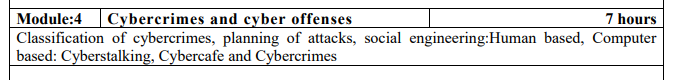
****

**Classification of Cyber Crime**

1. Crime is the target as well as victim. For e.g.: hacking cyber theft cyber block mailing etc.

2. Crime is incidental to other crime. Cyber pornography, harassment unlawful banking transaction & others.

Donn Parker identified four forms of computer abuse namely:-

1. Computer might serve as the victim of crime.

2. Computer might constitute the environment with in which a crime is committed

3. Computer might provide the means by which crime is committed

4. Computer might symbolically be used to frighten, mislead or defraud victims.

We can classify cybercrime as:-

**Unauthorized Access**

Knowingly and intentionally use or access without prevision or consent of the owner or possessor whole or any part of a computer systems, computer network to commit any cybercrime as denied above is unauthorized access.

**Cyber theft**

Cyber theft is when your financial or personal information is stolen via computers. Cyber thieves can target both corporations and individuals. One cyber theft example happened back in 2013, when Target announced that cyber thieves stole the credit and debit card information of nearly 40 million Target shoppers nationwide.

**Cyber hacking**

Hacking would means destruction or alteration of any information residing in a computer resource i.e. computer resource of tangible or intangible. Tangible assets include the hardware, components of the computer resources whereas intangible assets include information in the electronic form, magnetic or optical impulses. Hacking is the most common form of cybercrime in these days. The reason why hackers indulge in this crime may vary from monetary gain to political interest or it may even be for the sake of shear thrill. Hacking may be different forms such as web-spoofing, e-mail bombing, Trojan attacks, virus attacks, password hacking etc. in simple words hacking means seeking of unauthorized access through computer network.

**Cyber Fraud**

Fraud committed through computer, computer system, computer network or internet related communications are to be treated as cyber fraud. Any unauthorized access to commit fraud is to be treated as double crime in cyberspace one is unauthorized access which is similar to criminal trespass under s. 441 of the Indian Penal Code and another is commission of fraud after this unauthorized access. Internet fraud can be committed through websites, e-mail junk mail, spamming, posting a message on an online bulletin board chat room is discussion, which is very difficult for the victims to identify whether the act in internet in fraudulent or actual fact.

**Cyber pornography**

Pornography on the internet may take various forms. It may include hosting of website containing some obscene or prohibited material or use of computer for producing obscene materials. Such material tends to pervert the thinking of adolescents and corrupt their mind set. A person who publishes or transmits or causes to be published in the electronic form any material which is lascivious, or if its effects in such as to tend to deprave or corrupt the persons who are likely to see, wad or hear the matter contained or embodied in it, is liable to punishment which may extend to imprisonment upto five year and liable to fine, which may extend to rupees one lakh (S/67 of Information Technology Act. 2000)

**Cyber Terrorism**

Cyber terrorism has domestic as well as international ramifications. It may be defined as the premeditated use of disruptive activities or the threat there of in cyber space with the intention to further social, ideological, religious, political or similar objectives or to intimidate any person in furtherance of such objectives, A cyber terrorist’ may be defined as a person who uses computer system as a means to achieve any of the following objectives:-

(i) Putting the public or any section of the public in far

(ii) Affecting adversely the harmony between different religious, racial language or regional groups or casted or communities.

(iii) Covering or over a wing the government established by law

(iv) Endangering the sovereignty and integrity of the nation.

**Cyber stalking**

In stalking persistant message are sent to unwilling mental torture. Sending of unsolicited e-mail or spamming is an infringement of might of privacy. Online harassment and threats may take many forms. Cyber stalking would occur with women who are staked by men adolescents and adult pedophiles. A cyber stalker does not have to leave his home to harass his targets and has no fear of physical avenge since he cannot be physically touched in cyber space.

A cyber stalker generally collects all the personal information about the victim such as name, age, family background, telephone or mobile numbers, workplace etc. He collects this information from the internet resources such as various profiles the victim may have filled in while opening the chat or e-mail account.

