I.J. Wireless and Microwave Technologies, **2018, 5, 19-26**
Published Online September 2018 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2018.05.03

Available online at ***http://www.mecs-press.net/ijwmt***

Cybercrime as a Matter of the Art in Palestine and its Effect on Individuals

Belal Amro

College of Information Technology, Hebron University, Hebron, Palestine

Received: 08 February 2018; Accepted: 04 June 2018; Published: 08 September 2018

Abstract

According to Palestinian police records, cybercrimes have become common last few years in Palestine. The most commonly reported cybercrimes are mainly based on social networks to hack victims asking for some service. Many efforts are carried out by police and related agencies to handle these crimes and save the victims. In this paper, we will study cybercrimes in Palestine as a matter of the art and we will focus on parties involved in thwarting cybercrimes. These parties include: 1) ministry of higher education where they have a great role to afford knowledge about cybercrimes and ethical issues related to IT in school curricula. 2) Palestinian legislative council for adopting concrete cybercrime laws and regulations. and 3) Police department by broadening the role of cybercrime unit and gaining the trust of people about that unit. A survey designed and distributes and aimed to test the effect of cybercrime on individuals in Palestine, the survey results are reported. According to the findings and survey results, recommendations are provided with the aim of leveraging the ability to fight cybercrimes in Palestine in the near future.

Index Terms: Malware, cybercrime, mobile device, security, privacy.

1. Introduction

According to [1], Cybercrime is defined as “any illegal act that involves a computer, its systems, or its applications.” This definition implies that cybercrimes are intentional since they are carried out by cybercriminal with advanced technical skills.

Cybercrimes are widely categorized into two categories according to the tools used to commit the crime and the target of the crime itself. The Tools of the crime might be used as evidence and must be investigated by a

* Corresponding author. Tel.: 00970599769876; fax: 00970 2 2229303
E-mail address: bilala@hebron.edu

forensics expert. The Target of the crime is simply the victim which might be an organization, a website, … etc.

Cybercrimes vary according to tools used and the target of the crime, there are many types of cybercrimes, and Table 1 lists the most popular ones in Palestine:

Table 1. Most popular cybercrimes in Palestine

	Type	definition
1	Identity theft	fraud committed or attempted using the identifying information of another person without permission [2]
2	Hacking	Intentionally accesses a computer without authorization or exceeds authorized access. Various state and federal laws govern computer hacking. [3]
3	Malware	According to Oxford dictionary, malware is defined as “Software which is specifically designed to disrupt, damage, or gain authorized access to a computer system. “
4	Cyberstalking	Involves the use of the Internet, e-mail, or any other technological tools in electronic communication to stalk or harass an individual. [4]
5	Financial fraud	It is defined as an intentional plan of deception to gain profit. The action involves financial transactions.
6	Defamation	Defamation aims to destruct the reputation of an object and might be: • Libel: written defamation • Slander: oral defamation
7	Electronic Spamming	The use of a messaging system to automatically send an unsolicited message. The message might be sent repeatedly on the same site.
8	Software piracy	Unauthorized copying and distribution of commercial software with copyrights.
9	Denial of Service	Sakes for making a machine or a resource unavailable to serve legitimate users.

Victims of cybercrimes might be organizations or persons. As a person, being a victim of any type of cybercrime might leave a negative effect on the person. These consequences vary from feeling angry to feeling violated and sometimes need to get revenge. According [5], the top 10 emotional reactions to cybercrimes are shown in Figure 1.

