Cybercrime and how to confront it through an educational security perspective

الجريمة السيبرية و كيفية مجابهتها من خلال منظور أمني تربوي

Prepared by:

Nashwa Mahmoud Shabana
Ph.D. researcher
Methodology and curricula –English Department - Faculty of Education
Port Said University
English senior teacher at Al Azhar Al Sharif

Major /Ahmed Mohamed Shehab
Ph.D. researcher
Faculty of Law
Mansoura University

٢٠١٨

Table of Contents

Lists of Abbreviations

Abbreviations	Stands for
CoE	**Council of Europe**
DOD	**The United States Department of Defense**
DOS	**The United States Department of State**
FBI	**Federal Bureau of Investigation**
FIPS	**Federal Information Processing Standard**
ICT	**Information Communication Technology**
IS	**Information Systems**
IT	**Information Technology**
ITU	**International Telecommunication Union**
NATO	**North Atlantic Treaty Organization**
NCSA	**NATO Communication and Information Systems Services Agency**
NIAOC	**NATO Information Assurance Operations Centre**
OSCE	**Organization for Security and Co-operation in Europe**
UN	**United Nations**
UNESCO	**United Nations Educational Scientific Cultural Organization**
Generation X	**The generation of people born during the 1980s and early 1990s.**
Generation Y	**Members of Generation Y are often referred to as "echo boomers" because they are the children of parents born during the baby boom (the "baby boomers"). Because children born during this time period have had constant access to technology (computers, cell phones) in their youth, they have required many employers to update their hiring strategy in order to incorporate updated forms of**

	technology. Also called millennials, echo boomers, internet generation, iGen, net generation.

Introduction

Millions of people throughout the world use different kinds of information communication technology (ICTs) daily. We live in a world where technology is integrated with our daily lives. We spend more and more time using the internet for work, education and socializing. Being part of this cyber world is no longer a luxury, but a necessity for many cyber users.

Data security is crucial for all small businesses. Customer and client information, payment information, personal files, bank account details- all of this information is often impossible replace if lost and dangerous in the hands of criminals. Data lost due to disasters such as a flood or fire is devastating, but losing it to hackers or a malware infection can have far greater consequences. How users handle and protect their data is central to the security of their business and the privacy expectations of customers, employees and partners.

Cyber security is the body of rules put in place for the protection of this cyberspace which refers to the boundless space known as the Internet. The increasing use of e-Learning systems has been documented by numerous studies and shows continuing growth; little attention has been given to the issue of security of e-Learning systems both in research and education.

Cyber crime threatens all of us and thanks to the ever greater use of computers in every area of our lives, this even includes people who do not go online. Cyber crime has witnessed an astonishing growth since the millennium and represents perhaps the greatest challenge for public law enforcement worldwide. Cyber police suffer from both poor funding and a lack of qualified personnel, although they use digital evidence to follow the offenders by special programs which analyzed the magnetic field and its pullets and analyzed these evidences which could be reliable in the court.

The cyber terrorism is real threat to fast technology development. Potential targets are systems which control the nation's defenses and critical infrastructure. The terrorist of the future will win the wars without firing a shot- just by destroying infrastructure that significantly relies on information technology. The fast growth of the Internet users and Internet dependence dramatically increased the security risks, unless there are appropriate security measures to help prevention. To understand cyber terrorism it is important to look at its background, to see how the terrorist organizations or individuals are using the advantage of new technology and what kind of measures governments and international organizations are taking to help the fight against cyber terrorism.

The integration of crime prevention and criminal justice into all levels of education is essential in building long-term approaches to countering crime and violence. It is also critical in ensuring that the rule of law is respected from an early age in

order to build safe and prosperous societies for all.

The lack of minimum education and of the informatics ethical norms is reflected in an irresponsible behavior and lack of discernment in a professional use of the Internet. This is leading in some cases to a real "passion" for illegal activities in the computer networks and a glorification of the ones that are good in this endeavor.

Education is broadly recognized as a tool to promote peace, justice and equality for sustainable development. It has a major role to play in shaping the values of future generations, building collective consciousness, reshaping societal preferences and complementing this with the necessary skills to enact these values."

Chapter one

1.1 Statement of the problem

The problem of the present research is the weak level of awareness about cyber crimes among students in different grades. Additionally, Cybercrime is now an ever-present element of society. It does not discriminate between individuals, entities or governments. Everyone – and everything – is at risk.

1.2 Questions of research

The problem of the present research can be restated in the following question:

"How to confront Cybercrime through an educational security perspective?"

The above main research question will be investigated through the following sub-questions:

1-What is the students' level of awareness about cybercrimes?

2-What is Cyber Generation?

3-What is Cyber space?

4-What are Cyber crimes?

5-What are Forms of Cyber Crimes?

6-What are Reasons of Cyber Crimes?

7-What is Cyber War?

8-What is the Cyber Terrorism?

9-What is the Definition of Security?

10-What are the Security Features?

11- What are the Principles of Ensuring Cyber Security?

12-What are the layers of security?

13-What is the Role of Education in Confronting the Cyber Crimes?

14-What is the International Response against Cybercrimes?

1.3 Importance of research

This research paper is part of the cyber security awareness and education research project focuses primarily on issues relating to cyber security that have both a direct and an indirect impact on school learners, parents and education. This research report investigates a number of current cyber security problems faced by school learners, including social acceptance of mobile use, cyber bullying and access to inappropriate material. The findings of this research report highlight the urgent need for proper cyber security awareness, education and protection among school learners.

1.4 Research Methodology

Design

To achieve the proposed research, will adopt descriptive analytic design methodology

Instruments

- **The researchers developed a questionnaire to define the level of students' awareness about cyber crimes. (appendix1)**
- **The researchers developed a questionnaire to define if the teachers participated in raise the level of students' awareness**

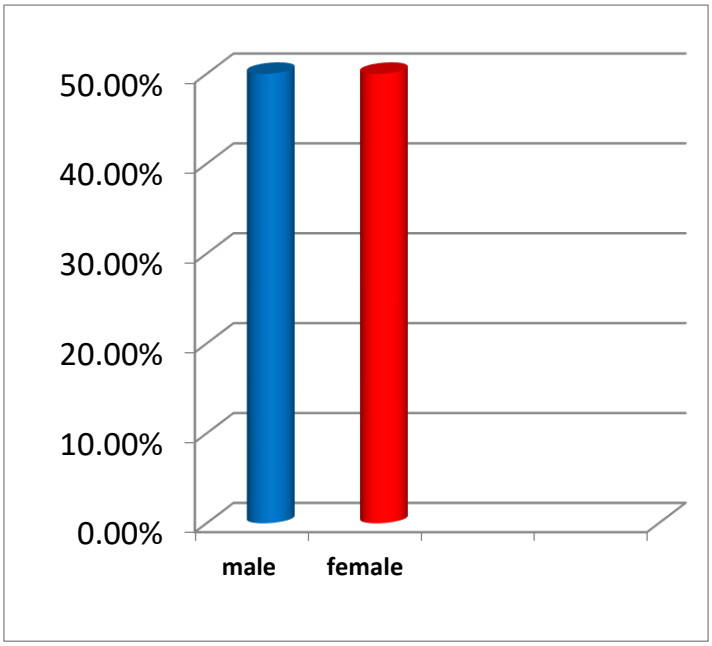
about cyber crimes through the school subjects they teach or through scholar activities. (appendix2)

1.5 Sample of the Research

The sample of this study were 100 participants(50 female/ 50 male) who were selected at random from prep/secondary stage students of prep/secondary schools for Port Said/ Alexandria/Suez/ Assuit cities of the academic year 2017/2018.

Table (1) Characteristics of the participants.

Sample	Gender	Grade	Mean of age
50	Female	Prep/secondary	15-18
50	Male	Prep/secondary	15-18



1.6 Limitations of the Research

Place: Port Said/ Alexandria/Suez/ Assiut

Time: academic year 2017/2018

1.7 Hypotheses of research

H1. Schools do not educate pupils to correct attitude towards protection from cyber crimes nor educate students about cyber security.

H2. There aren't enough security programs from the administration of fighting cyber crimes to raise the awareness of students against cyber crimes.

H3. Most of the students consider necessary to protect themselves from cyber crimes.

H4. Teachers and parents don't discuss the dangers of using the internet with the students.

1.8 Procedures of the Study

<u>The proposed study proceeded as follows:</u>

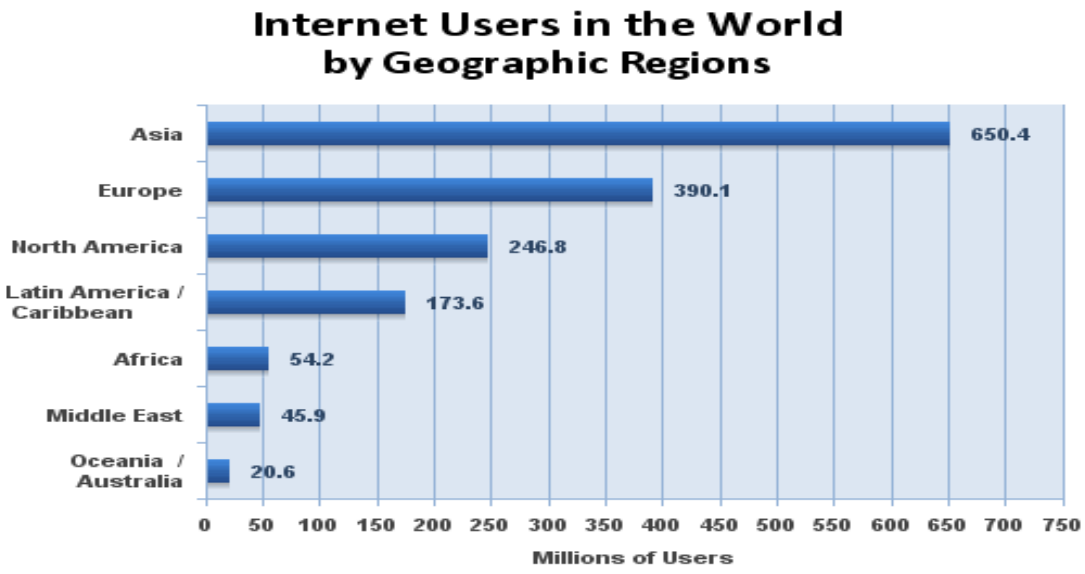
- **Reviewing the related literature and previous studies with special reference to Cybercrimes and cyber security.**
- **The researchers developed a questionnaire to define the level of students' awareness about cyber crimes. (appendix1)**
- **The researchers developed a questionnaire to define if the teachers participated in raise the level of students' awareness about cyber crimes through the school subjects they teach or through scholar activities. (appendix2)**
- **The researchers analyzed school subjects to determine if the school subjects include materials related to cyber crimes and cyber security.**
- **Recording and statistically processing of research findings.**
- **Analysis, interpretation and discussion of the obtained results.**

- **Presentation of research conclusions, recommendations and suggestions.**

Chapter Two

2.1 Cyber Generation

Kritzinger (2017) reported that it is important to understand that in order to be part of the cyber generation (generation Y) all cyber users must protect themselves and their personal information, and need to understand the possible cyber threats associated with using cyber devices and tools such as mobile phones, tablets and desktops, and connectivity to the internet. Generation Y has seen the world grow so much in their lifetime that they don't even realize what it was like in the past. 17 people found this helpful. In comparison to Generation X, members of Generation Y are more technologically savvy due to growing up within the Information Age and are prone to use media in everyday life.



