ICS
Unit 4
Part-II

Cyber Security: Definition and origin, Cyber Crime and information security, Types of Cyber Crime, Classification of Cyber Criminals, Tools used in Cyber Crime, Challenges, Strategies, The Legal Perspective-Indian/Global Perspective, Types of Attack, Social Engineering, Cyber stalking, Ransomware.

Cybercrime

- Definition and origin:
- A crime in which a computer was directly and significantly instrumental
  - not universally accepted

- Other definitions:

- Any illegal act where special knowledge of computer technology is essential for its perpetration, investigation or prosecution

- Any traditional crime that has acquired a new dimension or order or magnitude through the aid of a computer, and abuses that have come into being because of computers

- Any threat to computer itself, such as theft of hardware or software, sabotage and demands for ransom

Cybercrime

- Cyber crime has evolved since adoption of internet connection on a global scale with millions of users

- Cybercrime refers to the act of performing a criminal act using cyberspace as the communication vehicle

Cybercrime

- **Cybercrimes** are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.

or

- **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).

Cybercrime

- Any illegal/criminal activity done through internet or on the computer

- Computer used to commit a crime
  - Child porn, threatening email, assuming someone’s identity, sexual harassment, defamation, spam, phishing

- Computer as a target of a crime
  - Viruses, worms, industrial espionage(spying), software piracy, hacking

Cybercrime and Information Security

- Lack of information security gives rise to cybercrimes

- Indian Information Technology Act 2000
- From an Indian perspective,, the new version of act (ITA 2008) provides a new focus on “Information Security in India”

- Cyber security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

- The term incorporates both physical security of devices as well as information stored in them

Cybercrime and Information Security

- Typical network misuses are for internet radio/streaming audio, streaming video, file sharing, instant messaging and online gaming(such as online poker, online casinos, online betting, etc).

- Online gambling is illegal in India
- India has yet to pass laws that specifically deal with the issue, leaving sort of legal loophole

Who are Cybercriminals

- Cybercriminals are those who are involved in activities such as:
  1. Credit card fraud,
  2. Cyberstalking,
  3. Defaming another online,
  4. Gaining unauthorized access to computer,
  5. Ignoring copyright, software licensing and trademark protection,
  6. Overriding encryption to make illegal copies, software piracy,
  7. Identity theft to perform criminal act

Categories of Cybercriminals

- Categorized into 3 groups that reflect their motivation:

- **Type I: Cybercriminals-Hungry for recognition**

  - Hobby hackers
  - IT Professionals(social engineering is one of the biggest threat)
  - Politically motivated hackers
  - Terrorist organizations

Categories of Cybercriminals

- **Type II: Cybercriminals-not interested in recognition**
  - Psychological perverts (a person whose sexual behaviour is regarded as abnormal and unacceptable)
  - Financially motivated hackers (corporate espionage)
  - State-sponsored hacking (national espionage, sabotage)
  - Organized criminals

Categories of Cybercriminals

- **Type III: Cybercriminals-the insiders**
  - Disgruntled or former employees seeking revenge
  - Competing companies using employees to gain economic advantage through damage and/or theft
- Thus typical “motives” behind cybercrime seems to be:
  - greed, desire to gain power and/or publicity,
  - desire for revenge, a sense of adventure,
  - looking for thrill to access forbidden information,
  - destructive mindset

Classifying Cybercrimes-broad and narrow

Cybercrime in Narrow Sense			Cybercrime in Broad Sense
Role of computer	**Computer as an object:** The computer / information stored in it is the subject / target of crime	**Computer as a tool:** The computer / information stored in it constitutes an important tool for committing the crime	**Computer as the environment or context:** The computer/information stored in it plays a non-substantial role in the act of crime, but does not contain evidence of the crime
Examples	Hacking, Computer sabotage, DDoS Attacks	Computer fraud, forgery, distribution of child pornography	Murder using computer technique, bank robbery and drugs trade

Classification of Cybercrimes

1. Cybercrime against individual
2. Cybercrime against property
3. Cybercrime against organization
4. Cybercrime against society
5. Crimes emanating from Usenet newsgroup

Classification of Cybercrimes

1. Cybercrime against individual
   - E-mail spoofing and other online frauds
   - Phishing, Spear phishing, Vishing, Smishing
   - Spamming
   - Cyberdefamation
   - Cyberstalking and harassment
   - Computer sabotage
   - Pornographic offences
   - Password sniffing
2. Cybercrime against property
   - Credit card frauds
   - Intellectual property crimes
   - Internet time theft

