CSC ACADEMY

TOPICE-CYBER CRIME

PRESENTED BY-ABHIJIT PATRA

GUIDED BY-RAJESH DAS

On Cyber Crimes and Cyber Security

Abstract

The world has become more advanced In communication, especially after the invention of the Internet. A key issue facing today's society is the increase in cybercrime or e-crimes(electronic crimes), another term for cybercrime. Thus, e-crime pose threats to nations, organizations and individuals across the globe. It has become widespread in many parts of the world and millions of people are victims of e-crimes. Given the serious nature of e-crimes, its global nature and implications of e-crimes in different countries. Cybersecurity and searching methods to get secured are also part of the study.

Keyword: Cybercrime, e-crime, cyber security, computers, internet, social media, cyber laws

1. Introduction

The internet is the global system of interconnected computer networks that use the internet protocol suite to link billions of devices worldwide. Today, the Internet is one of the most important parts In daily life. The information technology revolution has brought two main function with internet. On one hand it has contributed positive values to the world. While, on the other hand, it has produced many problems that threaten the order of the society and also produce a new wave of crime in the world.

The internet is used for different purposes depending on user requirements such as communication, research, education, financial transaction, threading, etc. The internet has become an environment, where the most lucrative and safest crimes are conducted. This research focuses on cybercrime or e-crime (electronic crimes, another term for cybercrime. It refresh to criminal activity that involaves the internet , a computer or other electronic divices (Alex Rooney Mathew, Sayed Ai Hajj, and Khalil Ai Ruisi, 2010).

E-crimes are increasing in frequency and causing extensive damage to governments; companies, society, and individual (Broadhurst R. & Graboky P., 2005). Moreover, cyber criminals are motivated in various ways, including (but not limited to) financial gains, emotional instability, societal norms, and lack of legislation and punishment.

There are different names of e-crimes such as: the high-tech crimes, white collar crimes, and cybercrimes (Majid, 2012). Every year there is an increase of e-crimes due to the development of information technology and software changes (Rekouche, 2011). Thus, e-crimes have become very common and spread via various methods including malicious programs, which specially prepared to break through personal computer (OCs) or enterprise systems for copying confidential information or destroying systems. The most famous of these methods are hacking, Phishing, Spamming, Cyber stalking, Cyber defamation, Cyber terrorism, and Malware (Bruce S. Schaeffer, Henfree Chan, Henry Chan, and Susan Ogulnick, (2009) (Bhanu Sahu, Neeraj Sahu, Swatanra Kumar Sahu, and Priya Sahu, 2013).

Consequently, the first step to secure the information and deny access to anyone is Security programs. So many people and organizations have security programs to protect their software from the hackers (Bruce S. Schaeffer, Henfree Chan, Henry Chan, and Susan Ogulnick, 2009) Besides, many countries trying to enforce e-crimes laws pose danger to the society and the individuals. This is because of the spread and development of information technology and the ease acquisition of electronic appliances.

The purpose of this study is to have an overall survey concerning cybercrimes, social media, cyber laws and cyber security. It will also look at the e-crimes factors and the influence of factors that make e-crimes spreading in soc. Specifiiically, it examines the following points:

- Reserching and reviewing the most common types of e-crimes.
- Study the existing literatures on the factors influencing e-crimes.
- Finding out the concerns of the society in using the Internet.
- Identify the factors influencing e-crime in the Society. Especially, influence of demography and technology over different types of e-crime.
- Measurement and analysis of perceptions, experiences, and attitudes toward e-crimes.
- Determinig the relationship between social media and e-crimes.

Recommend the measures to reduce the e-crimes by the policy makersand awareness programs so that cyber security is made certain.

The rest of the chapter is organized as follows. Section 2 presents the detailed study on cybercrime . Section 3highlightes some of the common e-crime methods. Section 4 elaborates the factor of committing e-crimes . Cybercrimes in various countries are explored In Section 5. Section 6 discuses social media, cybercrimes and cyber laws . A survey of influenching factors towards e-crime is given in Section 7. The issue of cyber security is considered in Section 8 whereas Section 9 concludes the chapter .

2. Cyber Crimes

As mentioned in Section 1, the purpose of this chapter is to determine e-crimes factors and exmine the influence of the factors that make e-crimes spreading in society. Specifically, it examines the following : researching and reviewing the most common type of e-crimes, study the existing literatures on the factors influencing e-crimes , finding out concerns of the Kuwait society in using the Internet, identify the factors influencing e-crime in Kuwait Society. Especially, Influence of demography and technology over different types of e-crimes, determining the measurement and analysis of pereptions, experience, and attitudes toward e-crimes, determining the relationship between social media and e-crimes, finally, recommend the measures to reduce the e-crime by the policy makers and awareness programs. For the purposes of this researching, this chapter is arraneged in the following manner: the impact of e-crimes, classifications of e-crimes, then review the beginning and the growth of e-crimes . Methods of e-crimes will then be reviewed, Which will be followed by factors of e-crimes, protection and preservation of data, e-crimes in various countries, e-crimes in Kuwait. Finally, related work.

What is cybercrime or e-crime?

Cybercrime or e-crimes are offenses that are committed against individuals or grous with a
Criminal motive of intentionally harming the reputation of the victim, causing physical or
Mental harm, and cause loss of money or information on directly or indirectly or indirectly by using the internet and electronic devis (Johnson, 2013), (Broadhurst R. s abosky p., 2005) ,
(Alex Rooney Mathew, aayad Al Hajj, and khaki Al ruqeishi, 2010).

Impact of e-crimes

E-crimes affect the community in many ways. This includes (Amber stabek, paul waters, and
Robert Layton, 2010) (Bhanu sahu, Née raj sahu, swatantra kumar sahu, and priya sahu,
2013) (Balkh, 2013) (Brokenshire, 2013):

. Loos of online business and confidence in the digital economy,
. The potential for critical infrastructure to be compromised affecting watersupply, health
Services, national communications, energy distribution, finanacial services, and transport
. Loss of personal financial resources and the subsequent emotional damage.
. Loss of business assets,
. Costs to government agencies and business in re-establishing credit histories, Accounts and identities,
. Cost to businesses in improving cyber security measures,
. Stimulating other criminal activity, or
. costs in time and resources forlaw enforcement agencies.

