CYBER CRIME
&
IT'S TYPES

INTRODUCTION TO COMPUTER FORENSIC

- **Computer Forensic:** It is the process of identifying, preserving, analyzing and presenting the digital evidences, *computer and it's accessories (such as hard disk drive or USB drive)* for the purpose of justice. Sometimes it is known as digital forensic.

INTRODUCTION TO COMPUTER CRIME AND CYBER CRIME

- **Cyber Crime:** Crime in which *internet along with computer and its accessories* used to commit crime that crime known as cyber-crime

DIFFERENT TYPES OF CYBER CRIME

Cyber Crime Against Individual

- E-mail Spoofing
- Spamming
- Phishing
- Cyber defamation
- Cyber Stalking or Harassment
- Computer Sabotage

Cyber Crime Against Property

- Intellectual Property Crimes
- Cyber Squatting
- Cyber Vandalism
- Hacking Computer System

Cyber Crime Against Organization

- Hacking
- Password Sniffing
- DOS Attack
- E-mail Bombing
- Salami Attack

- **_E-Mail Spoofing_:** This means a spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-Mail forging or identity spoofing.

- **_Phishing_:** It is a type of social engineering attack often used to steal user data, including login credentials (user ID and passwords) and credit card numbers. It occurs when an attacker, pretend to be as a trusted entity, dupes a victim into opening an email, instant message, or text message.

CYBER CRIME AGAINST INDIVIDUAL[2]

- *Spamming*: Spam is the abuse of electronic messaging system to send bulk messages indiscriminately

- *Cyber defamation*: It involves any person with intent to lower down the dignity/image of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

CYBER CRIME AGAINST INDIVIDUAL[3]

- *Cyber stalking and harassment*: The use of Internet to repeatedly harass another person, group, or organization. This harassment could be sexual in nature, or it could have other motivations including anger.

- *Computer sabotage*: the use of the internet to halt the normal functioning of a computer system through the introduction of worms or viruses is referred to as computer sabotage.

- *Intellectual Property Crimes*: Any unlawful act by which the owner is deprived completely or partially of his rights is a crime. The most common type of crimes are software piracy, violation of copyright, trademark , theft of computer source code, etc.

- *Cyber Squatting*: It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first.

CYBER CRIME AGAINST PROPERTY[2]

- *Cyber Vandalism*: Vandalism means damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted.

- *Hacking Computer System*: Hacking in simple terms means illegal intrusion into a computer system and/or network.

- Hacking attacks include Famous social networking sites such as Facebook, Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system.

CYBER CRIME AGAINST ORGANIZATION[1]

- *Password sniffing*: Password sniffers are programs that monitor and record the name and password of network users as they login, at site.

- *E-mail bombing/mail bomb*: refers to sending a large no of emails to the victim to crash victim's E-mail account or server crash.

- ***Denial of service attacks***: The criminal floods the bandwidth of the victim's network. Denial of service attacks are designed to consume resources so that other users are unable to use the resources and are therefore —denied service. The attackers typically target site or service hosted on high-profile web servers such as bank, credit card payment gateways, mobile phone networks .

- ***Salami attack*:** these attacks used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers that deducts a small amount from the account of every customer.

SYMPTOMS OF CYBER ATTACK

- Files, applications, or services cannot be accessed by user.

- Accounts have been locked or the passwords have been changed without your knowledge.

- Files or software have been deleted or installed, or the contents have been changed without your involvement.

- Suspicious pop-ups load when you access the internet, or unknown files or programmes appear.

- Slower than normal internet speeds due to a spike in network traffic (or computers "hang" or crash).

- Files have been automatically encrypted, blocking your access to them.

- Emails sent automatically without the user's knowledge.

- No control over functions of the computer.

PREVENTION

- Use strong passwords

- Secure your computer

- Block spyware attacks

- Install the latest operating system updates

- Protect your data

- Secure your wireless network

- Avoid being scammed

LEGAL ACTS AGAINST CYBER CRIME

- The India Information Technology Act of 2000.

- CLOUD Act (Clarifying Lawful Overseas Use of Data)

- Govt. Initiatives

Thank You

Mr. Bhupeshkumar Nanhe, Assistant Professor, Dept. of Forensic Science, SoS, JECRC University, Jaipur (RJ), India. Email: bhupeshkumar.nanhe@jecrcu.edu.in