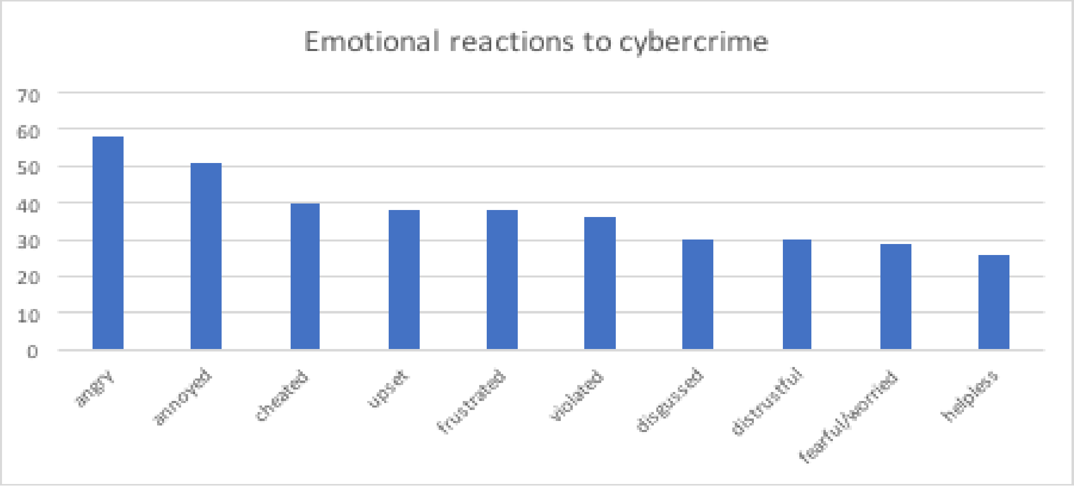

Fig.1. Emotional reactions to cybercrime

In this paper, we will study cybercrime as a matter of the art in Palestine and its effect on youth people. The rest of the paper is organized as follows; a summary of related work is introduced in the next section. Cybercrime in Palestine is then provided. Analysis of a survey is then provided. And at last, we conclude our findings of cybercrimes in Palestine and their effect on people.

2. Related Work

According to [6], about 689 million people in 21 countries experienced cybercrime. Cybercrime victims paid about $126 billion, besides spending on average 19.7 hours dealing with cybercrime. 86% of people said they may have experienced a phishing incident where 30% of them took a compromising action like responding with personal details. Internet Security Threat Report – ISTR [7], showed that the year 2016 has greater and more critical attacks than that of 2015. The number of revealed identities and other forms of attacks became larger with new disciplines of attacks like IoT and mobile attacks.

Since attacks might be targeted to people, then these attacks will leave an emotional effect on those targeted people. As a study of the impact of cybercrimes on social networking pattern of girls [8] in India showed that cybercrimes leave an everlasting scar in the minds of users and change the way they communicate and may cause them to stop using the social networking sites.

In [9], the authors showed that becoming cybercrime victim carries emotional costs, which vary across cybercrime types, and that individual personality traits influence the victims’ perceptions of impact.

A study aimed to examine the relationship between perception about cybercrime and other factors [10]. The authors found that female students are more aware and have affirmative insights than male, and students with higher academic qualifications are more aware of cybercrime and perceived the issue of risk differently. I another study [11], the author reported that the governments and commercial software and hardware companies must work together to reduce the stress and anxiety effects of cybercrimes on customers.

In [12], the authors proposed a school education curriculum for cyber safety. The proposed curriculum covers four sections; Cyber Threats, Protecting Ourselves, Cyber Ethics, and Cyber Laws. The aim of the new curriculum is to raise awareness among youth students which might reduce cybercrime consequences.

The Nature, Causes, and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria has been studied [13], and they found that most cybercrimes were carried out by people who seek for money to become rich. They recommended that there should be legislation on cybercrime besides educating the society and training them about cybercrimes.

In [14], the authors studied the nature of cybercrime and its impacts on young people in Bangladesh. They reported that most of the people are unaware of cybercrimes and hence cannot decide whether they were victims or not. So, it is worthy to study the nature of cybercrimes in developing countries and to have countermeasures accordingly.

3. Cybercrime in Palestine

In this section, we will introduce an overview of cybercrime in Palestine, and then we will explain our research methodology and hypothesis, a section of the survey is then provided.

3.1 Nature of cybercrime in Palestine

In Palestine, like any other developing country, cybercrime awareness has risen lately. The majority of people are being affected by technology and connected to the Internet, however, the knowledge about cybercrime is limited to some forms of identity theft, financial fraud, and defamation.

The Palestinian Police have recently established a special unit called cybercrime unit. The unit deals with claims of people and then works on that claim and take an action accordingly. A cyber law has been newly adopted and still not that effective to punish cybercriminals and prohibit them from conducting such crimes.

According to police records, there were 1327 cases reported in the year 2016, and about 450 cases until mid of April 2017[15]. Most of these cases are related to females using their social network profiles. The cybercrime unit has a dissemination program to raise awareness about cybercrimes and to tell people about cybercrime unit. However, statistics report that 80% of cybercrimes in Palestine are not transferred to the Police, and victims prefer to keep silent.

After reviewing the new Palestinian school curricula, which can be downloaded from [16]; Technology courses are taught starting from the fifth grade. The Palestinian Curricula does not have material related to cybercrime and security except a unit of securing information for the sixth grade; the unit merely talks about authentication and better selection of passwords with some hints about data sharing. There were not topics related to cybercrime or ethics of information systems. Hence, the majority of youth might not be aware of safe internet usage and good security practices.