Classifications of e-crimes

. computer crime: Using of direct electronic operation that can attack security to obtain data
And information illegally (kumara, 2009).
. High-tech crime: A board range of criminal activities that penetrate computers, hacking,
Money laundering, malware, harassment, electronic, and identity theft (Broadhurst R. s graboky
P.,2005).
. White –collar crime: A crime committed by a person of respectability and high social status in

The course of his occupation to obtain money. The famous persons who were convicted of white
Collars are Kenneth lay, Bernard mad off, and Bernard Embers. (Majid, 2012) (Rubino, 2014)
. Cybercrime: It is a criminal activity that is done by using computers and the internet
Including anything from illegal downloading of music files and games to the internet including
Anything from illegal downloading of music files and games to stealing millions of dollars from
Online accounts (grazed mask , and glory brink, 2010). Also non- monetary offenses, such as
Creating and distributing viruses on other computers or posting confidential business
Information on interthrough music and game files. (Schaeff B, chan H., and ogulnick S., 2009)
. cyber terrorism: premeditated and politically motivated attack against information, computer
Systems, computer programs, and data, which results in violence against (Brokrnshire, 2013).
Possible cyber terrorism targets include the banking industry, military installations,power plants
Air traffic control centers (Dogul M., Aslan A.sCelik E., 2011)

Beginning and growth of e-crimes

This section indicates several general tends, since 1960, about how e-crimes began and grew . the summary is as follows:
. In the early decades of modern information technology (IT), computer crimes were largely
Committed byunsatisfied individuals and dishonest employees.
. Physical damage to computer systems was a prominent threat until the 1982s (sterling, 1992)
. criminals often used authorized access to subvert security systems as they modified data for
Financial gain or destroyed data for revenge (Louw C. , von solms S. , 2014).
. Early attacks on telecommunications systems in the 1960s led to sabotage of the long distance
Phone systems for am segment and for theft of service (kebab , 2008).
. As telecommunications technology spread throught the IT word, people with criminal

Tenderned to penetrate systems and networks for amusement (Kennewick, 2008).
. programmers In the 1980s began writing malicious software, including self-replicating
Programs, to interfere with personal computers (Kebab, 2008.
. As the internert increased access to increasing numbers of systems of numbers of systems
Worldwide, criminals used unauthorized access to poorly protected systems for sabotage,
Political action and financial gain (Erbschloe, 2004).
. As the 1990s progressed, fiancée using penetgration and destabilization of computer systems
Increased (Sterling, 1992).
. the types of malware shifted during the 1990s, taking advantage of new vulnerabilities as
Operating system were strengthened, only to give way to new attack routes (Kenefick, 2008) .
. Illeal applications of e-mail grew rapidely from the mid-1990s onward, generating plenty of
Unwanted commercial and fraudulent emails (Hussinat M. , 2013).
. social networking has become an increasingly important tool for cyber criminals to recruit
People to assist threir money launderations around the globe (Erbschioe, 2004).
. mobile devices penetration – from smart phones to tablet PCs-accessing the internet by
2013 surpassed 1 billon, creating more opportunities for cybercrime (Rubino , 2014).

Specific e-crimes

The real beginning of e-crime started in 1960, when there attacks in the united states on the
Telecommunication systems, it led to destroying long distance phone communications (Kabay , 2008). In 1971, wire fraud by communication was escalated in united states when
The rogue program called creeper, which spread through early bulleted board network. In
The same yare, a person called Deaper built a blue box that allowed making long distance free

famous virus ‘Chen Ing-Hua’ (CIH) eas sent to the internet users around theworld (Kenefick, 2008).

Calls (Sterling, 1992).

Email spam was discovered in 1976, when it was sent out over the Advanced Research Project Agency Network (ARPANET) (Sterling, 1992). ARPANET kernel led to the advent of modern Internet (Ping, 2011). The first criminal convicted on e-crime was lan Murphy in 1981. Murphy penetrated and altered the billing clock in American Telephone & Telegraphs (AT&T’s) and people could get discounted rates during normal hours of business . In the early decades of the modern information technology the first virus on an Apple computer was detected in 1982 (Louw C. , Von Solms S. , 2014).

In 1986, the oldest virus called ‘Pakistani Brain’ was created by unauthorized cricumstances, which attacked the computers of International Business Machines (IBM) Corporation (Kenefick, 2008). And then, in 1988, Kevin Mitnick was sentenced for spying on e-mails for Microwave Communications Inc. (MCI) and Digital Equipment Corporation (DEC) (Kabay , 2008).

At the same year, the first worm of ARPANET surfaced on the government systems and got out control, which caused the closure of universities and government as it spread over 6000 networked computers. This was done by a graduate student at Cornell University called Robert T. Morris, who was dismissed form Cornell University and sentenced to three years’ probation with $10K fine (Sterling, 1992).After that, criminal activities began to make malicious software including self-replicating problem to interfere with personal computers (Kabay, 2008).

With the increasing of internet use, criminals started using malicious problems to get their goals. By mid-1990, e-crimes had gone too advanced and used software systems to computer breakthroughs and frauds spread by email (Hussainat M. , 2013). As that

In 1992, the first virus called 'Dark Avenger', was released (Sterling, 1992).In the late Nineties , the famous malware named 'Melissa' appeared . As well as the other famous virus 'Chen Ing-Hua' (CIH) was sent to the internet users around the world (Kenefick, 2008).

At the beginning of the millennium, the technological deve lopments of e-crimes increased significantly. In 2000, Denial of service (DOS) was sent to corrupt websites such as Yahoo, eBay, CNN, Amazon, Bey, etc. The famous virus in that periode 'I LOVE YOU', was spread by forwarding itself and sent to all contacts on the mail lists form their accounts (Erbschloe, 2004).

The most famous e-crimes took place in 2001, when Microsoft was attacked and corrupted form a new Domain Name server (DNS), which blocked Microsoft's Web sites for two days (Erbschloe, 2004). In addition, more new worms were discovered in the millenniun. These include The L10n worm, Code Red, Sadmind, Nimda memory-only, the Klez. H, Multiple variants of the MyDoom worm, and Storm Worm (Erschloe, 2004).

One of the most dangerous cyber-attacks is the Structured Query Language (SQL) – injection attack, launched through the web browsers, that leaves a lot of doors widely openfor the attackers to exploit these and gaining access to confidential Information that residesin the website server databases. In 2008, attackers used SQL injection techniques to malicious iFrame blocks on legitimate Web sites (Totarotech, 2013).

In recent years, conutries had begun to absorb the gravity of e-crimes to society and the individual because of electronic-attacks, as experienced by hakers in 2010. According to Spanish investigators, there were over 13 million infacted computers around the world, including PCs, affecting thousands of organization, and above forty major banks (Tabuchi,2011).

The imoportant historical event of e-crime was exposed by associateed press in 2013 about theft on Twitter account. The criminal wrote tweets about attacks in the White House that left president Obama injured. This tweet had led to a drop in Dow Jons by 130 points and withdrawal of 136 billion dollars form stock markets in the United States of America (Rubino,2014).

3. Method of e-crimes

The routine uses of the internet such as downloading songs, games, and free music from insecure sites as well as opening an unknown sender's message lead to the possibility of a threat via the internet (Fawn T. & Paternoster R., 2011). Cybercrimes are escalating by various method such as: malicious programs, which facilitated in penetrating devices (Dixon, 2005). These programs are progressing year after year with highest techniques that can help hackers to be hidden (Oweise N., Owais S.,Alrababa M., Alansari M.,2014). This section explains methods of e-crimes by using some of famous malicious programs such as:Hacking, Phishing, Spam, Cyber stalking, Cyber terrorism, Cyber defamation, and Malware as follows (WD Kearney & HA Kruger, 2014).

