

Cyber-Crime and Cyber Criminals: A Study to Combat the Threat

Nilay Das Nayan

Lecturer of Law

Rabindra Maitree University, Kushtia
and

Tanushri Das

*BSS (Hons), Department of Social Welfare,
Islamic University, Kushtia*

Keywords:

Financial crime,
cyber stalking,
telegraph fraud,
email crime,
cybercrime,
email spoofing,
email blasting,
combat

Abstract: Cybercrime today affects individuals, organizations, and even governments. Cybercrime detection and classification methods have varying levels of success in protecting and preventing data from such attacks. Several laws and methods have been put in place to prevent cybercrime and the penalties are laid down for the criminals. However, research shows that many countries are already facing this problem. The United States suffering the most from cybercrime over the years. This document describes the common areas where cybercrime is common and the different types of cybercrime that are occurring today. Since email is the most common means of cybercrime, this treatise also presents research on email crime. Several options can be discussed to effectively combat cybercrime.

I. Introduction

The term crime is denoted as an offense punishable by the state. However, no specific purpose is stipulated by law. Criminal offenses are also known as crimes or felonies. It harms not only individuals but also communities and countries. Cybercrime has nothing to do with the Act. According to its creator, cyber is a prefix used to describe a person, thing, or idea as part of the computer and information age. These are computers or computer networks. A computer network is a collection of communicating nodes that facilitate the transfer of data. At any point in time, a node can be a computer, laptop, smart phone, etc. Cybercrime includes all criminal activities related to computers and networks. This includes crimes committed online. The Internet is a network of networks used for communication and data exchange. Cybercrime, also known as computer crime, is the use of devices for illegal purposes such as fraud, child pornography, intellectual property trafficking, identity theft, and breach of confidentiality. With advances in Internet technologies such as 2G and 3G, Global Village effectively shares and communicates important data over networks. However, some people try to track to extract sensitive information that is important to their personal use, financial gain, and so on.

II. Cyber Crime

Cybercrime includes a variety of crimes, including spoofing, fraud, financial crime, pornography, the sale of smuggled goods, and the download of illegal files. According to the author- all computer and internet crimes are called cybercrime. Listed below are some of the crimes that are popular and alarming in the cyber world.

A. Financial Crimes

As the demand for online banking grows, financial crime has become a serious problem. Financial crimes include credit card fraud, theft of money from online banks, etc. Credit card fraud criminals often obtain information from victims by requesting credit information by impersonating government

officials or financial institutions. Victims become victims without proper investigation and share their credit card information with these criminals. This allows criminals to steal the identities of these helpless victims, with devastating consequences.

B. Cyber Pornography

All erotic sites that allow you to download erotic videos, videos, images, and net erotic magazines (images, text, etc.) fall into this category. A study in the UK Home Affairs Commission's report on computer pornography (House of Commons, 1994) found that "computer pornography is a new fear" (House of Commons, 1994:5). Carnegie USA Mellon University is also the institution that conducted the extensive investigation and collected evidence of child and computer pornography.

C. Drug Trafficking

Drug sellers contribute to the majority of cybercrime by selling drugs that use the latest technology to encrypt email. They mainly use courier services to arrange where and how to exchange. These swap sites are more convenient for people at risk of buying illegal drugs and other items because there is no direct communication between the buyer and the dealer.

D. Cyber Terrorism

Acts of terrorism that take place in cyberspace are called cyber terrorism. Cyber terrorism may involve transmitting information over the Internet about a bombing that may occur at a specific time in the future. A cyber terrorist is someone who threatens and coerces individuals, organizations, and even governments by attacking them through computers and networks for personal, political, or social gain.

E. Online Gambling

Online gambling is provided by thousands of websites whose servers are hosted abroad. These sites are among the top of the money laundering sites.

F. Cyber Stalking

As defined by the Oxford Dictionary, 'stalker' means 'surveillance'. Cyber stalkers track the whereabouts of individuals and organizations online. This may include sending, threatening, or not threatening messages to message boards. According to David Wall, cyber stalking is one of the main forms of cybercrime. If a person is constantly being harassed by another by constantly sending inappropriate content or sending threatening emails to someone, it is a criminal offense.

