Question Bank Chapter 1 : Introduction to Cybercrime

1. Define cybercrime. Explain the two types of cybercrimes.

Ans: **Cybercrime specifically can be defined in a number of ways;**

1. *A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband(illegal items) or stalk victims or disrupt operations with malevolent(causing harm) programs.*
2. *Crimes completed either on or with a computer.*
3. *Any illegal activity done through the Internet or on the computer.*
4. *All criminal activities done using the medium of computers, the Internet, cyberspace and the WWW(*World Wide Web*)*

- Two types of cyber attacks are prevalent: **Techno-crime and Techno-vandalism**

Techno-crime:

- A premeditated (Planned beforehand) act against a system or systems, with the intent to copy, steal, prevent access, corrupt or otherwise deface or damage parts of or the complete computer system.
- The 24 × 7 connection to the Internet makes this type of cybercrime a real possibility to engineer from anywhere in the world, leaving few, if any, "finger prints."

Techno-vandalism:

- These acts of "brainless" defacement of websites and/or other activities, such as copying files and publicizing their contents publicly, are usually opportunistic in nature.
- Tight internal security, allied to strong technical safeguards, should prevent the vast majority of such incidents.

2. Define the term "Cybersecurity" according to Indian Information Technology Act -2008 (ITA-2008)

Ans: *"Cybersecurity" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. (**Indian Information Technology Act (ITA-2008**))*

3. Categorized cyber criminals into groups that reflect their motivation. Write a note on any two cybercriminals in each group.

Ans: They can be categorized into three groups that reflect their motivation

1. Type I: **Cybercriminals** – **hungry for recognition**

- **Hobby hackers:**
    - A considerable number of hackers are doing hacking for fun.
    - Some of them hack significant accounts or systems just in case of fun and show that they are powerful.
    - Some of them hack the accounts or systems or even emails of their friends or people they know to find out what are they doing or threaten them and having some fun by doing that.
    - Most of the hackers find it quite funny and entertaining to hack something.
- **IT professionals**
    - Professional hacking is a legally sanctioned practice of identifying weaknesses and vulnerabilities in computer systems and networks to protect them from malicious attacks.
    - Professional hacker, also known as ethical hackers, operate with the explicit permission and cooperation of the organization.
- **Politically motivated hackers**
    - Act of accessing a computer system without authorization for political or social purposes(Hacktivism)
    - It is intended to draw public attention to an issue or cause that the hacker believe to be significant – for example, freedom of information, human rights, or a religious point of view.
    - Hackers commonly deface websites to protest social and political injustice around the globe
- **Terrorist organizations (Cyber terrorism)**
    - Defined as disruptive attacks by recognized terrorist organizations against computer systems with the intent of generating alarm, panic, or the physical disruption of the information system.
    - The more mainstream idea of cyber terrorism is the hacking of government or private servers to access sensitive information or even siphon funds for use in terror activities.

2.. Type II: **Cybercriminals** – not interested in recognition

- **Psychological perverts**
    - Perversion is a form of human behavior which deviates from what is considered to be orthodox or normal.
    - Although most often used to refer to some sort of psychological corruption or abnormal, the word perversion can actually refer to anything that is used for a distorted or wrong purpose.
- **Financially motivated hackers (corporate espionage);**
    - Attackers want money and they try to get it through various coercive means, such as phishing or ransomware.
    - **Social engineering** will be employed to trick people into handing over money.
    - In the case of **ransomware**, cyber criminals will encrypt (lock) their victim's data and ask for a ransom in return for decrypting (unlocking) the information.
- **State-sponsored hacking**
    - State-sponsored cyber warfare (**hacking**) is a form of cyber warfare in which a government or state sponsors or carries out cyber attacks against other governments, businesses, organizations, or individuals.
    - The primary goal of these attacks is to achieve strategic objectives, such as **disrupting critical infrastructure, stealing sensitive information, or compromising the integrity of information systems**
    - Governments also use cyber espionage (spies) to gather sensitive information, such as trade secrets, military plans, and diplomatic communications.
- O**rganized criminals.**
    - In organized cybercrime, cybercriminals structure and run their operations in ways that darkly mirror the workings of a real business.
    - It involves organized crime groups with ringleaders located in one country and developers in others, further supported by operations, marketing, finance, and call center teams in yet other locations—**just like a legitimate business**