3.1 Hacking

Hacking developed by a highly skills programmer (Hacker) that enters a computer system and network in an illegal way (Bhanu Sahu, Neeraj Sahu, Swatantra kumar sahu, and Priya sahu, 2013). Hackers have easy targets and objectives, by hacking over websites' security to take and manage the theft data, such as edit, delete, install any file in any user's directory (Erbschloe, 2004). However, there are experts in machine code and operating systems and well-known in latest bugs, latest patches, latest in the patches, etc. (Oweis N., Owais S., Alrababa M., Alansari M., 2014). Finally, hackers are able to increasingly rely upon the community to identify bugs and create programs that can adapt for their specific purpose (Rekouche, 2011). Table 1 shows highest targets of e-crimes by hacking (Saina Das, Arunabha Mukhopadhyay, and Girja.K. Shukla, 2013) (Balkhi,2013) (Barnes B. and Perlroth N., 2014).

Table 1: Highest targets of e-crimes by hacking from 2011 to 2014.

Date	Target	Type of attack	Loss
2011	Citigroup	Hacking the system of the company	2.7 million Dollar
			Theft over 200000 customer sensitive information
2011	Citi Bank	Individual hackers	Over 2.7 million Dollar
			Customer data loss
2012	USDJ[1], FBI[2], RIAA[3],	Hacking website Defacement	Website downtime
			Website downtime

famous virus 'Chen Ing-Hua' (CIH) eas sent to the internet users around theworld (Kenefick, 2008).

Calls (Sterling, 1992).

Email spam was discovered in 1976, when it was sent out over the Advanced Research Project Agency Network (ARPANET) (Sterling, 1992). ARPANET kernel led to the advent of modern Internet (Ping, 2011). The first criminal convicted on e-crime was lan Murphy in 1981. Murphy penetrated and altered the billing clock in American Telephone & Telegraphs (AT&T's) and people could get discounted rates during normal hours of business . In the early decades of the modern information technology the first virus on an Apple computer was detected in 1982 (Louw C. , Von Solms S. , 2014).

In 1986, the oldest virus called 'Pakistani Brain' was created by unauthorized cricumstances, which attacked the computers of International Business Machines (IBM) Corporation (Kenefick, 2008). And then, in 1988, Kevin Mitnick was sentenced for spying on e-mails for Microwave Communications Inc. (MCI) and Digital Equipment Corporation (DEC) (Kabay , 2008).

At the same year, the first worm of ARPANET surfaced on the government systems and got out control, which caused the closure of universities and government as it spread over 6000 networked computers. This was done by a graduate student at Cornell University called Robert T. Morris, who was dismissed form Cornell University and sentenced to three years' probation with $10K fine (Sterling, 1992).After that, criminal activities began to make malicious software including self-replicating problem to interfere with personal computers (Kabay, 2008).

With the increasing of internet use, criminals started using malicious problems to get their goals. By mid-1990, e-crimes had gone too advanced and used software systems to computer breakthroughs and frauds spread by email (Hussainat M. , 2013). As that

In 1992, the first virus called 'Dark Avenger', was released (Sterling, 1992).In the late Nineties , the famous malware named 'Melissa' appeared . As well as the other famous virus 'Chen Ing-Hua' (CIH) was sent to the internet users around the world (Kenefick, 2008).

At the beginning of the millennium, the technological deve lopments of e-crimes increased significantly. In 2000, Denial of service (DOS) was sent to corrupt websites such as Yahoo, eBay, CNN, Amazon, Bey, etc. The famous virus in that periode 'I LOVE YOU', was spread by forwarding itself and sent to all contacts on the mail lists form their accounts (Erbschloe, 2004).

The most famous e-crimes took place in 2001, when Microsoft was attacked and corrupted form a new Domain Name server (DNS), which blocked Microsoft's Web sites for two days (Erbschloe, 2004). In addition, more new worms were discovered in the millenniun. These include The L10n worm, Code Red, Sadmind, Nimda memory-only, the Klez. H, Multiple variants of the MyDoom worm, and Storm Worm (Erschloe, 2004).

One of the most dangerous cyber-attacks is the Structured Query Language (SQL) – injection attack, launched through the web browsers, that leaves a lot of doors widely openfor the attackers to exploit these and gaining access to confidential Information

that residesin the website server databases. In 2008, attackers used SQL injection techniques to malicious iFrame blocks on legitimate Web sites (Totarotech, 2013).

In recent years, conutries had begun to absorb the gravity of e-crimes to society and the individual because of electronic-attacks, as experienced by hakers in 2010. According to Spanish investigators, there were over 13 million infacted computers around the world, including PCs, affecting thousands of organization, and above forty major banks (Tabuchi,2011).

The imoportant historical event of e-crime was exposed by associateed press in 2013 about theft on Twitter account. The criminal wrote tweets about attacks in the White House that left president Obama injured. This tweet had led to a drop in Dow Jons by 130 points and withdrawal of 136 billion dollars form stock markets in the United States of America (Rubino,2014).

3. Method of e-crimes

The routine uses of the internet such as downloading songs, games, and free music from insecure sites as well as opening an unknown sender's message lead to the possibility of a threat via the internet (Fawn T. & Paternoster R., 2011). Cybercrimes are escalating by various method such as: malicious programs, which facilitated in penetrating devices (Dixon, 2005). These programs are progressing year after year with highest techniques that can help hackers to be hidden (Oweise N., Owais S.,Alrababa M., Alansari M.,2014). This section explains methods of e-crimes by using some of famous malicious programs such as:Hacking, Phishing, Spam, Cyber stalking, Cyber terrorism, Cyber defamation, and Malware as follows (WD Kearney & HA Kruger, 2014).

3.1 Hacking

Hacking developed by a highly skills programmer (Hacker) that enters a computer system and network in an illegal way (Bhanu Sahu, Neeraj Sahu, Swatantra kumar sahu, and Priya sahu, 2013). Hackers have easy targets and objectives, by hacking over websites' security to take and manage the theft data, such as edit, delete, install

any file in any user's directory (Erbschloe, 2004). However, there are experts in machine code and operating systems and well-known in latest bugs, latest patches, latest in the patches, etc. (Oweis N., Owais S., Alrababa M., Alansari M., 2014). Finally, hackers are able to increasingly rely upon the community to identify bugs and create programs that can adapt for their specific purpose (Rekouche, 2011). Table 1 shows highest targets of e-crimes by hacking (Saina Das, Arunabha Mukhopadhyay, and Girja.K. Shukla, 2013) (Balkhi,2013) (Barnes B. and Perlroth N., 2014).

Table 1: Highest targets of e-crimes by hacking from 2011 to 2014.

Date	**Target**	**Type of attack**	**Loss**
2011	Citigroup	Hacking the system of the company	2.7 million Dollar
			Theft over 200000 customer sensitive information
2011	Citi Bank	Individual hackers	Over 2.7 million Dollar
			Customer data loss
2012	USDJ[1], FBI[2], RIAA[3],	Hacking website Defacement	Website downtime
			Website downtime

3.5Cyber defamation

Cyber defamation is a crime taking place in cyberspace through the internet to libel and damage the reputation of the victim (berg,2013).Defamation can categorized as libel and slander. Table 3 shows categories of cyber defamation(Linda L. Edwards, J. Stanley Edwards, Patricia kittle wells, 2008).frequently, it occurs during the election or while taking senior positions in the country . also, some persons defame others the elections or while taking senior positions in the country. Also, some persons defame others through publication across online networks (Bhatt S.& pant D.,2011).