3.2 Survey description

The hypothesis of our research is:

1. Youth people in Palestine are aware of cybercrimes and their effects.
2. People of IT background are less affected by cybercrimes
3. People trust closed fried rather that Police cybercrime unit
4. There is a need to include topics about cybersecurity and ethics in high school curricula

In the next section, we will analyze the result of our survey and check our hypothesis. then a conclusion and recommendations will be provided.

3.3 Survey Analysis

300 copies of the survey have been collected. The majority of the respondents 93.0% were less than 30 years old. Users on average spend 4 hours using technology tools. Most of them (87.5%) uses the internet in their homes where other use in their work or study place. 85.2% of the respondents reported that they use their smartphones while other reported the use of laptops and tablets. 14.8% reported that they use 3G technology and this is justified because 3G has recently been deployed in Palestine. Figure 2 shows the most used services by users:

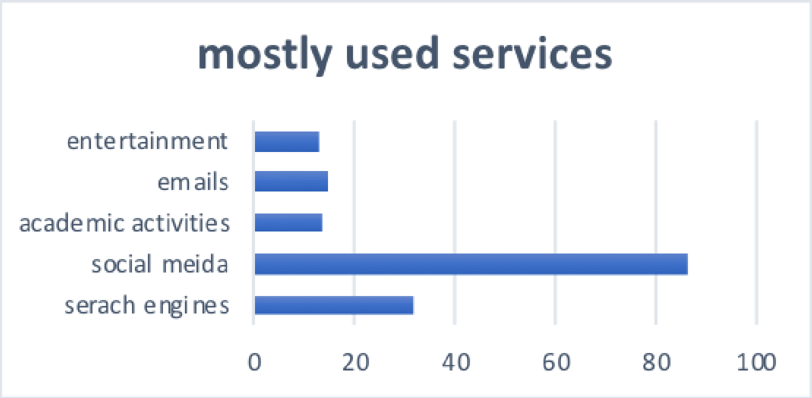

Fig.2. Mostly used services

A surprising result showing that 95.7% of the respondents know about cybercrimes despite the fact that it is not taught at schools or even Universities for non-IT students. Most of them heard about cybercrimes through media.

Related to cybercrimes, 55% of respondents reported that they or one of their relatives have been a victim of a cybercrime. When asking about the type of the cybercrime, the answers varied and are summarized in Figure 3:

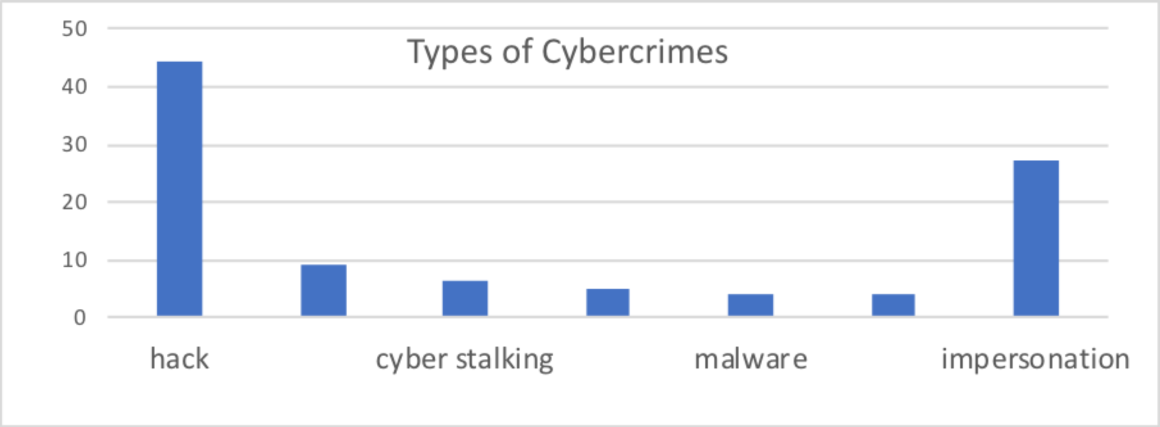

Fig.3. Types of Cybercrimes

In relevance to the effect of the cybercrime on respondents, the answers varied among them as shown in Figure 4.

