International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

RESEARCH PAPER

ON
Cyber Crimes and Cyber Security

PRINCE RIXON HADLIN

Keraleeya Samajam's Model College, Dombivali East, Mumbai, Maharashtra, India

1. 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-crimes 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, it is clear that there is a crucial need for a common understanding of such criminal activity internationally to deal with it effectively. This research covers the definitions, types, and intrusions of e-crimes. It has also focused on the laws against e-crimes in different countries. Cybersecurity and searching methods to get secured are also part of the study.

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

2. 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 functions 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 transactions, threading, etc. The internet has become an environment, where the most profitable and safest crimes are conducted. This research focuses on cybercrime or e-crimes (electronic crimes), another term for cybercrime. It refers to criminal activity that involves the internet, a computer or other electronic devices. E-crimes are increasing in frequency and causing extensive damage to governments companies, society, and individual. 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. Every year there is an increase of e-crimes due to the development of information technology and software changes. Thus, e-crimes have become very common and spread via various methods including malicious programs, which specially prepared to break through personal computers 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. 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. Besides, many countries trying to enforce e-crime 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, cyberlaws and cyber security. It will also look at the e-crimes factors and the influence of factors that make e-crimes spreading in society. Specifically, it examines the following points:

• Researching and reviewing the most common types of e-crimes.

• Study the existing literatures on the factors influencing e-crime.

• 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-crimes.

• Measurement and analysis of perceptions, experiences, and attitudes toward e-crimes.

• Determining the relationship between social media and e-crimes.

• Recommend the measures to reduce the e-crime by the policy makers and awareness

3. Cyber Crimes

E-crimes factors and examine the influence of the factors that make e-crimes spreading in society. Specifically, it examines the following: researching and reviewing the most common types of e-crimes, study the existing literatures on the factors influencing e-crime, finding out the concerns of the Kuwait society in using the Internet, identify the factors influencing e-crime in Kuwait Society

3.1 What is Cybercrime or e-crime?

Cybercrime or e-crimes are offenses that are committed against individuals or groups with a criminal motive of intentionally harming the reputation of the victim, causing physical or mental harm, and cause loss of money or information directly or indirectly by using the Internet and electronic devices

3.2 Impact of e-crimes

E-crimes affect the community in many ways.

- Loss of online business and consumer confidence in the digital economy,
- The potential for critical infrastructure to be compromised affecting water supply, health services, national communications, energy distribution, financial services, and transport,
- Loss of personal financial resources and the subsequent emotional damage.
- Loss of business assets,
- Costs to government agencies and businesses in re-establishing credit histories, accounts and identities,
- Stimulating other criminal activity, or
- Costs in time and resources for law enforcement agencies.

3.3 Beginning and growth of e-crimes

- In the early decades of modern information technology (IT), computer crimes were largely committed by unsatisfied individuals and dishonest employees.
- Early attacks on telecommunications systems in the 1960s led to sabotage of the long distance phone systems for amusement and for theft of services.

4. Methods 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. Cybercrimes are escalating by various methods such as: malicious programs, which facilitated in penetrating devices. These programs are progressing year after year with highest techniques that can help hackers to be hidden. 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

5. Hacking

Hacking developed by a highly skills programmer (Hacker) that enters a computer system and network in an illegal way. 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. However, there are experts in machine code and operating systems and well-known in latest bugs, latest patches, latest bugs in the patches, etc. Finally, hackers are able to increasingly rely upon the community to identify bugs and create programs that can adapt for their specific purpose

6. Phishing

Phishing is defined as a way to get sensitive information illegally such as passwords, user name, credit card details, and electronic signature through online networks, websites, and online payment. Another definition of phishing "is a method of stealing personal data whereby an authentic looking e-mail is made to appear as if it is coming from a real company or institution, the idea is to trick the recipient into sending secret information such as account information or login data to the scammer". The process of phishing is through the illusion users to enter personal data, which is almost identical to the legitimate site with makes recorded use of phishing described in detail was in 1987 and the first used in phishing meaning was in 1996. Phishing scams are increasing day after day under the evolution of technology; the United States faced the problem of phishing in 1995, when passwords were stolen from a large number of people online through the use of software piracy.