G.E-mail Spoofing and Phishing Scams

Cybercriminals often forge emails with known and unknown people. Email spoofing means sending her E-mail from one source and making it look like it came from another of her E-mails. Email Spoofing is a very common cause of financial loss. Phishing is an attempt to masquerade as a trusted entity in an electronics store to obtain sensitive information such as passwords or credit card details. Phishing emails may contain hyperlinks to malware websites.

III. Types of Cybercrime

There are many types of cybercrime today. But the eight most commons are:

A. The ft in the Services of Telecommunication

Individuals and criminal organizations can access the organization's telephone exchange (PBX) and access dial-in or dial-out lines. This allows you to make free domestic or international calls. Communication service theft is one of the oldest forms of cybercrime and is considered a misdemeanor. Criminals are usually fined and they must be sentenced to a short imprisonment.

B. Piracy of Telecommunication

Today's digital technologies make it possible to perfectly duplicate printed matter and improve the combination of graphics, sound, and other multimedia content. This is a major concern for owners of copyrighted material. If the creator of a particular work fails to profit from his or her work, it can result in serious financial loss and generally have a significant impact on creative activity.

C. Dissemination of Offensive Materials

These are the disadvantaged s of s and the s material that is believed to be s in cyberspace. This includes material that is more explicit than sexual, racist propaganda, explosives objects, and devices, and incendiary code. Telecommunications services are also commonly used to harass, intimidate, and invade by phone to bring modern signs of cyber stalking. Computer networks have also proven useful for s, as they facilitate blackmail. The type of equipment used, the location of the perpetrator who distributed the material, and the location of the victim determine the fines and fines paid.

D. Laundering E-money and Evasion of Taxes

For a long time, wire transfers have helped s hide s and transfer crimes. The origins of fraudulent profits are largely obscured by today's emerging technologies. Tax authorities can easily disguise legitimate income. Central bank supervision is circumvented by the development of informal banking institutions or parallel banking systems. There is no separate law on this type of computer and network crime that applies directly to the law covering all of these crimes.

E. Extortion, Terrorism and Electronic Vandalism

In contrast to its predecessor, Western industrial society relies on complex data processing and communication systems. Disabling or damaging these systems can have devastating consequences. Vandalism can usually be viewed as a denial of service attack, botnet, or another malicious network attack. Extortion is the act of using money to deter an attack or demand that an attack stop. Penalties for computer vandalism vary widely in terms of damage and monetary value, but extortion penalties for such crimes are subject to laws and regulations.

F. Fraud in Sales and Investments

The use and development of applications in digital technology are becoming increasingly fraudulent, is tied to, and e-commerce is becoming more important. Cyberspace currently utilizes many investment opportunities, including bonds and stocks, ATM sales and loans, and phone lotteries. You can create a fake website to make look like the real thing. According to the US, the U.S. Securities and Exchange Commission is part of the investment scam targeting Americans:

- Pyramid Schemes and
- —Ponzil schemes,
- High-return or —risk—free investments.

G. Illegal interception of communication signals

The rapid development of telecommunications has opened up new opportunities for electronic interception. Their fields of application range from personal surveillance to economic and political espionage. Current legislation does not prevent remote monitoring of computer radiation.

H. Fraud in Transfer of Electronic Funds

The rise of electronic transmission systems increases the risk of interception or rerouting of these types of transactions. There is no doubt that e-commerce payment systems have spread rapidly around the world. If they use the e-commerce system, there is no doubt that this system increases their risk. Bank transfers over the internet can be redirected by hackers. Bank transfers have a very high incidence of crimes such as theft and fraud. There is no doubt that business services technology has brought significant benefits to both businesses and consumers. However, cybercrime has a darker side to this technological advancement. organizations detect types of cybercrime. They find it very difficult to truly understand the capabilities of cybercriminals. Understanding cyber criminals' next target and the value of that target can be very difficult for organizations. It was too late when your organization was attacked and you realized that they had already suffered damage. Organizations are working to prevent such cybercrime, but it is still in the hands of cybercriminals. The graph in Figure 1 shows statistics on the total amount of financial damage caused by cybercrime from 2001 to 2013. Statistics have been reported to IC3. The total loss in 2001 was \$ 17.8 million. In 2009, there was an increase of \$559.7million and in 2013, an increase of about \$781.84 million.