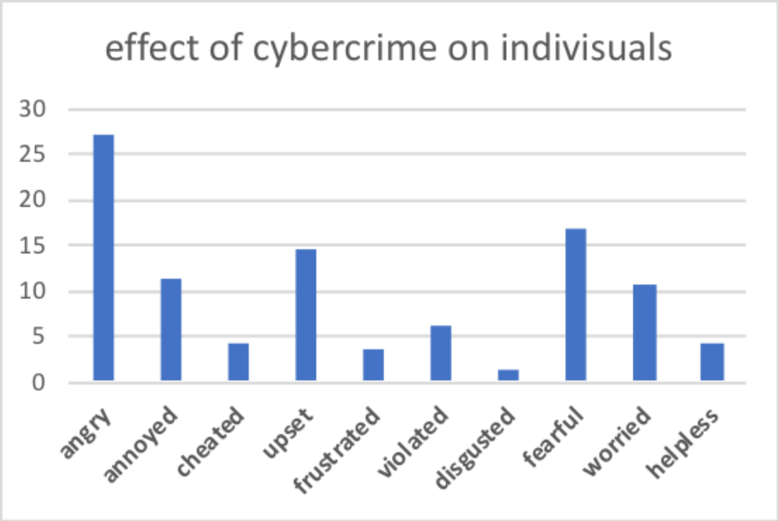

Fig.4. Effect of cybercrime on individuals

The consequences of the cybercrime on individuals varied from no consequences to a real physical harm. Figure 5 below shows the percentages of these consequences on respondents.

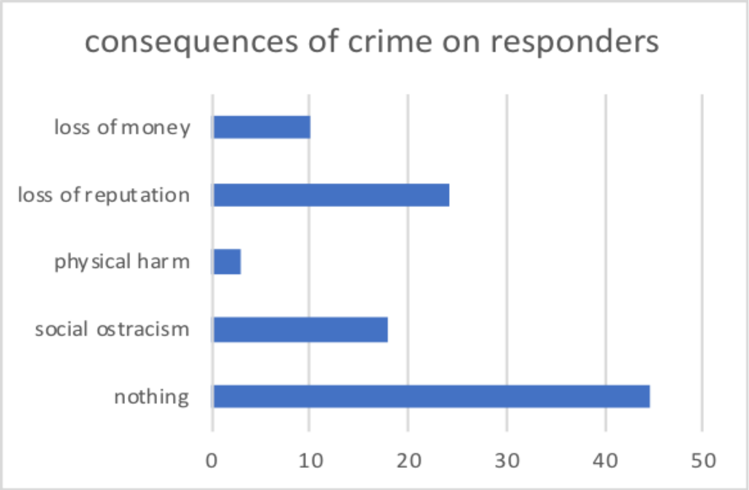

Fig.5. Consequences of cybercrime on victims

When people were asked about the action they took when a victim occurred, most of them consulted a close friend (43.7%), while others reported that they had consulted information security expert (26.9%). The remaining either reported an official claim to the authorities (22.8%) or accepted the effect as it without taking any action (6.6%). For those who consulted an information security expert, 67.1% reported that this consultation helped them to well manage during the crime period and avoid unnecessary consequences. For those who did not make an official claim, the reasons behind that are listed in Table 2 below.

Table 2. Reasons for avoiding official claims

Reason	Percentage %
avoid a scandal	47.5
crime is not worthy	20.8
fear of criminal	13.7
untrusty official agencies	9.3
else	8.7

According to the survey, the most two major forces for committing a cybercrime in Palestine are poor laws and regulations (30.5%) and ease of internet access (30.5%).

4. Results and Recommendations

According to the facts proposed in the previous section of this paper and the results of the survey conducted, we came up with the following results regarding cybercrimes in Palestine:

1. The rate of cybercrimes is increasing in Palestine making it a must to be handled carefully
2. Individual are affected by cybercrime and the most affected category are those who lack basic information about cybercrimes and cybersecurity.
3. The high rate of unemployment and availability of technology and Internet access made the cybercrime rate to increase.

To mitigate cybercrime effects and consequences in Palestine, we provide the following recommendations.

1. It is clearly obvious that previous knowledge about cybercrimes enhanced the ability of the victim to better control the events and reduce the effects and consequences. According to our study of the current Palestinian school curricula, we find that the information technology curricula must be updated with topics related to cybersecurity and ethics of information systems. Providing such knowledge to students might help them behave correctly once they find themselves in an attack.
2. It seems that people in Palestine believe that cybercrime law and regulations are poor and does not have that power to punish criminals and dissuade others from committing such crimes. Hence, and intensive revision of the law has to be carried out were all cybercrimes are clearly stated as well as the punishment related to each crim. This will make people more satisfied with these regulations and will make it criminals think more before conducting a cybercrime.
3. The police cybercrime unit is a matter of the fact and works on different types of cybercrimes. However, a dissemination program for the unit and its capabilities must be carried out to make it reachable for all people. Many respondents reported that they do not know about the cybercrime unit. However, they know that they might go to the police for reporting cybercrimes. According to our survey, people trust information security experts and find their advice helpful to them. So, having an official agency like cybercrime unit will definitely encourage people to report incidents.

