagwell, T.C. (2016) Ethical Issues and Citizen Rights in the Era of Digital Government Surveillance. USA: IGI Global.

Dashora K. (2011) Cyber Crime in the Society: Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences, J 3(1), pp. 240-259.

Defender Center (2022) *Libya: DCHRA and 18 human rights groups call for immediate repeal Anti-Cybercrime Law due to its threats to freedom of expression* [WWW] Defender Center for Human Rights. Available from:

https://defendercenter.org/6797 [Accessed 7/8/2023]

El–Guindy, M. (2008) Cybercrime in the Middle East. ISSA Journal, 17 (June), pp. 16-19.

Goodman, M.D. and Brenner, S.W. (2002) The emerging consensus on criminal conduct in cyberspace. International Journal of Law and Information Technology, 10(2), pp. 139-223.

Human Rights Watch (2023) *Libya: Revoke Repressive Anti-Cybercrime Law* [WWW] Human Rights Watch. Available from:

https://www.hrw.org/news/2023/04/03/libya-revoke-repressive-anti-cybercrime-law [Accessed 5/11/2023].

IC3 (Internet Crime Complaint Centre) (2020) Internet Crime Report [WWW] Federal Bureau of Investigation. Available from: https://www.ic3.gov/Home/AnnualReports [Accessed 17/10/2023]

Johansen, A.J. (2020) 11 ways to help protect yourself against cybercrime [WWW] Norton. Available from: https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html [Accessed 19/10/2023]

Katos, V. and Bednar, P.M. (2008) A cyber-crime investigation framework. Computer Standards & Interfaces, 30 (May), pp. 223-228.

Ksherti, N. (2010) Diffusion and Effects of Cyber-Crime in Developing Economies. Third World Quarterly, 31(7), pp. 1057-1079.

Lagazio, M., Sherif, N. and Cushman, M. (2014) A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers and Security, pp. 1-32.

Li, X (2017) A Review of Motivations of Illegal Cyber Activities. Criminology and Social Integration Journal, 25(1), pp. 110-126.

Mshangi, M., Nfuka, E.N. and Sanga, C. (2014) The Rapid Growth of Cybercrimes Affecting Information Systems in the Global: is this a Myth or Reality in Tanzania? International Journal of Information Security Science, 3(2), pp. 182-199.

Neufeld, D.J. (2010) Understanding Cybercrime. In: Proceedings of the 43rd Hawaii International Conference on System Sciences, January 2010. US: IEEE Computer Society, pp. 1-10.

Nykodym, N., Taylor, R. and Vilela, J. (2005) Criminal Profiling and Insider Cybercrime. Digital Investigation, 2, pp. 261-267.

Osama Ali (2024) The growing threat of cybercrime in Libya. *The new Alaraby*, 25th Feb, pp. 17.

Sabillon, R. et al. (2016) Cybercrime and Cybercriminals: A Comprehensive Study. International Journal of Computer Networks and Communications Security, 4(6), pp. 165–176.

Sarre, R., Lau, L.Y. and Chang L.Y.C. (2018) Responding to cybercrime: current trends. Police Practice and Research, 19(6), pp. 515–518.

Setiawan, N. et al. (2018) Impact of Cybercrime in E-Business and Trust. International Journal of Civil Engineering and Technology, 9(7), pp. 652–656.

Shinder, D. and Tittel, E. (2002) Scene of the cybercrime: Computer forensics handbook. Rockland, MA: Syngress Publishing.

Stair, R.M. and Reynolds, G.W. (2016) Principles of Information Systems. 12th ed. USA: Cengage.

The Law Society of Libya (2022) *Law No. 5 of 2022 Regarding Combating Cybercrimes* [WWW] The Law Society of Libya. Available from:

https://lawsociety.ly/en/legislation/law-no-5-of-2022-regarding-combating-cybercrimes/ [Accessed 1/8/2024].

Wall, D. (2001) Cybercrimes and the Internet. In: WALL, D.S. (ed.) *Crime and the Internet*. London and New York: Routledge, pp. 1-17.

Whitman, M. and Mattord, H. (2004) *Management of Information Security*. Boston: Course Technology.

Wolak J, et al. (2008) Online "Predators" and Their Victims. *American Psychologist*, 63(2), pp. 111–128.

Zhang, Y. et al. (2012) A survey of cybercrimes. Security and Communication Networks, 5, pp. 422–437.