2.2 Cyberspace

Singer and Friedman (2014,p.13) assure that cyberspace is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared. This means that it is not merely a physical

place and thus defies measurement in any kind of physical dimension. But cyberspace isn't purely virtual. It comprises the computers that store data plus the systems and infrastructure that allow it to flow. This includes the Internet of networked computers, closed intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has also come to encompass the people behind those computers and how their connectivity has altered their society. Cyberspace is becoming "the dominant platform for life in the 21st century."

2.3 Cyber crimes

Wexler (2014) defined a cybercrime as a new kind of threat. Cyber-criminals can commit crimes against victims who are thousands of miles away. So, people today are vulnerable to threats from criminals who would never have had access to them 20 years ago. It is easier for cyber-criminals to hide from the police, because in some cases they never show their face to the police or even to victims.

In other ways, cybercrime is a new means to commit crimes police have dealt with for decades. Fraud committed over the Internet is still fraud. Sex traffickers use social media to advertise prostitution. Street gangs increasingly are generating income by selling fake tickets to sports or musical events.

Cybercrime can have significant impacts. As police succeed in preventing traditional crimes such as bank robberies, those gains are dwarfed by increases in cybercrime. Criminal organizations are turning to cybercrime to finance their operations. Criminals and gangs have learned that cybercrime puts them at less risk for arrest or injury, and can earn them more money, than selling illegal drugs or committing other street crimes.

2.3.1 Forms of Cyber Crimes (Broadhurst and Chantler ,2009,33)

Computer crime, cybercrime, e-crime, hi-tech crime, electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. Such crimes may be divided broadly into 2 types of categories: (1) crimes that target computer networks or devices directly; (2) crimes facilitated by computer networks or devices,

the primary target of which is independent of the computer network or device.

Broadhurst and Chantler (2009,34) also added that although there is no definitive list of what constitutes cybercrime or computer related crime, a general consensus appears to have emerged about what falls within the scope of the offences that occur in cyberspace:

• Telecommunications Theft. • Sales and Investment Fraud, Forgery.

•Hacking another forms of illegal access to computer systems.

• Piracy Copyright Theft. • Cyber Stalking.

• Electronic money laundering and Tax evasion.

• Electronic Vandalism, Use of the Internet for Terrorist Purposes

• Electronic Funds Transfer Fraud and Counterfeiting (Carding).

• Identity Theft and Misrepresentation. •Sales of personal information

• Content Crime - Offensive Materials. • Espionage.

• Resource Theft - illegal use of PC. •Sales of illegal items

•Online child abuse and exploitation •Hacking

•Cyber-bullying •Sabotage

•Spread of virus/malware •Illegal gambling

•Sales of pharmaceuticals, including counterfeit or fake drugs.

2.3.2 Cybercrime Survey (Harteau, 2014)

In August 2013, PERF conducted a survey of 498 law enforcement agencies to examine the role of local police in combating cybercrime. 213 agencies responded, for a 43 percent response rate. PERF found that agencies use different definitions of cybercrime. For this survey, cybercrime was defined as a range of crimes involving: (1) the use of computers, smart phones, tablets, or other electronic devices as tools to commit a "traditional" crime such as theft or fraud; (2) the use of computers to commit online crimes, such as hacking, stealing data, and spreading computer viruses; and (3) the use of computers for storage of illegal material, such as child pornography.

Definitions and Criminal Codes: 13 percent of responding agencies said they have an official definition of computer or cybercrime, and 84 percent said they have specific state or local criminal codes governing computer crime and/or cybercrime. 25 percent of responding agencies said they analyze data on cybercrimes to identify trends and/or guide investigations. PERF asked agencies to list the criminal codes they most frequently use when charging cyber-specific crimes. The most common responses, in descending order, were: child exploitation, unlawful access to computer/ networks, fraud, harassment/stalking, identity theft, and general "computer crime." Thus, the most common area of cybercrime investigations by local police continues to be their longstanding role in criminal.

protecting children against pornographers or other threats.

Computer/Cybercrime Personnel: 42 percent of responding agencies reported having a computer crime or cybercrime unit. Among those agencies, 92 percent of the computer crime units involve evidence recovery (such as tracking stolen laptops); 46 percent conduct mobile phone tracking; 45 percent perform video enhancement (such as security camera footage); and 62percent conduct analyses of social media. easier to fund gang efforts through cybercrime than it is to rob somebody or sell drugs on the street corner, because you are much less likely to get caught. We can't physically see these cybercrimes, so there's less evidence, and less risk to the

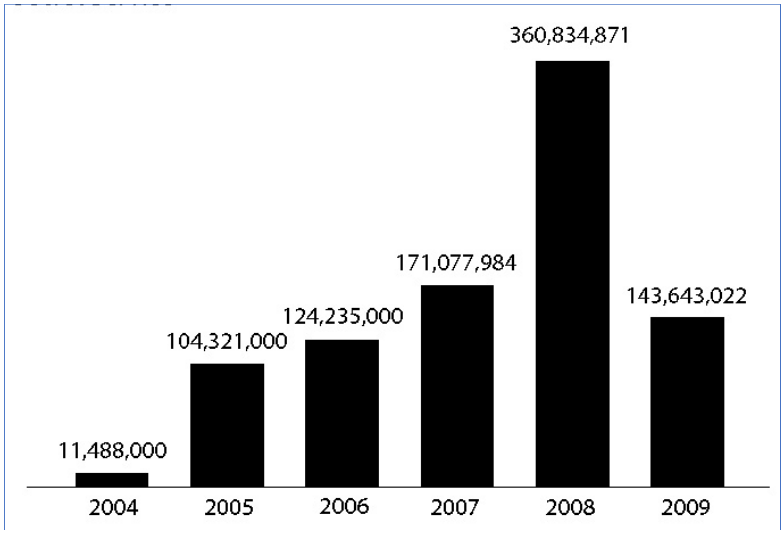


Figure Number of compromised records reported by VERIZONE

Why we use 2008 data? Because it seems that the year 2008 represented a peak in cyber criminal activity if the number of compromised records are taken into consideration (fig. 2)

2.3.3 Reasons of Cybercrimes

Why become a hacker?

Árpád (2013) answered that question. Maybe the most complex part of being a hacker is finding the motivation. The main aspects should be resumed in the followings:

a) Psychological motivation.

The need to prove something to themselves but especially to the circle of friends. Step up, show off, be somebody no matter how. Sometimes it is doubled by a desire to revenge after being rejected for some reasons from the circle of friends. What could have better taste than a revenge like stealing someone's credentials to his favorite socializing site and making fun of him or even hurting the person who make us feel bad ?! But this first successful step has the potential to open the appetite of a young mind to such kind of activities.

Another psychological factor is the need for adrenalin rush. The hacking can provide that feeling in almost the safest way because there is no danger to the physical health, no such activities that can cause injuries. A successful hacking and the action of deleting the trace of it, in some cases may have the same

physiological effect as a chase and escape after a robbery.

b) Financial, economical reasons

The next step in the evolution of a hacker is when the psychological needs are replaced by socio-economical ones. Let's face it, we talk about MONEY, SOCIAL STATUS. Successful hackers are discovered by criminal groups/organizations or they start by themselves to act in disrespect for the law. They use their knowledge, their expertise for "making money". Such a hacker is motivated financially and will work for interest not for pleasure.

c) Reaction of the public

The society has its own guilt by not condemning firmly the cyber criminals. Even more in several cases the society rises their cyber criminals to the rank of hero, glorifying their achievement. Often it is related to some kind of national pride something like " my fellow citizen hacked the FBI network, how good we are…..". This kind of reaction has an unwanted effect of encouraging cyber criminality. (a.n. especially in eastern European countries) . Often multimedia organizations, news studios present such persons as the results of an excellent educational system diverting the attention from the criminal act itself to the intellectual potential of the citizens of the country.

d) The ignorance of the public

Due mainly to the lack of information of the society regarding the imminent risks of the internet. The painful truth is that the majority of home users, also a considerable amount of SOHO users has no idea about the risks they face each time they connect to the internet, read a mail, download a "free" application. There are people who hear about cyber criminality when it is too late for them, being already a victim of some form of internet fraud. While in the case of older generations the only solution for them to be informed about cyber threats would be mainly the media (TV), in the case of students there is a huge opportunity to inform them while they are in school.

El Sayed (2012,64) added more reasons and motivations for cyber crimes as:

e) political motivations

This is due to the political conflicts that many governmental websites could be hacked or destroyed. It also includes spying with other governments and other security departments.

f) profit motivations

Statically, 43% of the motivations related to money. Financial sector and banks are considered the most targets for this kind of criminals. This is due to the electronic transferring systems which depend on decoding. As soon as this code is known for the criminals, they could transfer millions of dollar in no time and without any evidence which lead to them.

2.4 Cyber War

Singer and Friedman (2014) state that in the future, wars will not just be fought by soldiers with guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications, and energy. Such attacks could also disable military networks that control the movement of troops, the path of jet fighters, the command and control of warships."

2.5 Cyber Terrorism

Gordon and Ford (2003) mentioned that there are an almost uncountable number of ways that the terrorist can use the computer as a tool. Facilitating identity theft, computer viruses, hacking, using of malware, destruction or manipulation of data all fall under this category. These uses of the computer, when combined with 'computer as target' form the 'traditional' picture of cyber terrorism.

