Int. J. Advance Soft Compu. Appl, Vol. 12, No. 3, November 2020
ISSN 2074-8523; Copyright © ICSRS Publication, 2020
www.i-csrs.org

Cyber-Crime Effect on Jordanian Society

Haya Al-Masalha[1], Adnan A. Hnaif[2], and Tarek Kanan[3]

Al-Zaytoonah University of Jordan, Jordan
email: [1]h.masalha@zuj.edu.jo, [2]adnan_hnaif@zuj.edu.jo, [3]tarek.kanan@zuj.edu.jo

Received 1 May 2020; Accepted 3 August 2020

Abstract

Due to the increasing use of social media applications, it is essential to ensure that the connection is secure because sometimes it is required to fill secret information such as username and password. Many anonymous messages reach to the computer client, which may contain Trojan, virus (Malware). If the user is not an expert in the field of information security, then the user will open the incoming messages without ensuring its integrity, which allows hackers to enter the devices and planting malicious software in the client devices without their knowledge. In this paper, we will identify the concept of syntactic attack and its types, which leads to Cyber-Bullying attack—and also discussing the effect of penetration of devices on the Jordanian society. As shown in the result, the most common electronic crimes are crimes related to defamation, threats and extortion. The results also show the prevalence of Cyber-crime in densely populated places. Besides, Cyber-crime decreases in the regions where clans and tribes live. At the same time, the most age groups that have been exposed to electronic crimes are the groups 18-29 and 30-44.

Keywords: *Cyber-attack, Cyber-Bullying, Phishing, Semantic attack, Syntactic attack.*

1 Introduction

In the world of modern networks, the devices are connected. Hence the users can exchange online data, chat with each other, playing games, watching movies buying and selling online etc.

Due to the existence of many hardware or software applications (Cyber-attacks) that can be used to hack or spy on devices, it is imperative to ensure that the system environment is secure and non-invasive. Cyber-attacks are divided into two types: Syntactic attack and Semantic attack [1]. The Syntactic attack is also called Malware, which defined as a software program planted in the devices for data theft without the knowledge of the user [2]. The following are some examples of malware: Trojan horse or Trojan virus, computer viruses, worms, keyloggers, rootkit and adware [3].

Trojan horse or virus is the most dangerous type of Malware; it gives complete access to the victim's device rather than destroying files [3]. Meanwhile, a computer virus is a program designed to infect the computer, and once the computer becomes infected, this program copies or reproduces itself and it needs another host to be attached to infect a computer [3]. Worms are similar to the computer virus but do not need another host to attach to in order to infect a computer. Worms are considered a significant threat to computer networks [4].

A Rootkit is a hidden program in the operating system that destroys the devices. This program runs without restriction. It can control the ACL (Access Control List) one of the features of the Windows operating system and thus control the software that can be installed on the computer [4]. Rootkit program is invisible to all applications running on the computer and cannot be seen in the list of applications that can be removed or updated.

Adware is an advertisement that appears to computer users; these ads may contain malicious software or spyware programs that harm the computer system [5].

In addition, a keylogger is a hardware or software program, which used to record all inputs to the device or any website that has been visited in a particular file to monitor the device and send the critical data to the intruder without the user's knowledge [6].

Keylogger used to spy on users of computers or mobile devices. Keylogger applications stores every keystroke pressed in the keyboard in a particular file, which has been planted in advance in the infected device. Then the device automatically sends the file to a particular Email address for a specific period. This type of spyware cannot be detected manually or even using an anti-virus, because no suspicious behaviour can be detected, and hence make the seriousness of this type of snooping [7]. Keylogger is also invisible to all applications running on the background and cannot be seen in the list of applications that can be removed or updated. The keylogger divided into two types, software and hardware. The hardware is a device placed between the keyboard and the (I/O) Units to record the keyboard strokes in a particular file.

While software keylogger is the installation of an invisible application directly in the device of the user so that the application is linked to the operating system of the victim's device records keyboard strokes in a particular file to be sent later via email to the intruder. This application cannot be seen in the list of programs installed in the device or even using anti-viruses [7].