Classification of Cybercrimes

3. Cybercrime against organization
   - Unauthorized accessing of computer
   - Password sniffing
   - Denial of Service attacks
   - Virus attack / dissemination of viruses
   - E-mail bombing / mail bombs
   - Salami attack / salami technique
   - Logic bomb
   - Trojan Horse
   - Data diddling
   - Industrial espionage / spying
   - Computer network intrusions
   - Software piracy

Classification of Cybercrimes

4. Cybercrime against society
   - Forgery
   - Cyberterrorism
   - Web jacking

5. Crimes emanating from Usenet newsgroup
   - **Usenet** is a worldwide distributed discussion system available on computers (an early non-centralized computer network for the discussion of particular topics and the sharing of files via newsgroups)

   - Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive(misleading) in another way

Cybercrime against individual: E-mail Spoofing

- E-mail spoofing is the forgery of an e-mail header so that the message appears to have originated from someone or somewhere other than the actual source.

- **Email spoofing** is a tactic used in phishing and spam campaigns because people are more likely to open an **email** when they think it has been sent by a legitimate source.

- Basically in a spoofed email the **from:** field is modified to make it look like the email is coming from a person the recipient know.

- The result is that the email recipient sees the email as having come from the address in the ***From:*** field; but if they reply to the email it will go to ***Reply-to*** email address which is an email address the spammer might have setup to receive those replies.

Cybercrime against individual: E-mail Spoofing

- **Why is email spoofing possible?**
- The reason why email spoofing is possible and relatively easy for spammers to do is because of a vulnerability in the protocol used to transport emails through the Internet.
- **SMTP (Simple Mail Transport Protocol)** does not use any authentication mechanism for header fields like **from**, **Reply-to**, **Return-Path.**
- Spammers forge these headers using certain commands to make it appear that is coming from a different source than its original one.
- **Prevention:**
- Use cryptographic signatures (e.g., PGP "Pretty Good Privacy" or other encryption technologies) to exchange authenticated email messages.
- Authenticated email provides a mechanism for ensuring that messages are from whom they appear to be, as well as ensuring that the message has not been altered in transit.
- Similarly, sites may wish to consider enabling SSL/TLS in their mail transfer software.

Cybercrime against individual:
Phishing

- Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication

- Communications purporting (Pretending) to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting victims.

- Phishing e-mails and websites have a similar/familiar appearance as original websites e.g. banking website

- Phishing emails may contain links to websites that are infected with malware

Cybercrime against individual: Phishing

- Methods of Phishing

1. **Dragnet method**
2. **Rod – and – Reel method**
3. **Lobsterpot method**
4. **Gillnet phishing**

Cybercrime against individual:
Phishing

Methods of Phishing

1. Dragnet method

This method involves the use of spammed emails, bearing falsified corporate identification (e.g., trademarks, logos, and corporate names), that are addressed to a large class of people (e.g., customers of a particular financial institution or members of a particular auction site) to websites or pop-up windows with similarly falsified identification.

2. Rod – and – Reel method

In rod and reel method, phishers identify specific prospective victims in advance, and convey false information to them to prompt their disclosure of personal and financial data.

Cybercrime against individual: Phishing

Methods of Phishing

3. Lobsterpot method

- It focuses on the use of spoofed websites.
- It consists in the creation of spoofed websites, similar to legitimate corporate ones, that a narrowly defined class of victims is likely to seek out.

4. Gillnet phishing

- In gillnet phishing, phishers introduce malicious code into emails and websites. They can, for example misuse browser functionality by injecting hostile content into another site's pop – up window.
- Merely by opening a particular email, or browsing a particular website, Internet users may have a Trojan horse introduced into their systems.
- In some cases, the malicious code will change settings in user's systems, so that users who want to visit legitimate banking websites will be redirected to a lookalike phishing site.
- In other cases, the malicious code will record user's keystrokes and passwords when they visit legitimate banking sites, then transmit those data to phishers for later illegal access to users' financial accounts.

Cybercrime against individual:
Spear phishing

- **Spear phishing** is an email that appears to be from an individual or business that you know. But it isn't.