Having 3G technology recently deployed, with increased dependency on technology to perform daily tasks of individuals; it is highly probable that cybercrime rate in Palestine will grow faster. Hence, there is a necessity to take preventive actions to control cyberspace. Following the previously mentioned points will positively affect the rate of cybercrimes and will reduce the effects and consequences of cybercrimes on individuals.

5. Conclusions

In this paper, we studied cybercrime in Palestine as a matter of fact. The study included investigation of Information Technology course in Palestinian school curricula. Investigations found that the curricula lack essential knowledge about cybercrimes and ethics of information systems. A newly established cybercrime unit is doing well in computer forensics investigations and a newly adopted cybercrime law and regulations exist as well. People in Palestine feel that the newly adopted law is weak and does not prohibit criminals from conducting a crime. According to the survey results, many people have been a victim of a particular type of a cybercrime. Many people were afraid to report being a victim of a cybercrime for social and personal issues. The paper concludes that cybercrime in Palestine will grow dramatically and steps to mitigate the effect and consequences must be taken into consideration. These steps include enrichment of school curricula with material about cybersecurity and ethical issues related to IT, cybercrime law and regulations must be revised to effectively punish the criminal, and the cybercrime unit must perform extra efforts to reach all people and persuade them to report incidents once occurred.

References

[1] Investigation Procedures and Response : EC-Council | Press , Cengage Learning, 2010.

[2] Kristin Finklea, Identity Theft: Trends and Issues, Congressional Research Service, 2014.

[3] website: https://definitions.uslegal.com/c/computer-hacking/ last seen 6/1/2018.

[4] Naomi Harlin Goodno, Cyberstalking , a New Crime: Evaluating the Effectiveness of Current State and Federal Laws, 72 Mo. L. Rev. (2007).

[5] Norton cyber crime report: The human impact, 2010.

[6] Norton cyber security insight report: Understanding cybercrime and the consequences of constant connectivity , 2016.

[7] Internet Security Threat Report - ISTR, Symantec, April 2017.

[8] M. Neela Malar, “Impact of Cyber Crimes on Social Networking Pattern of Girls “, international Journal of Internet of Things 2012.

[9] Modic, D., & Anderson, R. (2015). It’s All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. Ieee Security & Privacy, 13(5), 99-103. doi:10.1109/MSP.2015.107.

[10] Md Shamimul Hasan et. al., “Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia “, Journal of Social Sciences , 2015.

[11] Sumanjit Das and Tapaswini Nayak, “IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES” , International Journal of Engineering Sciences & Emerging Technologies, October 2013.

[12] K Samridh Saluja et.al. , “Cyber Safety Education in High Schools” , International Conference on Computer Technology and Science (ICCTS 2012).

[13] Folashade B. Okeshola and Abimbola K. Adeta, “The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria “ American International Journal of Contemporary Research , 2013.

[14] Mohammad Mostufa Kamal et. al. , “Nature of Cyber Crime and Its Impacts on Young People: A Case from Bangladesh ”, Asian Social Science, 2012.

[15] Website, “http://www.sadaa.ps/43722.html “ , last seen 7/1/2018.

[16] Website , “http://rawafed.edu.ps/portal/elearning/ “ last seen 5/2/2018.

Author’s Profile

Belal Amro is an assistant professor at Faculty of Information Technology in Hebron University - Palestine, where he has been working since 2003. From 2003 to 2004, he was a research assistant at Hebron University. From 2005 to 2007, he was an instructor in the Computer Science Department at Hebron University after having his MSc. degree in complexity and its interdisciplinary applications form Pavia- Italy. During 2008-2011 he received an ERASMUS PhD grant at Sabanci University-Turkey. From 2011-2012 he worked as research assistant at Sabanci University. In 2012, Mr Amro has received his PhD in Computer Science and Engineering From Sabanci University- Istanbul, turkey. From 2012 till now, Mr Amro has been working as an assistant professor at Faculty of Information Technology – Hebron University. From 2014 to 2017 Mr Amro has worked as chairman of Computer Science Department at Hebron University. Mr Amro has served as technical program committee member for different international conferences and journals, and reviewed more than 50 papers in the field of information technology including privacy and security. Currently, Mr Amro is conducting research in network security, wireless security, privacy preserving data mining techniques and has published more than 10 papers in international journals and conferences in the field of computer security and privacy.

How to cite this paper: Belal Amro, " Cybercrime as a Matter of the Art in Palestine and its Effect on Individuals ", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.8, No.5, pp. 19-26, 2018.DOI: 10.5815/ijwmt.2018.05.03