3. Type III: **Cybercriminals** – the insiders

- **Disgruntled or former employees seeking revenge.**
    - These insider threats are often attributed to dissatisfied employees or ex-employees who believe that the organization was doing something wrong with them in some way, and they feel justified in seeking revenge.
    - The consequences of a successful insider threat can take a variety of forms, including a data breach, fraud, theft of trade secrets or intellectual property, and sabotage of security measures.
- C**ompeting companies using employees to gain economic advantage through damage and/or theft.**
    - The illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. (Industrial espionage)
    - This activity is a covert practice often done by an insider or an employee who gains employment for the express purpose of spying and stealing information for a competitor.
    - Industrial espionage is conducted by companies for commercial purposes

4. Explain the following cybercrimes/cyberattack a. Email spoofing b. Spamming c. Password sniffing

Ans:

- **Email Spoofing-** A spoofed E-Mail is one that appears to originate from one source but actually has been sent from another source.

- **Example**

Let us say, Roopa has an E-Mail address **roopa@asianlaws.org**. Let us say her boyfriend Suresh and she happen to have a showdown. Then Suresh, having become her enemy, spoofs her E-Mail and sends obscene/vulgar messages to all her acquaintances. Since the E-Mails appear to have originated from Roopa, her friends could take offense and relationships could be spoiled for life.

- **Spamming**-
    - People who create electronic spam are called **spammers.**
    - ***Spam is the abuse of electronic messaging systems(including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately.***
    - Although the **most widely recognized form of Spam is E-Mail Spam**, the term is applied to similar abuses in other media: **instant messaging spam**, **Usenet newsgroup spam**, **web search engine spam**, **spam in blogs**, **wiki spam**, **online**

classified ads spam, **mobile phone messaging spam**, **Internet forum spam**, **junk fax transmissions**, **social networking** spam, **file sharing network spam**, **video sharing sites**, etc.

- Spamming is difficult to control because it has economic viability – advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings.
- In the context of **search engine spamming,** spamming is alteration or creation of a document with the intent to deceive an electronic catalog or a filing system.
- Some web authors use "**subversive techniques**" to ensure that their site appears more frequently or higher number in returned search results – this is strongly discouraged by search engines and there are fines/ penalties associated with the use of such subversive techniques.

- **Password sniffing**

- These are programs that monitor and record the name and password of network users as they login
- Whoever installs the Sniffer can then impersonate an authorized user and login to access restricted documents.
- Laws are not yet set up to adequately prosecute a person for impersonating another person online.
- Laws designed to prevent unauthorized access to information may be effective in apprehending crackers using Sniffer programs.

5. Write a note each of the following. a. Internet time theft b. Data diddling c. Salami attack

Ans:

Internet Time Theft

- Such a theft occurs when an unauthorized person uses the Internet hours paid for by another person.
- Basically, Internet time theft comes under hacking because the person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.
- However, one can identify time theft if the Internet time has to be recharged often, even when one's own use of the Internet is not frequent. (related to the crimes conducted through "identity theft.")

Data diddling attack

- A cybercrime where a person intentionally enters wrong information into a computer, system, or document. It is often used when businesses and individuals want to hide part of their profits for tax evasion purposes.
- It also involves altering the raw data just before a computer processes it and then changing it back after the processing is completed.
- Electricity boards in India have been victims to data diddling programs inserted when private parties computerize their systems.
- Data diddling can lead to financial loss, either directly or indirectly. For example, a hacker may alter the payment information in a company's database to redirect payments to his account, causing the company to lose money
- Data diddling is a form of cyber crime, and is punishable by large fines or imprisonment

Salami Attack/Salami Technique

- These attacks are used for committing financial crimes. The idea here is to make the alteration so insignificant that in a single case it would go completely unnoticed
- **Example :**

A bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say ` 2/- or a few cents in a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount every month.

6. Explain the terms Logic bomb, E-Mail bombing, industrial espionage.

Ans:

Logic Bombs

- **Logic bombs** are event-dependent programs created to do something only when a certain event occurs.
- Some viruses may be termed as logic bombs because they lie **dormant** all through the year and become active only on a particular date(**eg., Chernobyl virus and Y2K viruses**).