Bogdanoski (2014, 62) assured that the cyber terrorism as a concept has various definitions, mostly because every expert in security has its own definition. This term can be defined as the use of information technology by terrorist groups or individuals to achieve their goals. This may include the use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructure, and to exchange information and perform electronic threat.

Singer and Friedman (2014,96) reported that the FBI

defines cyber terrorism as a premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.

Denning(2000) defined cyber terrorism as the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

The United States Federal Bureau of Investigation (FBI, 2002). defines terrorism as the unlawful use of force or violence, committed by a group(s) of two or more individuals, against persons or property, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

The United States Department of Defense (DOD, 2002) defines terrorism using a slightly broader brush, calling it the unlawful use of, or threatened use, of force or violence against individuals or property, to coerce and intimidate governments or societies, often to achieve political, religious or ideological objectives. Whereas, the United States Department of State (DOS, 2002) definition states that terrorism is premeditated, politically motivated violence perpetrated against noncombatant targets by sub national groups or clandestine agents.

Cereijo (2006) considered the fact that the terrorists have limited funds, cyber attacks are increasingly attractive, because, their implementation requires a

smaller number of people and certainly smaller funds. Another advantage of cyber attacks is that they allow terrorists to remain unknown, because they can be very far from the place where the act of terrorism is committed. Unlike the terrorists that place their camps in countries with weak governance, cyber terrorists can store anywhere and remain anonymous.

Bogdanoski (2014, 64) believed that the most effective use of cyber terrorism is when it is used in combination with physical terrorism. For example, disabling the operation of emergency services in situations where the need for deployment of such services is caused by the use of physical terrorism is really an effective way of pooling of mentioned types of terrorism.

Bogdanoski (2014, 64) also added that as possible targets of cyber terrorism can be considered government computer networks, financial networks, power plants, and the reason for this is that the terrorists identifies all the above as most suitable targets to be damaged or put out of operation in order to cause chaos. Systems manipulation through "secret entrance" software, stealing classified information, data deletion, Web sites damaging, viruses inserting are just a few examples of how terrorists can enter into the secured system. The terrorist attacks enabled by computer technology can be also conducted through the air traffic control system or by remote damage of the power supply networks.

Lemos, R. (2002, 4) added that the terrorists use cyberspace to cause uncertainty. They, for their own reasons, are struggling against state authorities and governments and use all available means to achieve their own aim. Cyber attacks occur in two forms, one used to attack data, and others focused on control systems. Data theft and destruction leads to service sabotage and this is the most common form of Internet and computer attacks. The attacks focused on the control systems are used to disable or manipulate the physical infrastructure.

2.6 Cyber Security

2.6.1 Definition Security

Security is the process of maintaining an acceptable level of perceived risk. Security isn't just the notion of being free from danger, as it is commonly

conceived, but is associated with the presence of an adversary.

2.6.2 Security Features

a) Confidentiality

Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. It means the assurance that information is shared only among authorized persons or organizations

b) Integrity

Integrity means the assurance that the information is authentic and complete. In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

c) Availability

Availability is the assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. Availability of information refers to ensuring that authorized parties are able to access the information when needed

2.6.3 Principles of Ensuring Cyber Security (Retel ,2014,p.8)

1. Cyber security is an integral part of national security, it supports the functioning of the state and society, the competitiveness of the economy and innovation.

2. Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity.

3. Cyber security is ensured on the basis of the principle of proportionality while taking into account existing and potential risks and resources.

4. Cyber security starts with individual responsibility for safe use of ICT tools.

5. A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats that materialize.

6. Cyber security is supported by intensive and internationally competitive research and development.

2.6.4 Create layers of security

Protecting data, like any other security challenge, is about creating layers of protection. The idea of layering security is simple: the user cannot and should not rely on just one security mechanism – such as a password – to protect something sensitive. If that security mechanism fails, the user has nothing left to protect him/her. When it comes to data security, there are a number of key procedural and technical layers the user should consider:

1-Inventory data 2- Identify and protect sensitive and valuable data

3- Control access to data 4- Secure data 5- Back up your data

1-Inventory data

There is a great need to conduct a data inventory so the user has a complete picture of all the data his/her business possesses or controls. It's essential to get a complete inventory, so the user doesn't overlook some sensitive data that could be exposed.

2-Identify and protect sensitive and valuable data

Data classification is one of the most important steps in data security. Not all data is created equal, and few businesses have the time or resources to provide maximum protection to all their data. That's why it's important to classify data based on how sensitive or valuable it is – so that the user know what the most sensitive data is, where it is and how well it's protected.

<u>Common data classifications include:</u>

a) <u>HIGHLY CONFIDENTIAL</u>: This classification applies to the most sensitive business information that is intended strictly for use within the company. Its unauthorized disclosure could seriously and adversely impact the company, business partners, vendors and/or customers in the short and long term. It could include credit-card transaction data, customer names and addresses, card magnetic stripe contents, passwords and PINs, employee payroll files, Social Security numbers, patient information (if you're a healthcare business) and similar data.

b) <u>SENSITIVE:</u> This classification applies to sensitive business information that is

intended for use within the company, and information that would consider to be private should be included in this classification. Examples include employee performance evaluations, internal audit reports, various financial reports, product designs, partnership agreements, marketing plans and email marketing lists.

c) <u>INTERNAL USE ONLY:</u> This classification applies to sensitive information that is generally accessible by a wide audience and is intended for use only within the company. While its unauthorized disclosure to outsiders should be against policy and may be harmful, the unlawful disclosure of the information is not expected to impact the company, employees, business partners, vendors and the like.

3- Control access to data

No matter what kind of data the person has, he/she must control access to it. The more sensitive the data, the more restrictive the access. As a general rule, access to data should be on a need-to-know basis. Only individuals who have a specific need to access certain data should be allowed to do so. Once the person classified his/her data, begin the process of assigning access privileges and rights – that means creating a list of who can access what data, under what circumstances, what they are and are not allowed to do with it and how they are required to protect it. As part of this process, a business should consider developing a straightforward plan and policy – a set of guidelines – about how each type of data should be handled and protected based on who needs access to it and the level of classification.

4- Secure data

In addition to administrative safeguards that determine who has access to what data, technical safeguards are essential. The two primary safeguards for data are passwords and encryption. Passwords implemented to protect the most sensitive data should be the strongest they can reasonably be. That means passwords that are random, complex and long (at least 10 characters), that are changed regularly and that are closely guarded by those who know them. Employee training on the basics of secure passwords and their importance is a must.

Passwords alone may not be sufficient to protect sensitive data. Businesses may want to consider two-factor authentication, which often combines a password with another verification method, such as a dynamic personal identification number, or PIN.

Some popular methods of two-factor identification include:

- **Something the requestor individually knows as a secret, such as a password or a PIN.**
- **Something the requestor uniquely possesses, such as a passport, physical token or ID card.**
- **Something the requestor can uniquely provide as biometric data, such as a fingerprint or face geometry.**

Another essential data protection technology is encryption. Encryption has been used to protect sensitive data and communications for decades, and today's encryption is very affordable, easy-to-use and highly effective in protecting data from prying eyes. Encryption encodes or scrambles information to such an advanced degree that it is unreadable and unusable by anyone who does not have the proper key to unlock the data. The key is like a password, so it's very important that the key is properly protected at all times. Encryption is affordable for even the smallest business, and some encryption software is free. The user can use encryption to encrypt or protect an entire hard drive, a specific folder on a drive or just a single document. The user can also use encryption to protect data on a USB or thumb drive and on any other removable media. Because not all levels of encryption are created equal, businesses should consider using a data encryption method that is FIPS-certified (Federal Information Processing Standard), which means it has been certified for compliance with federal government security protocols.

5- Back up data

Just as critical as protecting the data is backing it up. In the event that data is stolen by thieves or hackers, or even erased accidentally by an employee, at least have a copy to fall back on. Put a policy in place that specifies what data is backed up and how; how often it's backed up; who is responsible for creating backups; where and how the backups are stored; and

who has access to those backups. Small businesses have lots of affordable backup options, whether it's backing up to an external drive in office, or backing up automatically and online so that all data is stored at a remote and secure data center. Remember, physical media such as a disc or drive used to store a data backup is vulnerable no matter where it is, so make sure to guard any backups stored in office or off site and also make sure that backup data storage systems are encrypted.

2.7 The Role of Ministry of Interior in Confronting the Cyber Crimes

- **The ministry of interior set up the administration of cyber and informative crimes which includes a unit that follow and trace the current events of social media and correlated with the security of the home country and citizens.**
- **The ministry of interior set up a unit to receive the citizens' complaints online and social media.**
- **There are several geographical branches all over the Republic of Egypt to enlarge the role of the central administration of Cairo to encompass Canal Zone, East Delta, North and South of Upper Egypt to confront the cyber crimes.**
- **There are plans to secure the informative system of the ministry of interior devices to protect them from hacking and that happens through co-operative protocol with the ministry of communications.**
- **There is also a law to fight and confront the informative and cyber crimes which committed through electronic devices.**
- **The members of the informative administration made lawful and technical researches to confront the cyber crimes.**
- **Arrest numerous cyber criminals who committed crimes through computers.**
- **Trace the websites and online pages of the terrorist troops and arrest the terrorist who publish terrorist information.**
- **The officers of the administration made**

lectures for university students.

- There are TV programs to raise the citizens' awareness of the secure use of the internet.
- The members of the fighting crime sector have been developed through training courses inside Egypt and abroad to raise their knowledge with the latest methods to confront crimes.
- The research efforts of fighting crimes have been developed through using the modern techniques.

2.8 The Role of Education in Confronting the Cyber Crimes

Strach (2011) proved that school is the one that offers the first official meeting of children with the computer systems. Many children currently have the possibility to use computer at home, however, it is the school that should teach children to use information technologies the right way and instruct them on the dangers that can lead to committing criminal acts by wrong usage. Especially, it is needful to show how easy it is to breach the copyright or commit a criminal act on the Internet.

Johnson H. (2007) assured that the Higher Education sector is increasingly exploring the use of information systems and technology to meet the needs and expectations of diverse learners who demand more than just traditional classroom-based experiences. New course delivery models attempt to blend face-to-face elements with e-Learning, Webinars and other online digital content. Building trust and encouraging engagement amongst users of online learning systems is important because there are opportunities for both synchronous and asynchronous interactions with the system. Synchronous learning occurs in real-time, with all participants interacting at the same time, while asynchronous learning is self-paced and allows participants to engage in the exchange of ideas or information without the dependency of other participants′ involvement at the same time.