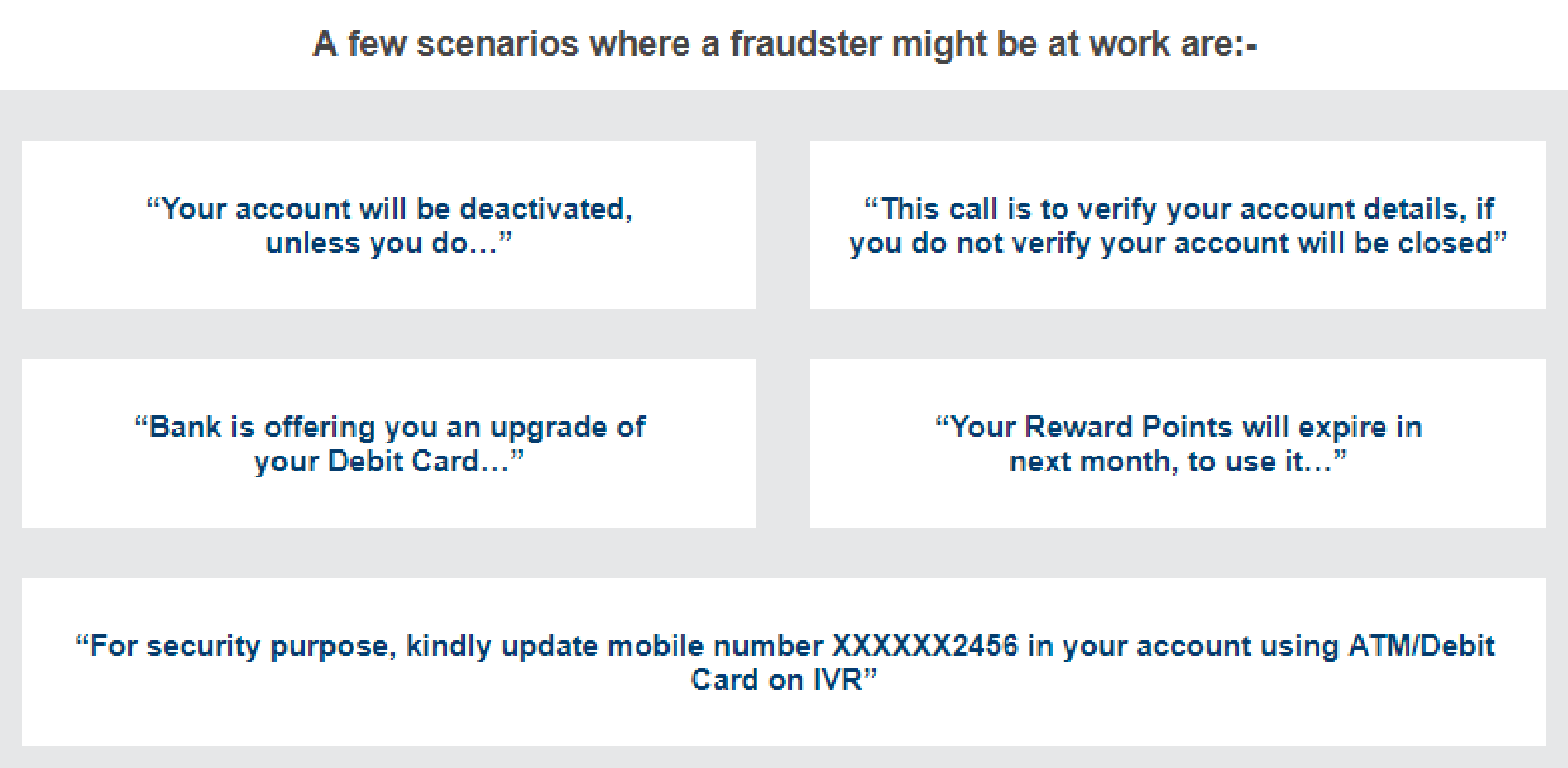
- It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC.

Cybercrime against individual: Vishing

- **Vishing** is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.

- The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

Cybercrime against individual: Vishing



A few scenarios where a fraudster might be at work are:-

"Your account will be deactivated, unless you do..."

"This call is to verify your account details, if you do not verify your account will be closed"

"Bank is offering you an upgrade of your Debit Card..."

"Your Reward Points will expire in next month, to use it..."

"For security purpose, kindly update mobile number XXXXXX2456 in your account using ATM/Debit Card on IVR"

Cybercrime against individual: Smishing

- **SMiShing** is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device.
- **SMiShing** is short for “SMS phishing”

- A combination of phishing and Short Message Service (SMS) text messages is called SMISHING. These messages are usually crafted to provoke an immediate action from the user, requiring them to share their sensitive and confidential banking details.