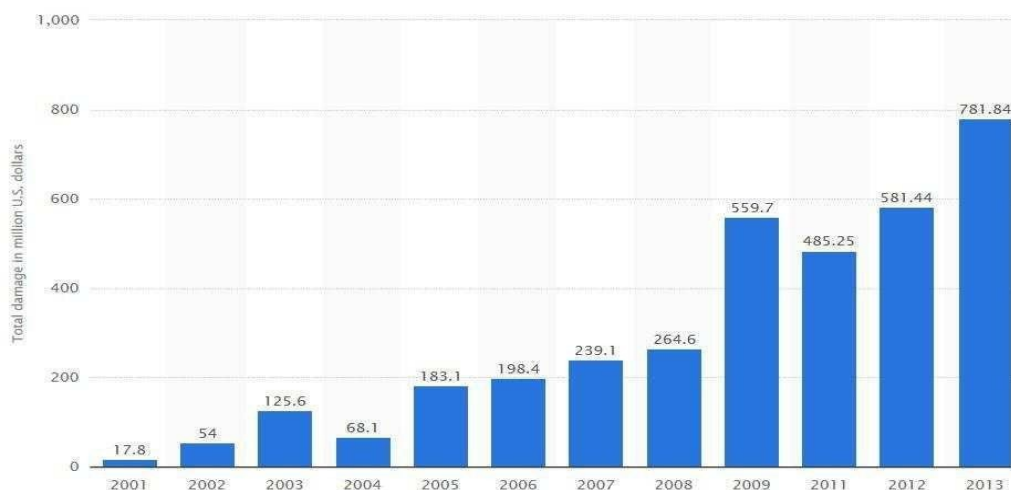


Figure1. The amount of financial damage (US \$ 1 million) caused by cybercrime between 2001 and 2013 was reported to IC3.

A detailed investigation by renowned security firm Symantec identifies the 20 countries with the highest cybercrime. I was able to do it. During the processing of this list, Symantec observed and discovered the number of websites hosting phishing sites. These phishing websites are intended to prevent end users from distinguishing between real and fake websites. This topic is designed to trick users into disclosing personal and bank account information to users of computers. Norton Life Lock has succeeded in obtaining data such as the number of systems infected with bots through scrutiny. Cybercrime rates are high in the United States. This may be due to the country being blessed with broadband connections that provide uninterrupted internet connectivity.

It shows countries affected by cybercrimes, including malicious computer activity, spam messages, and phishing.

- Malicious computer activity sharing and
- Spam zombie rank,
- Phishing website host rank,
- Bot rank and
- Source of attack

These factors help the Cybercrime rankings certified by Symantec's security organizations.

The pie chart in Figure 2 shows that the United States suffers heavily from cybercrime. The losses suffered were in other countries as well. China is in second place. After that, countries such as Germany and England said he was, then he was, had to carry against her loss, and he was against cybercrime for he caused. Countries such as Brazil and Spain have nearly the same rate of cybercrime cases. Similarly, Italy, France, Turkey, and Poland have similar percentages of cybercrime occurring in their own countries. India shares 3% of its malicious activities on computers. Argentina, Australia, and Israel share only 1% of malicious computer activity. Mexico ranks first by hosting phishing websites. Australia is at the forefront of bot activity.