E-Mail Bombing/Mail Bombs

- E-Mail bombing refers to sending **a large number of E-Mails** to the victim to crash victim's E-Mail account (in the case of an individual) or to make victim's mail servers crash (in the case of a company or an E-Mail service provider).

- Computer program can be **written to instruct a computer** to do such tasks **on a repeated basis**.

- In recent times, terrorism has hit the Internet in the form of mail bombings. By instructing a computer to repeatedly send E-Mail to a specified person's E-Mail address, the cybercriminal can overwhelm the recipient's personal account and potentially shut down entire systems.

- This may or may not be illegal, but it is certainly disruptive.

Industrial Spying/Industrial Espionage

- Highly skilled hackers are contracted by high-profile companies or certain governments to carryout spying

- With the growing public availability of **Trojans and Spyware** material even a low-skilled one can generate high volume profit out of industrial spying. This is referred to as "**Targeted Attacks**"

- **Real Example:**

  *One interesting case is the **famous Israeli Trojan story**, where a software engineer in London created a Trojan Horse program specifically designed to extract critical data gathered from machines infected by his program. He had made a business out of selling his Trojan Horse program to companies in Israel, which would use it for industrial spying by planting it into competitors' networks.*

- There are also **the E-Mail worms** automating similar "**data exfiltration features".**

- A computer worm is a subset of the Trojan horse malware that can propagate or self-replicate from one computer to another without human activation after breaching a system. Typically, a worm spreads across a network through your Internet or LAN (Local Area Network) connection.

7. What is cyber defamation according to the IPC section 499?

Ans: **According to the IPC section 499:**

1. It may amount to defamation to impute anything to a deceased person, if the imputation would harm the reputation of that person if living, and is intended to be hurtful to the feelings of his family or other near relatives.

2. It may amount to defamation to make an imputation concerning a company or an association or collection of persons as such.

3. An imputation in the form of an alternative or expressed ironically, may amount to defamation.

4. No imputation is said to harm a person's reputation unless that imputation directly or indirectly, in the estimation of others, lowers the moral or intellectual character of that person, or lowers the character of that person in respect of his caste or of his calling, or lowers the credit of that person, or causes it to be believed that the body of that person is in a loathsome state or in a state generally considered as disgraceful.

8. Define child pornography. Explain how paedophiles operate.

Ans: "**Child pornography"** means any visual depiction, including **but not limited** to the following:

1. Any photograph that can be considered obscene and/or unsuitable for the age of child viewer;
2. film, video, picture;
3. computer-generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of **a minor engaging in sexually explicit conduct.**

- **"Child pornography" is considered an offense.**
- The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. Its explosion has made the children a viable victim to the cybercrime.
- As the broad-band connections get into the reach of more and more homes, larger child population will be using the Internet and therefore greater would be the chances of falling victim to the aggression of **pedophiles**.
- **"Pedophiles**" are people who physically or psychologically **coerce minors** to engage in sexual activities, which the minors would not consciously consent to.
    - **Here is how pedophiles operate:**
- **Step 1:** Pedophiles use **a false identity** to trap the children/teenagers (using "false identity")
- **Step 2:** They seek children/teens in the kids' areas on the services, such as the Teens BB, Games BB or chat areas where the children gather.
- **Step 3:** They befriend children/teens.
- **Step 4:** They extract personal information from the child/teen by winning his/her confidence.
- **Step 5:** Pedophiles get E-Mail address of the child/teen and start making contacts on the victim's E-Mail address as well. Sometimes, these E-Mails contain sexually explicit language
- **Step 6:** They start sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his/her inhibitions so that a feeling is

created in the mind of the victim that what is being fed to him is normal and that everybody does it.

- **Step 7:** At the end of it, the pedophiles set up a meeting with the child/teen out of the house and then drag him/her into the net to further sexually assault him/her or to use him/her as a sex object.

