Unit – 1

Introduction to Cyber Crime and Cyber Security

Cyber Crime

Meaning –

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

Definition –

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

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

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

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

Origin of the word Cyber Crime

Cyber came from cybernetics. Cybernetics influences game, system, and organizational theory. Cybernetics derived from the Greek kubernētēs which refers to a

pilot or steersman. Related is the Greek word kubernēsis which means "the gift of governance" and applies to leadership.

Who are cyber criminals?

A cybercriminal is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both.

- Types of Cyber Criminals:

1. Hackers:
   The term hacker may refer to anyone with technical skills, however, it typically refers to an individual who uses his or her skills to achieve unauthorized access to systems or networks so as to commit crimes.
2. Organized Hackers:
   These criminals embody organizations of cyber criminals, terrorists, and state-sponsored hackers. Cyber criminals are typically teams of skilled criminals targeted on control, power, and wealth. These criminals are extremely organized, and should even give crime as a service. These attackers are usually profoundly prepared and well-funded.
3. Internet stalkers:
   Internet stalkers are people who maliciously monitor the web activity of their victims to acquire personal data. This type of cyber crime is conducted through the use of social networking platforms and malware, that are able to track an individual's PC activity with little or no detection.
4. Disgruntled Employees:
   Disgruntled employees become hackers with a particular motive and also commit cyber crimes. It is hard to believe that dissatisfied employees can become such malicious hackers. In the previous time, they had the only option of going on strike against employers. But with the advancement of technology there is increased in work on computers and the automation of processes, it is simple for disgruntled employees to do more damage to their employers and organization by committing cyber crimes. The attacks by such employees bring the entire system down.

Classification of Cyber Crimes

Email spoofing

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

Spamming

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

Cyber defamation

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

- Cyber defamation is a new concept but it virtually defames a person through new medium. The medium of defaming the individual's identity is through the help of computers via internet.

Internet time theft

- It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person.
- The authorized person gets access to another person's ISP user ID and password, either by hacking or by illegal means without that person's knowledge.
- Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person.
- **Salami Attack**
- A salami attack is a small attack that can be repeated many times very efficiently. Thus the combined output of the attack is great.
- In the example above, it refers to stealing the round-off from interest in bank accounts.
- Even though it is less than 1 cent per account, when multiplied by millions of accounts over many months, the adversary can retrieve quite a large amount. It is also less likely to be noticeable since your average customer would assume that the amount was rounded down to the nearest cent.

Data Diddling

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

Forgery

- Forger" redirects here.

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

Web Jacking

- Illegally seeking control of a website by taking over a domain is know as Web Jacking.
- Web jacking attack method is one kind of trap which is spread by the attacker to steal the sensitive data of any people, and those people got trapped who are not aware about cyber security.
- Web jacking attack method is another type of social engineering phishing attack where an attacker create a fake web page of victim website
- An attacker send it to the victim and when a victim click on that link, a message display on the browser "the site abc.com has move on another address, click here to go to the new location"
- If a victim does click on the link, he/she will redirect on the fake website page where an attacker can ask for any sensitive data such as credit card number, username, password etc.

Emanating from UseNet

- Usenet is a kind of discussion group where people can share views on topic of their interest. The article posted to a newsgroup becomes available to all readers of the newsgroup.
- By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way.

- Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.

Industrial Espionage

- Industrial espionage describes a series of covert activities in the corporate world such as the theft of trade secrets by the removal, copying, or recording of confidential or valuable information in a company. The information obtained is meant for use by a competitor.
- Economic or industrial espionage commonly occurs in one of two ways.

  i) a dissatisfied employee appropriates information to advance interests or to damage the company.

  ii) Secondly, a competitor or foreign government seeks information to advance its own technological or financial interest.
- Industrial espionage and spying can occur in any industry -- from food and beverage to fashion and entertainment.
- However, technology is one of the most targeted industries.
- Key technology industries that are often targeted include computer, semiconductor, electronics, automotive, aerospace, biotechnology, energy, pharmaceutical and high-tech manufacturing.

Hacking

- Hacking refers to activities that seek to compromise digital devices, such as computers, smartphones, tablets, and even entire networks.
- Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose.
- They can destroy, steal or even prevent authorized users from accessing the system.
- Kevin Mitnick likely holds the title as the world's best hacker ever. Kevin Mitnick started hacking at an early age. He broke into the realm of public attention in the 1980s after he hacked into the North American Defense Command
-

- Ankit Fadia (born 1985) is an Indian author, speaker, television host, a security charlatan, and self-proclaimed white-hat computer hacker.

Types of Hackers

a) White Hat Hackers – These hackers utilize their programming aptitudes for a good and lawful reason. These hackers may perform network penetration tests in an attempt to compromise networks to discover network vulnerabilities. Security vulnerabilities are then reported to developers to fix them.

b) Black Hat Hackers –
These hackers are unethical criminals who violate network security for personal gain. They misuse vulnerabilities to bargain PC frameworks.

c) Gray Hat Hackers – These hackers carry out violations and do seemingly deceptive things however not for individual addition or to cause harm. These hackers may disclose a vulnerability to the affected organization after having compromised their network.

Email bombing

- An email bomb or "mail bomb" is a malicious act in which a large number of email messages are sent to a single email address in a short period of time. The purpose of an email bomb is typically to overflow a user's inbox. In some cases, it will also make the mail server unresponsive.
- Email bombing is often done from a single system in which one user sends hundreds or thousands of messages to another user. In order to send the messages quickly, the email bomber may use a script to automate the process. By sending emails with a script, it is possible to send several thousand messages per minute.
- Fortunately, most mail servers are capable of detecting email bombs before a large number of messages are sent. For example, if the server detects that more than ten messages are received from the same email address within one minute,

it may block the sender's email address or IP address. This simple action will stop the email bomb by rejecting additional emails from the sender.