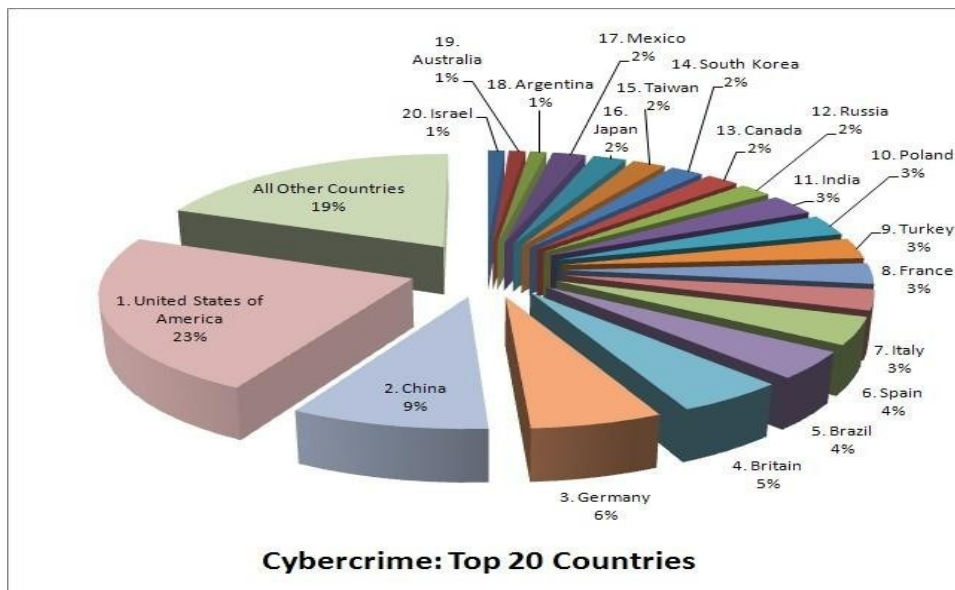


Figure2:Top20CountrieswithCyber Crime

IV. Crimes on the Internet

Crime committed online over the Internet is primarily called cybercrime. According to David Wall, the term cybercrime refers to malicious activity performed primarily on the Internet using digital devices. Cybercrime is a concept widely promoted by the media, independent of the law. Generally, the term cybercrime includes crimes such as phishing, bank robbery, credit card fraud, fraud, child pornography, kidnapping, chat removal viruses, and creation or distribution. All of this contributes to computer crime.

A. E-mail-related Crimes

An email has quickly become the most popular means of communication in the world. Millions of emails, including his message, are sent and received worldwide every day. Email, like any other form of communication, is abused by criminals. Its simplicity, transmission speed, and relative anonymity make it a powerful tool for criminals.

1) E-mail Spoofing: E-mail spoofing is usually done by forging the sender's email address or the name of the email sender. You will typically need to enter the following information:

- i. Recipient's E-mail address.
- ii. Recipient's email address (called copy C).
- iii. The E-mail address of the person who received the copy (called copy CC).
- iv. Message subject which is a short title or description of the message.

2) Email Defamation: Cyber defamation and cyber slanders are often very dangerous and deadly, even for people with little computer skills, eventually becoming blackmailers who threaten victims by email.

3) Email Bombing: Crashing an email account or server due to too many emails being received by a victim is known as a general subject of email bombing exchanges or with the help of emails.

4) Malicious Code Distribution: Email is often the most common and quickest way to spread malicious code. An email virus called Love Bug spread to millions of computers. Trojans, viruses, worms, or other computer infections are often associated with greeting cards emailed to unsuspecting people.

5) E-mail Fraud: Financial crime is usually perpetrated by email spoofing. Assuming identities and -, it is becoming easier and easier to hide one's identity. Criminals are aware that they have been identified with a minimum probability.

6) Threat Send Via Email: People with little knowledge of email can easily threaten or intimidate someone without identifying them.

V. What is a cybercriminal?

Cybercriminals come from different age groups.

A. Children (ages 9-16)

Believe it or not, even children can become cybercriminals, knowingly or unwittingly.

B. Organized Hacktivists

Hacktivists who come together for a specific purpose are called hacktivists. These groups are run primarily for political reasons. In other cases, their motives may be social or religious movements.

C. Disgruntled Employees

It's hard to imagine how a mean employee would be frustrated. So far, out of his worker's dissatisfaction, he has opportunities to strike against employers. But now computers and automated processes are becoming more reliant on disgruntled employees committing crimes computers all in to his Doing so could result in greater harm to the employer. The system has been shut down.