On the other hand, Semantic attack such as Phishing depends on exploiting weaknesses in the users' systems or devices to trick the victim. Phisher is a type of intruders how are trying to steal sensitive users' information such as username and password by using a variety of forms to fool the victim—for example receiving an email, fake link or attachment, or voice call.

Intrusion Detection System (IDS) is a system that can be used to detect and prevent this type of attack. The IDS has two methods to detect the intruders: First: signature-based. Second: behaviour-based detection engine [8]. The signature-based detection engine depends on the use of any exact string matching algorithms to find a match between the device files and the database predefined. This type of detection has one limitation, which is needed to update the database continuously to detect the new possible software attack. The behaviour-based detection engine uses the features, attributes, and methods that the intruders may use. This type is considered more effective than the signature-based detection engine.

Ultimately, if the intruder can penetrate the victim's device with any of the previous software applications or hardware, then the victim could be exposed to Cyber-bullying. Cyber-Bullying defined as using the means of social media, mobile phones, and video games in an immoral and bad way. Cyber-Bullying happened by sending SMS messages, images, and videos in a hostile and offensive way. The target of Cyber-Bullying is to make others feel humiliated, in addition to irritating and threatening them. Cyber-Bullying involves sharing pornographic contents without the permission of people, spreading rumours and redirecting ruthless content. Cyber-bullying has very adverse possessions on the victims, including problems in establishing friendships and social connections, loneliness, low self-esteem, depression, suicide due to threat or self-deprecation, etc.

2 Related Work

This section is divided into two subsections: The first section is related to detect and prevent hackers, and the second section is related to Cyber-Bullying.

2.1 Detect and prevent Hackers

Akhil S et al. [9] have developed a server that detects and prevent a keylogger within the local network. It monitors and collects all the data sent between the devices if a device sends an email to a suspicious email address within a specific time, which means that the device contains a keylogger. Then the server immediately closes the port from which the information is sent to the email address, and also removes the keylogger from that device.

Christopher A et al. [10] have designed and build a strategy for discovering keylogger depending on: The infected medium, type of target device, lifetime of keylogger and the level of stealth. The keylogger can be a software to be placed in the operating system or through the hardware, examples of keylogger development are through the web browser exploit software, where the attacker attacks the buffer (buffer overflow) and allows malicious code to execute. If the device becomes infected, a variable is implemented to store the keystroke, and accordingly, an attack can obtain the file in which the data is stored.

S.vinothkumar et al. [11] designed a model to discover the keylogger, which contains three components: A component for the mobile application and its permission, permission analyzer and keylogger detector. The first component identifies applications and permissions for each application installed on the device. The second component analyses the permissions for applications that want to access the device files through SVM (Support Vector Machine) for training on uninfected applications. The third component detects the keylogger by machine learning, and when detecting the keylogger, it works its disable directly.

Tasabeeh O. M. Ali et al. [12] have proposed a technique to detect the keylogger, which is trying to steal any sending email by recording the keystroke in a special file and send it to a particular destination. [12] have also proposed to create three layouts in a way, that each character has its symbol. In each time, a random layout will appear based on the character pressed. For example, when clicking on any character in the keyboard, the system creates a special code for that character and specify which layout of the third layouts should appear where the three layouts have the same symbol shuffled. Thus, the intruders will not be able to know exactly which character has been clicked.

Donghai Tiana et al. [13] developed a two-stage program to detect the keylogger. The first stage is to isolate the keyboard drivers from the OS kernel in a clean execution environment. Thus they make sure that the implementation of the driver’s code will not be executed through the implementation of the OS kernel’s execution. Hence, the proposed system can capture the transfer between the execution of the keyboard driver and the OS kernel.

The second phase is the online detection stage, where the system creates three protection domains and have the same memory mapping. Still, the access permissions are different; if the run-time information does not match with the average execution profile, this may indicate a keylogger.

Ahsan Wajahat et al. [14] have developed a C++ code to detect the userspace keylogger, based on the “GetKeyboardState” or “GetAsyncKeystate” function in Windows, which returns any key pressed on the keyboard. The researchers studied the techniques used to obtain information that is used on the Windows system, such as the key email by collecting and executing source codes to reach their run time. In the experiments, it was found that the keyloggers worked in the same pattern. Therefore the behaviour of the keylogger was discovered by recording the inputs from keystrokes and using the output in which the keylogger formed the I/O patterns.