7. Spam

Spam is the irrelevant or unwanted e-mails/messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. The most common form recognized on a large scale is the spam e-mail. This term is applied to similar abuses in other media like: instant messaging spam, Usenet newsgroup spam, web search engine spam, spam in blogs, wiki spam, online classified ads, spam, mobile phone

messaging spam, internet forum spam, and social networking spam. Furthermore, the size of a spam email has become very high, because many spammers enter process easily, even after preventing senders to sending spam through emails. The amount cost of spam in 2011 about seven trillion dollars paid by the client and Internet service providers. Countries have different views on how to deal with spam. For example, in South Africa, Electronic Communications and Transactions Act stipulates that any person who sends unsolicited commercial communications named spam to consumers is required to provide the consumer option of stopping their subscription from the mailing list.

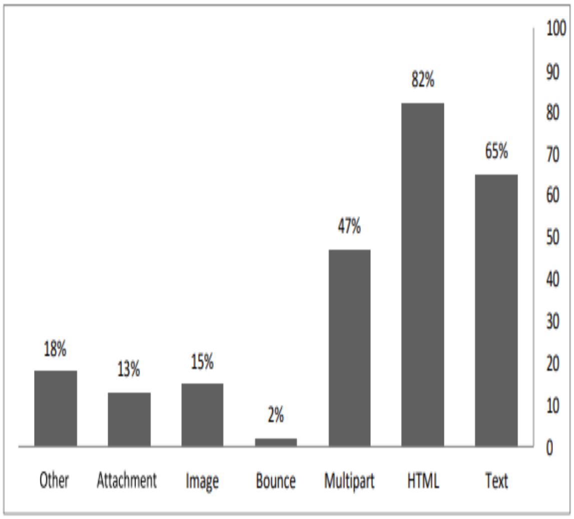
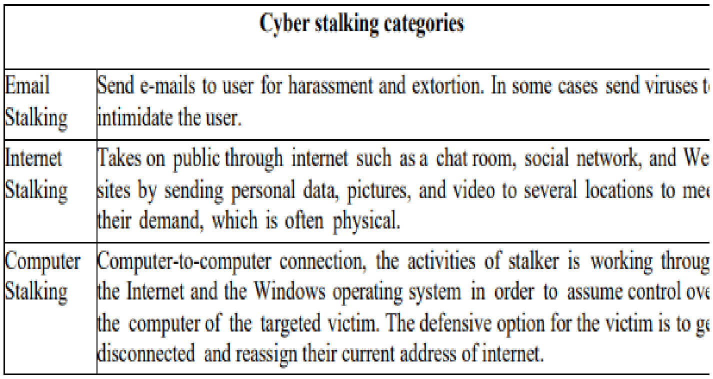


Figure 1: Latest seven types of spam trends in 2014.

8.Cyber Stalking

Cyber stalking is defined as using the internet or other electronic means with a view to harass or threaten any individual, group of individuals, or an organization. It includes monitoring, false accusations, identity theft, making threats, damage to data or equipment, the request of minors for sex, or gathering information that may be used to threaten or harass

Table 2: Three ways of cyber stalking



Cyber stalking categories	
Email Stalking	Send e-mails to user for harassment and extortion. In some cases send viruses t intimidate the user.
Internet Stalking	Takes on public through internet such as a chat room, social network, and We sites by sending personal data, pictures, and video to several locations to mee their demand, which is often physical.
Computer Stalking	Computer-to-computer connection, the activities of stalker is working throug the Internet and the Windows operating system in order to assume control ove the computer of the targeted victim. The defensive option for the victim is to ge disconnected and reassign their current address of internet.

