CYBER CRIME

Introduction

Cybercrime is not an old type of crime in the world**.** It’s defined as any criminal activity taking place on or with the aid of a computer or Internet or other technology recognized by the Information Technology Act. Cybercrime is the most prevalent crime that plays a devastating role in the Modern India. Not only the culprits are causing enormous losses to the society and the government but are also suitable to conceal their identity to a great extent. There are number of illegal activities which are committed over the internet by technically professed criminals. Taking a wider interpretation it can be said that, Cybercrime includes any illegal activity where computer or internet is either a tool or target or both. The term cybercrime may be judicially interpreted in some judgments passed by courts in India, however it is not defined in any act or statute passed by the Indian Legislature.

Cybercrime includes any crime deals with computers and networks. It includes crimes committed over the Internet. The Internet is principally the network of networks used across for communication and sharing of data. Cybercrime also known as the computer crime is the use of an instrument for illegal ends, such as committing fraud, intellectual property, stealing identities, or violating privacy. With the advancement of internet technologies such as 2G and 3G, the global village is efficiently sharing and communicating vital data over the network. However, some intentionally try to illegally track and extract vital and confidential information for their personal use or financial fulfillment and many more.

Classification Of Cyber Crimes

Cyber crimes can be classified in to 4 major categories as the following:

(1) Cyber crime against Individual

(2) Cyber crime Against Property

(3) Cyber crime Against Organization

(4) Cyber crime Against Society

Against Individuals

1. Email Spoofing:

A spoofed email is an email in which the email header is forged in such a way that the email appears to come from one source but is actually from another source was sent.

1. Spamming:

Spamming means sending multiple copies of unsolicited emails or bulk emails such as chain letters.

1. Cyber Defamation :

This occurs when defamation takes place with the help of computers and/or the Internet. E.g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information

1. Harassment & Cyber stalking :

Cyber Stalking means that following an individual' activity over internet.

(2) Against Property

1. Credit Card Fraud :

As the name suggests, this is a fraud that happens by the use of a credit card. This generally happens if someone gets to know the card number or the card gets stolen.

1. Intellectual Property crimes :

These include Software piracy: Illegal copying of programs, distribution of copies of software. Copyright infringement: Using copyrighted material without proper permission. Trademarks violations: Using trademarks and associated rights without permission of the actual holder. Theft of computer source code: Stealing, destroying or misusing the source code of a computer.

1. Internet time theft :

This happens by the usage of the Internet hours by an unauthorized person which is actually paid by another person.

(3) Against Organizations

1. Unauthorized access of the computer: access to the computer / network without permission of the owner. Unauthorized Accessing of Computer: Accessing the computer/network without permission from the owner. It can be of 2 forms:

a) Changing/deleting data: Unauthorized changing of data.

b) Computer voyeur: The criminal reads or copies confidential or proprietary information, but the data is neither deleted nor changed.

1. Denial Of Service:

When Internet server is flooded with continuous bogus requests so as to denying legitimate users to use the server or to crash the server.

1. Computer contamination / Virus attack:

A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Viruses can be file infecting or affecting boot sector of the computer. Worms, unlike viruses do not need the host to attach themselves to.

1. Email Bombing:
2. Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.
3. Salami Attack:
4. When negligible amounts are removed & accumulated in to something larger. These attacks are used for the commission of financial crimes
5. Logic Bomb:

It is an event dependent program. Once the designated event occurs, it crashes the computer, releases a virus or some other harmful possibility.

1. Trojan horse:

This is an unauthorized program that works inside an apparently authorized program, thereby disguising what it is actually doing.

1. Data manipulation:

In this type of attack, raw data is altered by a computer just before it is processed, and altered back after processing is complete.

(4) Against Society

1. Forgery:

Banknotes, revenue stamps, stamp sheets, etc. They can be counterfeited using high-quality computers, scanners and printers.

1. Cyber ​​Terrorism:

Using computer resources to intimidate or coerce people and to carry out terrorist activities.

1. Web Jacking:

Hackers gain access to and control over another's website, even if they change the content of the website to achieve a political goal or to make money.

How to Fight Cybercrime

* Become vigilant when browsing websites.
* Flag and report suspicious emails.
* Never click on unfamiliar links or ads.
* Use a [VPN](https://www.pandasecurity.com/en-us/homeusers/vpn/) whenever possible.
* Ensure websites are safe before entering credentials.
* Keep antivirus/application systems up to date.
* Use [strong passwords](https://www.pandasecurity.com/en/mediacenter/tips/how-to-protect-your-password/) with 14+ characters

Conclusion

Criminal behavior on the Internet, or cyber crime, presents as one of the Major challenges of the future to India and International law enforcement. As ICT become even more pervasive, aspects of electronic crime will feature in all forms of criminal behavior, even those matters currently regarded as more traditional offences. It already feature in many international crime involving drug trafficking, people smuggling, terrorism and money laundering. Digital evidence will become more commonplace, even in traditional crimes, and we must be prepared to deal with this

new challenge.

References

https://www.researchgate.net/publication/307594049\_A\_Study\_on\_the\_Cyber\_-\_Crime\_and\_Cyber\_Criminals\_A\_Global\_Problem

https://www.bbau.ac.in/dept/Law/TM/1.pdf

https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/#:~:text=There%20are%20three%20major%20categories,%3A%20individual%2C%20property%20and%20government.&text=A%20crime%20against%20the%20government,military%20websites%20or%20distributing%20propaganda.

https://www.lawyersclubindia.com/articles/classification-of-cybercrimes--1484.asp