NameHemita Pathak et al. [15] suggested changing the keyboard when entering the websites at each electronic payment process requesting the password of the electronic payment card. Whenever the user wants to access a website, the current keyboard is immediately changed to a virtual keyboard, making it difficult to read the passwords.

Mohammad Wazid et al. [16] used a honeypot mechanism to monitor the network, and if a keylogger was detected, it was removed from the network immediately. This approach cannot be used if the intruder uses database or email addresses to send an email of system key log to the intruder.

Francis Balazon [17] used encryption and decryption for the key pressed in the keyboard, where two different keys are used for encryption and decryption processes, a public key and a private key. The public key is used to encrypt the pressed button, and the private key is used to decrypt the key so that the keylogger cannot find out which key was clicked.

2.2 Cyber-Bullying

In this subsection, we will introduce the most recent researches that present Cyber-Bullying. Huascar Sanchez et al. [18], suggested a methodology for extracting data from social networks, which is known as Data Mining. In this study, the power of sentiment analysis is used to detect cyberbullying on Twitter. They used LingPipe tool to apply Naïve Bayes classifier; the result was achieved around 70%. While, Elizabeth Whittaker et al. [19], three studies have been conducted to examine the prevalence of cyberbullying among university and college students and places where bullying occurs on the Internet, in addition to focusing mainly on social media.

Giuseppe Riva et al. [20], focused on increasing the prevalence of online social networking sites (SNS), where it offers opportunities for cyberbullying. The study indicates that the causes of the emergence of electronic bullying are psychological distress. The proposed approach tested the relationship between online social networking and the experience of cyber-bullying. Four hundred results encourage the importance of continuing the search on the nature of internet activities used by young adolescents and the possible exposure to online victimization.

3 Problem Formulations

As mentioned, Semantic attack (Fishing) tries to steal sensitive users' information to blackmail the victim, and if the hacker succeeds in penetrating the victim, there is a Cyber Bullying.

We contacted with the Cybercrime Unit in the Hashemite Kingdom of Jordan, which is responsible for following up all cases that produce the result of Cyber-bullying, we will review all cases and classify them in such a way that it is possible to conclude the seriousness of Cyber-Bullying on societies in general and the Jordanian society in particular. Hence, Cyber-Bullying has categorized into three categories: First, according to Residential Area (divided into 7 Cyber-crimes types). Second, according to the victim's Age and third, according to Gender.

3.1 According to the residential area

The Hashemite Kingdom of Jordan has a population of about 10 million, of whom 5 million live in Amman (the capital city of Jordan) see Table 1. Thus, Jordan was divided into three regions: the North, the Central and the South. Due to the importance of Amman city (Central region), because the population is a mixture and does not belong to a specific clan, therefore Amman divided into four geographical regions: East Amman, West Amman, North Amman, and South Amman.

Table 1: Estimated Population of the Kingdom by Governorate at End-year 2019 [21]

Governorate	Total	
	%	No.
Amman	42.0	4430700
Balqa	5.2	543600
Zarqa	14.3	1509000
Madaba	2.0	209200
Irbid	18.5	1957000
Mafraq	5.8	608000
Jarash	2.5	262100
Ajlun	1.8	194700
Karak	3.3	350000
Tafeila	1.0	106500
Ma’an	1.7	175200
Aqaba	2.0	208000
Total	100.0	10554000

Table 2 shows the number of all types of cybercrimes in Jordan, which were recorded in the Jordanian Cybercrime Unit from 2013 until the end of 2019. Given the importance of the city of Amman, we have made a comprehensive study on the number of Cyber-crimes in Amman and compared it with other Jordanian regions. Table 3 shows the number of Cyber-crimes in Jordan according to geographical regions and compare it with the rest of the Jordanian regions.

