Cyber-Crime

Cyber-Crime

Cyber-crime refers to any crime that involves a computer and a network. It includes those criminal acts which are performed with the aid of a computer. It is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.

Cyber-crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.

- **Debarati Halder and K. Jaishankar defines Cybercrimes as:**

"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones "

- **According to Duggal:**

Any criminal activity that uses a computer either as an instrument, target or a means for perpetuating further crimes comes within the ambit of cyber-crime.

Reasons of Cyber-Crime

There are several reasons for the wide spread of cyber-crime all over the world. Some of the notable reasons are –

- Expertise of offenders in technology
- Increasing dependence on computer and information technologies
- Minimum risk
- Complexity in taking legal action against offender
- Chance of huge monetary gain
- Carelessness and unskilled behavior of user of computer and internet
- Problems in identification of offenders
- Unwillingness of victims of cyber-crime to take legal measures
- Taking resort of new and sophisticated means for the commission of crime which exceeds the capability of law enforcement authorities
- Revenge
- Negligence

Different Modes of Cyber-Crimes

1. Hacking

Hacking is usually understood to be the unauthorized access of a computer system and networks. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously is said to commit hacking.

2. Email bombing

It refers to sending large numbers of mail to the victim and thereby ultimately resulting into crashing the computer network system. In Internet usage, an email bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or crush down the mail server.

Shimla Case

In one case, a foreigner who had been residing in Shimla, India for almost thirty years wanted to avail of a scheme introduced by the Shimla Housing Board to buy land at lower rates. When he made an application, it was rejected on the grounds that the schemes were available only for citizens of India. He decided to take his revenge. Consequently, he sent thousands of mails to the Shimla Housing Board and repeatedly kept sending e-mails till their servers crashed.

3. E-mail spoofing

It is a kind of e-mail that appears to originate from one source although it has actually been sent from another source. Such kind of crime can be done for reasons like defaming a person or for monetary gain etc.

4. Data diddling

Data diddling (also called false data entry) is the unauthorized changing of data before or during their input to a computer system. It involves altering raw data just before a computer processes it and then changing it back after the processing is completed.

5. Logic Bomb

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files. It’s an event dependent program, as soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities. Some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date, like the Chernobyl virus.

6. Salami Attacks

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed. E.g. The Ziegler case, where a logic bomb was introduced in the bank system, which deducted 10 cents from every account and deposited it in a particular account.

The Ziegler Case

an employee of a bank in USA had his employment terminated. Angered by the supposed mistreatment by his employers, the man introduced a logic bomb into the bank's servers. The logic bomb was programmed to debit ten cents from all the accounts registered in the bank and transfer them into the account of the person whose name was alphabetically the last in the bank's records. Later, he had opened an account in the name of Ziegler. The amount transferred was so little that nobody had noticed the fault. However, it had been brought to light when a person by the name of Zygler opened his account in the same bank. He was surprised to find a large amount of money being transferred into his account every week. He reported the 'mistake' to the bank and the former employee was prosecuted.

7. Web Jacking

This term is derived from the term hi jacking. In these kinds of offences, the hacker gains access and control over the web site of another. He may even change the information on the site.

This occurs when someone forcefully takes control of a website by cracking the password and later changing it. The actual owner of the website does not have any more control over what appears on that website.

Piranha case

In a recent incident reported in the USA the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website. They demanded a ransom of 1 million dollars from her. The owner, a schoolteacher, did not take the threat seriously. She felt that it was just a scare tactic and ignored the e-mail. It was three days later that she came to know, following many telephone calls from all over the country, that the hackers had web jacked her website. Subsequently, they had altered a portion of the website which was entitled 'How to have fun with goldfish'. In all the places where it had been mentioned, they had replaced the word 'goldfish' with the word 'piranhas'. Piranhas are tiny but extremely dangerous flesh-eating fish.

Many children had visited the popular website and had believed what the contents of the website suggested. These unfortunate children followed the instructions, tried to play with piranhas, which they bought from pet shops, and were very seriously injured.

8. Cyber Pornography

Cyber pornography includes conducting pornographic websites; publish and print pornographic magazines by using computer and the Internet, to download and transmit pornographic pictures, photos; writing etc.

9. Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets, certificate etc. can be forged using sophisticated computers, printers and scanners. These are made using computers, and high-quality scanners and printers. This is becoming a booming business now days.

10. Denial of Service Attack

In case of Denial of Service attack the targeted computer received so many requests which it cannot handle. This crashes the computer resources. As a result, the computer resource denies giving proper service to the authorized user.

11. Cyber Defamation

This occurs when defamation takes place with the help of computers or the Internet. For example, someone publishes defamatory matter about someone on a website or sends E-mails to his friends containing defamatory information.

12. Trojan attacks

It is an unauthorized programme, which passively gains control over another's system by representing itself as an authorized programme. It is concealing what it is actually doing.

Lady Director Case

A Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber-criminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady.

13. Fraud & Cheating

Online fraud and cheating are one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

Azim's Cheating Case

Recently the Court of Metropolitan Magistrate Delhi found guilty a 24-year-old engineer Azim of fraudulently gaining the details of customers credit card. Metropolitan magistrate Gulshan Kumar convicted Azim for cheating but did not send him to jail. Instead, Azim was asked to furnish a personal bond of Rs 20,000 and was released on a year's probation.