Intrusion

- The definition of an intrusion is an unwelcome interruption or a situation where somewhere private has an unwelcome visit or addition. When you are having a quiet nap in your backyard and your neighbor's dog comes in uninvited and jumps all over you to wake you up, this is an example of an intrusion.
- A network intrusion refers to any unauthorized activity on a digital network. Network intrusions often involve stealing valuable network resources and almost always jeopardize the security of networks and/or their data. In order to proactively detect and respond to network intrusions, organizations and their cybersecurity teams need to have a thorough understanding of how network intrusions work and implement network intrusion, detection, and response systems that are designed with attack techniques and cover-up methods in mind.

Password sniffing

- Password Sniffing is a hacking technique that uses a special software application that allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic. This often happens on public WiFi networks where it is relatively easy to spy on weak or unencrypted traffic.
- Password sniffing is an attack on the Internet that is used to steal user names and passwords from the network. Today, it is mostly of historical interest, as most protocols nowadays use strong encryption for passwords. However, it used to be the worst security problem on the Internet in the 1990s, when news of major password sniffing attacks were almost weekly.
- The typical implementation of a password sniffing attack involves gaining access to a computer connected to a local area network and installing a password sniffer on it. The password sniffer is a small program that listens to all traffic in the attached network(s), builds data streams out of TCP/IP packets,

and extracts user names and passwords from those streams that contain protocols that send cleartext passwords.

- The attack can also be performed in switches, routers, and printers. It is common nowadays for attackers to install presence on such devices. They don't run anti-virus and aren't easy to audit. Furthermore, traffic naturally goes through switches and routers, so no extra network packets need to be sent to fool switches into sending traffic of interest to the listening node.

Credit card fraud

- Credit card fraud occurs when an unauthorized person gains access to your information and uses it to make purchases. ... Skimming your credit card, such as at a gas station pump. Hacking your computer. Calling about fake prizes or wire transfers.
- Here criminals make purchases or obtain cash advances using a credit card account assigned to you. This can occur through one of your existing accounts, via theft of your physical credit card or your account numbers and PINs, or by means of new credit card accounts being opened in your name without your knowledge. Once they're in, thieves then run up charges and stick you and your credit card company with the bill.

Identity Theft

- Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases.

CYBER SECURITY

Definition-

Cyber security is the technique of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

OR

Cyber security refers to the measures taken to keep electronic information private and safe from damage or theft. It is also used to make sure electronic devices and data are not misused.

OR

Cyber security is the body of technology, processes and practices designed to protect network, computers, computer programs and data from attack, damage or unauthorized access.

Cyber Security Threats-

A cyber or cyber security threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.

Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks and other attack vectors.

Viruses-

- A computer virus is a program which can harm our device and files and infect them for no further use.
- When a virus program is executed, it replicates itself by modifying other computer programs and instead enters its own coding.
- This code infects a file or program and if it spreads massively, it may ultimately result in crashing of the device.
- Viruses affect your computer by corrupting files, interrupting Internet traffic and taking over basic functions of your operating system.
- These behaviors can knock a system offline and cause crashes.

- Viruses can record keystrokes and screen data, and they may steal personal information and passwords to transmit back to the malware author.
- Particularly malicious viruses completely take over a computer and use it as a weapon against others.

Trojan -

- A Trojan horse is malicious software that is concealed as a useful host program.
- When the host program is run, the Trojan performs a harmful/unwanted
- A Trojan horse, often known as a Trojan, is malicious malware or software that appears to be legal yet has the ability to take control of your computer.
- A Trojan is a computer program that is designed to disturb, steal, or otherwise harm your data or network.

Malwares-

- Malware ("malicious software") is a type of computer program that infiltrates and damages systems without the users' knowledge.
- Malware tries to go unnoticed by either hiding or not letting the user know about its presence on the system.
- You may notice that your system is processing at a slower rate than usual.

Ransom wares-

- Ransom ware is a type of malware that threatens to publish the victim's personal data or block access to it unless a ransom is paid.
- While some simple ransom ware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called crypto viral extortion.
- It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

- Ransom ware attacks are typically carried out using a Trojan as a file that the user is tricked into downloading or opening when it arrives as an email attachment.

Vulnerability-

- In cyber security, a vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system.
- After exploiting a vulnerability, a cyber attack can run malicious code, install malware and even steal sensitive data.

Security Vulnerability Types

Computer security vulnerabilities can be divided into numerous types based on different criteria—such as where the vulnerability exists, what caused it, or how it could be used. Some broad categories of these vulnerability types include:

- Network Vulnerabilities
- Operating System Vulnerabilities
- Human Vulnerabilities
- Process Vulnerabilities

Network Vulnerabilities

- These are issues with a network's hardware or software that expose it to possible intrusion by an outside party.
- Examples include insecure Wi-Fi access points and poorly-configured firewalls.

Operating System Vulnerabilities

- These are vulnerabilities within a particular operating system that hackers may exploit to gain access to an asset the OS is installed on—or to cause damage.
- Examples include default superuser accounts that may exist in some OS installs and hidden backdoor programs.

Human Vulnerabilities

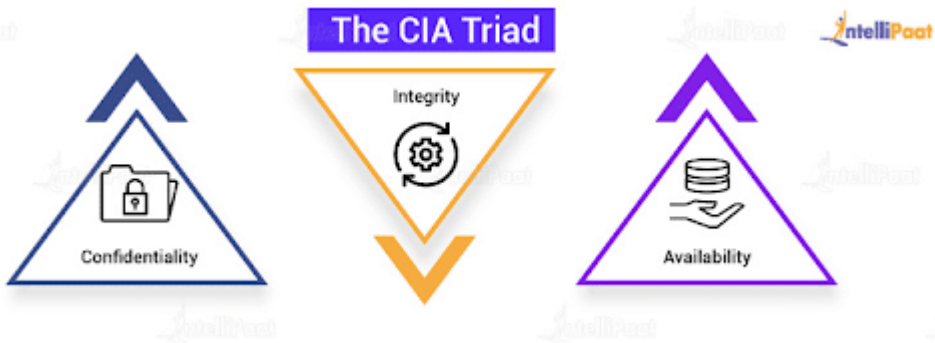
- The weakest link in many cyber security architectures is the human element.
- User errors can easily expose sensitive data, create exploitable access points for attackers, or disrupt systems.