9. What is software piracy? What are the disadvantages of using pirated software?

Ans: **Software piracy**

- It Is defined as theft of software through the illegal copying of genuine programs, or the counterfeiting and distribution of original software products.
- **There are many examples of software piracy:**
    - ***end-user copying*** – friends loaning disks (CD/DVD) to each other, or organizations under-reporting the number of software installations they have made, or organizations not tracking their software licenses;
    - ***hard disk loading with illicit means*** – hard disk vendors load pirated software;
    - ***counterfeiting*** – large-scale duplication and distribution of illegally copied software;
    - ***illegal downloads from the Internet*** – by intrusion, by cracking serial numbers, etc.
- Beware that those who buy pirated software have a lot to lose:
    - (a) getting untested software that may have been copied thousands of times over,
    - (b) the software, if pirated, may potentially contain hard-drive-infecting viruses,
    - (c) there is no technical support in the case of software failure, that is, lack of technical product support available to properly licensed users,
    - (d) there is no warranty protection
    - (e) there is no legal right to use the product, etc.
- **Economic impact** : According to some Study in Asia Pacific 55% of the software installed in 2006 on personal computers (PCs) was obtained illegally. Financial losses due to software piracy **was amounted to US$ 11.6 billion**.
- The Study covered software that runs on personal **computers, including desktops, laptops and ultra-portables.**
- The study includes operating systems, systems software such as databases and security packages, business applications and consumer applications such as PC games, personal finance and reference software

Chapter 2 : Cyberoffenses: How criminals Plan them

1. Explain the six Types of Hackers.

Ans: There are six types of hackers:

Black hat hacker:

- **A black hat** is also called a "**cracker**" or "**dark side hacker**." Such a person is a malicious or criminal hacker with intention making money
- They usually have the **expertise and knowledge to break into computer** networks without the owners' permission, **exploit security vulnerabilities**, and **bypass security protocols**. Typically, the term **"cracker"** is used within the security industry.

White hat hacker:

- **A white hat hacker** is a person who is ethically opposed to the abuse of computer systems. one. A "white hat" generally focuses on securing IT systems, whereas a "black hat" (the opposite) would like to break into them.
- A black hat will wish to secure his/her own machine whereas a white hat might need to break into a black hat's machine in course of an investigation.

Grey hat hacker:

- **Grey Hat** hackers fall somewhere between white hat and black hat hackers. Grey hat hackers' intentions are often good, but they don't always take the ethical route with their hacking technics.

For example, they may penetrate your website, application, or IT systems to look for vulnerabilities without your consent. But they typically don't try to cause any harm.

- **A grey hat** releases information about any exploits or security holes he/she finds openly to the public.
- He/she does so without concern for how the information is used in the end(whether for patching or exploiting).

Red hat hacker:

- Much like white hat hackers, **red hat** hackers also want to save the world from evil hackers. But they choose extreme and sometimes illegal routes to achieve their goals.
- When they find a black hat hacker, they deploy dangerous cyber attacks against them.
- In short, red hats are the types of hackers who often choose to **take aggressive steps** to stop black hat hackers.

- They're known to launch **full-scale attacks to bring down the bad guys' servers** and destroy their resources.

Blue hat hacker:

- Blue Hat hackers don't necessarily care about money or fame. They hack to take personal revenge for a real — or perceived — sleight from a person, employer, institution, or government.
- Blue hat hackers use malware and deploy various cyber attacks on their enemies' servers/networks to cause harm to their data, websites, or devices.
- Companies often invite them to test the new software and find security vulnerabilities before releasing it.
- Sometimes, companies organize periodic conferences for **blue hat hackers** to find the bugs in their crucial online systems.

Green hat hacker:

- Green Hat hackers are the "newbies" in the world of hacking. Green hat hackers are not aware of the security mechanism and the inner workings of the web, but they are keen learners and determined (and even desperate) to elevate their position in the hacker community.
- Although their intention is not necessarily to cause harm, they may do so while "playing" with various malware and attack techniques.

2. Explain the terms: active attacks, passive attacks, inside attack and outside attack.

Ans:

<u>Active attacks:</u>

- Active attacks are usually used to alter the system. Active attacks may affect the availability, integrity and authenticity of data. Due to active attack system is always damaged and System resources can be changed. The most important thing is that, In an active attack, Victim gets informed about the attack.

<u>Passive attacks:</u>

- passive attacks attempt to gain information about the target. passive attacks lead to breaches of confidentiality. Due to passive attack, there is no harm to the system. The most important thing is that In a passive attack, Victim does not get informed about the attack

Inside attacks:

- An attack originating and/or attempted within the security parameter of an organization is an inside attack; it is usually attempted by an insider who gains access to more resources than expected.