With the advancement of internet technology, people have a large area to search and transfer the information. It also allows people to express their opinions where anyone can leave comments that can be libel, whether intentionally or unintentionally (berg,2013).

- Public comment on media like newspapers, magazines, and web sites.
- Comment on social media such as blogs, twitter, Facebook , instagram

- , and chat room (berg , 2013).

Table 3:cyber defamation categories.

Cyber defamation categoriese	
libel	Words or pictures that are written,printed,and copied in internte
Slander	Spoken words or sounds, sign language, and gesticulations

3.6 cyber terrorism

Cyber terrorism is defined as the act of internet terrorism in terrorist activities online. It includes destruction deliberate disruption of computer network connected to the internet, by the means of tools such as viruses and malware to security sites, official sites, or commercial sites (Neff, 1994). Terrorism in cyberspace can be as follows:

- Physical destruction of machinery an d it infrastructure.
- Penetration of computer network.
- Disruption of government network
- Disruption of financial networks or social media network.

Therefore, cyber terrorism has been used by terrorist groups to get their goals. it carries out attacks against the computer system, communications, infrastructure, and to launch electronic threats(Brokenshire,2013).

3.7 malware

Malware is the name of the program that are permitted in a way that they are hidden under the useful program. The term of malware generally cover viruses, worms and Trojans (Schaeff B, Chan H., and ogulnick S., 2009)(Erbschloe, 2004).

The viruses are programs having the ability to self-replicate and attach themselves to other executable programs. Viruses spread on the infected computer and it is difficult remove the, which leads to data loss (sheaf B, Chan H., and ogulnick S., 2009). Table 4 shows the different forms of viruses (swain,2009).

Table 4:virus categories

Virus categories	
Resident virus	A virus that is implanted in the memory on a target system .it become active whenever the system starts to operate. It implement specific action on the work every time .
Non-resident virus	A virus that transmits infection on network locations, removable, and local system. It does not remain in the system for a long time
Boot sector virus	A virus that targets a boot sector on the hard drive. It is being loaded into memory each time when an attempt is being made to boot from the infected drive.
Macro virus	A virus that has written especially in macro language in word, outlook, excel, Etc. it is being executed as soon as the document are contained and automatically open

The worm is one of the programs that distribute full function or parts o0f them to computer (Erbschloe,2004). Worms are famous in reproduction and publishing, it is often used for the transfer of viruses from computer to break through barriers (Bruce S.scheffer,henfreechan,henrys Chan, and Susan ogulnick,2009).table 5 shows worms categorize (Sebastian,2013)

Table 5: worms categorizes

Worms categorize	
Email worms	Spread through email messages, especially with attachments.

Internet worms	Spread directly over the internet by abusing access to open system weaknesses

Network worms	Spread over open ,unprotected network shares
Multi vector worms	Spread over two more various capabilities

In the world of computer, it is infiltrating across malware and hidden under the useful programs. Table 6 shows some of the most common Trojan categories (Sebastian, 2013). The name of the original Trojan is changing and activated every time you open the computer, so it is difficult to detect the damage and determine the place of attack (Schaeff B,Chan H., and Ogulnick.,2009).

Table 6: Trojan categories

Trojan categories	
Proxy Trojan	Designed to use a target computer through proxy server, which can attach to perform a multitude of operations anonymously.
Password Stealer Trojan	Designed to steal password from the targeted systems. This Trojan will very often first drop a key logging component into infected device

IM Trojan	Designed to steal account information or data through instant messaging programs such as Skype, MSN, and etc.
Dropper Trojan	Designed to install other malware on target systems .It is usually used in the beginning of a malware attack.
Game Thief Trojan	Designed to steal information through online gaming account.
Trojan -Banker	Designed to steal online banking information that allows hackers to access bank account or credit information.

4. Factors of committing e-crimes

The previous section mention methods that help committing of e-crimes, in which a person can steal personal data and confidential data .foremost among the causes of e-crimes that are often infringed on information systems, this section explains the factors that lead to the commission of e-crimes, which are: Financial, Cultural, Political, and Sexual crimes as follows.

4.1 Financial e-crimes

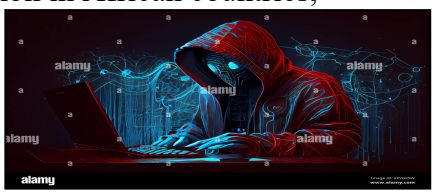
Financial e-crime, also often referred to as white –collar crime, which are committed via the Internet and have a major impact on the international banking and financial sectors.

Moreover-financial e-crime affect private individuals-companies, organization, and even nation .It has a negative influence on the entire economic and social system through the significant loss of money incurred (Alex Antonius and Gauri Sinha , 2012) .

Hiding behind a network, the perception of low risk and very high financial reward prompts many cyber criminals to engage in malware, phishing , indentity theft and fruaduient money request attacks (Hussainat M. ,2013).Business week estimates that cybercrimes targeting online banking account nearly 700 million dollars per year globally (Nadiah Salman, 2014). Few examples of financial crimes are as follows:

- Using phishing to create a page similar to the official homepage. For example, they make a fake web page of the bank and asking the customer to enter the card number and PIN with intent to copy personal data and steal bank account (Rekouche, 2011).
- The false e-mails sent by criminals as in money laundering with promise to giving up a high commission in the event of conversion ,not to mention some of the fake emails sent by winning lottery or an award ,where people are asked to send a bank account number to deposit the amount (Erbschloe , 2024)(Alex Antonious and Gauri Sinha .2012).

Theft Automated Teller Machine (ATM) from bank and copied the credit number of the machine .These cases were common in African countries, especially south Africa (Warner.2010).



4.2 Cultural e –crimes

Theft method of cultural e-crimes refers to the theft of intellectual rights or a person exercise one of the exclusive rights of the copyright holder without authorization and

attribute them to oneself without mentioning the name of the source/author. It can be one of the following forms :(Broadhurst R .& Grabosky p ..2005)(Diane Lending & Sandra A. Slaughter,19990)

- Copying software or movies on digital video discs (DVDs) from any intemational companies and selling them to the people at the lowest cost .
- Decoding private satellite channels ,which are encrypted and have subscription fees. It is done by technology like soft copy.
- Copying scientific literature electronically.

4.3 Political e-crimes

The spread of bad habits and cultures through internet network , which are alien to our society . The most widely spreads of political e-crimes are: terrorism ,addiction ,adultery and theft of money ,which lead to the corruption politically in the first place (Schaeff B Chan H., and Ogulnick S.,2009).

- Theft of government websites , critical information and spread of viruses as happened in the United States in 1997, when teenagers broken through a system of air traffic control and disrupted air navigation system .

In the United States in 1997, when teenager broken troughs a system of air traffic control and disrupted air navigation system.

- Information Technology is easier for terrorist group to make communication because they are using the least tools to convey their thoughts to the world (Neff, 1994). There are many reasons why terrorist using internet such as :
    - Limited money, they have considered them online form cheap materials that acquires the largest segment in the world.
    - The internet facilitates them to stay Unknown; these groups often choose countries with weak governments.
    - Their goals are easy to access, especially if the sites are not protected and secured.
    - There are no security barriers that hinder their movement.
    - Speed in the formation of attacks by internet communications.