Table 2: the number of all types of Cybercrimes in Jordan from 2013 until the end of 2019

2019	2018	2017	2016	2015	2014	2013	Cybercrime
4868	1885	2734	1023	970	456	474	The threat, Account theft, Defamation, Blackmail, Email theft
244	590	139	159	91	93	98	Financial fraud
3	0	0	51	4	23	21	Child sexual abuse
8	930	93	167	76	25	35	Malware
458	970	462	884	321	341	190	Impersonation
121	970	183	80	16	36	0	Manipulating electronic content
373	210	101	187	141	91	101	Spoil the marital bond

Table 3: Number of Cyber-crimes in Jordan according to geographical regions

Cyber-crime type	Central Amman	Southern Amman	North Amman	East Amman	West Amman	Southern Region	North Region	Center Region	Aqaba	Total
Blackmail	252	71	98	46	8	21	112	193	57	858
the threat	1162	269	328	208	116	10	98	415	7	2613
Financial fraud	101	19	27	17	7	2	67	25	6	271
Stealing accounts	309	47	71	36	29	2	67	131	13	705
Child sexual abuse	2	0	0	0	0	0	0	1	0	3
Defamation	1256	235	313	215	178	24	122	347	51	2741

Malware	5	0	0	0	0	0	1	2	0	8
Impersonation	186	25	36	28	20	11	41	98	4	449
Website hacking	279	43	63	54	27	2	51	79	40	638
Theft of electronic content	1	1	0	0	0	0	0	1	0	3
Manipulating electronic content	62	6	12	8	3	1	9	19	1	121
Total	3615	716	948	612	388	73	568	1311	179	8410

Among the 8,231 documented cases of cybercrime in 2019, 31 cases referred to the administrative governor (meaning that the crime has been repeated for the same persons) only in Amman with all types of Cyber-crimes.

3.2 According to the victim's Age

The ages of the victims of the Cyber-Bullying, and who submitted a formal complaint to the administrative governor, were divided into five age groups: under 18, 18-30, 30-45, and 45-60 and older than 60. Table 4 presents the official complaints at the Jordanian Electronic Crimes Unit according to the age group.

Table 4: the official complaints at the Jordanian Electronic Crimes Unit according to the age group

Cyber-crime type	Victim’s Age					
	Under 18	18 - 29	30 – 44	45 – 59	Above 60	Total
Cyberattack	109	356	168	9	0	642
Blackmail	0	413	305	154	1	873
The threat	0	1061	1197	349	38	2645
Financial fraud	0	3	87	143	11	244
Stealing accounts	85	329	205	89	0	708

Child sexual abuse	3	0	0	0	0	3
Defamation	51	1218	1007	471	24	2771
Malware	0	2	5	1	0	8
Impersonation	4	197	241	16	0	458
Theft of electronic content	0	2	1	0	0	3
Manipulating electronic content	0	71	34	16	0	121
Total	252	3652	3250	1248	74	8476

3.3 According to the Gender

The demographic literature indicates that the gender ratio at the time of birth in any population reaches 105 males per 100 females, which is somewhat close, and Table 5 shows the distribution of sex in Jordan at a rate consistent with the declared by the official authorities**.**

Table 5: Estimated Population of Jordan by Sex at End-year 2019 [21]

Governorate	Female	Male
Amman	2051900	2378800
Balqa	251700	291900
Zarqa	711100	797900
Madaba	98600	110600
Irbid	945800	1011200
Mafraq	294500	313500
Jarash	125800	136300
Ajlun	94500	100200
Karak	167100	182900
Tafeila	50800	55700
Ma'an	83800	91400
Aqaba	90400	117600
Total	4966000	5588000

Table 6 shows the number of complaints submitted to the Cyber-crime Unit by Gender.

Table 6: The number of complaints submitted to the Cyber-crime Unit by Gender

Cyber-crime type	Female	Male	Total

Blackmail	502	371	873
the threat	1832	813	2645
Financial fraud	68	176	244
Stealing accounts	322	386	708
Child sexual abuse	2	1	3
Defamation	1613	1158	2771
Malware	0	8	8
Impersonation	233	225	458
Website hacking	7	43	50
Theft of electronic content	0	3	3
Manipulating electronic content	7	114	121
Total	4586	3298	7884

4 Results, Analysis and Discussions

4.1 Results, Analysis and Discussion according to a residential area

As shown by Table 2, it was found that there is a noticeable increase in the number of Cyber-crimes from 2013-2019, due to the widespread use of social media applications. And also, the access of the Internet to all geographical areas in Jordan, by all segments of society, as well as the presence of real statistics to the reality of Cyber-crime to increase awareness among individuals of the existence of a specialized official government agency to file complaints against those who misuse of social media sites.