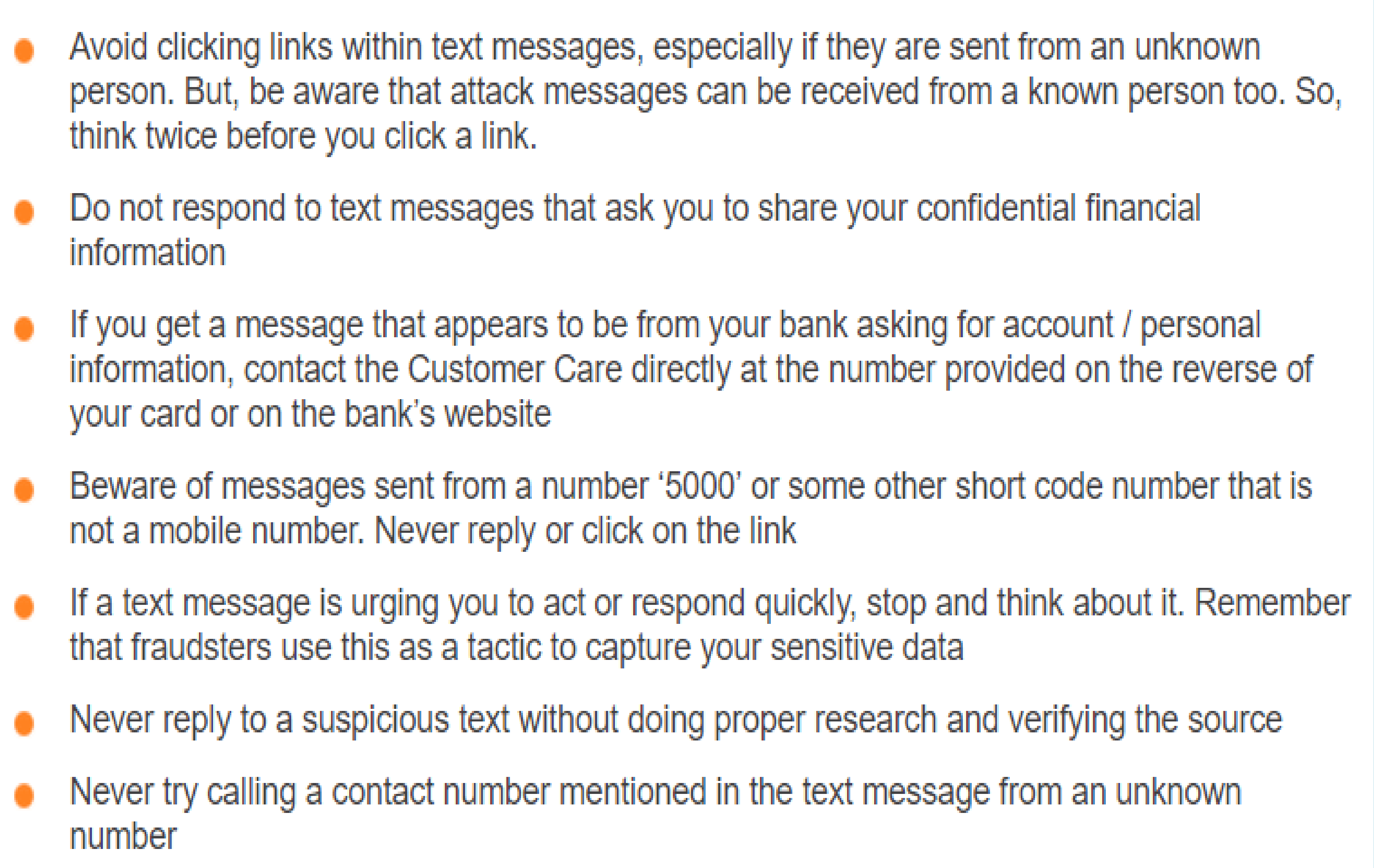
Smishing

- In ‘Smishing’, the message can also ask the users to click on a link or call on toll free numbers.

- If the user clicks on the link provided in the message, then a malicious software can get downloaded on their mobile or a single click on the link can take the user to a malicious website in pretext of an offer, discount or account credit.

- The text message can also create an urgency, by informing an account closure due to delinquency (negligence) or in need of an important information or even to register for a new programme.

Cybercrime against individual: Smishing: A Few Safety Tips



- Avoid clicking links within text messages, especially if they are sent from an unknown person. But, be aware that attack messages can be received from a known person too. So, think twice before you click a link.
- Do not respond to text messages that ask you to share your confidential financial information
- If you get a message that appears to be from your bank asking for account / personal information, contact the Customer Care directly at the number provided on the reverse of your card or on the bank's website
- Beware of messages sent from a number '5000' or some other short code number that is not a mobile number. Never reply or click on the link
- If a text message is urging you to act or respond quickly, stop and think about it. Remember that fraudsters use this as a tactic to capture your sensitive data
- Never reply to a suspicious text without doing proper research and verifying the source
- Never try calling a contact number mentioned in the text message from an unknown number

Cybercrime against individual: Pharming

- Pharming is a tactic used by criminals to redirect a legitimate web site to a fraudulent site.

- Unlike phishing and its variations, pharming does not try to trick you into clicking a URL or talk you into providing sensitive information.