4.4 Sexual e- crimes

Sexual e-crime offenders have associated through the internet. Offenders have become active creators and distributors to distribute abusive content through online or offline by saving data .Sexual e-crimes are summarized as follow:

- Flattering: When there is a relationship between a young man and a girl through chatting and developing this relationship with exchanging words of love until the trust becomes strong, then the young man exploits this relationship and threatens to blackmail the girl through her recorded calls, or saved chats for purpose of meeting his demands.

- Extortion: The most famous is a breakthrough personal computer of girls to take images and personal data, then threatening to expose the material online.
- Corrupting thoughts and weakening the faith of young minds through the dissemination of pornographic images and video via the internet.
- Pornographic websites: Is one of the most prevalent ways through the Internet have been the dissemination of sexual images and movies, which is not limited to a particular age group, But sex can also enter these sites if unsupervised.
- Child abuse can occur in a child s home, organizations, schools, or communities the child interacts with. Each year, too many children fall prey to sexual predators and all too often, these heinous acts are recorded in photos and on video and released on the Internet. For example, in 2010, the largest sexual e-crime in the United States was detected and prosecution was

made to 52 members of pedophile international child pornography for distributing up to 16,000 DVDs of child pornography.

5 .CYBERCRIMES IN VARIOUS COUNTRIES

As mentioned before, there are many types of e-crime involved to breach human and information privacy, theft, and illegal alteration of system critical information.

Every year there are increasing of e-crimes in the World, due to the development of information technology and software changes.

With this spreading, countries are trying to protect the society from e-crimes. Different types of e-crime have necessitated the introduction and use of news effective security measures in many countries.

Recently , many countries carried out e-crime laws to limit their spread, especially after the expansion of communication networks using social media that resulted in adoption and implementation of these laws to reduce the e-crimes .Figure 2 shows the top twenty countries exposed to external attacks from malicious programs in 2014.

Each country lists 6 contributing tools mentioned in each subsection of countries.

This section explains and clarifies the spread of e-crimes and the applicable laws in various countries, which are: Malaysia, Mexico, Taiwan, Brazil, India, Japan, United Kingdom, United States of America as follows.

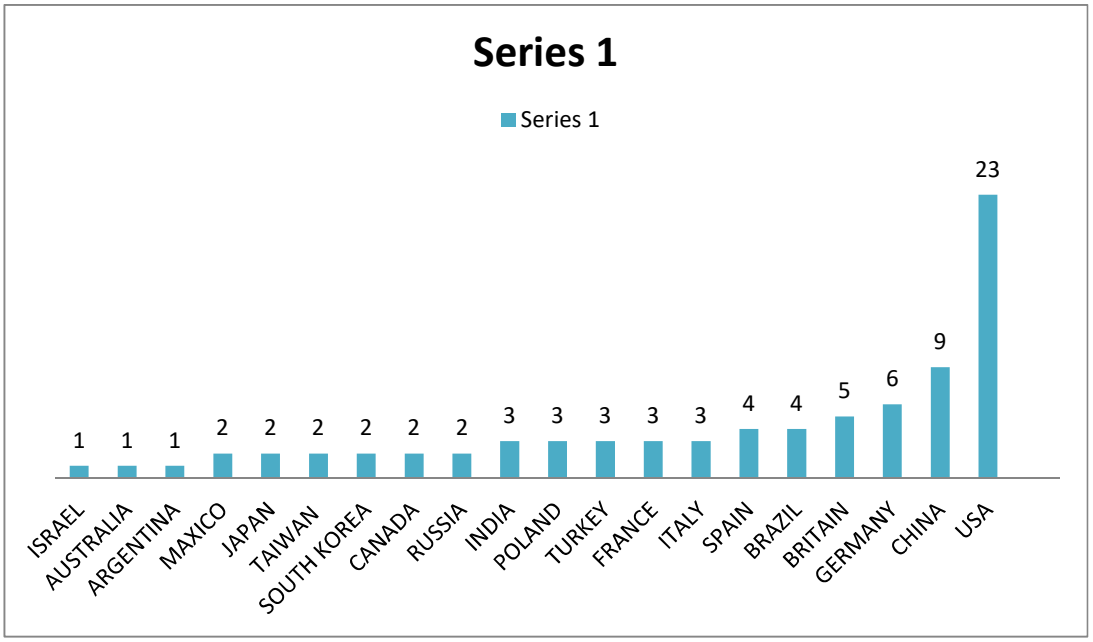


Figure 2: Top 20 countries exposed to external attacks from malicious programs in 2014.

The selection explains and clarifies the spread of e-crimes and the applicable laws in various countries, which are: Malaysia, Mexico, Taiwan, Brazil, India, Japan, UK, and USA Das follows.

5.1 MALAYSIA

Malaysia aims to achieve the democratic potentials of technology. The Government is committed to provide best practices, cyber security of information, training, and awareness programs. Among several forms of e-crimes, the royal Malaysia police reported that the top three types of e-crimes are:

1. E-commerce fraud-online purchase.
2. Parcel scam.
3. Voice-over-Internet Protocol (VOIP) scam across border syndicates.

After confrontation, Malaysia amended the copyright Act in 1990 that came into force initially in 1987 as per accession to the Berne Convention, which provides explicit protection for literary and Artistic works viewed on computer.

After a few year, in 1997 the act was passed to computer crime, digital signature, and

COPYRIGHT Also in 1998 an act was passed to the communications and multimedia (CMA)

(KUMAR, 2009) . AT the beginning of the millennium an was passed to optical disc ,

and in 2006 an act was passed to electronic transactions (Chang Yew, Wong, 2002). In

addition , the Malaysian police have given staistical date on e-crimes from 2007 to 20120 on the number of issues and losses and losses year wise as shown in table 7 (Majid ,2012).

Table 7: statistics of e-crimes from 2007 to 2011 in malaysia .

Year	Total cases	Losses (RM MILLION)
2007	1139	11.4
2008	1821	12.9
2009	3863	22.3
2010	6167	63.0
2011	6586	8.5
2012	4738	96.1

FACTORS	RANK
Share of malicious computer activity	2
Malicious code	6
Spam zombies	18
A phishing web site hosts	31

5.2 MEXICO

MEXICO faced different types of e-crimes; the first type discover was in copyright

Infringement . in 1991 ,Mexico MADE amendments and additions to the federal law of

Copyright . these amendments feature the restriction of copying by users of a file or backup

Copy . it also improved the protection of computer programs (Neff, 1994).

Mexico faced different types of e-crimes ; the first type discovered was in copyright

Cydercrime-mexico (DC Mexico) (velasco ,2007). Table 8 shows the of e-crimes in

Mexico (Symantec , 2014).

Table 8 : tools of e-crimes in mexico.

DC Mexico was formed by the ministry of public security in 2002, and headed by the

Cybercrime police unit as technical secretariat ,and it is formed in by government entities of

The legislature federal executive, and judicial power power through representatives of the Chamber of deputies , state governments , telecommunications companies , the senate , the civil society groups (Velasco , 2007) .