Bandara and Ioras (2014) states Higher Education is a very different environment to what it was several years ago and is now offering significant student engagement via online learning systems. Students have an increasing understanding of

information systems (IS) and information technology (IT) issues, so overall learning strategies devised by course providers must be intrinsically linked with IS/IT strategies to meet student needs now and in the future. Digital natives and digital immigrants will share high expectations of their e-Learning system, in terms of usability, security and protection of their personal information. This could include the secure handling of a student's bank details associated with payments for course fees and other products.

Universities in the UK hold significant intellectual property through research and other academic materials, which could be attractive targets for cyber-criminals. Researchers will expect their sensitive work and commercially important information to be securely stored, with no risk of theft or misuse. Institutions should perform a cyber security risk assessment and determine best arrangements for technology, people and processes.

Schneider (2013) assured that the evolution of a university level cyber security curriculum is being stunted by the culture and values in universities as well as by our ignorance. Change is needed on all of these fronts. The failure of faculty to take action leaves a door open to others who will. And those outsiders are waiting—not only does the private sector offer cyber security training that could easily encroach, but governments (such as the US National Initiative for Cyber security Careers and Studies; www. niccs.us-cert.gov) show a growing interest in cyber security education at all levels.

Alw and Fan (2010) have reviewed the security issues that relate to e-Learning systems. They have presented a useful overview of the most serious threats:

- **Deliberate software attacks (viruses, worms, macros, denial of service)**
- **Technical software failures and errors (bugs, coding problems, unknown loopholes)**
- **Acts of human error or failure (accidents, employee mistakes)**
- **Deliberate acts of espionage or trespass (unauthorised access and/or data collection)**

• Deliberate acts of sabotage or vandalism (destruction of information or system)

• Technical hardware failures or errors (equipment failure)

• Deliberate acts of theft (illegal confiscation of equipment or information)

• Compromises to intellectual property (piracy, copyright, infringement)

•Quality of Service deviations from service providers (power and WAN service issues)

• Technological obsolescence (antiquated or out-dated technologies)

• Deliberate acts of information extortion (blackmail for information disclosure).

Table (2), describes protection against data manipulation, user authentication and confidentiality as important security issues in e-learning.

Chen and He (2013) reviewed the academic research literature in order to discover the main security risks and protection measures in e-Learning systems (online learning).

Table (2): Protection against data manipulation, user authentication and confidentiality

Security risks	Protection measures
•ARP cache poisoning and MITM attack • Brute force attack • Cross-Site Request Forgery (CSRF) • Cross Site Scripting (XSS) • Denial of Service (DoS) • IP spoofing • Masquerade • Rootkits • SQL Injection • Session Hijacking • Session Prediction • Stack-smashing attacks	•Installing firewalls and anti-virus software • Implementing Security Management (ISM) • Improving authentication, authorization, confidentiality, and accountability • Using digital right management and cryptography • Training security professionals

Hanewald (2008) suggested that schools and educational authorities may set up educational programs to alert to cyber crimes, inform about its potential damage and thus prevent incidents. Establishing of school policies and monitoring school computers accordingly are intervention approaches available to the institutions to curve or eradicate the abuse. Punitive action such as the loss of internet privileges for perpetrators, detention or even dismals from school for sever or repeat offenders are other measures. The battle against cyber crimes can be fought electronically by institutions and individuals through the installation of filtering and blocking software. Parents may wish to invest into specific parental control software, which is easily switched on and off. If activated, it restricts their children's access to Internet content. Disabling unwanted contact option is a very effective method for blogs, websites, emails and mobile phone users.

2.9The International Response against Cybercrimes

2.9.1 The Role of UNESCO in Confronting the Cybercrimes

UNESCO (2015) announced that the Broadband Commission Working Group on Gender launched today a report titled 'Combatting Online Violence Against Women and Girls: A Worldwide Wake-Up Call.' Which reported that 73 percent of women have already been exposed to, or have experienced, some form of online violence. Online violence against women exists in many forms, including online harassment, public shaming, sexual assaults and induced suicides. In the European Union, 9 million women -some as young as 15 years old- have experienced online violence.

Violence against girls and women – offline as well as online – is an affront to individual dignity, a violation of human rights and a barrier to development. Cyber violence is complex – our action must be equally multi-dimensional" said UNESCO's Director for Gender Equality, Ms Saniye Gülser Corat, on the occasion of the launch of the report.

The report highlights how online violence against women has caused the Internet to become a "chilling space" that permits anonymous cruelty and

consequently impedes the freedom of women to participate in the uptake of broadband services. This has led to a call to reclaim and expand the freedoms offered by the Internet

The report emphasizes the need to address complacency and hostility towards the issue of cyber-violence. Despite the rapid spread of the Internet, law enforcement agencies have largely responded inappropriately to the threat of cyber violence against women. One in five female Internet users lives in countries where harassment and abuse of women online is extremely unlikely to be punished. In many countries, women are reluctant to report their victimization for fear of social repercussions. The report warns that without effective legal and social controls of online anti-social and criminal behaviors, online violence will continue to grow as a threat to women. The report sets out three key recommendations for establishing a global framework to counter online violence. These are:

- **Sensitization – Preventing cyber violence against women through training, learning, campaigning and community development to promote changes in social attitudes and behavior,**
- **Safeguards – Implementing oversight and maintaining a responsible Internet infrastructure through technical solutions and more informed customer care practices, while ensuring the respect of other freedoms and rights,**
- **Sanctions – Develop and uphold laws, regulations and governance mechanisms to deter perpetrators from committing these acts.**

2.9.2 The Role of North Atlantic Treaty Organization (NATO) in Confronting the Cybercrimes

NATO (2002) repot declared that as sophisticated political-military alliance, NATO has long been familiar with the use and defense of electronic and information warfare. For years, NATO is involved in efforts to transform the military organization and conduct of operations by "networking oriented warfare" and "network enabled capabilities". At the Prague Summit in November 2002, NATO leaders decided to

strengthen its capabilities to defend against cyber attacks. Decision in Prague resulted in many initiatives.

A new NATO Cyber Terrorism Program is initiated, involving various NATO bodies: NATO Communication and Information Systems Services Agency (NCSA), described as the "first line of defense against cyber terrorism," NATO INFOSEC Techinical Center (NITC), responsible for communication and computer security; NATO Information Assurance Operations Centre (NIAOC), responsible for management and coordination of cryptographic equipment in response to a cyber attack against NATO; NATO Computer Incident Response Capability (NCIRC), whose task is to protect the NATO encrypted communications systems.

NATO (2008) reported that after the cyber attack against Estonia in April and May 2007, NATO ministers agreed on the outline of the NATO's cyber defense concept, which was brought in Nordwijk, in October 2008.This concept at the beginning of 2008 was developed into a NATO Policy on Cyber Defense. The NATO members were informed in more details about this policy on the NATO Summit held in Bucharest at the beginning of April 2008. Following the Summit, NATO established Cyber Defence Management Authority (CDMA), in order to bring together all key players in the NATO activities related to cyber defense, and better management of the cyber defense support to any member of the alliance in defense against cyber attack, upon request.

2.9.3 The Role of United Nations (UN) in Confronting the Cybercrimes

UN(2001) Cyber security is one of the main themes on the traditional debates on security policy in the UN system. Normally this refers to those debates related to the threat of terrorism and in the form of Resolutions of the UN Security Council. The topic is covered in the work of the Counter Terrorism Committee established by Security Council, and it is mentioned in the UN Global Counter-Terrorism Strategy. In the UN system, the International Telecommunication Union (ITU) has highest responsibility for the practical aspects and

applications of the international cyber security.

ITU(2007) The ITU mission statement embraces the issue of cyber security in direct terms. The purpose of the organization is to develop confidence in the use of cyberspace through enhanced online security. Achieving of the cyber security and cyber peace are some of the most critical concerns in the ICT development, and ITU takes concrete measures through its Global Cyber security Agenda (GCA).

2.9.4 The Role of Organization for Security and Co-operation in Europe (OSCE) in Confronting the Cybercrimes

OECD(2002) OSCE's interest in the challenges of cyber security is increasing. In December 2004, the OSCE Ministerial Council decided to dedicate to the "extent of use of the Internet by terrorist organizations," including a number of activities, such as recruiting of the terrorists, foundation, organization and propaganda .Two years later, the foreign ministers called for greater international cooperation and utilizing more effort to protect vital critical information infrastructures and networks from the threat of cyber attacks. The participating countries were asked to closely monitor Web pages of the terrorist and extremist organizations and to exchange information with other governments in the OSCE and other relevant forums and it is asked more active participation of civil society institutions and the private sector in preventing and countering the use of the Internet for terrorist purposes. OSCE's Permanent Council has also been a venue for debate and discussion concerning cyber security.

2.9.5 The Role of Council of Europe (CoE) in Confronting the Cybercrimes

COE(2008) the Contribution of the CoE in the international cyber security policy is primarily through the Convention on Cyber Crime, which was opened for signature in November 2001 and which entered into force in July 2004. It is important to note that, although the Convention was signed by 46 countries, including Canada, Japan, South Africa

and the U.S., until today it has been ratified by only 26 countries, including Macedonia, Albania, Croatia, Estonia, Hungary, Lithuania, Romania and Slovenia, Sixteen other countries that are not members of the Council of Europe are reported as "known to use the Convention as a guideline for their national legislation" (including Brazil and India).

The CoE Convention on Cybercrime is important for several aspects. First, the Convention addresses the illegal activities and practices that features across spectrum of cyber security threats. Second, the Convention establishes common standards and procedures that are legally binding on its signatories. Third, the Convention is open to the Member States of the CoE and others, which increases its authority as an international instrument. Finally, the Convention introduced requirements for handling data and access that have led to concerns about the privacy law and civil liberties.