Outside attacks:

- An outside attack is attempted by a source outside of the security parameter, maybe attempted by an outsider, who is indirectly associated with the organization, it is attempted through the Internet or a remote access connection.

3. What is Reconnaissance? Discuss passive and active Reconnaissance.

Ans: The literal meaning of "Reconnaissance" is an act of reconnoitering – explore, often with the goal of finding something or somebody (especially to gain information about an enemy or potential enemy).

In the world of **"hacking,"** reconnaissance phase begins with "**Footprinting**" – this is the preparation toward preattack phase, and involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.

- **Footprinting** gives an overview about system vulnerabilities and provides a judgment about possible exploitation of those vulnerabilities.
- The objective of this preparatory phase is to understand the system, its networking ports and services, and any other aspects of its security that are needful for launching the attack.
- Thus, an attacker attempts to gather information in two phases: **passive and active reconnaissance.**

- **Reconnaissance -** passive **:**

- A passive reconnaissance involves gathering information about a target without his/her (individual's or company's) knowledge.
- it is usually done using Internet searches or by Googling an individual or company to gain information.
    - **Google or Yahoo search**: People search to locate information about employees
    - **Surfing online community groups like Orkut/Facebook** will prove useful to gain the information about an individual.
    - **Organization's website** may provide a personnel directory or information about key employees, for example, contact details, E-Mail address, etc. These can be used in a social engineering attack to reach the target.

- **Blogs, newsgroups, press releases**, etc. are generally used as the mediums to gain information about the company or employees.
- **Going through the job postings in particular job profiles** for technical persons can provide information about type of technology, that is, servers or infrastructure devices a company maybe using on its network.

- **Reconnaissance -** Active

- An active reconnaissance involves probing the network to discover individual hosts to confirm the information (IP addresses, operating system type and version, and services on the network) gathered in the passive attack phase.
- Active reconnaissance can provide confirmation to an attacker about security measures in place, but the process can also increase the chance of being caught or raise a suspicion

4. Discuss the activities carried out by an attacker in second phase of a cyberattack.

Ans: Second phase of a cyberattack is Scanning and Scrutinizing Gathered Information

- Scanning is a key step to **examine intelligently** while gathering information about the target.
- The objectives of scanning are :
    1. **Port scanning**: Identify **open/close ports** and services.
    2. **Network scanning:** Understand IP Addresses and related information about the computer network systems.
    3. **Vulnerability scanning**: Understand the existing weaknesses in the system.
- Scanning is a key step to **examine intelligently** while gathering information about the target.

- The **scrutinizing phase** is always called "**enumeration**" in the hacking world.
- The objective behind this step is to identify:
    1. The **valid user accounts or groups**;
    2. **Network resources** and/or shared resources;
    3. **Different applications** that are running on the OS.

Ports Scanning

- A port is an interface on a computer to which one can connect a device.
- A "port" is a place where information goes into and out of a computer and so, with **port scanning,** one can identify open doors to a computer.
- There are some **well-known IP ports** (0–999), which public servers use. They are important for communication over the Internet. **they open the door to potential security breaches by threat agents.**
- Tools such as **Nmap** offer an automated mechanism for an attacker to not only scan the system to find out what **ports are "open**" (meaning being used), but also help to identify what operating system (OS) is being used by the system.
- The result of a scan on a port is usually generalized into one of the following three categories:
    - **Open or accepted:** The host sent a reply indicating that a service is listening on the port.
    - **Closed or not listening:** The host sent a reply indicating that connections will be denied to the port.
    - **Filtered or blocked:** There was no reply from the host.
- **Open ports present two vulnerabilities** of which administrators must be wary:
        - **Vulnerabilities associated with the program** that is delivering the service.
        - **Vulnerabilities associated with the OS** that is running on the host.
- **Closed ports** present only the latter of the two vulnerabilities that open ports do.
- **Blocked ports** do not present any reasonable vulnerabilities in either the software (program) or the OS at the given time.

5. What is social engineering? Briefly explain the two types of social engineering.

Ans:

- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- A **social engineer** usually uses telecommunication (i.e., telephone and/or cell phone) or Internet to get them to do something that is against the security practices and/or policies of the organization.
- It is an **art of exploiting the trust of people**, which is not doubted while speaking in a normal manner.