5.3 Taiwan

The large number of counterfeiting industries in Taiwan IS impacting economically the outside community that became a necessary intervention of outside parties to reduce

There industries , which is considered by many countries as e- crimes . republic of china, where Taiwan is a part of it, has issued a law in 1985 , as amended due to the influence

And pressure from the united states , which explicitly programs (Neff, 1994) .

In 1992 ,Taiwan has protected the rights of authts of authors through the adoption of new measures limiting the export of computer programs that contain software . they also insect and control all related products and software that require the presence of a copyright or a valid license for the export of these software products (Neff, 1994)

The largest historical operations that were carried out by Taiwan regards to e- crimes

After the signing of joint agreement between the chinese authorizes and the officials of

Taiwan in 2010 , which resulted in 450 scammers arrested in all parts of Taiwan AND the chinese provinces. They carried out more than 16 joint raids , which lead to more Then 1,000 arrests (Warner ,2010) .

In this case ,the activity initially focused on telephone fraud and auction fraud on the internet . also , they had been doing ATM fraud through hacking into foreign banks and using ATM card readers to steal from more than 200 foreign financial impersonation and bank accounts . In addition , money laundering , online shopping scams , and impersonation of public and of e- crimes in Taiwan by Symantec in 2014(Symantec , 2014)

TABLE 9: TOOOLS OF E- crimes In Taiwan.

FACTORS	Rank
Share of malicious computer activity	2
Malicious code	11
Spam zombies	21
Attack origin	15
Bot	11
A phishing web site hosts	12

5.4 Brazil

Brazil is one of the counties keen to protect society from the e- crimes . In 1985 ,Brazil issued law No . 7646 that provides protection of copyright and establishes penalties for

Owners to register the names and addressed of all persons who visit the café and also a list of sites they surfed .The Information Technology Act has been implemented in the year 2000.However,with the growth of information technology they need to amend some of the provisions of this IT Act and inclusion new types of e-crimes were found necessary and the amended Act was made effective in2009(Researcher,2007).

The study in India on different types of e-crimes between 2001-2011 is shown in table 11.The study had tried to find out the cause of the rapid changes in the occurrence of crimes and its impact on the individual in society. All data were collected from the media as well as from various electronic gates.(BhattS.&PantD.,2011)

In the early years, the growth rate of reported cases was very high because people did not realize this type of crime, but after 2005 the rate of reported cases increased suddenly making it evident that individuals are starting to be aware of these crimes. The study is on the basic of data collected during ten years that growth is increasing rapidly year after year and new types of crime affecting the community in a different ways (Bhatt S. &Pant D.,2011)

Table 11: Report of e-crimes factors between 2001 and 2011 in India.

ariants	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
ACKING	12	25	20	35	45	39	75	87	123	145	109
HISHING	08	14	26	54	40	58	103	92	97	109	74

SPAM	04	17	19	29	43	67	86	94	89	105	57
STALKING	02	08	06	15	19	27	34	29	47	58	36
DEFAMATION	03	11	09	13	17	24	32	37	59	46	45
PORNOGRAPHY	NIL	NIL	02	07	03	23	27	15	35	42	31

5.6 Japan

The Japanese government has created a vast network of regulatory bodies, institution that operate under the umbrella of center for information security, the National Secretariat of Council of ministers ,Which was founded in2005, after the cyber-attacks on the websites of many government ministries and agencies in 2000(Shimbun,2011). The Japanese government tried to stem any cyber-attacks through the formation of cyber Security forces, which consist of four categories(Russell,2011)

1-Polocies to protect the industry led by the Ministry of Economy Trade and Industry.

2-Initiatives to combat cybercrime, led by the National policy Agency .

3-The Ministry of Internal Affairs and Communications.

4- 4.Security measures coordinated by the Ministry of National Defense.

In addition, Japan depends on the self-regulation in the private sector to protect personal data. Japan approved a low to protect personal information in 2005 on the protection of privacy and data at the companies. Failure to comply law, it is punishable by a fine of up to about 30,000 USD or imprisoned for up to six months (warner,2010). Table 12 shows the tools of e-crimes in Japan by (Symantec,2014) .

Table-12:Tools of e-crime in Japan.

Factors	Rank
Share of malicious computer activity	2
Malicious code	7
Spam zombies	29
Attack origin	11
Bot	22
A phishing web site hosts	11

Mitsubishi industries exposed to cyber-attacks in 2011 that resulted in the burning of 83 PCs in11 locations including headquarters in Tokyo, research and development center ,and many factories. As well as, parliament and Kawasaki Heavy Industries were exposed to cyber-attacks at the same time (Bhatt S.& Pant D .,2011)

As the part of initiative ,an information technology forum established working groups in 2012. The report of the group released in may 2013 recommended using intermediary organizations to provide information that assist in building a relationship based on trust between businesses and consumer to use the personal data. Also ,it stated that companies use, which set of personal information for any of their services instead of asking consumers to identify their data. As well as the need to provide different levels of services based on the type of consumers (Andreasson,2011).

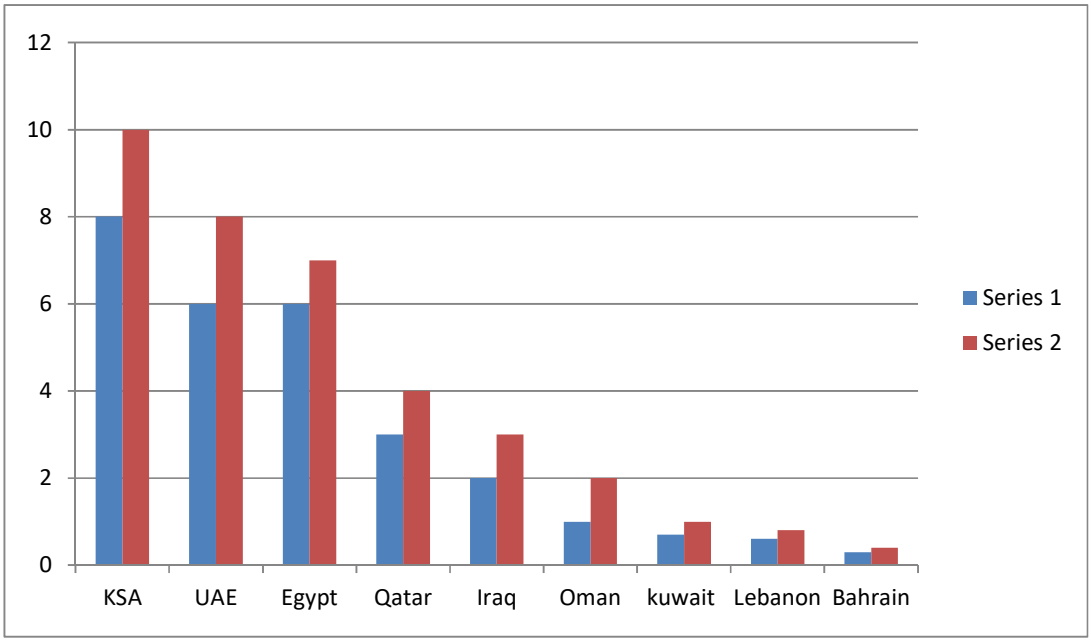
5.7 United kingdom

United Kingdom is interested in information technology ,copyright in databases, regulations and the code of advertising. In 2000 an Act was passed for electronic communications and the consumer protection regulation (Obrien A.& Marakas G.,2007)Table 13 shows the tools of e-crimes in the united Kingdom by Symantec in 2014(Symantec,2014).