- Instead, it uses malicious code to redirect you to the criminal’s site without your consent or knowledge, making it more difficult to detect.

Cybercrime against individual: Spamming

- Spamming means sending multiple copies of unsolicited mails or mass e-mails such as chain letters.
- Spammers create spams
- Most widely recognized is e-mail spam
- Other are: instant messaging spam, web search engine spam, spam in blogs, online classified ads spam, socoal networking spam

Cybercrime against individual: Spamming

- Search engine spam:
- Some web authors use “subversive techniques” to ensure that their site appears more frequently or higher number in returned results
- This is strongly discouraged by search engines and there are fines/penalties for this
- Those who continuously subvert or spam the search engine may be permanently excluded from search engine
- Therefore following web publishing techniques should be avoided:

  Repeating keywords, non related keywords, redirection, IP cloaking, duplication of pages with different URLs, hidden links etc.

IP cloaking is the process of delivering different versions of a website to search engines than to human readers. It is often used to boost a site's search ranking, as it allows sites to recognize when engines such as Google are requesting data before sending them a version of their page that is full of keywords.

Cybercrime against individual: Cyberdefamation

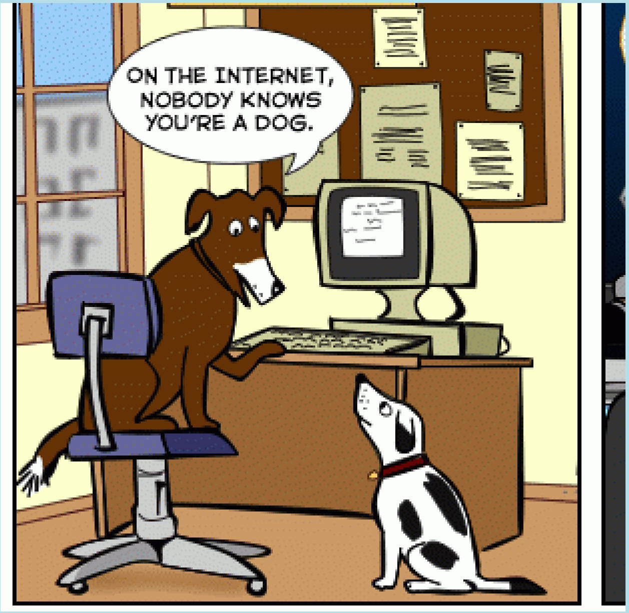
- The term defamation is used to define the injury that is caused to the reputation of a person in the eyes of a third person.
- The injury can be done by words oral or written, or by signs or by visible representations.

- Cyber defamation is publishing of defamatory material against another person with the help of computers or internet.
- If someone publishes some defamatory statement about some other person on a website or send emails containing defamatory material to other persons with the intention to defame the other person about whom the statement has been made would amount to cyber defamation.

Cybercrime against individual: Cyberdefamation

- There are two main types of defamation: libel, or written defamation, and slander, or verbal defamation.

- When a potentially defamatory statement is made online or through social media -- such as via Facebook or Linkedin that involves the written (or "posted") word, and so it is considered libel.



Cybercrime against individual:

Cyberstalking and harassment

- The repeated use of electronic communications to harass or frighten someone, for example by sending threatening emails.
- Cyberstalking can include many things including threats, demand for sex, false **accusations** (claim that someone has done something illegal or wrong), defamation, slander, libel, identity theft, and **vandalism** (willful or malicious destruction or defacement of public or private property.).
- Cyberstalking is often used in conjunction with offline stalking, as both are an expression of a desire to control, intimidate, or manipulate a victim.
- A cyberstalker may be someone the victim is familiar with, or a complete stranger, and is a criminal offense.
- Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously.

Cybercrime against individual:
Cyberstalking and harassment

- **Types of stalkers:**
- **Online Stalkers:**
- Communicate with victim directly with the help of internet (E-mail and Chat rooms) rather than using cellphone or telephone

- **Offline Stalker:**
- Follow the victim, watch daily routine of victim,
- Searching personal profiles and websites to gather information

Cybercrime against individual:
Cyberstalking and harassment

- **How do they Operate**

- Collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

- The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.

- People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.

- Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

Cybercrime against individual: Cyberstalking and harassment

- **How do they Operate**
- Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.
- In online stalking the stalker can make third party to harass the victim.
- Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.
- Contact victim via telephone. If the stalker is able to access the victims telephone, he will many times make calls to the victim to threaten, harass them.
- Track the victim to his/her home.