The highest rates of Cyber-crimes during the years 2013-2019 were for threats, account theft, defamation, blackmail and Email-theft. These Cyber-crimes have a direct relationship to the reputation of the individual and the social value associated with it. While, the lowest rates were for Child sexual abuse because such crimes in Jordanian society are directly related to the reputation of the individual, whether he/she is a criminal or a victim.

Therefore, the informants are keen to fall into such crimes for fear of social reactions, which are opposed to not giving them up, and the most severe punishments for the perpetrators and it lead to honour crimes that lead to the killing of the perpetrator.

By reference to Table 3, which is related to the distribution of Cyber-crimes in the Jordan, which includes all of Karak Governorate, Tafila, Ma'an, and Aqaba, and the specificity of Aqaba governorate from other southern governorates, as it is known that other southern governorates are closed governorates. Clans linked by a historical presence to these areas and the southern governorates are considered remote governorates far from Amman. In contrast, Aqaba governorate is a free economic zone, and it is the port of Jordan and inhabited by residents from all governorates of Jordan to provide job opportunities in addition to its original inhabitants. Aqaba was clearly reflected in the high number of Cyber-crimes.

The number of complaints submitted by those concerned to the Cyber-crime Unit as the total number of complaints in the Southern governorates (Karak, Tafila, Ma'an) reached 73. In contrast, in Aqaba, the total number of complaints reached 179, the highest of these Cyber-crimes of extortion reached 57, followed by the crime of defamation which reached 51. Then, the crime of hacking websites, which reached 40, followed by the crime of defamation, which reached 13, then the crime of threatening, which reached 7, financial theft reached 6 offences, eventually, the abuse of electronic information, which reached just one crime.

All these numbers illustrate the lack of social regulation, and the rise of non-standardization in this governorate (unlike other governorates in the southern region), in which the influence of social regulation on the refinement of human conduct, and conformity to social norms and expectations, which has been shown by looking at the overall number of Cyber-crimes committed against it relatively to the amount of its population.

In Table 6, which shows the number of Genders who submitted a complaint to the Cyber-crime Unit, due to their exposure to crimes resulting from the misuse of websites, the number of males who filed a complaint exceeds the number of females 5751, while the number of males 2732. The highest percentage of Cyber-crimes that females were subjected to was the crime of defamation, which reached 2157, followed by the threatening, where the number of Cyber-crimes that females were subjected to 1910, followed by the crime of extortion, where the number of Cyber-crimes that females were subjected to 592, then the crime of stealing accounts, where the number of crimes that females were subjected to 416, then the crime of impersonation, where the number of crimes that females were exposed to 262, followed by the crime of corrupting the marital bond, which reached 156, then the crime of financial fraud, where the number of crimes reached Females were subjected to 21, then the crime of manipulating electronic content, where the number of crimes that females were subjected to 3, and finally the crime of sexual abuse of children, as mothers of children who were exposed to this crime filed a complaint with the Electronic Crimes Unit.

The numbers reflect that the females who have submitted complaints to the Cybercrime Unit are the most aware of the necessity to file a complaint until the competent authority deters the perpetrators. As shown in Table 6, which reflects the females are the exploited group within the Jordanian society, especially in crimes that reflect this such as defamation, threats, extortion and corruption of the marital bond.

Regarding males, we found that the percentage of those who filed complaints about various Cyber-crimes is lower than females, due to the nature of males who tend to solve their problems away from the interference of official authorities, especially if the official authorities Unit knows the perpetrator if He is seen as unable to confront the opponent (unlike entirely female) and may file a complaint if he is exposed to a Cyber-crime from fake websites and numbers.

4.2 Results, Analysis and Discussion according to victim's Age

As presented in Table 4, it was found that there is a significant relationship between Age and Cyber-crime. The most age group filed a complaint with the Cyber Crime Unit are the age groups (18-29), and the age group (30-44). The number of complaints about the first category reached (3739), and the number of complaints about the second category was (3275). On the other hand, the number of complaints submitted in the age group (under 18) reached (252), and the lowest group is the category (over 60).