According to a study carried out by cyber-security experts at the University of Kent in 2011, more than 9million adults in Britain were victims of hacked, and 8% of the population say they have lost money in the last year due to e-crimes ,also it started that 2.3% of the population reported a loss of more than 10,000 pounds to online predators (Hernandez-Castro E., BoitenE.,2013). In addition, the study found that 18.3% of those surveyed have seen attempt to break into one or more of their accounts on the internet, including online banking, e-mail, games, and social media

5.9 cybercrimes in Middle East

Like other countries, Middle East is also not free of e-crimes. Various countries including kingdom of Saudi Arabia (KSA), United Arab of Emirates (UAE), Egypt, Lebanon, Bahrain, Qatar, Syria, and etc., have been found to suffer through e-crimes. Figure 4 demonstrates the summary of nine countries in the middle east. This section describes specially about KSA and UAE in details.



5.10 kingdom of Saudi Arabia

Saudi Arabia is at the forefront of countries of countries in using social networking, offical statistics in 2013(see figure 6) revealed the results of using the Internet in the Arab world that saudi Arabia has the highest rate among the Arab countries in terms of mobile usage of up to 63% and the number of connected Internet more than 8 millon, as shown in Figura 5. Saudi Arabia also ranked first in the highest percentage of watching TV channels on the Internet up to 25%(Abdulaziz Alarifi, Holly Tootell, and peter Hyland, 2012).

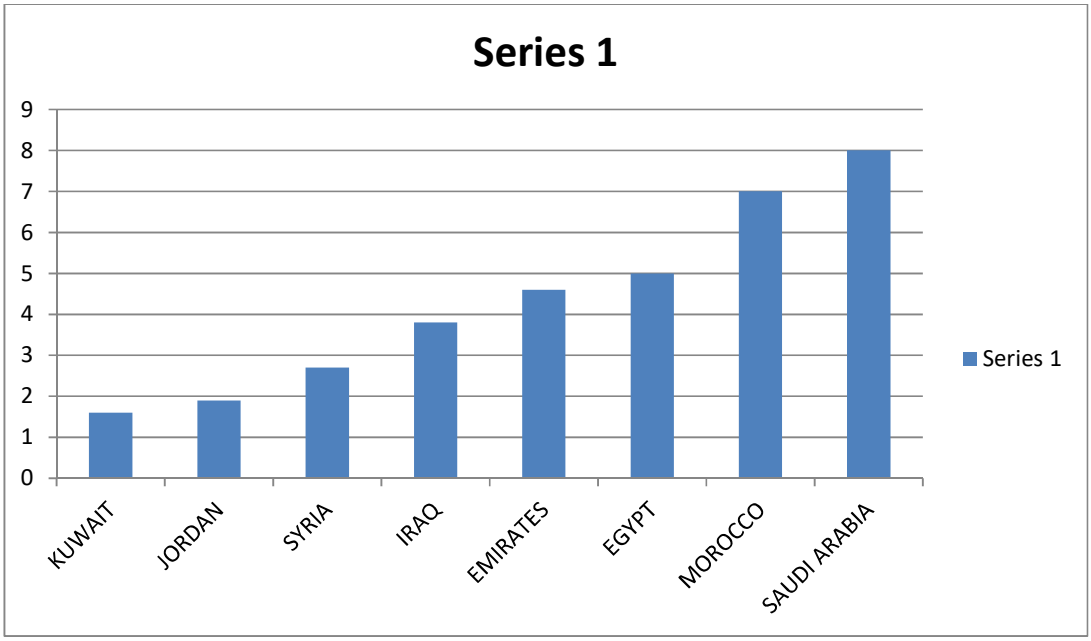


Figure 5: Number of people connected to the Internet in 2013.

The Ministry of Interior in collaboration with the communication and Information Technology commission declared strict punishments for computer crimes, including identity crimes by cabinet decision No. 79 dated 07/03/1428 AH, and was approved by the Royal Decree No. M/17 dated 03/08/1428 AH in 2014. This Law aims to reduce the occurrence of computer crime, by identifying these crimes and determining penalties for each of them to ensure the following:

1. Enhancement of information security.

2. Protection of rights relating to the lawful use of computer and information networks.
3. Protection of publice interest, ethics, and morals.
4. Prptection of national economy.

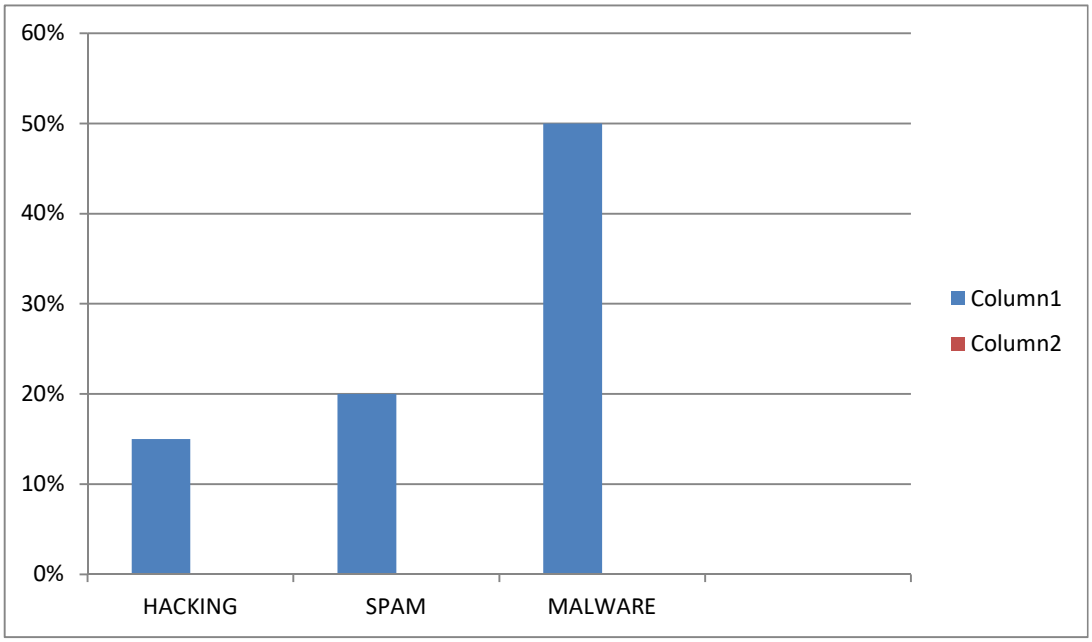


Figure 6: Tools prevalent of e-crimes in the United Arab Emirates.

5.11 United Arab Emirates

In United Arab Emirates(UAE), the perpetrators of-crimes have stepped up their activity in recent times in varied styles and age groups. According to statistics issued by Dubai police in 2013, email fraud, extortion to get money and unethical goals up to 25% of total cases.