Cybercrime against individual:

Cyberstalking and harassment

- **Cyberbullying**
- Cyberbullying and cyber harassment are sometimes used interchangeably, but cyber bullying is used for electronic harassment or bullying among minors.
- "Cyberbullying" is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones.
- It has to have a minor on both sides, or at least have been instigated by a minor against another minor.
- Once adults become involved, it is plain and simple cyber-harassment or cyberstalking.
- Adult cyber-harassment or cyberstalking is NEVER called cyberbullying.

Cybercrime against individual: Computer sabotage

- **Sabotage** is defined as deliberate and malicious acts that result in the disruption of the normal processes and functions or the destruction or damage of equipment or information.
- Hinder the normal functioning of computer system using malware (viruses, worms, Trojan horses, mobile malware), denial of service attacks and Data/Program/site alterations.
- The best methods to protect against **computer sabotage** is by using security software.

Cybercrime against individual: Pornographic offences

- Child pornography is considered as offence.

- It refers to any content that depicts sexually explicit activities involving a child.

- These Visual depictions include photographs, videos, film, digital or computer generated images or pictures of sexually explicit conduct involves the use of minor.

- Unfortunately, Child pornography is the reality of the Internet

- The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide.

- Pedophiles take advantage of this situation and lure the children, who are not advised by their parents or by their teachers about what is wrong and what is right for them while browsing the internet.

Cybercrime against individual: Pornographic offences

- **Pedophiles:** A person who is sexually attracted to children.
- **Pedophiles** use false identity to trap the children/teenagers
- Pedophiles contact children/teens in various chat rooms which are used by children/teen to interact with other children/teen.
- Befriend the child/teen.
- Extract personal information from the child/teen by winning his confidence.
- Gets the e-mail address of the child/teen and starts making contacts on the victims e-mail address as well.
- Starts sending pornographic images/text to the victim including child pornographic images in order to help child/teen shed his 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.
- Extract personal information from child/teen
- At the end of it, the pedophile set up a meeting with the child/teen out of the house and then drag him into the net to further sexually assault him or to use him as a sex object.

Cybercrime against individual: Password Sniffing

- A password sniffer is a software application that scans and records passwords that are used or broadcasted on a computer or network interface.

- It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password.

Cybercrime against property: Credit card frauds

- Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction.
- The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

- **Credit Card Skimming**
- Credit card skimming is a type of credit card theft where crooks use a small device to steal credit card information in an otherwise legitimate credit or debit card transaction.
- When a credit or debit card is swiped through a skimmer, the device captures and stores all the details stored in the card's magnetic strip.
- Thieves use the stolen data to make fraudulent charges either online or with a counterfeit credit card.

Cybercrime against property: Intellectual property crimes

- These include:
  - Software piracy: illegal copying of programs, distribution of copies of software
  - Copyright infringement
  - Trademarks violations
  - Theft of computer source code

Cybercrime against property: Internet time theft

- The usage of the Internet hours by an unauthorized person which is actually paid by another person.

Cybercrime against organization: Unauthorized accessing of computer

- "Unauthorized access" entails approaching, trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and changing computer resources without consent.

- These laws relate to either or both, or any other actions that interfere with computers, systems, programs or networks.

Cybercrime against organization: Denial of Service attacks

- Denial-of-service (or DoS) attacks are usually launched to make a particular service unavailable to someone who is authorized to use it.

- These attacks may be launched using one single computer or many computers across the world.

- In the latter scenario, the attack is known as a distributed denial of service attack.

Cybercrime against organization: Virus attack / dissemination of viruses

- Virus is a malicious software that attaches itself to other software and causes break down of the operating system in extreme cases.

Cybercrime against organization:
Email Bombing, Logic Bomb & Trojan Horse

- **Email Bombing:**
- Sending large numbers of mails to the individual or company or mail servers thereby ultimately resulting into crashing.
- Email Bombing is sending large number to a email id in a single click.
- Email Spamming is like sending a email to large number of emails id on a single click.

- **Logic Bomb:**
- Its an event dependent program , as soon as the designated event occurs, it crashes the computer, release a virus or any other harmful possibilities.

- **Trojan Horse:**
- An unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Cybercrime against organization: Salami Attack/Salami Technique

- Used for committing financial crimes
- When negligible amounts are removed & accumulated in to something larger.
- E.g. bank employee inserts program into bank servers, that deducts very small amount say Rs. 2 from account of every customer
- This is unnoticeable but bank employee will make huge amount

Cybercrime against organization: Data diddling

- This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

Cybercrime against organization: Industrial espionage / spying

- Spying directed towards discovering the secrets of a rival manufacturer or other industrial company

- Most business organizations store their sensitive information in computer systems.

- This information is targeted by rivals, criminal and sometimes disgruntled employees.