CIA Triad-

- **Confidentiality, integrity and availability**, also known as the CIA triad, is a model designed to guide policies for information security within an organization.
- The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency.
- The CIA triad is a common, respected model that forms the basis for the development of security systems and policies.
- These are used for the identification of vulnerabilities and methods for addressing problems and creating effective solutions.

Examples of CIA Triad

- The two-factor authentication (debit card with the PIN code) provides confidentiality before authorizing access to sensitive data.
- The ATM and bank software ensure data integrity by maintaining all transfer and withdrawal records made via the ATM in the user's bank accounting.



Confidentiality

- Confidentiality involves the efforts of an organization to make sure data is kept secret or private.
- To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data—whether intentional or accidental.
- A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.
- For example, those who work with an organization's finances should be able to access the spreadsheets, bank accounts, and other information related to the flow of money. However, the vast majority of other employees—and perhaps even certain executives—may not be granted access. To ensure these policies are followed, stringent restrictions have to be in place to limit who can see what.

Integrity

- Integrity involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable.
- For example, if your company provides information about senior managers on your website, this information needs to have integrity. If it is inaccurate, those visiting the website for information may feel your organization is not trustworthy. Someone with a vested interest in damaging the reputation of your organization may try to hack your website and alter the descriptions, photographs, or titles of the executives to hurt their reputation or that of the company as a whole.

Availability

- Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve.
- This means that systems, networks, and applications must be functioning as they should and when they should.

- Also, individuals with access to specific information must be able to consume it when they need to, and getting to the data should not take an inordinate amount of time.
- If, for example, there is a power outage and there is no disaster recovery system in place to help users regain access to critical systems, availability will be compromised. Also, a natural disaster like a flood or even a severe snowstorm may prevent users from getting to the office, which can interrupt the availability of their workstations and other devices that provide business-critical information or applications. Availability can also be compromised through deliberate acts of sabotage, such as the use of denial-of-service (DoS) attacks or ransomware.

CIA Triad-

Ideally, when all three standards have been met, the security profile of the organization is stronger and better equipped to handle threat incidents.

Cyber security policy –

- Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information.
- It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur.
- A security policy also considered as a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Types of cyber security policies-

1. **Virus and Spyware Protection policy**
   - It helps to detect, removes, and repairs the side effects of viruses and security risks.
   - It helps to detect the threats in the files which the users try to download by using reputation data from different sites.

- It helps to detect the applications that exhibit suspicious behavior.

2**. Firewall Policy**

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic.

3. Intrusion Prevention policy

- This policy automatically detects and blocks the network attacks and browser attacks.
- It also protects applications from vulnerabilities.
- It checks the contents of one or more data packages and detects malware which is coming through legal ways.

4. Live Update policy

- Live Update Content policy – The Live Update policy contains the setting which determines when and how client computers download the content updates from Live Update.
- Live Update Setting Policy - We can define the computer that clients contact to check for updates and schedule when and how often clients computer check for updates.

5. Application and Device Control

- This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system.
- The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

6. Exceptions policy

- This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

7. Host Integrity policy

- This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure.
- This policy requires that the client system must have installed antivirus.

Unit – 2

Cyber Offenses and Cyber Stalking

Attacks

The **attack phase** is the last step in the attack process. It involves the hacker gaining and maintaining full control of the system access. It comes immediately after scanning and enumeration, and it launched sequentially as listed in the below steps.

Brute force attack or any other relevant method to bypass the password.

Exploit the password.

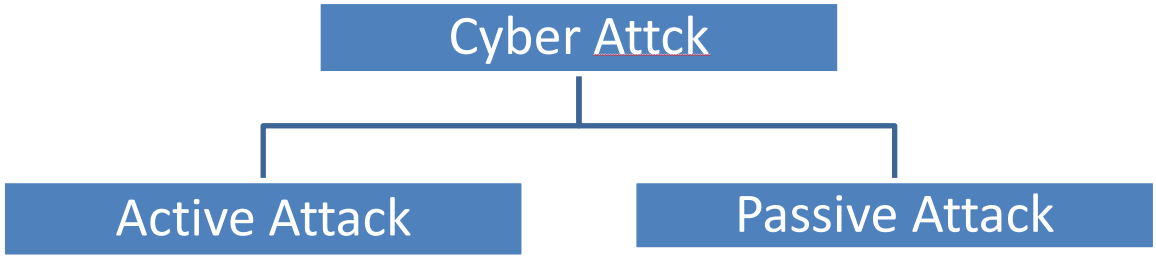
Launch the malicious command or applications.

If requires, then hide the files.

Cover the tracks, don't leave any trail that can lead back to you as the malicious third party. This can be achieved by deleting logs so that there is no trail for your illicit actions.

Types of Attacks-

Cyber attacks can be defined as exploitation of computer system, resources, networks and technology connected through internet.



Types of Attacks-

Reconnaissance attack

- A proper recon would provide detailed information and open doors to attackers for scanning and attacking all the way.
- By using a recon, an attacker can directly interact with potential open ports, services running etc. or attempt to gain information without actively engaging with the network.
- Reconnaissance attacks are general knowledge gathering attacks. These attacks can happen in both logical and physical approaches.
- Some common examples of reconnaissance attacks include packet sniffing, ping sweeping, port scanning, phishing, social engineering and internet information queries.

Passive Attack

In Passive attack, an attacker observes the messages, copies them and may use them for malicious purposes.

The main goal of a passive attack is to obtain unauthorized access to the information

Types of Passive Attacks-

1) Release of Message (Eavesdropping)-

- It is a theft of information as it is transmitted over a network by a computer, smart phone, or another connected device.

- The attack takes advantage of unsecured network communications to access data as it is being sent or received by its user.
- It is similar to hearing a telephone conversation between two users.
- In this attack, the attacker can monitor the content of the transmitted data such as email messages, etc.

2) Traffic analysis –

- Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
- The attacker could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of the communication that was taking place.

3) Scrutinizing and Scanning the Gathered Information

- Scanning is a key step to intelligently examine after as you collect information about the network infrastructure. The process has the following objectives;
  - Network scanning is executed to understand better the IP address and other related information about the computer network system.
  - Port Scanning – to identify any closed or open ports and services
  - Vulnerability scanning – to identify existing weak links within the system.