By analyzing the data in Table 4, the crimes that occurred against persons under the Age of 18 years are crimes consistent with the developmental characteristics of the age stage based on the love of adventure, exploration, and the search for self. We find that the crimes at this Age were limited to crimes of electronic penetration, as it amounted to (109) crimes, followed by the crime of stealing accounts, which reached (85) crimes, then the crime of defamation, where the number reached (51) crimes. The crime of impersonation reached (4) crimes, and finally, the crime of child sexual abuse, which reached (3) crimes, as this category is the most vulnerable to exploitation.

In addition, the crimes that occurred against persons of the age group (18-29), the highest of which was recorded for the crime of defamation, where the number reached (1218) crimes, followed by the crime of threatening, which reached (990) crimes, then the crime of extortion, which reached (413) crimes. The Electronic hacking ranked at Fourth place, where it reached (356) crimes. The crime of stealing accounts is close to Electronic hacking crime, which reached (329), and then the crime of impersonation, where reached (197) crimes, followed by the crime of spoiling the marital bond, which reached (156) crimes, then the crime of content tampering As the number reached (71) crimes, then financial fraud, which reached (3) crimes, then the two crimes of stealing accounts and Malware, where the number of each of them reached (2) crimes.

The crime of defamation is the highest in the age group (18-29), the defamation is one of the acute problems in Jordanian society because it affects the reputation of the individual and affects his social status. The same applies to threatening crime, as it is ranked second among crimes in this category, which are usually the result of personal differences between the two parties, or because of bullying one party over the other.

And in the third place was the crime of extortion, which may be related to the financial aspect or other aspects such as defamation, or related to issues of honour, and the reputation of the individual. Also, we find that theft of accounts, tampering with electronic content and electronic penetration recorded numbers to be reckoned with, and this may be due to the ability of this group and its possession of technical skills that enable it to do so.

Besides, the crime of spoiling the marital bond has had a large share in the electronic trials of this category, as this crime is considered a severe social crime on the structure of society, which may lead to divorce and its repercussions on the family and children.

The age group (30-44), and through analyzing the data contained in the Table 4, we may find them similar to the age group (18-29).

The age group (45-59), we find that the number of those who filed a complaint with the Cyber Crime Unit constituted one-third of the number of complainants from each of the age groups (18-29) and (30-44). Their highest complaints about defamation were recorded, followed by threats.

The age group (over 60), it is the lowest group that submitted complaints to the Cyber-crime Unit, as the number of complaints reached (54) complaints, which is a minimal number compared with the total complaints submitted to the Cyber-crime Unit. The age group (over 60), it is the lowest group that submitted complaints to the Cybercrime Unit, as the number of complaints reached (54) complaints, which is a minimal number compared with the total complaints submitted to the Cybercrime Unit.

Defamation crime recorded the highest number of Cyber-crime, which reached (24) crimes, followed by the crime of intimidation, as it reached (18), then the crime of financial fraud, its number (11), then extortion, as its number reached (1). Defamation crime recorded the highest number due to the nature of this age group, which is characterized by a lack of impulsivity and the right mind.

4.3 Results, Analysis and Discussion according to Gender

As shown by Table 6, it was found that the number of females, who submitted a complaint to the Cyber-crime Unit for being exposed to crimes resulting from the misuse of websites, exceeds the number of males who filed a complaint about the same crime, the number of females reached 5751. In contrast, the number of males reached 2732.

The highest percentage of crimes to which females were subjected was the crime of defamation, which reached 2157, followed by the crime of threatening, where the number of threatening crimes that women were subjected to 1910, then the crime of extortion, where the number of crimes of extortion to which females were exposed reached 59. Then, the crime of stealing accounts, where the number of crimes that females were subjected reached 416, followed by the crime of impersonation, where the number of crimes that females were exposed to was 262, and the crime of corrupting the marital bond reached 156. The crime of financial fraud committed against females recorded 21 crimes, the crime of manipulating electronic content that females were exposed reached three. Finally, the crime of child sexual abuse, as mothers of children who were exposed to this crime filed a complaint with the Cyber-crime Unit.