14. Cyber Bullying

According to Cambridge Dictionary, Cyber bullying means the activity of using the internet to harm or frighten another person, especially by sending them unpleasant messages.

Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.

Hinduja defines cyberbullying as "willful and repeated harm through the use of computers, cell phones or other electronic devices.''

These elements include the following:

Willful: The behavior has to be deliberate, not accidental.

Repeated: Bullying reflects a pattern of behavior, not just one isolated incident.

Harm: The target must perceive that harm was inflicted.

Computers, cell phones, and other electronic devices: This, of course, is what differentiates cyberbullying from traditional bullying.

The most common places where cyberbullying occurs are:

- Social Media, such as- Facebook, Instagram, WhatsApp, Imo, Viber, Tiktok, Twitter etc.
- SMS (Short Message Service) also known as Text Message sent through devices
- Instant Message (via devices, email provider services, apps, and social media messaging features)
- Email

Cyberbullying in Bangladesh

Cyberbullying is not a new thing for Bangladesh and day by day it become a very serious issue. A recent study conducted by Telenor Group has found out that 49% school students of Bangladesh are the victims of cyberbullying (Telenor Group, 2016).

In case of cyberbullying, personal information, images are captured and videos of victims are recorded through digital devices and posted in the internet. This trend is increasing among students with the wide usage of digital devices.

According to IT specialist K.M. Nafiul Haque, Cyberbullying is pretty serious issue in Bangladesh. People are using different platforms and insulting each other randomly. He added that, it is happening because the zone of tolerance of the people is very low in our country.

The rate of Cyber bullying not only increases among the general people but also the celebrities are frequently being bullied online. We all know about the incident when the cricketer Mohammad Nasir put a picture with his sister and people started bullying them, even they used slangs. As a result, Nasir had to remove the picture. Then, the worldwide recognized, number one all-rounder in all three formats of cricket Sakib Al Hasan, he is being very often bullied when he put any picture with his family.

Legal Action Against Cyber bullying in Bangladesh

The victims of Cyber-bullying can directly contact with the BTRC and lodge complain. BTRC is supposed to take necessary actions within 24 hours and the perpetrators will be brought to justice within 3 days after the complaint is filed. The government has also launched a cyber-crime helpline. Victims can call at +8801766678888 to submit their complaints. Beside this, if the victim is a child or a woman, then there is a National Helpline number for their redress and the number is 10921.

Moreover, any victim of Cyber-bullying can also take resort the help of Police through dialing National Emergency Help Service Number 999.

Furthermore, Crime Research and Analysis Foundation (CRAF) a non-profit voluntary Organization also helped the victims of Cyber-bullying.

According to the Survey of CRAF, in our country every 20 second cyber-crime happened.

In order to prevent Cyber bullying Ain o Salish Kendro(ASK) and Insight Bangladesh Foundation also took lots of initiatives.

ReThink: Smart Solution to stop Cyber Bullying

Trisha Prabhu, a US innovator in 2015 launched the ReThink keyboard, which proved as highly effective way to detect and stop online hate speech and control the high rate of Cyber-bullying.

In the fall of 2013, Trisha, then just 13 years old, read the shocking news story of Rebecca Sedwick's suicide. After being cyberbullied for over a year and a half, Rebecca, a 12-year-old girl from Florida, took her own life.

Trisha herself was also the victim of cyber bullying for her wardrobe. For these reasons Trisha was shocked, heartbroken, and outraged. Deeply moved to action by the silent pandemic of cyberbullying and passionate to end online hate, Trisha created the patented technology product ReThink™, that detects and stops online hate at the source, before the bullying occurs, before the damage is done.

Her globally acclaimed research has found that with ReThink, adolescents change their mind 93% of the time and decide not to post an offensive message thus it can reduce the cyber-bullying a lot.

Rethink is an Anti-Cyberbullying keyboard app available for both Android and iOS. It compares the words and phrases that anyone type, with its database of offensive words and warns the netizen who typed hurtful words or phrases. This stops the writer from posting offensive messages on social media and social messaging apps, thus preventing Cyberbullying.

Technologies for preventing cyber crimes

As has been referred in 2010 Chu Journal Section, at page 349, Dr. R.C. Mishra, IPS, in his book "Cyber-crimes: Impact in new millennium" stated about certain technologies to prevent cyber-crimes.

a) **Firewall:** Firewall implemented with secure standards will not allow any intruder into the system.
b) **Encrypted tunneling:** An encrypted tunnel allows secure communications across internet. In this the data packets on internet are encrypted and then wrapped in IP at the initiation point of the tunnel. The encrypted packets can then be transmitted over the Internet when the packets came at the other end of the tunnel, they are unwrapped and decrypted.
c) **Secure Sockets Layer (SSL) and Secure HTTP:** This provides an encrypted TCP/IP Pathways between two hosts on the internet SSL can be used to encrypt any TCP protocol to encrypt HTTP.

d) **Secure Electric Transform (SET):** This technology involves cryptographic algorithms encrypt the credit card numbers, so it cannot be seen on the internet.
e) **Digital Signature:** Cryptographic techniques is used so that only authorized authenticated person can enter in the system.
f) **Employee Training**.