4) Scrutinizing and Scanning the Gathered Information

- In the hacking world, the scrutinizing phase is also referred to as *enumeration.*
- The objective of scrutinizing includes:
- To validate the authenticity of the user running the given account, be it an individual or a group of persons.
- To identify network resources and or shared resources
- To verify the operating system and various applications that are running on the computer OS.

Social Engineering

- Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.
- Social engineers are clever and use manipulative tactics to trick their victims into disclosing private or sensitive information.
- Social engineering is a term that encompasses a broad spectrum of malicious activity.
- The five most common attack types that social engineers use to target their victims. These are

1) Phishing
2) Vishing and Smishing
3) Pretexting
4) Paiting
5) Quid Pro Quo
6) Tailgating and Piggybacking

1) **Phishing**
   - Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a genuine (legal) organization to ensnare individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
   - The information is then used to access important accounts and can result in identity theft and financial loss.
   - Phishers frequently use emotions like fear, curiosity, urgency, and greed to force recipients to open attachments or click on links.
   - Phishing attacks are designed to appear to come from legitimate (legal) companies and individuals.

Types of Phishing

Spear phishing -

- Spear phishing targets specific individuals instead of a wide group of people.

- That way, the attackers can customize their communications and appear more authentic.
- Spear phishing is often the first step used to penetrate a company's defenses and carry out a targeted attack.
- Imagine that an individual regularly posts on social media that she is a member of a particular gym. In that case, the attacker could create a spear phishing email that appears to come from her local gym. The victim is more likely to fall for the scam since she recognized her gym as the supposed sender.

Whaling-

- When attackers go after a "big fish" like a CEO, it's called whaling. These attackers often spend considerable time profiling the target to find the opportunity and means to steal login credentials.
- Whaling is of particular concern because high-level executives are able to access a great deal of sensitive company information.

Social media phishing-

- Attackers often research their victims on social media and other sites to collect detailed information, and then plan their attack accordingly.

2) Vishing and Smishing

- While phishing is used to describe fraudulent email practices, similar manipulative techniques are practiced using other communication methods such as phone calls and text messages.
- Vishing (short for voice phishing) occurs when a fraudster attempts to trick a victim into disclosing sensitive information or giving them access to the victim's computer over the telephone.
- Smishing (short for SMS phishing) is similar to and incorporates the same techniques as email phishing and vishing, but it is done through SMS/text messaging.

3) Pretexting

- Pretexting is a type of social engineering technique where the attacker creates a scenario where the victim feels compelled to comply under false pretenses. Typically, the attacker will impersonate someone in a powerful position to persuade the victim to follow their orders.
- During this type of social engineering attack, a bad actor may impersonate police officers, higher-ups within the company, auditors, investigators or any other persona they believe will help them get the information they seek.

4) Baiting

- Baiting puts something enticing (tempting) or curious in front of the victim to lure (trap) them into the social engineering trap. A baiting scheme could offer a free music download or gift card in an attempt to trick the user into providing credentials.
- A social engineer may hand out free USB drives to users at a conference. The user may believe they are just getting a free storage device, but the attacker could have loaded it with remote access malware which infects the computer when plugged in.

5. **Tailgating and Piggybacking**

- Tailgating is a simplistic social engineering attack used to gain physical access to access to an unauthorized location.
- Tailgating is achieved by closely following an authorized user into the area without being noticed by the authorized user.
- An attacker may tailgate another individual by quickly sticking their foot or another object into the door right before the door is completely shut and locked.

5. **Tailgating and Piggybacking**

- Piggybacking is exceptionally similar to tailgating.
- The main difference between the two is that, in a piggybacking scenario, the authorized user is aware and allows the other individual to "piggyback" off their credentials.
- An authorized user may feel compelled by kindness to hold a secure door open for a woman holding what appears to be heavy boxes or for a

person claiming to be a new employee who has forgotten his access badge.

6. Quid Pro Quo

- Quid pro quo (Latin for 'something for something') is a type of social engineering tactic in which the attacker attempts a trade of service for information.
- A quid pro quo scenario could involve an attacker calling the main lines of companies pretending to be from the IT department, attempting to reach someone who was having a technical issue.
- Once the attacker finds a user who requires technical assistance, they would say something along the lines of, "I can fix that for you. I'll just need your login credentials to continue."
- This is a simple and unsophisticated way of obtaining a user's credentials.

Cyber Stalking

- Cyberstalking is a crime in which someone harasses or stalks a victim using electronic or digital means, such as social media, email, instant messaging (IM), or messages posted to a discussion group or forum.
- Cyberstalkers take advantage of the anonymity afforded by the internet to stalk or harass their victims, sometimes without being caught, punished or even detected.
- Although *cyberstalking* is a general term for online harassment, it can take many forms, including slander, defamation, false accusations, trolling and even outright threats.

- In many cases, especially when both the harasser and victim are individuals, the motive may be the following:

a) monitor the victim's online -- and, in some cases, offline -- activities;

b) track the victim's locations and follow them online or offline;

c) intimidate (scare), frighten, control or blackmail the victim;

d) reveal private information about the victim, a practice known as *doxing*; or gather more information about the victim to steal their identity or perpetrate other real-world crimes, like theft or harassment.

I. Rejected Cyberstalkers:

- This type of cyberstalker is motivated to pursue their victim in attempt to reverse what they perceive as a wrongful set of circumstances causing a prior divorce, separation or termination of a relationship.
- These offenders either feel misunderstood hoping to reverse the breakup or feel angry and seeking revenge because their attempts at reconciliation with the victim has failed in the past.

II. Resentful Cyberstalkers:

- This type of cyberstalker can be dangerous given their perceived motivation for stalking.
- Resentful cyberstalkers are fully aware the victim is cognizant of the stalking but continues to fulfill a distorted (biased or one-sided) vendetta (quarrel) he/she feels is warranted.
- Fear and distress experienced by the victim are the goals of this type of cyberstalker.
- For this type of profile, the cyberstalker believes the victim both deserves and requires being frightened because they have caused them and/or others distress.