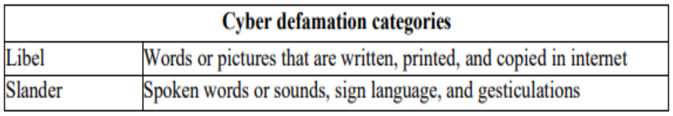
8.1 **Cyber defamation**

Cyber defamation is a crime taking place in cyberspace through the internet to libel and damage the reputation of the victim. Defamation can be categorized as libel and slander. Table 3 shows categories of cyber defamation. Frequently, it occurs during the elections or while taking senior positions in the country. Also, some persons defame others through publication across online networks. People comment on the internet by using the following:

- Public comments on media like newspapers, magazines, and web sites.

- Comments on social media such as Blogs, Twitter, Facebook, Instagram, and Chat Room .

Table 3: Cyber defamation categories.



Cyber defamation categories	
Libel	Words or pictures that are written, printed, and copied in internet
Slander	Spoken words or sounds, sign language, and gesticulations

8.2 **Cyber terrorism**

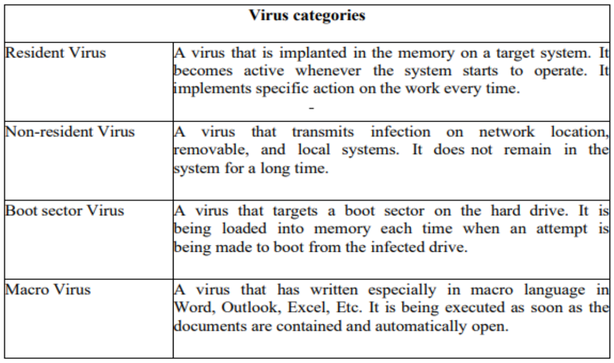
Cyber terrorism is defined as the act of Internet terrorism in terrorist activities online. It includes deliberate disruption of computer networks connected to the internet, by the means of tools such as viruses and malware to security sites, official sites, or commercial sites. Terrorism in cyberspace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

- Physical destruction of machinery and IT infrastructure.
- Penetration of computer networks.
- Disruption of government networks.
- Disruption of financial networks or social media networks. Therefore, cyber terrorism has been used by terrorist groups to get their goals. It carries out attacks against the computer systems, communications, infrastructure, and to launch electronic threats

8.3 **Malware**

Malware is the name of the programs that are permitted in a way that they are hidden under the useful programs. The term of malware generally covers viruses, worms and Trojans. 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 to remove them, which leads to data loss.

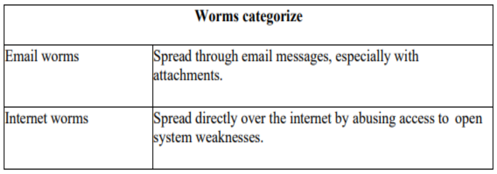
Table 4: Virus categories



Virus categories	
Resident Virus	A virus that is implanted in the memory on a target system. It becomes active whenever the system starts to operate. It implements specific action on the work every time. -
Non-resident Virus	A virus that transmits infection on network location, removable, and local systems. 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 documents are contained and automatically open.

The worm is one of the programs that distribute full function or parts of them to computers. Worms are famous in reproduction and publishing, it is often used for the transfer of viruses from computers to break through barriers.

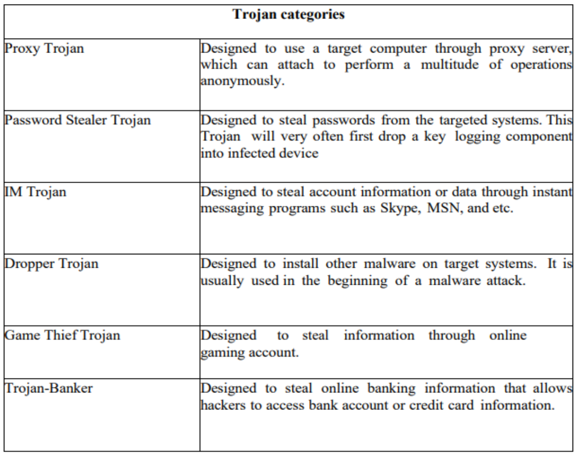
Table 5: Worms categorizes



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.