**Flowing of virus**

Flowing of programmed through computer network by human agent such as virus, Trojan Horse, works, Logic Bombs can cause damage, alter, debate destroy computer, computer system, computer network, computer data base are also cybercrime. There are three types of viruses. They are popularly known as fill infectors through spread sheet programmed of games, boot, sector viruses through diskette or hard dies i.e., read into memory and exacted when a computer first start, and make versus, which depend on operating system and infect files and which contain data. For example, I love you buy, virus and was the total threat worldwide which was the cause of innovation of several new and more effective antivirus software e.g., Jaw, Quick Heal, Mobile Anti viruses, Main characteristics, of viruses are:

1. A virus is a self-replicating programmed whose main purpose is to propagate itself at as many different places as possible

2. A virus can any propagate itself by an unknown act of a user of the system in which it exists.

3. A virus propagates itself by modifying the anthem programme to include itself.

**Violation of privacy**

Privacy is the claim of individual, group or institutions to determine for themselves when, how and to what extend information about them is communicated to other on not .**Invasion of privacy** is the intrusion upon, or revelation of, something private. One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his/her private affairs or concerns, is subject to liability to the other for **invasion of privacy**

There are four main types of invasion of privacy, all of which can lead to a civil lawsuit. These include (1) intrusion of solitude, (2) appropriation of name or likeness, (3) public disclosure of private facts, and (4) false light.

**Spamming**

E-mail is an inexpensive and popular device for distributing, fraudulent message to potential victims, This technical not only helps of to assume someone else’ identity, but also helps to hide one’s own. Therefore the person community the e-mail has little of being detached and identified. The most common e-mail fraud in phishing I.e., personal information fraud the purpose of such spasm is to trick the person for divulging his person information so that the offender can steal his identity and commit crime in that person’s name.

**E-Mail spoofing**

A hacker logging in to a computer of under was to his victim often will login under a different identity. This is called spoofing. The hacker able to having previously actual password or having created a new identity by fooling the computer into thinking he is the system’s operator. A spoofed email may be said to be one which the be miss represent its origin. That is, it shows its online to be different from which it actually originates. For example, where A sends a threatening a email to the president of the students a union threatening to detente a nuclear sent from the college compos and this email was sent from the account of some other student “A” would a be quality of email spoofing.

**Computer Vandalism**

Cyber-Vandalism accounts to the act of damaging someone’s data from the computer that in a way disrupts the victim’s business or image due to editing the data into something invasive, embarrassing or absurd. The thieves create malevolent programs that prove injurious to the hard disk data or login credentials of the victim. Cyber-vandalism is different from computer viruses that attach into the programs and Wikipedia being one of the famous sites, is prone to potential damage of content because anyone can edit the site. However, Wikipedia has presently sustained an equilibrium between the types of users that there are articles that cannot be edited by unregistered or new users.

Today’s vandalism felony surrounds the computers and in some countries, new laws have also been updated that has resulted in the punishment for vandalism. The gaming company networks have paved a productive way for the computer-literate youth to indulge their knowledge and talents into creating games rather than becoming malware designers. Cyber-Vandalism leads to other risks also that could be dangerous for your computer system, your identity, your precious personal data and your finances.

**Money Laundering**

Money laundering is crime which related the money of banking system. In the money laundering the money in transfer unauthorized way to own account in the theft of identity of person, his password and account number of this type of crime is increase in day and by day. This type of crime in increase in computer and other electronic devices and theft of hour’s identity password, account number of to transfer the money to an account number of to another, this is new type of crime.

**Data Diddling**

**Data diddling** is the changing of **data** before or during entry into the computer system. Examples include forging or counterfeiting documents used for **data** entry and exchanging valid disks and tapes with modified replacements.

**Cyber Defamation**

Defamation is defined is as an international false communication either published or publicly spoken, that injustice another’s reputation or good name: The gift of defamation is actual or presumed damage to reputation flowing from publication. In other words defamation flows, from publication or communities of making publicly known. Publication means that action of making internet the term publication includes dissemination, transmission and storage, of information or data in electronic form.

**Sale of illegal Articles**

Interest sales of illegal articles beverage have caused the direct shipments of such beverages of to consumers to proliferate. Selling over the interest allows small illegal Articles producers to reach consumers well beyond their immediate areas. These Interest sales of illegal articles enable adults and potentials sinuous to receive products and that are not ordinary available through the traditional distribution channels.

**Page–Jacking**

Page Jacking involves the appropriation of web site description key words, of metaware from other sites. The page jacked is sites, these items into his our sites, seeking to draw consumer to a particular site this is a because the descriptions, key words, and meta tag and used by search engines when sorting and displaying sits on a particular topic requested appear on individual.