III. Intimacy Seekers:

- This type of cyberstalker does not have will towards their victim and simply wants to engage in a loving relationship with them.
- Intimacy seekers view their victims as their soulmate destined to be together at all costs. Within their mind, they believe it is their job and purpose to make sure destiny of a loving relationship is fulfilled. Intimacy seeking cyberstalkers are often the segment of men or women who harass celebrities and public figures.
- Blinded by their distorted perceptions of a destined love, they lose sight of the distress and fear they are causing the person they cyberstalk.

IV. Incompetent Suitors:

- These people who fit this profile are cyberstalkers deeply enamored (loving) with their victim.
- Their interest for the victim at times can reach a state of fixation whereby their entire waking life is focused on the endeavor (try) of one day becoming a couple.
- They tend to lack social, communication or courting skills and may feel entitled that their fantasy of a loving relationship is inevitable (expected).
- Feeling entitled and/or deserving of a relationship with the victim inspires the cyberstalker to gradually increase their frequency of contact.
- Although like the Intimacy Seeker cyberstalker, incompetent suitors are more gradual in their means and methods of contact.

V. Predatory Cyberstalkers:

- Of the six types, the predatory cyberstalker can be the most dangerous and determined.
- This type of cyberstalker is motivated by a perverted sexual need.
- They do not have feelings of love for their victim nor motivated by a belief of predestination.

VI. Ghost Cyberstalkers:

- Ghost Cyber stalkers are online assailants (mask) who their target cannot identify.
- Using Cyberstealth, the ghost cyberstalker repeatedly makes direct or indirect threats of physical harm and inspires fear.
- They can represent an amalgamation (union) of the other five types.
- Ghost cyberstalkers rely upon the veil of secrecy afforded to all online users.

Real Life Examples of Cyber Stalking

- Placing orders for delivery in someone else's name.
- Gathering personal information on the victim.
- Spreading false rumors.
- Encouraging others to join in the harassment.
- Threatening harm through email.
- Creating fear and paranoia(terror / distrust) for someone else.
- Post rude, offensive, or suggestive comments online.
- Follow the target online by joining the same groups and forums.
- Send threatening, controlling, or lewd messages or emails to the target.
- Use technology to threaten or blackmail the target.

To guard against cyberstalking include the following:

- update all software to prevent information leaks;
- mask your Internet Protocol address with a virtual private network;
- strengthen privacy settings on social media;
- strengthen all devices with strong passwords or, better, use multifactor authentication;
- avoid using public Wi-Fi networks;
- send private information via private messages, not by posting on public forums;
- safeguard mobile devices by using password protection and never leave devices unattended;
- disable geo location settings on devices;
- install antivirus software on devices to detect malicious software;
- always log out of all accounts at the end of a session; and
- beware of installing apps that ask to access your personal information.

What to do in case you are being cyberstalked

- **Block the person**

Don't hesitate to apply all measures permitted by law, especially those offered by web services.

If the tools are there, block anyone who you wish to stop hearing from, even if these messages are just annoying and not yet threatening.

Only you can decide when this boundary has been passed.

- **Report to the platform involved**

If someone is harassing or threatening you, you should block them immediately and report their behavior to the platform involved.

Twitter, Facebook, LinkedIn,and many other platforms have created easy-to-use buttons to quickly report abusive behavior.

Law enforcement agencies do not always have the technical ability to protect you from cyberstalking, but platform moderators usually respond quickly and delete attackers' profiles.

- **Call the Police**

If you believe their behavior is illegal or you fear for your safety, then you should contact the police and report the cyberstalker.

Even if you don't have enough information or evidence for them to prosecute immediately, the report will go on record and the police can offer advice about what to do if the perpetrator persists.

Cyber Café and Cyber Crime

- A cybercafe is a type of business where computers are provided for accessing the internet, playing games, chatting with friends or doing other computer-related tasks.
- In most cases, access to the computer and internet is charged based on time.
- A cybercafe is also known as an internet café.

- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.
- Cybercriminals prefer cybercafes to carry out their activities.
- The criminals tend to identify one particular personal computer PC to prepare it for their use.

BOTNET

- The term botnet is derived from the words robot and network.
- A botnet (short for "robot network") is a network of computers infected by malware that are under the control of a single attacking party, known as the "bot-herder."
- Each individual machine under the control of the bot-herder is known as a bot.
- They are also used to spread bots to recruit more computers to the botnet.
- A botnet is a number of Internet-connected devices, each of which is running one or more bots.
- Botnets can be used to perform Distributed Denial-of-Service attacks, steal data, send spam, and allow the attacker to access the device and its connection.

ATTACK VECTOR

- An attack vector is a pathway or method used by a hacker to illegally access a network or computer in an attempt to exploit system vulnerabilities.
- Hackers use numerous attack vectors to launch attacks that take advantage of system weaknesses, cause a data breach, or steal login credentials.

Credit Card Fraud

Credit card fraud is an inclusive term for fraud committed using a payment card, such as a credit card or debit card. The purpose may be to obtain goods or services or to make payment to another account, which is controlled by a criminal. The Payment Card Industry Data Security Standard (PCI DSS) is the data security standard created to help financial institutions process card payments securely and reduce card fraud.

Credit card fraud can be authorized, where the genuine customer themselves processes a payment to another account which is controlled by a criminal, or unauthorized, where the account holder does not provide authorization for the payment to proceed and the transaction is carried out by a third party.

In 2018, unauthorized financial fraud losses across payment cards and remote banking totaled £844.8 million in the United Kingdom. Whereas banks and card companies prevented £1.66 billion in unauthorized fraud in 2018.

Credit cards are more secure than ever, with regulators, card providers and banks taking considerable time and effort to collaborate with investigators worldwide to ensure fraudsters aren't successful. Cardholders' money is usually protected from scammers with regulations that make the card provider and bank accountable. The technology and security measures behind credit cards are becoming increasingly sophisticated making it harder for fraudsters to steal money.

Means of payment card fraud

There are two kinds of card fraud: card-present fraud (not so common nowadays) and card-not-present fraud (more common). The compromise can occur in a

number of ways and can usually occur without the knowledge of the cardholder. The internet has made database security lapses particularly costly, in some cases, millions of accounts have been compromised.