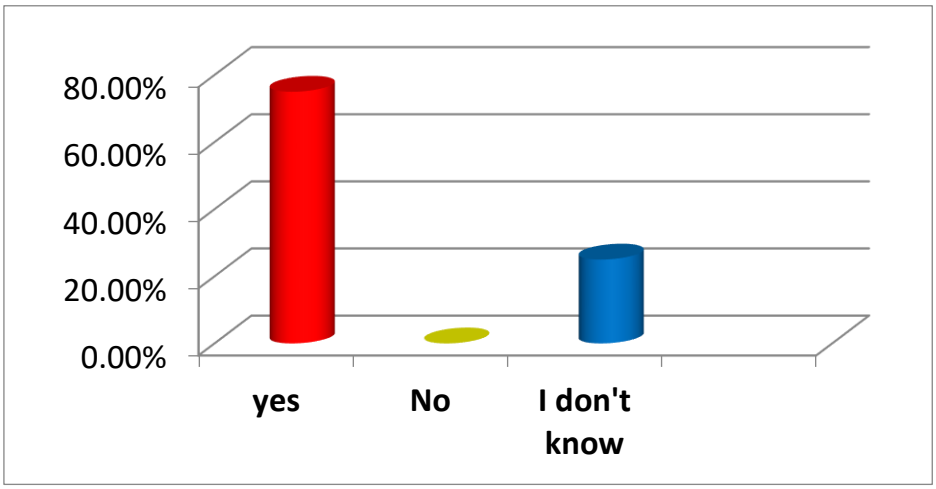
Chapter three

Results of the Research

Questionnaire (For Students)

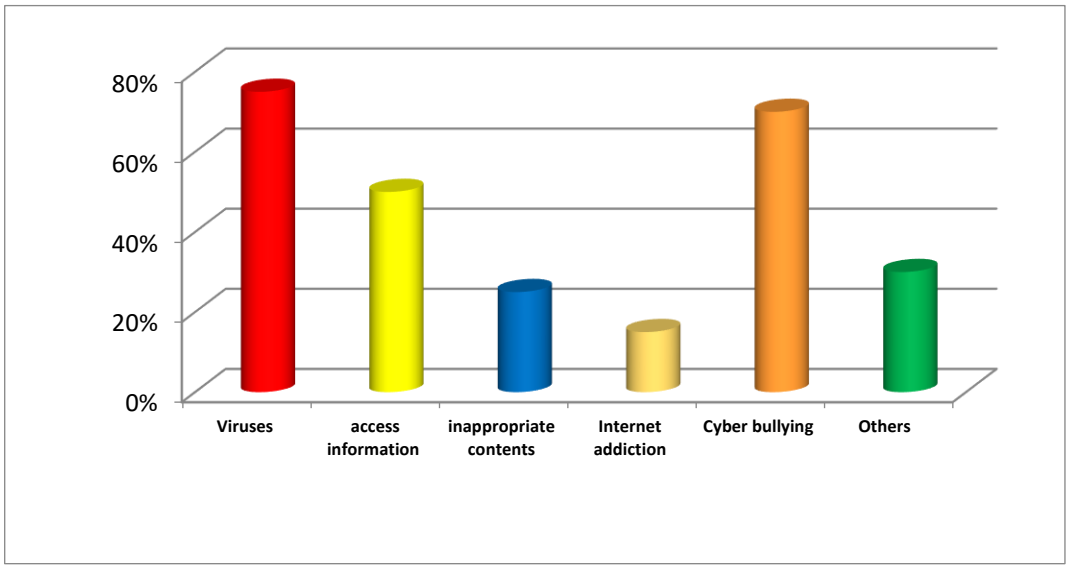
1-Do you think there are possible dangers or threats when you use the internet?

1	Yes	75%
2	No	0%
3	I don't know	25%



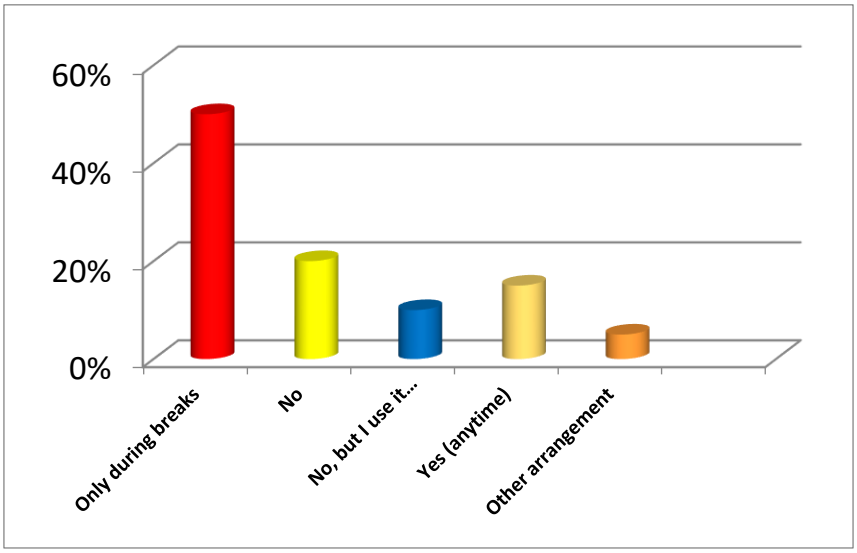
2-What do you think the possible dangers or threats when you use the internet?
(you can choose more than one answer)

1	Viruses	75%
2	Someone can access my personal information	50%
3	I may see inappropriate contents	25%
4	Internet addiction	15%
5	Cyber bullying	70%
6	Others	30%



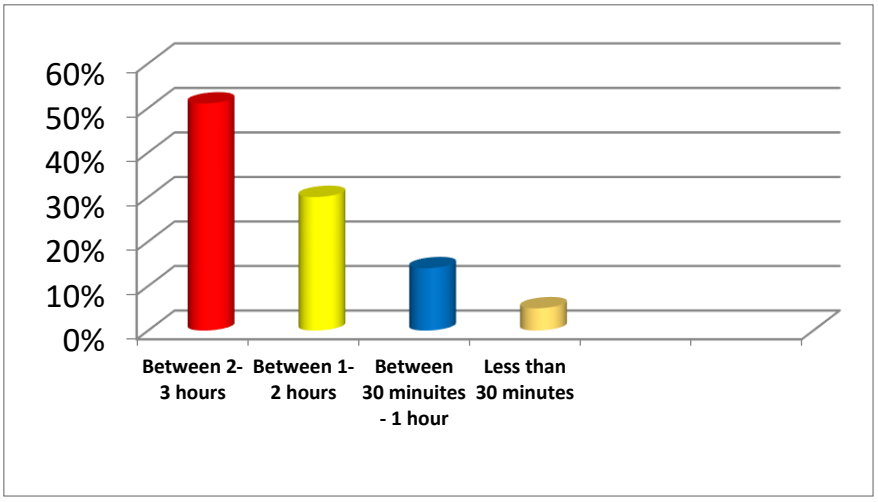
3-Are you allowed to use your cell phone during school hours?

1	Only during breaks	50%
2	No	20%
3	No, but I use it anyway	10%
4	Yes (anytime)	15%
5	Other arrangement	5%



4-On average, how many hours a day do you use your cell phone?

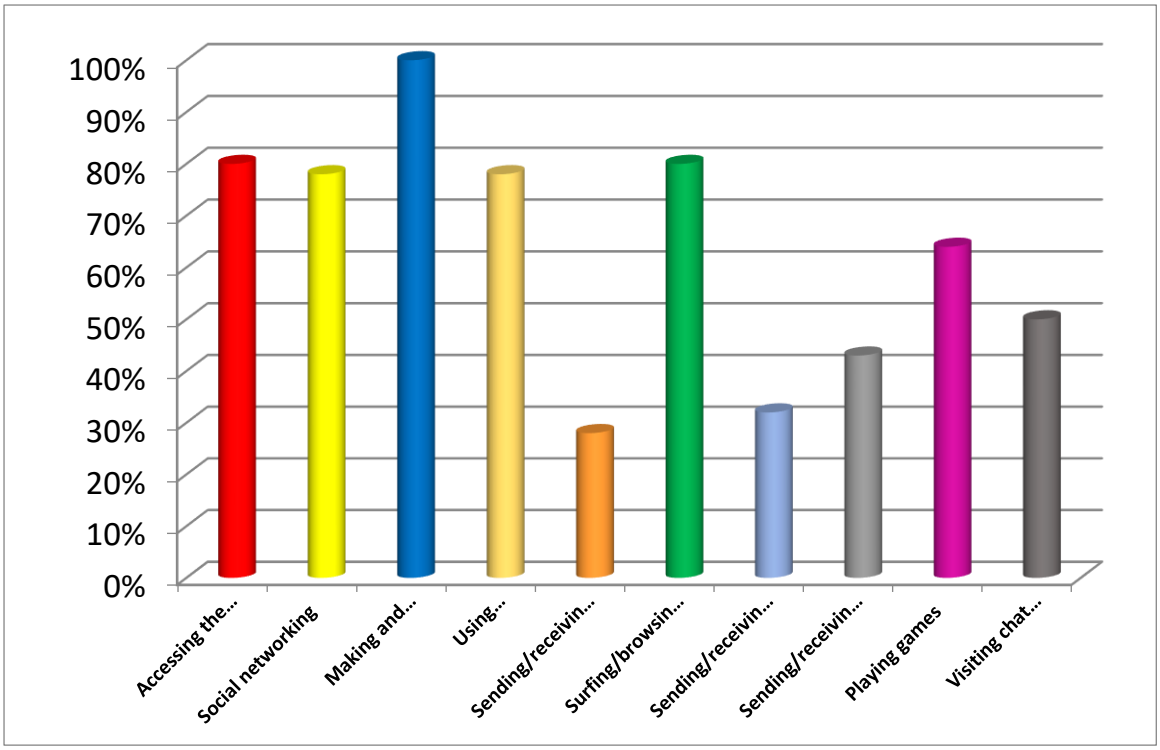
1	Between 2-3 hours	51%
2	Between 1-2 hours	30%
3	Between 30 minuites - 1 hour	14%
4	Less than 30 minutes	5%



5-What do you use your cell phone for? (you can choose more than one answer)