In 2012, the Norton company submitted a study on e-crimes factors in UAE, It tums out that during every two minutes there is victim to e-crimes. The report revealed the tools prevalent of e-crimes in UAE, as shown in Figure 6 (Norton, 2012).

As per the report, experts warned of e-crimes activity in the UAE, where nearly 20% of the intrusion aimed at mobile devices, because the mobile internet use were approximately 56% of the total mobile users. The study also showed that the measures

taken by the internet users to protect themselves are still not enough, that they cannot keep pace with the steady increase in e-crime activities(Norton, 2012).

UAE President Sheikh Khalifa bin Zayed AI Nahyan issued a decree (Federal Law No. 5 of 2012) regarding the fight against crimes of Information Technology; some of those laws are:

- Punish by imprisonment of any person using electronic sites or any information technology means to engage in the unauthorized use of, or provide unauthorized facilities for others to use, communication services or audio and video channels.
- Punish anyone who uses the Internet or an information technology device to defame sanctuaries or Muslim rites or holy people such as apostles and prophets, as well as offend religion.
- Punish by imprisonment those who use the Internet or an information technology device for trafficking or the promotion of drugs or psychotropic substances of abuse or facilitate the deal of drugs.
- Punish anyone who use the Internet or an information technology device in with the money transfer or deposit with the intention of concealing or disguising the illicit origin, as well as to hide or disguise the fact that the source of the money is illegal. Also use illegal money with the prior knowledge of its illegal source.

Table 15: Increasing of e-Crimes in Kuwait.

Years	Number of e-crime
2010	**371**
2011	**300**
2012	**563**
2013	**997**

2014	**1206**
2015	**1461**
total	**4904**

5.12 Kuwait

The e-crimes rate has increased recently in Kuwait because the deployment methods and techniques by criminals have become more complex and difficult to identify the offender, this is shown in Table 15. It is based on the studies of Kuwait General Department of Criminal Investigations (Kuwait General Department of Criminal Investigation, 2018). This section focuses on social media, e-crimes and law on e-crimes in Kuwait.

The director general of the General Department of Criminal Investigation in Kuwait, said that "the e-crimes rate in the State of Kuwait is evolving significantly". The goals of such e-crimes are: spreading destructive ideas, stealing money using fake internet cards, and destroying the information that has become difficult to be substantiated and tracked. He also added that "the e-crimes rate in the State of Kuwait is evolving significantly". The goals of such e-crimes are: spreading destructive ideas, stealing money using fake internet cards, and destroying the information that has become difficult to be substantiated and tracked. Table 16 shows the highest e-crimes activity until 2015 by the Kuwait General Department of Criminal Investigations (Kuwait General Department of Criminal Investigation, 2018).

Table 16: Types of e-crimes in Kuwait.

Activity	Number of crimes
Defamation	**305**

Abuse reputation	**65**
Fraud in the bank Editor	**9**
Libel and slander	**37**
Copyright	**1**
Stalking	**49**
Incitement to hatred of a category of society	**7**
Child pornography	**150**
Impersonate	**40**
Abuse means of communication	**301**
Incitement to immorality and debauchery	**114**
Threat and blackmail	**55**
Contempt of religions	**3**
The establishment of communities without a license	**1**
Theft	**21**
Compromising the very princely	**_**
Hacking	**14**
Insulting a public official **Fraud**	**_** **27**
Death threats	**5**
False news	**2**
Forgery	**_**

Divine insults	_
Total	**1206**

The Kuwait ministry of interior has established a special department called 'Fight against Electronic Crimes' to handle e-crimes. It is able to make achievements in the detection of e-crimes with the following tasks (Directorate General of Criminal Investigation, 2018):

- Supervising the detection of e-crimes such as theft of data , information and identity of individuals and institutions.
- Follow-up on the infringement of copyright.
- Supervise the development of strategies to prevent hackers, luring citizens to Financial transactions or personal relationship in an illegal way.
- Providing all the necessary work in area such as technological software, human resources and hardware technology.
- Supervise the Criminal lab for photographic film and pictures for the Directorate General of Criminal Investigation.
- Providing photographers to portray the e-crimes issues.

After viewing the factors of e-crimes in Kuwait, and measures taken by the ministry of Interior in Kuwait to reduce this type of crimes, it is important to explain the relation between social media and e-crimes, and law of e-crimes in Kuwait.

7. Influencing factors towards e - crimes Providing photographers to portray the e-crimes issues.

After viewing the factors of e-crimes in Kuwait, and ministry of Interior

In Kuwait to reduce this type of crimes, it is important to explain the relation

Between social media and e-crimes, and law of e-crimes in Kuwait.

6. Social media, Cyber crimes and Cyber Laws

Social media programs via the Internet swept a big part of our daily life

Due to the user friendliness of mobile phones. Here comes the decision of the individual in the use of the use of this latest technology either beneficial harmony of the world. These thoughts may also lead to rifts among

The communities and nations worldwide.

Kuwait News Agency (KUNA) published that Kuwait is one among the Five Arab countries in using Twitter and Facebook extensively among Its residents.

A recent study revealed the majority of young population used Facebook And that it will rise further in coming years. Many countries relate E – crimes with social network, including social media because contact With different societies through internet led to the creation of e – crimes And social media laws (LouW C. , Von Solms s. , 2014). In recent years, Many Arab countries witnessed political turmoil using social media, which led to civil unrest and street protests.

With the present social media, there is an increase of e – crimes in societies There is a need for stringent laws to be emphasized by notaries and dignitaries. At present, in many of the countries (specially under developed Countries) cyber laws are under the framework of the general laws and Carry lenient or no punishments.

As an example, it is surprising that, Kuwait did not have special e-crime laws until 2015 ; they were applying sanctions under the audiovisual law only .But it turns out later that they started making e-crime laws and also initiated applying in the beginning 2016. The Kuwait government aggressive enforced the audio –visual Law during 2013 , also prosecuting citizen fo internet –related offenses on social media platforms ,and often pursuing these cases in conjunction with other criminal charge s. The lawest

penalty under the audiovisual law is a six –month jail term and a fine of up to KD 2,OOO for those who illegally use computers that belong to other .The penalty increases if the misuse involves damaging or altering data or information stored in the computer .But the main penalty is a jail sentence of up to 10 years and a fine ranging between KD 20,000 AND KD 50,000 for those who set up a website for terror groups or publish news about them that could be used for raising donation .At that ,The Kuwait National Assembly passed a law to combat electronic crimes ,stipulating a jail term of up to 10 years for providing online assistance to terror groups and for money laundering .(Kuwait

\

Times ,2016). The safety of intellectual property is governed by the law No 64 of 1999 press and publishing is protected under the publications Law, which or harming to himself or others. The uses of social media are On the rise of all age groups, with the vast majority being adults and Young people. The arrival of smart phones has made it easier to access Social media. Besides, the most prominent social media programs at the Present time are Twitter, Facebook , and Instagram, which have become Forum for religious and political debates. This is threatening the security Of communities through the broadcasts and chats, which may undermine The

was issued in 2006.

The safety of intellectual property is governed by the law No 64 of 1999Provides copyright protection and penalties for copyright infringement AlsoThe copyright of the press and publishing is protected under the press and publications LAW, Which was issued in 2006.