Stolen cards can be reported quickly by cardholders, but a compromised account's details may be held by a fraudster for months before any theft, making it difficult to identify the source of the compromise. The cardholder may not discover fraudulent use until receiving a statement. Cardholders can mitigate this fraud risk by checking their account frequently to ensure there are not any suspicious or unknown transactions.

When a credit card is lost or stolen, it may be used for illegal purchases until the holder notifies the issuing bank and the bank puts a block on the account. Most banks have free 24-hour telephone numbers to encourage prompt reporting. Still, it is possible for a thief to make unauthorized purchases on a card before the card is canceled.

Mobile Devices

A mobile device is one that is made to be taken anywhere. Therefore, it needs an internal battery for power, and must be connected to a modern mobile network that can help it to send and receive data without attaching to a hardware infrastructure.

A lack of adequate security in wireless networks can lead to criminal attacks such as theft of data, corruption of system integrity, hacking, sabotage, espionage, theft of capacity, and loss or theft of mobile and portable devices.

Top Mobile Device Information Security Risks

1. Unsafe apps. Although the mobile phone vendors try to ensure app security through requiring apps to be signed to be downloaded from the official app stores, misuse of certificates means that even apps downloaded from vendor stores or enterprise sites aren't guaranteed to be free from malware. Even legitimate apps often request more permission than needed to perform their function, which can expose more data than necessary.
2. Unsafe operating systems. Large numbers of mobile devices are not kept up to date with operating system releases. Out of date operating systems mean devices are vulnerable to security threats that are patched in the later versions.
3. Unsafe devices. When users root devices, they work around the built-in restrictions of the device. While users feel that jailbreaking gives them freedom and more access to the device's capabilities, jailbreaking also eliminates many controls that provide security.
4. Unsafe connections. Users often rely on public Wi-Fi to stay connected when they work outside the office. These unsecured Wi-Fi networks can allow malware to be installed on devices or eavesdroppers to intercept data.
5. Lost devices. Portable devices are easily lost or stolen. When an employee loses physical control of their mobile device, they also lose control of the data on that device. If the device isn't appropriately protected with passwords and encryption, any data on that device may be exposed.
6. Uncontrollable users. No matter how well you publicize your safe mobile computing policies, there will be employees who find them too inconvenient to follow. Organizations need tools to enforce policies rather than relying on employees' good will.
7. Lack of monitoring. The large number of mobile devices used in an organization makes monitoring and managing them difficult. It isn't easy to understand the status of all mobile devices, users, and applications at a glance.

Security Challenges On Mobile Devices

Believe it or not there are security risks when using a mobile device. I know, it's surprising right, that your phone or tablet could be a possible threat to your safety.

When you consider all the potential threats that exists on the Internet, and the fact that most of today's mobile devices are connecting to and through the Internet with every function, I think it becomes easier to understand just how vulnerable they are. While many of the threats are the same as those faced by the average laptop or desktop user there are some unique to the mobile world. There are four basic types of threats mobile devices are susceptible to. Mobile phone security threats include application based, web based, network based and physical threats.

1) Smart Phone Security Threats

1. Downloadable applications threats

Downloadable applications pose the most common risk for mobile users; most devices don't do much on their own, it's the applications that make them so awesome and we all download apps. When it comes to apps the risks run from bugs and basic security risks on the low end of the scale all the way through malicious apps with no other purpose to commit cyber crime.

- Malware – malware is software that makes unwanted changes to your phone. This could include accessing email accounts, sending spam to your contacts or give control of your phone to a third party. Ransomware is a growing trend among Internet scammers and is being used on mobile devices too. Malware locks your computer until you pay the ransom to get control back.
- **Spyware** – spyware is software that is intended to track or monitor devices and their users. It can collect any and all data and information stored on your phone, or transmitted through text, email or Internet.
- **Privacy** – privacy threats exists above and beyond the scope of intentional malware or spyware. All websites and applications collect some information about you, and that information is at risk of loss. Profiles on a chat site aren't so much a problem but that change when the info includes a government ID, bank account or sensitive password.
- **Zero Day Vulnerabilities** – Zero Day Vulnerabilities are flaws and potential points of entry within existing and otherwise trustworthy apps that have yet to be reported and/or fixed. Usually caused by poor coding or improper development these flaws and loopholes allow hackers, malware and spyware easy access to your devices and information.

Date – 25 Nov 2021

2. General Cyber Security Threats

Due to the nature of mobile use, the fact that we have our devices with us everywhere we go and are connecting to the Internet while doing so, they face a number of unique web-based threats as well as the run-of-the-mill threats of general Internet use.

- **Phishing Scams** – Phishing scams can use your email, text messaging and even push notifications from social media to trick you into entering sensitive information. What makes them so hard to avoid is the sophisticated nature of the scams, many are impossible to distinguish from well know and trusted sites and often times all it takes is a simple click or like of a suggested page for malware to be downloaded to your device. Adding to the problem are small screen sizes and browsers that don't display full URLs for links which makes it even easier to follow a bad one.
- **Social Engineering** is the latest buzzword in mobile attacks. These can range in degree but are aimed at using a person's natural curiosity against them. One example is simply dropping a flash drive in a parking lot and waiting for someone to pick it up, and maybe look to see what's on it. In some cases it may just be a lost drive, in others the drive could set to deliver malware into a device or network.
- **Drive By Downloads** – Some websites are set up to automatically download apps to your device whether you want it to or not. In most cases you will have to enable the app for it to work but this is not always the case. The apps could be innocent, and they could be malware or spyware.
- **Browser Flaws** – Some websites and applications can exploit flaws in your browser software or other programs used by it such as a Flash, PDF or media application. Visiting the wrong webpage can trigger an automatic exploit, just like a drive by.
- **Operating System Flaws**– The operating systems of mobile devices are a common point of attack as well as hackers seek new points of entry. Android powered devices are most at risk, they are the ones most often targeted by hackers, and fixed with patches and updates. **Data Storage** – We store a lot of data on our phones and that amount grows daily. Most phones utilize some form of encryption to protect your data but once a hacker gets past your security it doesn't really matter.