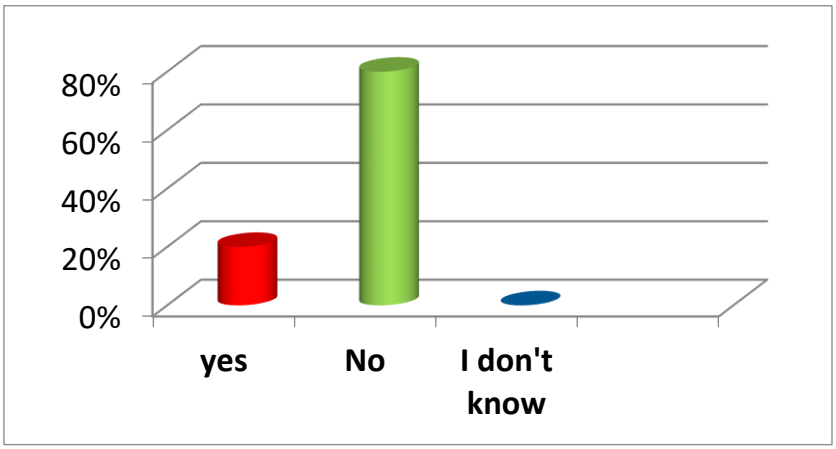
1	Accessing the internet	80%
2	Social networking	78%
3	Making and receiving calls	100%
4	Using ovoo/whatsapp/twitter	78%

5	Sending/receiving SMS's	28%
6	Surfing/browsing the internet	80%
7	Sending/receiving pictures	32%
8	Sending/receiving emails	43%
9	Playing games	64%
10	Visiting chat rooms	50%



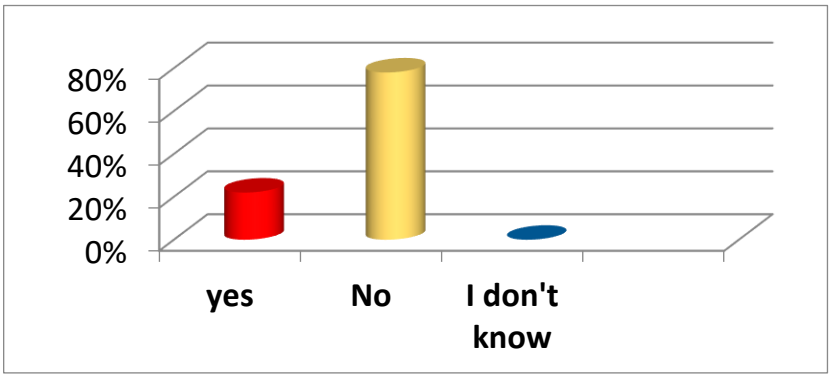
6-Have you ever tried to hide any of your online actions?

1	Yes	20%
2	No	80%
3	I don't know	0%



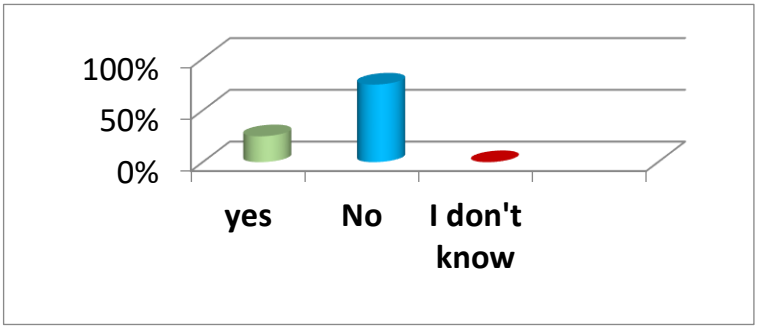
7-Do your parents or teachers monitor your internet use?

1	Yes	22%
2	No	78%
3	I don't know	0%



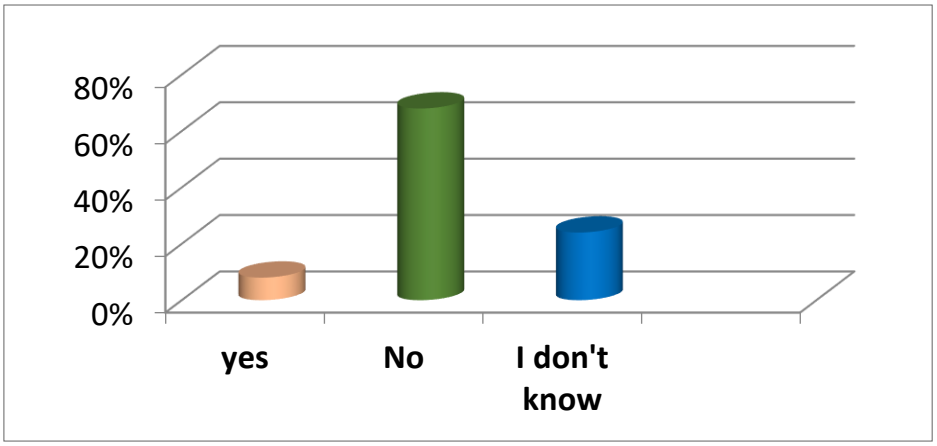
8-Have your parents or teachers discussed the dangers of using the internet?

1	Yes	25%
2	No	75%
3	I don't know	0%



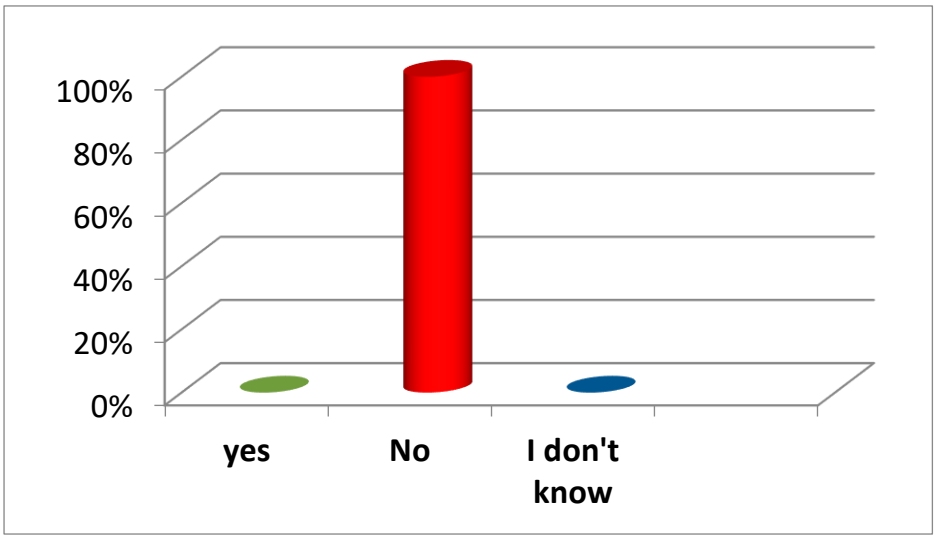
9-Have you ever accessed what you think may be inappropriate internet material?

1	**Yes**	**8%**
2	**No**	**68%**
3	**I don't know**	**24%**



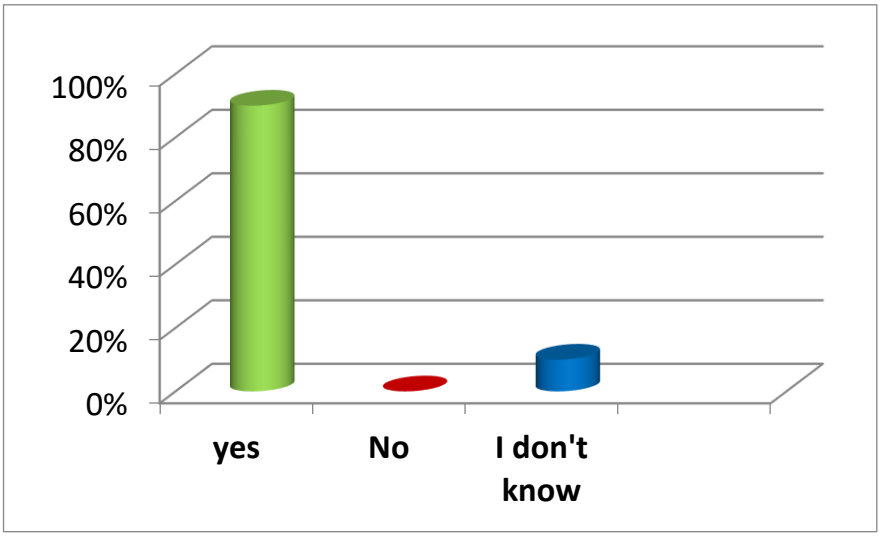
10-Have you been instructed in the lessons what cyber criminality is and what punishments are administered to those who commit the cyber crimes?“

1	**Yes**	**0%**
2	**No**	**100%**
3	**I don't know**	**0%**



11-Do you think your school should include cyber security awareness in the school curriculum?

1	**Yes**	**90%**
2	**No**	**0%**
3	**I don't know**	**10%**

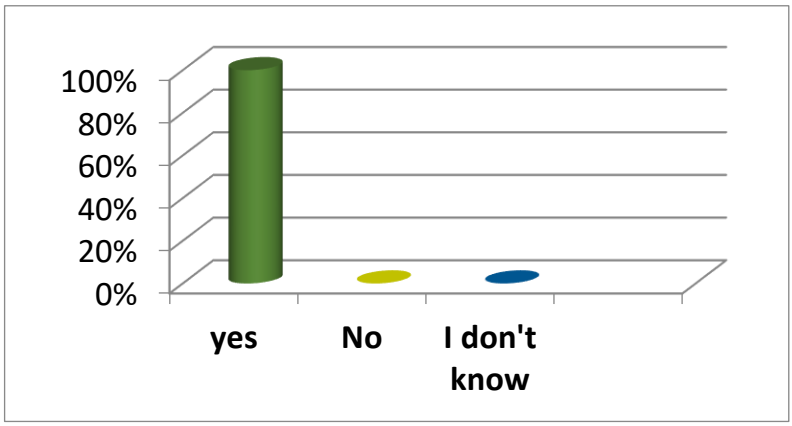


Results of the Research

Questionnaire (For Teachers)

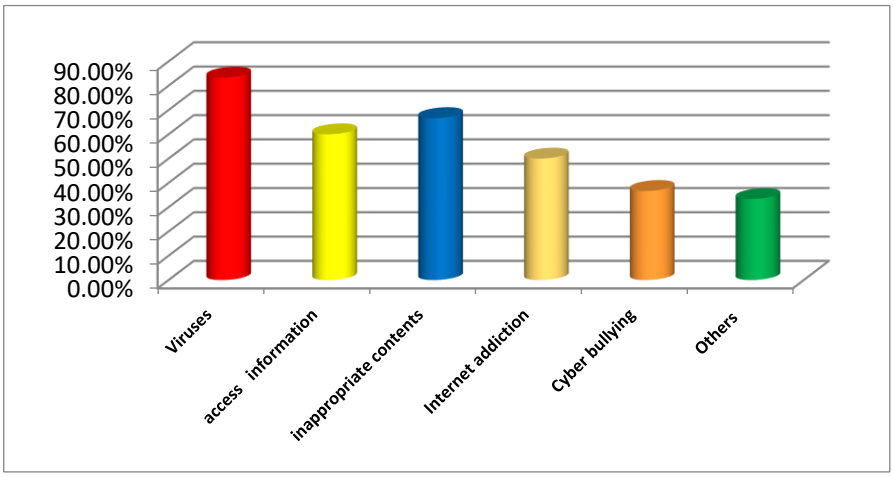
1-Do you think there are possible dangers or threats when your students use the internet?