• Cybercrimes under the IT Act Tampering with Computer source documents - Sec.65

• • Hacking with Computer systems, Data alteration - Sec.66

• • Publishing obscene information - Sec.67

• • Un-authorized access to protected system Sec.70 Breach of Confidentiality

• • and Privacy - Sec.72 Publishing false digital signature certificates - Sec.73

• • 2. Cyber Crimes under IPC and Special Laws Sending threatening messages by email - Sec 503 IPC

• Sending defamatory messages by email - Sec 499 IPC

• • Forgery of electronic records - Sec 463 IPC

• • Bogus websites, cyber frauds - Sec 420 IPC

• • Email spoofing - Sec 463 IPC

• • Web-Jacking - Sec. 383 IPC

• • E-Mail Abuse - Sec.500 IPC

• • 3. Cyber Crimes under the Special Acts Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act

• • Online sale of Arms Act•

**Preventive Measures For Cyber**

**Crimes:**

• Identification of exposures through education will assist responsible companies and firms to meet these challenges.

• One should avoid disclosing any personal information to strangers via e-mail or while chatting.

• One must avoid sending any photograph to strangers by online as misusing of photograph incidents increasing day by day.

• An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.

• A person should never send his credit card number to any site that is not secured, to guard against frauds.

• It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.

• Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.

• Web servers running public sites must be physically separately protected from internal

corporate network.

• It is better to use a security programmes by the body corporate to control information on sites.

• Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.

• IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.

• As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cyber crime.

• A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cyber crime.

**Human-Based Social Engineering Attacks**

In human-based social engineering attacks, the social engineer interacts directly   with the target to get information.  
  
An example of this type of attack would be where the attacker calls the database administrator asking to reset the password for the targets account from a remote location by gathering the user information from any remote social networking site of the XYZ company.  
  
Human-based social engineering can be categorized as follows:   
  
•  **Piggybacking**: In this type of  attack the  attacker takes advantage by tricking authorized personnel to get inside a restricted area of the targeted company, such as the server room. For example, attacker X enters the ABC Company as a candidate for an interview but later enters a restricted area by tricking an authorized person, claiming that he is a new employee of the company and so doesn’t have an employee ID, and using the targets ID card.

• **Impersonating**: In this type of attack, a social engineer pretends to be a valid employee of the organization and gains physical access. This can be perfectly carried out in the real world by wearing a suit or duplicate ID for the company. Once inside the premises, the social engineer can gain valuable information from a desktop computer.   
  
• **Eavesdropping**: This is the unauthorized listening to of communication between two people or the reading of private messages. It can be performed using communication channels such as telephone lines and e-mails.   
  
• **Reverse social engineering**: This is when the attacker creates a persona that appears to be in a position of authority. In such a situation, the target will ask for the information that they want.  Reverse engineering attacks usually occur in areas of marketing and technical support.   
  
• **Dumpster diving**: Dumpster diving involves looking in the trash can for information written on pieces of paper or computer printouts. The hacker   can often find passwords, filenames, or other pieces of confidential information in trash cans.   
  
• **Posing as a legitimate end user**: In this type of attack, the social engineer assumes the identity of a legitimate user and tries to get the information, for example, calling the helpdesk and saying, “Hi, I am Mary from the X department. I do not remember my account password; can you help me out?”

**Computer based social engineering attacks may include the below.**

* Email attachments
* Fake websites
* Pop-up windows
* Insider Attacks

**On-line Scams:** Emails sent by scammers may have attachments that include malicious code inside the attachment. Those attachments may include Keyloggers to capture user’s passwords, Viruses, Trojans, or worms.

**Worm attacks:** Attackers will trick users to click on a link or download a file then click on it, the executable file is a worm and will propagate from computer to computer copying itself.

A well-known example is the “LoveLetter” worm that comes as an attachment in an email. The email requests the user to open an attachment in an email. When the users open the attachment the worm copies itself to all the contacts in the users address book. This worm overloaded a huge number of email servers in the year 2000.

Sometimes pop-up windows can also be used in social engineering attacks. Pop-up windows that advertise special offers may tempt users to unintentionally install malicious software.

**Phishing attacks:** This type of social engineering attack commonly uses emails to trick users in getting credentials to their bank accounts or maybe email accounts. The email mostly claims to be from a well-known source, a highly reputed organization, and asks the user to click on a link that takes the users to a site similar to the organizations web site but this site is a fraudulent website that harvests users credentials. The fraudsters use these credentials to gain access to bank or email accounts and steal important information and money.