In the world of computers, it is infiltrating across malware and hidden under the useful programs. Table 6 shows some of the most common Trojan categories. 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

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 passwords 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 card information.

9.Cybercrimes in Various Countries

As mentioned before, there are many types of e-crimes 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-crimes have necessitated the introduction and use of newer 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.

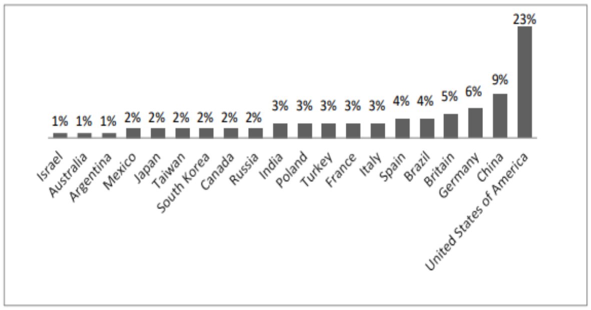


Figure 2: Top 20 countries exposed to external attacks from malicious programs in 2014.

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

9.1 India

Table 1: Report of e-crimes factors between 2001 and 2011in India

Variants	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011
Hacking	12	25	20	35	45	39	75	87	123	145	109
Phishing	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

9.2 United States of America

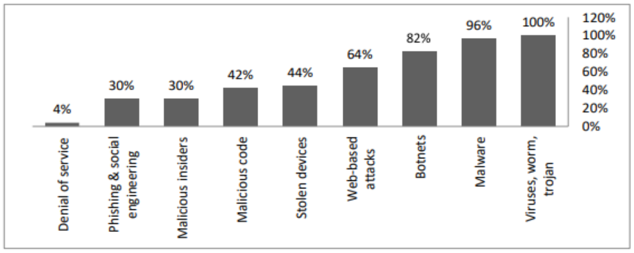


Table 14: Tools of e-crimes in USA.

Factors	Rank
Share of malicious computer activity	23
Malicious code	1
Spam zombies	3
Attack origin	1
Bot	2
A phishing web site hosts	1

6. Social media, Cybercrimes 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 this latest technology either beneficial 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 forums for religious and political debates. This is threatening the security of communities through the broadcasts and chats, which may undermine the harmony of the world. These thoughts may also lead to rifts among the communities and nations worldwide. Kuwait News Agency published that Kuwait is one among the five Arab countries in using Twitter and Facebook extensively among its residents. 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. With the present social media, there is an increase of e-crimes in societies across the globe.

9.Conclusion

Technology has become an integral part of our daily life in the world of the internet and cannot be dispensed with. It became necessary to take caution when using any technology so as not to be trapped by e-crimes. Many of the countries do not have specific laws related to e-crimes until today, so it is imperative to enact new laws to combat the worldwide scourge, which has no boundaries. Many of the studies in the current literature have focused on factors that affecting e-crimes such as demography, sexual, financial, cultural, and political. There is a need to improve and validate these studies region vise and country vise. Thus, as future work, it desired to do the followings: • Build new models to measure the influence of demography and technology over the factors of e-crimes leading political, cultural, financial

10. References

Abdulaziz Alarifi, Holly Tootell, and Peter Hyland. (2012). A study of information security awareness and practices in Saudi Arabia. International Conference on Communications and Information Technology (ICCIT) (pp. 6-12). Hammamet: IEEE. Alex Antoniou and Gauri Sinha. (2012). Laundering sexual deviance: Targeting online pornography through anti-money laundering. European Intelligence and Security Informatics Conference (pp. 91-98). Odense: IEEE. Alex Roney Mathew , Aayad Al Hajj , and Khalil Al Ruqeishi. (2010). Cybercrimes: Threats and protection. International Conference on Networking and Information Technology (pp. 16-18). Manila: IEEE. Alexios Mylonas, Anastasia Chang Yew, Wong. (2002). Malasian Law and Computer Crime . Malaysia: SANS. Diane Lending & Sandra A. Slaughter. (1999).