1	Yes	100%
2	No	0%
3	I don't know	0%



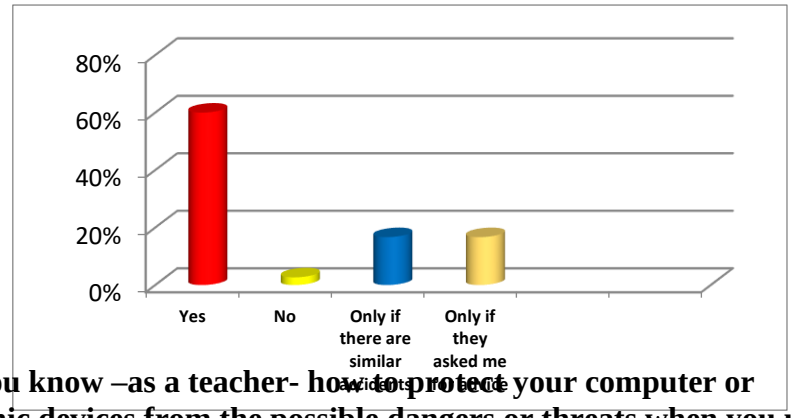
2-What do you think the possible dangers or threats when your students use the internet? (You can choose more than one answer)

1	Viruses	83.33%
2	Someone can access my personal information	60%
3	I may see inappropriate contents	66.67%
4	Internet addiction	50%
5	Cyber bullying	36.67%
6	Others	33.33%



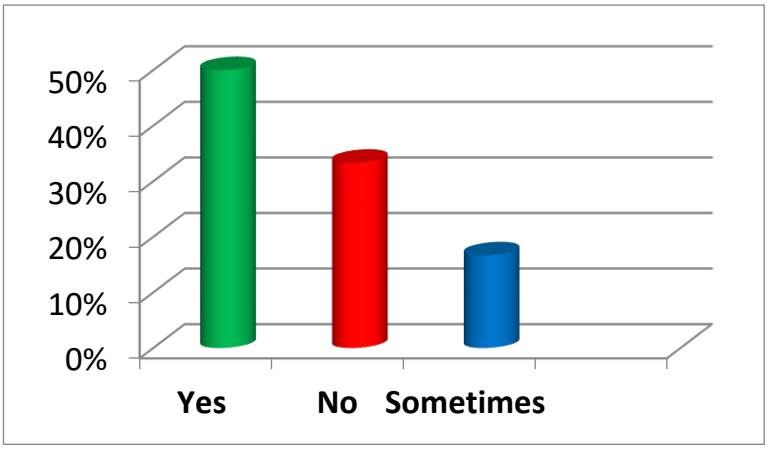
3-Have you ever warned your students about possible dangers or threats when they use the internet?

1	Yes	60%
2	No	6.67%
3	Only if there are similar accidents	16.67%
4	Only if they asked me for advice	16.67%



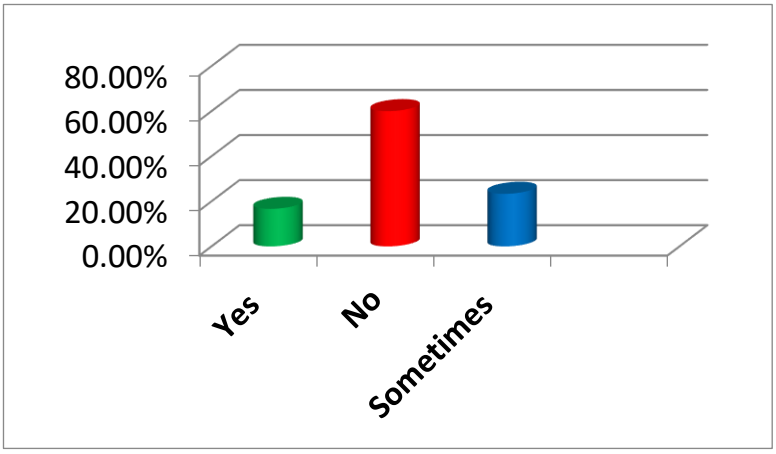
4-Do you know –as a teacher- how to protect your computer or electronic devices from the possible dangers or threats when you use the internet?

1	Yes	50%
2	No	33.33%
3	Sometimes	16.67%



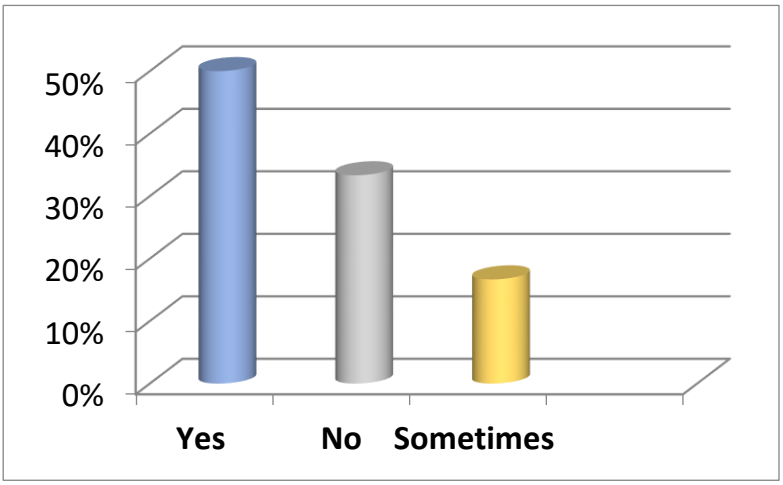
5-Have you ever co-operated with the students' parents to raise the awareness of the students with the dangers or threats when the students use the internet?

1	Yes	16.67%
2	No	60%
3	Sometimes	23.33%



6-Do you monitor your students while they use the internet inside the classroom?

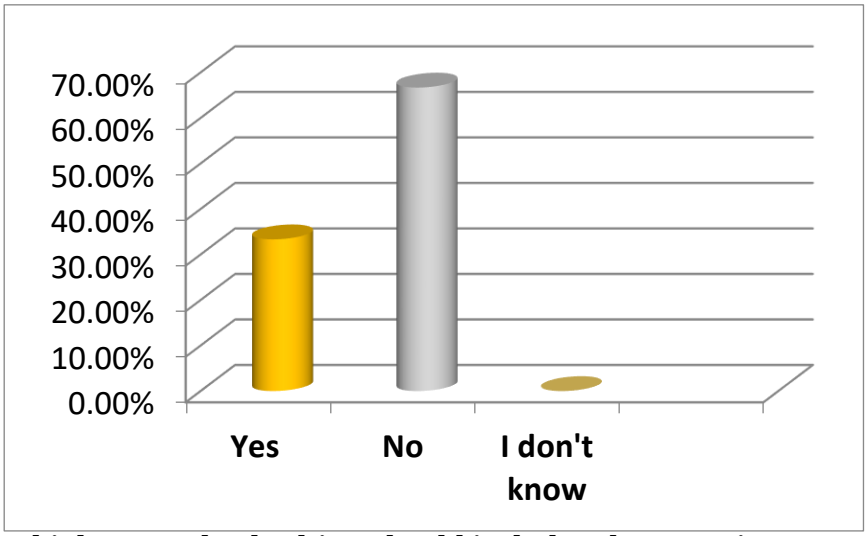
1	Yes	50%
2	No	33.33%
3	Sometimes	16.67%



7- Are there any parts of the school subject you teach discuss the cyber crimes and how to raise the students' awareness about cyber security?

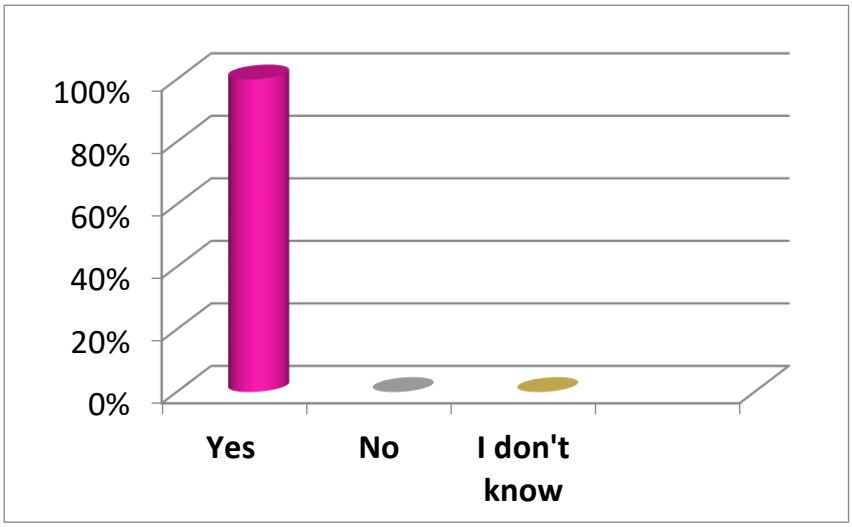
1	Yes	33.33%
2	No	66.67%

3	I don't know	0%



8-Do you think your school subject should include cyber security awareness in the curricula content?

1	Yes	100%
2	No	0%
3	I don't know	0%



Discussion and Summary of Results

The results based on investigating the hypotheses of

the present study can be listed as follows:

- **Schools do not educate pupils to correct attitude towards protection from cyber crimes nor educate students about cyber security.**
- **There aren't enough security programs from the administration of fighting cyber crimes to raise the awareness of students against cyber crimes.**
- **Most of the students consider necessary to protect themselves from cyber crimes.**
- **Teachers and parents don't discuss the dangers of using the internet with the students.**

These points have been investigated through:

- **Analyzing the students' questionnaire which developed by the researchers to define the level of students' awareness about cyber crimes. (appendix1)**
- **Analyzing the teachers' questionnaire which developed by the researchers to define if the teachers participated in raise the level of students' awareness about cyber crimes through the school subjects they teach or through scholar activities. (appendix2)**
- **Analyzing the contents of some school subjects of grades (3rd prep,1st sec,2nd sec&3rd sec) which include (English, Arabic, French, computer, social studies and science) the researchers found out that most school subjects don't include enough contents to raise the students' awareness against the cyber crimes except the curricula of computer 3rd**

prep&2nd sec which include units about cyber bullying and steps to secure websites and data base and the curricula of English 2nd sec experimental institutes (Enterprise4) which include unit about crimes but it discusses crimes and criminals in general and how to protect yourself against robbery but not online crimes . Some teachers (of Arabic and English) do their best by adding free discussion and written work about dangers and threats of internet.