The number in Table 6 reflects that the females who have submitted complaints to the Cyber-crime Unit are the most aware of the necessity to file a complaint in order to deter the perpetrators. Also, Table 6 reflects that females are the exploited group within the Jordanian society, especially in crimes that reflect this, such as defamation, threats, extortion and corruption of the marital bond.

While, for males, we find that the percentage of those who submitted complaints about various Cyber-crimes is less than females, this due to the nature of males, who tend to solve their problems away from the interference of official authorities, mostly if the perpetrator is known, because this reduces his status Social. Males are unable to confront the opponent, unlike the female, and he may submit a complaint if he is exposed to a Cyber-crime from fake websites and numbers.

6 Conclusion

The results of the research show that there is a vital role for the Cyber-crime Unit, as it takes deterrent measures against abuses of social networking sites. Likewise, the most common electronic crimes are crimes related to defamation, threats and extortion, and these crimes are considered among the moral crimes that affect the reputation of the individual, which is a valuable thing in Jordanian society. Its impact on people is more severe than other crimes except for honour crimes.

The results also show the prevalence of Cyber-crime in densely populated places, in which there is a heterogeneous mixture of individuals from different backgrounds and almost devoid of social control.

Cyber-crime decreases in the regions where clans and tribes live, and it is semi-closed areas such as the southern region (except for the Aqaba governorate) due to the presence of social controls there. Among the most important findings of the research is the impact of electronic crimes on the family structure, such as crimes of corrupting the marital bond and various crimes against females.

Finally, most age groups that have been exposed to electronic crimes are the groups (18-29) and (30-44).

As a Future work, awareness programs can be made about the Cyber-crime Unit, as well as awareness workshops through the competent authorities such as the Ministry of Social Development and civil society institutions, whose programs target crowded and poor areas about the seriousness of Cyber-crime. In addition, specialized workshops were held in high-risk areas on the optimal use of social media and websites.

ACKNOWLEDGEMENTS
The authors would like to thank Al-Zaytoonah University of Jordan for supporting this research, as well as the Cyber-crime Unit in the Hashemite kingdom of Jordan for their valuable information.

References

[1] Ammar odeh, Abdalraouf alarbi , Ismail keshta , Man abdelfattah. (2020). efficient prediction of phishing websites using multilayer perceptron (mlp). *Journal of Theoretical and Applied Information Technology*, 98(16), 3353 – 3363.

[2] Simms S., Maxwell M., Johnson S., Rrushi J. (2017). Keylogger Detection Using a Decoy Keyboard. In: Livraga G., Zhu S. (eds). *Data and Applications Security and Privacy XXXI.* DBSec 2017. Lecture Notes in Computer Science, vol 10359, 433-452.Springer, Cham.

[3] Hossein Rouhani Zeidanloo, S. Farzaneh Tabatabaei, Payam Vahdani Amoli and Atefeh Tajpour. (2010) Conference: *Proceedings of the 2010 International Conference on Security & Management. SAM 2010*, July 12-15, 2010, Las Vegas Nevada, USA.

[4] An Introduction To Keyloggers, RATS And Malware, Copyright 2011 Rafay Baloch. http://rafayhackingarticles.blogspot.com.

[5] Yilmaz, Seyhmus & Zavrak, Sultan. (2015). Adware: A Review. *International Journal of Computer Science and Information Technologies*. 6(6), 5599-5604.

[6] Creutzburg, Reiner. (2017). The strange world of keyloggers - an overview, Part I. *Electronic Imaging*.. 10.2352/ISSN.2470-1173.2017.6.MOBMU-313, 139-148

[7] Yahye Abukar Ahmed, Mohd Aizaini Maarof, Fuad Mire Hassan and Mohamed Muse Abshir. (2014). Survey of Keylogger Technologies.

International Journal of Computer Science and Information Technologies. 5(2), 25-31.

[8] Adnan A. Hnaif, Ali Aldahoud, Mohammad A. Alia, Issa S. Al’otoum and Duaa Nazzal. (2019). Multiprocessing scalable string matching algorithm for network intrusion detection system, *Int. J. High Performance Systems Architecture,* 8(3), 159-168

[9] Akhil S, Neeraja M Nair, Asst Prof. Arun R. (2014). *Proceedings of the International Conference on Emerging Trends in Engineering and Management (ICETEM14)* 30 – 31, Ernakulam, India.

