CYBER CRIME & INFORMATION SECURITY

Cyber Crime

Meaning – Criminal activities carried out by means of computers or the internet.

Definition –

- Cybercrime is defined as a crime where a computer is the object of the crime or is used as a tool to commit an offense.
- A cybercriminal may use a device to access a user's personal information, confidential business information, government information, or disable a device.
- Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.
- Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.
- Cyber crime or computer-oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target.

Cyber crime encloses a wide range of activities, but these can generally be divided into two categories:

a) Crimes that aim computer networks or devices. These types of crimes involve different threats (like virus, bugs etc.) and denial-of-service attacks.

b) Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

5.2 Classification of Cyber Crimes

Email spoofing

- Email spoofing is a form of cyber attack in which a hacker sends an email that has been manipulated to seem as if it originated from a trusted source.
- For example, a spoofed email may pretend to be from a well-known shopping website, asking the recipient to provide sensitive data, such as a password or credit card number.
- Alternatively, a spoofed email may include a link that installs malware on the user's device if clicked.

- An example of spoofing is when an email is sent from a false sender address, that asks the recipient to provide sensitive data.
- This email could also contain a link to a malicious website that contains malware.

Spamming

- Spamming is the use of electronic messaging systems like e-mails and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately.
- The term spamming is also applied to other media like in internet forums, instant messaging, and mobile text messaging, social networking spam, junk fax transmissions, television advertising and sharing network spam.
- Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

Cyber defamation

- The tort of cyber defamation is an act of intentionally insulting, defaming or offending another individual or a party through a virtual medium.
- It can be both written and oral.
- Defamation means giving an "injury to the reputation of a person" resulting from a statement which is false. The term defamation is used in the section 499 of Indian Penal Code, 1860.
- Cyber defamation is also known as internet defamation or online defamation in the world of internet and its users.
- Cyber defamation is also known as internet defamation or online defamation in the world of internet and its users.
- Cyber defamation is a new concept but it virtually defames a person through new medium. The medium of defaming the individual's identity is through the help of computers via internet.

Internet time theft

- It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person.
- The authorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.

- Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person.

Salami Attack

- A salami attack is a small attack that can be repeated many times very efficiently. Thus the combined output of the attack is great.
- In the example above, it refers to stealing the round-off from interest in bank accounts.
- Even though it is less than 1 cent per account, when multiplied by millions of accounts over many months, the adversary can retrieve quite a large amount. It is also less likely to be noticeable since your average customer would assume that the amount was rounded down to the nearest cent.

Data Diddling

- Data diddling is a type of cybercrime in which data is altered as it is entered into a computer system, most often by a data entry clerk or a computer virus.
- Data diddling is an illegal or unauthorized data alteration. Changing data before or as it is input into a computer or output.
- Example: Account executives can change the employee time sheet information of employees before entering to the HR payroll application.

Forgery

When a perpetrator alters documents stored in computerized form, the crime committed may be forgery. In this instance, computer systems are the target of criminal activity.

- The term forgery usually describes a message related attack against a cryptographic digital signature scheme. That is an attack trying to fabricate a digital signature for a message without having access to the respective signer's private signing key.
- Among the many examples of this crime, taking another's work, whether it be written or visual, such as a artwork, and attempting to distribute it as either your own or as an original is an example of forgery.
- Likewise, either creating fake documents or producing counterfeit items is considered to be forgery as well.

Hacking

- Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks.

- Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose

Email bombing

- An email bomb or "mail bomb" is a malicious act in which a large number of email messages are sent to a single email address in a short period of time. The purpose of an email bomb is typically to overflow a user's inbox. In some cases, it will also make the mail server unresponsive.