D. Professional Hackers

Extensive computerization has enabled business organizations to store information in electronic form. Hackers can be hired by competing companies to steal information and privacy from other industries. If the hacking attempt can obtain the required information from a competitor, the physical presence required for access is considered unnecessary. This also leads to the temptation of companies to hire professional hackers to do dirty work.

VI. Ways to combat cybercrime

Both government and private organizations need to take a holistic approach to combat cyber threats. Our government has already taken some steps in this regard through the ICT sector. But that's not enough. Hackers and intruders endanger our privacy, destroy valuable information and sometimes cause havoc. It will take years for a country like us to disappear. We propose measures that can be considered cyber security measures.

Investments in Cyber Security Aspects

Looking at cybercrime trends in Bangladesh, it goes without saying that both the private and public sectors will have to invest a significant portion of their budgets. Improving Cyber security Measures. The Bangladesh government has invested \$400 million to build a cyber-security division in the ICT sector. At the same time, we must encourage the private sector to invest in the cyber security aspects of our business.

Legal Framework

Governments have enacted various laws to prevent cyber-attacks and stop digital harassment. There are ICT Laws 2006, 2009, 2013 (as amended), and Digital Bill 2016. Digital Bill 2016 could come into effect as soon as possible. All of these laws unify our nation's cyber security.

Seminar and Training

The government holds various seminars and workshops at the college, university, and institutional levels to raise public awareness of the issue of cybercrime. These seminars and workshops educate people about cybercrime and how to fight cybercrime in our country and around the world. Many training courses are conducted under the supervision of bdCERT.

CERT Group Formation

CERT stands for Computer Emergency Response Team. The team's responsibility is to deal with the catastrophic situations that result from cyber-attacks. Bangladesh Government provides 24-hour * 7days CERT support called bdCERT. Each organization and institution must form its CERT individually.

Cyber Security Strategy

Every business should have a strategy in place to fight cybercrime and make instant decisions when needed. This strategy should be developed under the National Cyber security Strategy.

Code of Ethics

Every organization needs a culture in which its employees adhere to the Code of Ethics (ACM Code). The Government of Bangladesh has already mandated ICT education in secondary and high schools. The Computer Code of Ethics (ACM) may be included in this syllabus.

VII. Conclusion

This research shows that there are many ways and means by which people commit crimes in cyberspace. These crimes include email spoofing, email bombing, and spreading malicious code through email. Additionally, most amateur teens have seen a variety of cyber criminals, from hackers to professional hackers. They are often hired by competitors to break into their systems. It is therefore very important that all individuals are aware of these crimes and are vigilant to avoid casualties. To bring justice to victims and punish criminals, the judiciary has enacted several laws known as Cyber-laws. Therefore, everyone should know these laws. Also, cybercrime cannot be simply explained as a technical problem. Instead, this is an approach-based issue, as it is not the computer that is harming or attacking the organization, but the human being that is exploiting technology to cause damage. Therefore, you need to be vigilant to discover the different approaches that such criminals can take. Intellectual thinking is required to recognize the situation that leads to such harm. The solution to such a crime is not just technology-based. Technology is just a weapon to track and confuse such activities to some extent. This paper presents a comparison of cyber threats between countries. It also highlights cyber threat trends and statistics in various sectors such as industry, finance, and government. Here we discuss the measures taken abroad and in Bangladesh to combat cybercrime. Governments and the private sector are helping raise awareness about how to fight cybercrime by holding seminars, conferences, workshops, training courses, etc. The need for a culture of ethical compliance when dealing with cybercrime was also mentioned. Some suggestions were made in this paper to improve the strength of Bangladesh's cyber security.

Works Cited

- [1] en.wikipedia.org/wiki/Crime
- [2] David Wall, —Cyber-crimes and Internet, Crime and the Internet, by David S. Wall. ISBN 0-203-164504, Pageno.1
- [3] www.merriam-webster.com/dictionary/cyber
- [4] www.webopedia.com/TERM/C/cyber_crime.html
- [5] www.britannica.com/EBchecked/topic/130595/Cybercrime