3. Network and WiFi Security Threats

Mobile devices typically support a minimum of three network capabilities making them three-times vulnerable to network based attack. The networks often found on a mobile include cellular, WiFi and Bluetooth.

- **Network exploits** – no network is foolproof, there are flaws in the system, and they can be exploited for the purposes of downloading malware to your device. Bluetooth is especially vulnerable. Hackers can run programs to find any and all available Bluetooth connections within range and connect to them.
- **WiFi sniffing** – most websites do not use proper security when sending information across the web which makes it vulnerable to intercept. Mobile devices are constantly accessing this information across public WiFi networks which makes it easy to intercept. Black hats can easily scan the airwaves as they travel between your device and the WiFi access point, grab your data and steal it. They can also track the connections back to your devices and download malware, or mine your data.
- **Cross-Platform Attacks** – Hackers can deploy spyware to your computer which tracks data such as banking details. Once those are stolen a pop-up message suggests the Internet user download an app for "added security on your mobile device", all you have to do is enter your phone number to get an SMS message with the download link. If done the hacker then has control of the laptop and the phone.

4. Physical Threats

Unlike a desktop sitting at your workstation, or even a laptop in your bag, a mobile device is subject to a number of everyday physical threats.

- **Loss/Theft** – Loss or theft is the most prevalent physical threat to the security of your mobile device. The device itself has value and can be sold on the secondary market, after all your information is stolen and sold.

How to Ensure Your Mobile Security and Privacy

Despite all these issues the number one threat to mobile security remains us, the users. As mobile devices improve and our use of them grows the number, types and quality of threat will grow too. Here are some tips on how to ensure your mobile security.

- **Always password-protect your phone**. Use passwords and if possible, fingerprint detection. This way if you forget your phone, lose it or it is stolen whoever finds it won't have easy access.
- **Only download safe apps**. Apps are the easiest point of entry for hackers and malware because we willingly download them to our phone. All they have to do is make one attractive enough for us to want to download it. This is why it is important to get apps from trusted sources like the Google Play App Store or the iTunes App Store and even then it is important to verify an app's trustworthiness by checking reviews from other users.
- **Always read the terms and privacy policy**. All apps collect and use our information to some extent. Always be sure to read the terms of use and privacy policy to see what information is collected, how it is used and where it may be shared.

- **Turn off the Bluetooth**. It is a good idea to turn off the Bluetooth on your mobile device when not using it. Aside from closing down a potential point of entry it will also cut down on your battery usage.

- **Encrypt your phone**. Most of today's phones have some form of

  automatic encryption or encryption feature you can enable. Be sure to do so.

- **Set up remote locate/wipe**. Most phones have features that can be used to remotely wipe your phones memory and/or geolocate it. This feature is especially useful if there is sensitive data on your phone or you do not

expect to get it back. When used in conjunction with password protection, it can keep the loss of data to a minimum.

- **Back up your data**. Most mobile users back up their data about as often as they update their operating systems, which is to say not too often. You can upload your phone's settings, data, pictures, music and etc. to the cloud, which in itself poses a risk to your security, or directly to a laptop or PC.

- **Don't root your phone**. The difference depends on whether your device is iOS or Android but the meaning is the same: you've bypassed manufacturer settings in order to use your phone in a way not originally intended. Doing this weakens your device's natural security settings and exposes it to additional risks as well.

- **Update the operating system**. I know it's a pain but it needs to be done. When you get the message that says a new OS is available, take the time to set it up and do the download.
- **Download anti-malware**. Yes, it does exist and you can get it from a number of sources. If you are using an Android device I highly recommend it.

- **Use public WiFi with caution**. Public WiFi is one of the many perks of using a mobile device, you can connect anywhere, it's free and you can save on data minutes by using it. The downside is two-fold. First, the WiFi security – these connections are inherently insecure as they are open and available to anyone who wants to connect to them. This leads to the second problem which is that public WiFi connections attract black hats and hackers as a high-target environment. One way to protect yourself is with a VPN.

- **Use a VPN**. A VPN is a virtual private network. This technology uses software to encrypt your data before it leaves your device to travel across the WiFi network, and then sends it through a digital "tunnel" that is hard to detect and nearly impossible to track.

1) Data Leakage

Mobile apps are often the cause of unintentional data leakage. For example, "riskware" apps pose a real problem for mobile users who grant them broad permissions, but don't always check security. These are typically free apps found in official app stores that perform as advertised, but also send personal—and potentially corporate—data to a remote server, where it is mined by advertisers, and sometimes, by cybercriminals.

Data leakage can also happen through hostile enterprise-signed mobile apps. These mobile malware programs use distribution code native to popular mobile operating systems like iOS and Android to move valuable data across corporate networks without raising red flags.

o avoid these problems, only give apps the permissions that they absolutely need in order to properly function. And steer clear of any apps that asks for more than necessary. The September 2019 updates for Android and Apple iOS both added protocols to make users more aware of it and why apps collect users' location data.

2) Unsecured Wi-Fi

No one wants to burn through their cellular data when wireless hot spots are available—but free Wi-Fi networks are usually unsecured. According to V3, in fact, three British politicians who agreed to be part of a free wireless security

experiment were easily hacked by technology experts. Their social media, PayPal and even their VoIP conversations were compromised. To be safe, use free Wi-Fi sparingly on your mobile device. And never use it to access confidential or personal services, like banking or credit card information.

3) Network Spoofing

Network spoofing is when hackers set up fake access points—connections that look like Wi-Fi networks, but are actually traps—in high-traffic public locations such as coffee shops, libraries and airports. Cybercriminals give the access points common names like "Free Airport Wi-Fi" or "Coffeehouse" to encourage users to connect.

In some cases, attackers require users to create an "account" to access these free services, complete with a password. Because many users employ the same email and password combination for multiple services, hackers are then able to compromise users' email, e-commerce and other secure information. In addition to using caution when connecting to any free Wi-Fi, never provide personal information. And whenever you are asked to create a login, whether for Wi-Fi or any application, always create a unique password.