- Business rivals obtain information namely business plans, business strategies, marketing strategies, potential customers, confidential quotations etc. using cyber criminal and then uses the information for the benefit is his own business.

Cybercrime against organization: Computer network intrusions

- Computer networks pose a problem of security threat because people can get into them from anywhere.
- Network intrusions are illegal.
- Hackers can break into computer systems.

Cybercrime against organization: Software Piracy

- Software piracy is the illegal copying, distribution, or use of software.

Cybercrime against society: Forgery

- Currency notes, revenue stamps, mark sheets etc can be forged using computers and high quality scanners and printers

Cybercrime against society: Cyberterrorism

- Any person, group or organization who, with terrorist intent, utilizes a computer or computer network and thereby knowingly engages in or attempts to engage in terrorist act commits the offence of cyberterrorism

Cybercrime against society: Web Jacking

- Hackers gain access and control over the website of another, even they change the content of website for fulfilling political objective or for money.

What Is Cybersquatting? (1)

- Cybersquatting is registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark.
- It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit to those businesses.

What is Cybersquatting? (2)

- Cybersquatting is the practice of registering an Internet domain name that is likely to be wanted by another person, business, or organization in the hope that it can be sold to them for a profit.
- It involves the registration of trademarks and trade names as domain names by third parties, who do not possess rights in such names.
- Simply put, cybersquatters (or bad faith imitators) register trade-marks, trade names, business names and so on, belonging to third parties with the common motive of trading on the reputation and goodwill of such third parties by either confusing customers or potential customers, and at times, to even sell the domain name to the rightful owner at a profit.

What is Cybersquatting? (3)

- Cybersquatting:
- When a person other than the owner of a well-known trademark registers that trademark as an Internet domain name and then attempts to profit from it either by ransoming the domain name back to the trademark owner or by using the domain name to divert business from the trademark owner to the owner of the domain name.

Cybercrime: The Legal Perspective

- Computer crime was consequently defined as: encompass any illegal act for which knowledge of computer technology is essential for its perpetration (execution)
- Cybercrime is the outcome of globalization
- However, globalization does not mean globalized welfare at all
- Globalized information systems accommodate an increasing number of transactional offences
- The network context of cybercrime makes it one of the most globalized offences of the present and most modernized threats of the future
- The problem can be resolved in 2 ways:
  1. Divide information systems into segments bordered by state boundaries
  2. Other is to incorporate legal system into an integrated entity obliterating (removing) state boundaries

- First way is unrealistic
- In globally connected world, information systems become unique empire without tangible territory

Cybercrime: An Indian Perspective

- India has 4th highest number of internet users in the world
- 45 million internet users in India
- Cyber crime is increasing in India
- Indian Government is doing its best to control cybercrimes

Global perspective on Cybercrime

- A broad meaning is given to cybercrime at international level
- Cybercrime is used as an umbrella term to refer to an array of criminal activity including offences against computer data and systems, computer related offences, content offences, and copyright offences
- The wide definition of cybercrime overlaps in part with general offence categories that need not be Information and Communication technology (ICT)-dependent, such as white collar crime and economic crime
- There are no national boundaries to crimes under cybercrime realm such as e-mail spam
- The linkage of cyber security and critical infrastructure protection has become a big issue as a number of countries have begun assessment of threats and vulnerabilities and started mechanisms to redress them

Categories of Cybercrime

- Cybercrime can be categorized based on:

  1. Target of the crime
  2. Whether crime occurs as a single event or as a series of event

Cyber Attack Meaning : Attack in which Cyber criminals can be targeted against person, property or organization include government, business and social.

Categories of Cybercrime:

1. Crime Targeted at Person (individual)
2. Crime Targeted at Assets
3. Cyber Crime Against Organization
4. Cyber attacks using single event
5. Cyber attacks considering series of event

Categories of Cybercrime

1. Crime Targeted at Person(individual)

- The cyber criminals exploit human weakness such as greed and innocence.
- This kind of cyber-attack include financial frauds, copyright violation, harassment, sale of stolen or non–existing items etc.
- Latest technology development and growth of internet cyber criminals have a new attacking tools that make them to expand group of potential victim.

2. Crime Targeted at Assets

- In this kind of crime include stealing property such as mobile devices, laptop, pen drive, CD, DVD, iPad etc.
- Sometime attacker may insert harmful program such as Trojan virus and disturbed function of hard disk and pen drive.
- Shortcut virus is one type of Trojan used to steal information from computer.

Categories of Cybercrime

3. Cyber Crime Against Organization

- Cyber attacks perform against organization is also called as Cyber terrorism.
- Cyber attackers use computer and internet to perform Cyber terrorism, by stealing private information or destroying valuable files, damaging programs file or taking control of network system.