- The goal of a social engineer is to **fool someone** into providing valuable information or access to that information.
- The sign of truly successful social engineers is that they receive information without any suspicion.
- A **simple example is calling a user** and **pretending to be someone from the service desk** working on a network issue; the attacker then proceeds to ask questions about what the user is working on, what file shares he/she uses, what his/her password is, and so on.
- **Two types : Human-Based and computer Based**

    - **Human-Based Social Engineering**-refers to person-to-person interaction to get the required/desired information. An example is calling the help desk and trying to find out a password.

    - **Types of Human-Based Social**
        - **Impersonating an employee or valid user**
        - **Posing as an important user**
        - **Using a third person**
        - **Calling technical support**
        - **Shoulder surfing**
        - **Dumpster diving**

- **Computer-Based Social Engineering-** refers to an attempt made to get the required/desired information by using computer software/Internet.
- **Computer-Based Social Engineering: Methods**
    - **Fake E-Mails:**
    - **E-Mail attachments**
    - **Pop-Up windows**

6. What do you mean by Human-Based Social Engineering? Discuss its types.

- **Ans: Human-Based Social Engineering**-refers to person-to-person interaction to get the required/desired information. An example is calling the help desk and trying to find out a password.

- **Types of Human-Based Social**

- **Impersonating an employee or valid user**: Social engineers take advantage of the fact that most people are basically helpful, so it seems harmless to tell someone who appears to be lost where the computer room is located, or to let someone into the building who forgot his/her badge, etc., or pretending to be an employee or valid user on the system.

- **Posing as an important user:** For eg., a CEO or high-level manager who needs immediate assistance to gain access to a system. The attacker uses intimidation so that a lower-level employee such as a help-desk worker to help him/her in gaining access to the system.

- **Using a third person:** An attacker pretends to have permission from an authorized source to use a system. This trick is useful when the supposed authorized personnel is on vacation or cannot be contacted for verification.

- **Calling technical support: Help-desk and technical support personnel** are trained to help users, which makes them good prey for **social engineering attacks**.

- **Shoulder surfing:** It is a technique of gathering information such as usernames and passwords by watching over a person's shoulder while he/she logs into the system, thereby helping an attacker to gain access to the system.

- **Dumpster diving:**

  - It involves looking in the trash for information written on pieces of paper or computer printouts.
  - it is used to describe the practice of searching through commercial or residential trash to find useful free items that have been discarded.
  - It is also called **dumpstering, binning, trashing, garbing or garbage gleaning**. "Scavenging" is another term to describe these habits.
  - **Consider, for example,** going through someone's trash to recover documentation of his/her critical data [e.g., social security number (SSN) in the US, PAN number in India, credit card identity (ID) numbers, etc.].

7. What are cyberstalking and cyberbullying? Explain types of cyberstalking.

Ans:

Cyberstalking:

- The behaviour includes **false accusations**, **monitoring**, **transmission of threats**, **ID theft**, **damage to data** or **equipment**, **solicitation of minors** for **sexual purposes**, and **gathering information** for harassment purposes.

- It involves **harassing or threatening behaviour** that an individual will conduct repeatedly, for e.g., following a person, visiting a person's home and/or at business place, making phone calls, leaving written messages, or vandalizing against the person's property.

Cyberbullying:

- The National Crime Prevention Council (NCPC) defines **Cyberbullying** as ***"when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person.***"
- www.StopCyberbullying.org, an expert organization dedicated to Internet safety, security, and privacy defines cyberbullying as "**a situation when a child, tween, or teen is repeatedly 'tormented, threatened, harassed, humiliated, embarrassed, or otherwise targeted' by another child, tween, or teen using text messaging, E-Mail, instant messaging, or any other type of digital technology**."
- The practice of cyberbullying is not limited to children and, while the behavior is identified by the same definition in adults, the distinction in age groups is referred to as **cyberstalking or cyber harassment when** perpetrated by adults toward adults

Types of cyber stalking:

- **Online stalking:** In online stalking the attacker aims to start the interaction with the victim directly with the help of the Internet. The stalker makes sure that the victim recognizes the attack attempted on him/her. The stalker can make use of a third party to harass the victim.
- **Offline stalking:** The stalker may begin the attack using **traditional methods** such as following the victim, **watching the daily routine of the victim**, etc. Searching on **message boards/ newsgroups, personal websites, and people finding services or websites** are most common ways to gather information about the victim using the Internet.