[10] Christopher A. Wood and Rajendra K. Raj. (2010). Keyloggers in Cybersecurity Education. *10th International Conference on Intelligent Systems and Control (ISCO)*. 293-295

[11] S.vinothkumar, S.Aruna sankaralingam. (2014). Mobile Keylogger Detection By Using Machine Learning Technique. IJEDR - *Conference Proceeding (NCETSE-2014)* | ISSN: 2321-9939. 51-56. IEEEXplore.

[12] Tasabeeh O. M. Ali, Omer S. A. Awadelseed, Abeer E. W. Eldewahi. (2016). Random Multiple Layouts Keylogger Prevention Technique, *2016 Conference of Basic Sciences and Engineering Studies (SGCAC)*. 1-5. IEEEXplore.

[13] Donghai Tiana, Xiaoqi Jiac, Junhua Chenb, Changzhen Hua. (2017). An Online Approach for Kernel-level Keylogger Detection and Defense. *Journal of Information Science and Engineering* 33(2), 445-461.

[14] Ahsan Wajahat, Azhar Imran, Jahanzaib Latif, Ahsan Nazir, Anas Bilal. (2019). A Novel Approach of Unprivileged Keylogger Detection. *International Conference on Computing, Mathematics and Engineering Technologies – iCoMET*. 1-6.

[15] NameHemita Pathak, Apurva Pawar, Balaji Patil. (2015). A Survey on Keylogger: A malicious Attack. *International Journal of Advanced Research in Computer Engineering & Technology* (*IJARCET)* 4(4), 1465-1469.

[16] Mohammad Wazid, Avita Kata, R.H. Goudar, D.P. Singh and Asit Tyagi Robin Sharma and Priyanka Bhakuni. (2013). A Framework for Detection and Prevention of Novel Keylogger Spyware Attacks. *Proceedings of7'h International Conference on Intelligent Systems and Control* (ISCO 2013). 433-438. IEEEXplore.

[17] Francis Balazon. (2018). Anti-Keylogging Software Using Asymmetric Key Encryption Algorithm For Non-Hybrid Keyloggers. *International Journal of Recent Innovations in Academic Research*, 2(7), 326-336.

[18] Sanchez, H., Kumar, S. (2012). Twitter bullying detection. In: NSDI 2012, Berkeley, CA, USA, p. 15. *USENIX* Association.

[19] Elizabeth Whittaker & Robin M. Kowalski. (2015). Cyberbullying Via Social Media, *Journal of School Violence*, 14(1), 11-29

[20] Giuseppe Riva, Rosa M. Baños, Cristina Botella, Brenda K. Wiederhold, and Andrea Gaggioli. (2012). Positive Technology: Using Interactive Technologies to Promote Positive Functioning. *Cyberpsychology Behavior and Social Networking*. 15(2), 69-77.

[21] http://dosweb.dos.gov.jo/population/population-2/

Notes on contributors

Dr Haya Ali Al-Masalha is an Assistant professor at the Basic Sciences - Humanities and Sciences, Faculty of Arts, Al Zaytoonah University of Jordan, Dr Al-Masalha obtained her PhD from the University of Jordan in 2009 in Sociology. She received her MSc degree in 1996 Department of Sociology and her Bachelor's degree from the University of Jordan in 1986. Her research focuses on social problems, family and childhood problems.

Dr Adnan A. Hnaif is an associate professor at the computer science department, Faculty of Science and information technology, Al Zaytoonah University of Jordan. Dr Hnaif received his PhD degree in Computer Science from University Sains Malaysia (USM) – National Advanced IPv6 Centre and Excellence (NAV6) in 2010. He received his MSc degree in Computer Science from the Department of Computer Science in 2003 and obtained his Bachelor's degree in Computer Science from the Department of Computer Science in 1999/2000. His researches focus on computer networks and communications, wireless sensor networks, network security, parallel processing, and algorithms.

Dr Tarek Kanan is an assistant professor in the Department of Computer Science/Artificial Intelligence at Al-Zaytoonah University of Jordan. He obtained his PhD in 2015 from Virginia Tech. His research interests are in the Artificial Intelligence domains. He had several prestigious Journal/Conference publications and was in various journals and conferences’ committees.