4. Cyber attacks using single event

- This type of Cyber attacks perform in single event from victim point of view.
- For example, mistakenly open email may contain virus.
- Representation of incorrect website called as phishing and steal valuable financial information.
- This kind of attack is also called as hacking or online fraud.

Categories of Cybercrime

5. Cyber attacks considering series of event

- Sometime attacker perform series of event to track victim, interacting with victim.
- For example attacker perform communication with victim using phone or chat room establish connection with victim and then explore or steal valuable information.
- Then they exploit that communication to commit sexual assault.

How Cyber Criminals Plan cyber Attacks

- Cyber Criminals use many tool and methods to locate vulnerability of their victim.
- Attackers can be categorized as inside attacker or outside attacker.
- Attacks perform within the organization is called inside attack whereas attacker get information from outside is called outside attack.
- Inside attack are always more dangerous than outside, because inside attackers has get more resources than outsider.

- Following are three major phases are involved in planning of cyber crime.

1. **Reconnaissance**
2. **Scanning and scrutinizing**
3. **Launching an attack**

How Cyber Criminals Plan cyber Attacks

1. **Reconnaissance**

- This is first step towards cyber attacks, it is one kind of passive attack. “Reconnaissance” means an act of exploring.
- In this phase attacker try explore and gain every possible information about target.

- In hacking world, Hacking start with “foot printing”.
- Foot printing provide overall system structure, loop holes and exploration of those vulnerability.
- Attacker utilize this phase is to understand system, personal information, networking ports and services.

How Cyber Criminals Plan cyber Attacks

1. Reconnaissance

- Cyber attacker use two steps to gather this information.
- **Passive Attacks:**
- Passive attacks used to gain information about individual or organization.
- It exploit confidential information.
- Passive attacks involve gaining data about a target without target knowledge. Now day's passive attack are much easier.
- **Use Google or other search engine:** Gather information by searching on Google.
- **Social Media:** Search on social media like Facebook, Twitter, and LinkedIn.
- **Organization Website:** Attacker may get employee information using organizational website.
- **Blog or press release:** This are new source where attacker easily get company or individual information. Company.
- **Job Posting:** Search job profile provide valuable information about person an Job profile for technical person can give data about type of technology that is, software, server, database or network devices a company using on its network.
- **Network Sniffing:** This attack use to gather information such as IP address, network range, hidden server and other valuable services on network.

How Cyber Criminals Plan cyber Attacks

1. Reconnaissance

- **Active attacks:**
- Active attack mostly used to manipulate or alter the system.
- It may effect on integrity, authenticity and availability of data.
- Information from passive phase is act as input to active phase.
- In this phase attacker verify gather information (IP address, network range, hidden server, personal information).
- This is very important as cyber attacker point of view, it provide security measure.

How Cyber Criminals Plan cyber Attacks

2. Scanning and scrutinizing

- In this phase attacker collect validity of information as well as find out existing vulnerability.
- It is key phase before actual attack happen.
- **Port scanning:** Identify all ports and services (open / closed)
- **Network scanning:** Verify IP address and network information before cyber attacks.
- **Vulnerability scanning:** Checking loop hole in system.
- Scrutinizing phase is also called enumeration.
- Validate user accounts and groups
- Find out list of network resource and how many network devices are shared?
- Different types of OS and application.

How Cyber Criminals Plan cyber Attacks

3. Launching an attack

- Using step two information actual launching attack to gain system information.
- Once step two complete cyber attacker ready to launch attack.

- Attack is launched using following steps:
- Crack the password
- Exploit the privileges
- Execute malicious command
- Hide the files
- Final but most important is cover the track- delete the access logs

Social Engineering

- Involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.

- Classification of Social Engineering:

1. Human-based Social Engineering
2. Computer-based Social Engineering

Social Engineering

1. Human-based Social Engineering:

Person to person interaction to get required/desired information

1. **Impersonating an employee or valid user**
2. **Posing as an important user:** Attacker pretends to be an important user e.g. CEO of company, who needs immediate help to log on to system
3. **Using a third person**
4. **Calling technical support**
5. **Shoulder surfing:** Gathering information by watching over a person’s shoulder while he/she logs on to the system
6. **Dumpster diving:** Looking in trash/dustbin for information written on pieces of paper or computer printouts

Social Engineering

2. Computer-based Social Engineering

Attempt made to get required/desired information by using computer software / internet

1. Fake e-mails
2. E-mail attachments
3. Pop-up Windows

Ransomware

Ransomware is a kind of malware attack that restricts access to your devices or files and displays a pop-up message that demands payment for the restriction to be removed.

- ✓ Restricts access to devices
- ✓ Contains malicious attachments.