8. Explain how cyberstalking works.

Ans: Cyberstalking works in this manner:

1. **Personal information gathering about the victim:** Name; family background; contact details such as cell phone and telephone numbers(of residence as well as office); address of residence as well as of the office; E-Mail address; date of birth, etc.
2. **Establish a contact with victim through telephone/cell phone.** Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. **Stalkers will alsmost always establish a contact with the victims through E-Mail.** The letters may have the tone of loving, threatening or can be sexually explicit. The stalker may use multiple names while contacting the victim.
4. **Some stalkers keep on sending repeated E-Mails** asking for various kinds of favours or threaten the victim.
5. **The stalker may post the victim's personal information** on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted

the information and invite the people to call the victim on the given contact details to have **sexual services**.

6. Whosoever comes across the information, **start calling the victim on the given contact details**, asking for sexual services or relationships.
7. Some **stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites**, because of which victim will start receiving such kind of unsolicited E-Mails

9. List and explain some tips for safety and security while using the computer in a cybercafe.

Ans: Few tips for safety and security while using the computer in a cybercafe:

- **Be alert:** One should have to stay alert and aware of the surroundings while using a public computer.
- **Avoid online financial transactions**: Ideally one should avoid online banking, shopping or other transactions that require one to provide personal, confidential and sensitive information such as credit card or bank account details.
- **Change passwords:** Do not use the same pass.
- **Virtual keyboard**: Nowadays almost every bank has provided the virtual keyboard on their website.
- **Security warnings**: One should take utmost care while accessing the websites of any banks/financial institution.

10. What is botnet? How do you secure your system from botnet attack?

Ans:

- **Bot is "(computing) an automated program** for doing some particular task, often over a network."
- **Botnet is** a term used for collection of software robots, or Bots, that run autonomously and automatically.
- The term is often associated with **malicious software** but can also refer to the network of computers using distributed computing software.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting DDoS attacks.

- **A Botnet (Zombie networks) is a network of computers infected with a malicious program** that allows cybercriminals to control the infected machines remotely without the users' knowledge.

One can ensure following to secure the system from botnet attacks:

- **Use antivirus and anti-Spyware** software and keep it up-to-date.
- **Set the OS to download and install security patches** automatically.
- **Use a firewall to protect the system** from hacking attacks while it is connected on the Internet.
- **Disconnect from the Internet** when you are away from your computer.
- **Downloading the freeware only from websites that are known and trustworthy.**
- **Check regularly the folders in the mail box-** "sent items" or "outgoing" – for those messages you did not send.
- **Take an immediate action** if your system is infected

Chapter 3 : Cybercrime: Mobile and Wireless Devices

1. Discuss the types and techniques of Credit Card Frauds.

Ans:

1. Traditional techniques

- The traditional and the first type of credit card fraud is paper-based fraud- ***application fraud***, wherein a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful personally Identifiable Information to open an account in someone else's name.
- **Application fraud can be divided into**
    - **ID theft**: Where an individual pretends to be someone else.
    - **Financial fraud**: Where an individual gives false information about his or her financial status to acquire credit.

- Illegal use of lost and stolen cards is another form of traditional technique. Stealing a credit card is either by pickpocket or from postal service before it reaches its final destination.

2. Modern Techniques

- Sophisticated techniques enable criminals to produce fake and doctored cards. Then there are also those who use skimming to commit fraud.
- Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.
- **Site cloning and false merchant sites** on the Internet are becoming a popular method of fraud and to direct the users to such bogus/fake sites is called Phishing.

1. **Triangulation**:
    - The criminal offers the goods with heavy discounted rates through a website designed and hosted by him, which appears to be legitimate merchandise website.
    - The customer registers on this website with his/her name, address, shipping address and valid credit card details.
    - The criminal orders the goods from a legitimate website with the help of stolen credit card details and supply shipping address that have been provided by the customer while registering on the criminal's website.

- The goods are shipped to the customer and the transaction gets completed.
- The criminal keeps on purchasing other goods using fraudulent credit card details of different customers till the criminal closes existing website and starts a new one.