**Insider attack**: This type of attack is performed from inside the target network. Most insider attacks are orchestrated by disgruntled employees who are not happy with their position in the organization or because they have personal grudges against another employee or the management.

**Cyber Stalking:**

While most of us are aware of what stalking is, not many users know what cyber-stalking is! Cyber-stalking is a form of cyber-crime that takes place online when a criminal uses technology to harass or threaten a person or an organization. The assailant can blackmail the victims by gaining access to their emails, instant messages, chats, social media accounts, online-banking accounts and more. In simple words, it’s just like traditional stalking but in the cyber-world.

Examples of Cyber-Stalking

* Making and posting fake or real sexual images of the victim or their loved ones.
* Tracking their victims’ every movement by placing a GPS device on their car.
* Threatening the victim or their friends and family via emails.
* Uploading personal information such as name, address, social security number or phone number on the Internet.
* Hacking and saving emails, text messages and social media posts and using them to harass or blackmail a victim.
* Hacking into the victim’s social media account to post offensive material and comments.
* Using the victim’s social media account or email to stalk and contact others.

**Cyber Crime and CyberCafe:**

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers. Cybercrime may also be referred to as computer crime.

Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. More serious crimes like cyber terrorism are also of significant concern.

Cybercrime encompasses a wide range of activities, but these can generally be broken into two categories:

* Crimes that target computer networks or devices. These types of crimes include viruses and denial-of-service (DoS) attacks.
* Crimes that use computer networks to advance other criminal activities. These types of crimes include cyberstalking, phishing and fraud or identity theft.

Cybercafe hold two types of risks:

1. We do not know what programs are installed on the computer like keyloggers or spyware.

2. Over the shoulder peeping can enable others to find out your passwords

**IDENTITY THEFT**

Identity theft is the act of stealing another person’s personal identifying information in order to gain access to his financial resources, or obtain access to other benefits, such as money, credit, or insurance benefits.

According to the Identity Theft Resource Center, there are four distinct types of identity theft.

•Criminal Identity Theft

•Synthetic Identity Theft

•Medical Identity Theft

•Child Identity Theft

**Criminal Identity Theft**

•Criminal identity theft occurs when a person identifies himself as another person to avoid detection by law enforcement, to evade arrest, or to evade prosecution for a crime.

•Criminal identity theft might enable the perpetrator to commit a crime under the victim’s name, leaving the victim holding the bag.

•When this occurs, it may be difficult for the victim to clear his name completely, as it is an extensive process that involves the court system.

**Synthetic Identity Theft**

•This crime involves the creation of a completely or partially fabricated identity.

•This is done by combining an individual’s real social security number with a phony name and made-up date of birth.

•This type of identity theft is difficult to track, as it may not appear on either person’s credit report.

•It may create an entirely new credit report file, or appear on the victim’s report as a sub-file

**Medical Identity Theft**

•The term medical identity theft, coined in 2006,is a form of insurance fraud.

•This involves an individual obtaining medical care under another person’s name, using the victim’s name and birthdate, and possibly even his insurance policy information.

•Perpetrator’s medical information would be entered on to the victim’s medical records, and thus exposes the victim to financial losses for medical bills and insurance costs.

**Child Identity Theft**

•IRS requires that all children claimed as dependents on a parent’s income taxes have their own social security numbers.

•These social security numbers are valued commodities for fraudsters, as they have no information associated with them.

•Child identity theft may be committed by a family member or friend, but strangers might use the numbers to apply for loans, obtain credit cards, and even obtain a driver’s license.

•Because nobody thinks to obtain a child’s credit report, this crime may go undetected for many years.

**Identity Theft Protection Tips**

•Other tips for identity theft protection include:

•Protect PIN numbers by never writing the moncredit/ debitcards, or on a slip of paper in a wallet

•Shield keypads when using ATMs or checkout systems

•Collect the mail immediately

•Have the post office hold mail when away for more than a day or two

•Pay attention to whether bills arrive as scheduled

•Keep all receipts and account statements

•Shred unwanted statements or receipts

•Keep all personal information in a safe place at home

•Ignore unsolicited requests for personal information

•Use firewalls on home computers

•Always use secure passwords

•Check credit reports annually, or anytime theft is suspected