Recommendations

Based upon the results of the present research, the researchers recommend the following:

- **There should be co-operation between the administration of fighting electronic crimes and the ministry of education to raise the students' level of awareness for cyber crimes through courses and meeting and protecting programs suit the different school grades.**
- **School subject should be included cyber security awareness in the curricula content. The lessons like "Technology Literacy" or "Digital Ethic" could be involved the education faculty programs in order to gained these outcomes to today's teacher candidates who are Y generation and called as digital native. The concept of these lessons could be occurred coming strategies and methods of cyber bullying both individuals and teachers.**
- **School of all types should intensively work out prevention measures for increasing awareness as well as moral responsibility of their students when using the Internet for their publication work.**
- **It is necessary that all the pupils and students were informed on the obligation to quote the used material and honour copyright.**

- **The primary tool for cybercrime prevention is education which aimed at establishing greater awareness and knowledge regarding illegal Internet content and cybercrime among children and teenagers, as well as parents and educators.**
- **As many children have Smart phones, special attention should be paid to Smart phones and other mobile devices.**
- **Here is a great need for pre-service and in-service teacher education programs to prepare educators to manage how to confront cyber crimes.**
- **Cyberspace crosses geographic and governance boundaries. Continued efforts are needed to advance and coordinate cyber security policies, laws, regulations, guidelines, and best practices.**
- **Governments, industry, educational associations, and organizations play individual and integrated roles in protecting the privacy and security of data, networks, computers, and devices.**
- **Governments should provide legal protections for legitimate and beneficial computing privacy and security research.**
- **There should be a balance between security and civil liberties.**
- **Fighting cyber crimes nationally or internationally must be based on legal base and mass perspective to the concept of crime to define the deeds which form the cyber crimes.**

Reference

- **Alw N. and Fan I. (2010). E-Learning and Information Security Management. *International Journal of Digital Society*, vol. Volume 1, no. Issue 2.**
- **Árpád, I. (2013). A greater involvement of education in fight against cybercrime. 2nd World Conference on Educational Technology Researches Procedia - Social and Behavioral Sciences 83 (2013) 371 – 377. Available online at www.sciencedirect.com retrieved at 20/4/2018**
- **Bandara, I. and Ioras, F. (2014). *Cyber Security Concerns in E-Learning Education*. Buckinghamshire New University. UK.**
- **Bogdanoski, M. (2014). Cyber Terrorism– Global Security Threat. INTERNATIONAL SCIENTIFIC DEFENCE, SECURITY AND PEACE JOURNAL on 21 May 2014.**
- **Broadhurst, R. and Chantler, N. (2009). Cybercrime Update: Trends and Developments.**
- **Chen, Y. and He, W. (2013). Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning, 2013.[Online].Available:http://www.irrodl.org/index.php/irrodl/article/view/1632/2712 retrieved at 15 /9/ 2014**
- **Cereijo, M.(2006). *Cuba the threat II: Cyberterrorism and Cyberwar*. Available at: 16 May 2006: http://www.lanuevacuba.com/archivo/manuel-cereijo-110.htm**
- **CoE (2008). Council of Europe Convention on Cybercrime: http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG**
- **Denning, D. (2000). *Cyber terrorism*. Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services. US House of Representatives.**
- **El Sayed, S. (2012). *Innovative International Crimes*. Police Academy. Egypt.**
- **Gordon, S. and Ford, R. (2003). *Cyber terrorism*. Symantec Security Response Symantec Corporation. USA.**
- **Johnson H. (2007). *Dialogue and the Construction of Knowledge in E-Learning: Exploring Students' Perceptions of Their Learning While Using Blackboard's Asynchronous Discussion Board*. European journal of open, distance and e-learning, no. ISSN 1027-5207.**

- **Hanewald, R. (2008). Confronting the Pedagogical Challenge of Cyber Safety. *Australian Journal of Teacher Education* .33(3).**
- **ITU(2007).ITU Global Cyber security Agenda (GCA, Framework for International Cooperation in Cyber security), ITU 2007, http://www.ifap.ru/library/book169.pdf**
- **Kritzinger , E.(2017). *Cyber Security Awareness and Education Research.* University of South Africa.**
- **Lemos, R. (2002). *Cyberterrorism: The real risk*: http://www.crime-research.org/library/Robert1.htm**

- **NATO. (2002). NATO Prague Summit Declaration Article 4(f), 21 November 2002: http://www.nato.int/docu/pr/2002/p02-127e.htm.**
- **NATO. (2008). Defence against cyber attacks, 26 June 2008: http://www.nato.int/issues/cyber_defence/index.html.**
- **OECD.(2002). OECD Guidelines for the Security of Information Systems and Networks: Toward a Culture of Security (Paris: OECD, 25 July, 2002), pp. 9-12: http://www.oecd.org/document/42/0,3343.html**
- **Retel , S. (2014). *Cyber Security Strategy*. Ministry of Economic Affairs and Communication**
- **Schneider, F. (2013). *Cyber security Education in Universities*. IEEE Computer and Reliability Societies.**
- **Singer, W. and Friedman, A. (2014). *Cyber Security and* Cyber *War*. Oxford University Press.USA. New York.**
- **Strach, J.(2011). Prevention of Cyber Crime in the Primary and Secondary School. School and Health 21, 2011, Education and Healthcare**
- **UN .(2001). UN Security Council Resolution 1373: reference to 'use of communications technologies by terrorist groups' (28 September 2001, para. 3(a)): http://www.un.org/News/Press/docs/2001/sc7158.doc.htm.**
- **UNESCO. (2015). UNESCO calls to combat online and offline violence against women and girls. retrieved at 20/4/2018 from https://en.unesco.org/news/unesco-calls-combat-online-and-offline-violence-against-women-and-girls**
- **Wexler , Ch.(2014). *The Role of Local Law Enforcement Agencies In Preventing and Investigating* .Cybercrime Police Executive Research Forum, Washington,D.C.**
- **http://www.businessdictionary.com/definition/Generation-Y.html**

- **http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf**

Appendix (1)

Questionnaire (For Students)

Dear /……..

The researchers are conducting a research study entitled "Cybercrime and how to confront it through an educational security perspective". A part of this study is to determine the risks and threats of internet and cybercrimes attacks.

Thank you in advance for your effort and co-operation.

The Researchers

Name (optional)……..
Grade ……
School/institute……
Gender (male/female) Age……

1-Do you think there are possible dangers or threats when you use the internet?

1	**Yes**	
2	**No**	
3	**I don't know**	

2-What do you think the possible dangers or threats when you use the internet?
(you can choose more than one answer)

1	**Viruses**	
2	**Someone can access my personal information**	
3	**I may see inappropriate contents**	
4	**Internet addiction**	
5	**Cyber bullying**	
6	**Others**	

3-Are you allowed to use your cell phone during school hours?

1	**Only during breaks**	
2	**No**	
3	**No, but I use it anyway**	
4	**Yes (anytime)**	

5	Other arrangement	

4-On average, how many hours a day do you use your cell phone?

1	Between 2-3 hours	
2	Between 1-2 hours	
3	Between 30 minuites - 1 hour	
4	Less than 30 minutes	

5-What do you use your cell phone for? (you can choose more than one answer)

1	Accessing the internet	
2	Social networking	
3	Making and receiving calls	
4	Using ovoo/whatsapp/twitter	
5	Sending/receiving SMS's	
6	Surfing/browsing the internet	
7	Sending/receiving pictures	
8	Sending/receiving emails	
9	Playing games	
10	Visiting chat rooms	

6-Have you ever tried to hide any of your online actions?

1	Yes	
2	No	
3	I don't know	

7-Do your parents or teachers monitor your internet use?

1	Yes	
2	No	
3	I don't know	

8-Have your parents or teachers discussed the dangers of using the internet?

1	Yes	
2	No	
3	I don't know	

9-Have you ever accessed what you think may be inappropriate internet material?

1	Yes	
2	No	

3	I don't know	

10-Have you been instructed in the lessons what cyber criminality is and what punishments are administered to those who commit the said crimes?“

1	Yes	
2	No	
3	I don't know	

11-Do you think your school should include cyber security awareness in the school curriculum?

1	Yes	
2	No	
3	I don't know	

Appendix (2)
Questionnaire (For Teachers)

Dear /……..

The researchers are conducting a research study entitled “Cybercrime and how to confront it through an educational security perspective”. A part of this study is to determine the risks and threats of internet and cybercrimes attacks and if the school subjects cover these items through the curricula content.

Thank you in advance for your effort and co-operation.

The Researchers

Name (optional)……..
School Subject ……
School/institute……

1-Do you think there are possible dangers or threats when your students use the internet?

1	Yes	
2	No	
3	I don't know	

2-What do you think the possible dangers or threats when your students use the internet? (You can choose more than one answer)

1	Viruses	
2	Someone can access my personal information	
3	I may see inappropriate contents	
4	Internet addiction	
5	Cyber bullying	
6	Others	

3-Have you ever warned your students about possible dangers or threats when they use the internet?

1	Yes	
2	No	
3	Only if there are similar accidents	
4	Only if they asked me for advice	

4-Do you know –as a teacher- how to protect your computer or electronic devices from the possible dangers or threats when you use the internet?

1	Yes	
2	No	
3	Sometimes	

5-Have you ever co-operated with the students' parents to raise the awareness of the students with the dangers or threats when the students use the internet?

1	Yes	
2	No	
3	Sometimes	

6-Do you monitor your students while they use the internet inside the classroom?

1	Yes	
2	No	
3	Sometimes	

7- Are there any parts of the school subject you teach discuss the cyber crimes and how to raise the students' awareness about cyber security?

1	Yes	

2	**No**	
3	**I don't know**	

8-Do you think your school subject should include cyber security awareness in the curricula content?

1	**Yes**	
2	**No**	
3	**I don't know**	