Triangulation fraud denotes that there are three individuals who play a role in the order.

- An unsuspecting customer who places an order on an auction or marketplace using some form of credit, debit, or PayPal tender.
- A fraudulent seller who receives that order and then places the order for the actual product with a legitimate eCommerce website using a stolen credit card.
- A legitimate eCommerce website that then processes the criminal's order.

- The entire investigation process for tracking and reaching these criminals is time-consuming, and the criminals may close such fake website in between the process that may cause further difficulty to trace the criminal.
- The criminals aim to create a great deal of confusion for the authorities so that they can operate long enough to accumulate a vast amount of goods purchased through such fraudulent transactions.
-

2. **Credit card generators**:

- It is another modern technique- **computer emulation software** – that creates valid credit card numbers and expiry dates.
- The criminals highly rely on these generators to create valid credit cards. These are available for free download on the Internet.

2. Define the terms: Mishing, Vishing and Smishing . Explain how Vishing is carried out.

Ans:

Mishing:

- Mishing Is a combination of mobile phone and phishing.
- If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a mishing scam.
- A typical mishing attacker uses call termed as vishing or message known as smishing.
- Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.

- Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

Vishing:

- It is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward. The term is a combination of V- voice and Phishing.
- The most profitable uses of the information gained through a Vishing attack include:
    - ID theft;
    - Purchasing luxury goods and services;
    - Transferring money/funds
    - Monitoring the victim's bank accounts;
    - Making applications for loans and credit cards.

Smishing:

- **It is a criminal offense conducted by using social engineering techniques** similar to Phishing. The name is derived from "SMS Phishing".
- Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her personal information.
- The popular technique to hook the victim is either provide **a phone number to force the victim to call** or **provide a website URL to force the victim to access the URL**, wherein, the victim gets connected with bogus website and submits his/her Personal Information.
- Smishing works in the similar pattern as Vishing.

The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminal's will to reach a particular audience.

1. Internet E-Mail: It is also called Phishing mail.

2. Mobile text messaging

3. Voicemail: Here, victim is forced to call on the provided phone number, once he/she listens to voicemail.

4. Direct phone call

3. List any four tips to protect oneself from Smishing Attacks.

Ans: Following are some tips to protect oneself from Smishing Attacks:

- Do not answer a text message that you have received asking for your personal information. Even if the message seems to be received from your best friend, do not respond, because he/she may not be the one who has actually sent it.
- Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message. Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.
- Never click on a hot link received through message on your Smartphone or PDA. Hot links are links that you can click, which will take you directly to the Internet sites.
- Smishing messages may have hot links, wherein you click on the link and download Spyware to your phone without knowing. Once this software has been downloaded, criminals can easily steal any information that is available on your cell phone and have access to everything that you do on your cell phone.

4. List and explain Hacking Bluetooth Tools.

Ans:

1. **BlueScanner**-This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting with the target.
2. **BlueSniff**- This is a GUI-based utility **for finding discoverable and hidden Bluetooth enabled devices.**
3. **BlueBugger**-The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information.
4. **Bluesnarfer**- If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5. **BlueDiving**- BlueDiving is testing Bluetooth penetration. It implements attacks like Bluebug and BlueSnarf.

5. Explain Bluejacking and Bluesnarfing .

Ans:

1. **Bluejacking**
    - Bluetooth+Jacking where jacking is a short name for hijack - **act of taking over something.**

- **Bluejacking** is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field to another Bluetooth-enabled device

- If the user does not recognize/realize what the message is, he/she might allow the contact to be added to her/his address book, and the contact can send him messages that might be automatically opened because they are coming from a known contact.

- Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.

2. **Bluesnarfing**

- Bluesnarfing is a hacking technique in which a hacker accesses a wireless device through a Bluetooth connection.

- It happens without the device user's permission and often results in the theft of information or some other kind of damage to the device (and user).

- Bluesnarfing enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.

6. List the 5 security strategies for that a company can implement secure their mobile devices.

Ans: A few things that enterprises can use are:

1. Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.

2. Investigate alternatives that allow a secure access to the company information through a firewall such as mobile VPN.

3. Develop a system of more frequent and thorough security audits for mobile devices
4. Incorporate security awareness into your mobile training and support programs so that everyone understands just how an issue security is within a company's overall IT strategy
5. Notify then appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.