4) Phishing Attacks

Because mobile devices are always powered-on, they are the front lines of most phishing attack. According to CSO, mobile users are more vulnerable because they are often monitor their email in real-time, opening and reading emails when they are received. Mobile device users are also more susceptible because email apps display less information to accommodate the smaller screen sizes. For example, even when opened, an email may only display the sender's name unless you expand the header information bar. Never click on unfamiliar email links. And if the matter isn't urgent, then let the response or action items wait until you're at your computer.

5) Spyware

Although many mobile users worry about malware sending data streams back to cybercriminals, there's a key threat closer to home: Spyware. In many cases, it's not malware from unknown attackers that users should be worried about, but rather spyware installed by spouses, coworkers or employers to keep track of their

whereabouts and activity. Also known as stalkerware, many of these apps are designed to be loaded on the target's device without their consent or knowledge. A comprehensive antivirus and malware detection suite should use specialized scanning techniques for this type of program, which requires slightly different handling than does other malware owing to how it gets onto your device and its purpose.

6) Broken Cryptography

According to Infosec Institute training materials, broken cryptography can happen when app developers use weak encryption algorithms, or fail to properly implement strong encryption. In the first case, developers may use familiar encryption algorithms despite their known vulnerabilities to speed up the app development process. As a result, any motivated attacker can exploit the vulnerabilities to crack passwords and gain access. In the second example, developers use highly secure algorithms, but leave other "back doors" open that limit their effectiveness. For example, it may not be possible for hackers to crack the passwords, but if developers leave flaws in the code that allow attackers to modify high-level app functions—such as sending or receiving text messages—they may not need passwords to cause problems. Here, the onus is on developers and organizations to enforce encryption standards before apps are deployed.

7) Improper Session Handling

To facilitate ease-of-access for mobile device transactions, many apps make use of "tokens," which allow users to perform multiple actions without being forced to re-authenticate their identity. Like passwords for users, tokens are generated by apps to identify and validate devices. Secure apps generate new tokens with each access attempt, or "session," and should remain confidential. According to The Manifest, improper session handling occurs when apps unintentionally share session tokens, for example with malicious actors, allowing them to impersonate legitimate users. Often this is the result of a session that remains open after the user has navigated away from the app or website. For example, if you logged into a company intranet site from your tablet and neglected to log out when you finished the task, by remaining open, a cybercriminal would be free to explore the website and other connected parts of your employer's network.

Unit No. - 3

Tools and Methods used in Cyber Crime

Proxy Server

- It is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers.
- A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.
- Proxies were invented to add structure and encapsulation to distributed systems.
- Today, most proxies are web proxies, facilitating access to content on the World Wide Web and providing anonymity.

A proxy server may reside on the user's local computer, or at various points between the user's computer and destination servers on the Internet.

- A proxy server that passes requests and responses unmodified is usually called a gateway or sometimes a tunneling proxy.
- A forward proxy is an Internet-facing proxy used to retrieve from

  a wide range of sources (in most cases anywhere on the Internet).
- A reverse proxy is usually an Internet-facing proxy used as a front-end to control and protect access to a server on a private network. A reverse proxy commonly also performs tasks such as load-balancing, authentication, decryption or caching.

Anonymizer

- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.
- It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.
- It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information.

There are many reasons for using anonymizers.

- Anonymizers help minimize risk.
- They can be used to prevent identity theft, or to protect search histories from public disclosure.
- Some countries apply heavy censorship on the internet. Anonymizers can help in allowing free access to all of the internet content, but cannot help against persecution for accessing the Anonymizer website itself.
- Furthermore, as information itself about Anonymizer websites are banned in these countries, users are wary that they may be falling into a government-set trap.
- Anonymizers are also used by people who wish to receive objective information with the growing target marketing on the internet and targeted information.

- An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable.
- It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet.

It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information

Phishing

- Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a genuine (legal) organization to ensnare individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.
- The information is then used to access important accounts and can result in identity theft and financial loss.
- Phishers frequently use emotions like fear, curiosity, urgency, and greed to force recipients to open attachments or click on links.
- Phishing attacks are designed to appear to come from legitimate (legal) companies and individuals.

Viruses-

- A computer virus is a program which can harm our device and files and infect them for no further use.
- When a virus program is executed, it replicates itself by modifying other computer programs and instead enters its own coding.
- This code infects a file or program and if it spreads massively, it may ultimately result in crashing of the device.
- Viruses can record keystrokes and screen data, and they may steal personal information and passwords to transmit back to the malware author.
- Particularly malicious viruses completely take over a computer and use it as a weapon against others.
- Viruses can record keystrokes and screen data, and they may steal personal information and passwords to transmit back to the malware author.
- Particularly malicious viruses completely take over a computer and use it as a weapon against others.

Worms-

- Computer worms are similar to viruses in that they replicate themselves and can inflict similar damage.
- Unlike viruses, which spread by infecting a host file, worms are freestanding programs that do not require a host program or human assistance to propagate.
- Worms don't change programs; instead, they replicate themselves over and over.
- They just eat resources to make the system down.

Keylogger -

- Keyloggers are a form of spyware where users are unaware their actions are being tracked.
- Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities.
- A keylogger is a tool that captures and records a user's keystrokes. It can record instant messages, email, passwords and any other information you type at any time using your keyboard.

- Keyloggers can be hardware or software.

Trojan -

- A Trojan horse is malicious software that is concealed as a useful host program.
- When the host program is run, the Trojan performs a harmful/unwanted action.
- A Trojan horse, often known as a Trojan, is malicious malware or software that appears to be legal yet has the ability to take control of your computer.
- A Trojan is a computer program that is designed to disturb, steal, or otherwise harm your data or network.

Backdoor Attack

- A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.
- A well-known backdoor example is called FinSpy. When installed on a system, it enables the attacker to download and execute files remotely on the system the moment it connects to the internet, irrespective of the system's physical location. It compromises overall system security.

Keyloggers

Keyloggers are a form of spyware where users are unaware their actions are being tracked. Keyloggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities.

Spyware is largely invisible software that gathers information about your computer use, including browsing. Key loggers are a form of spyware that capture every keystroke you type; they can send this information to remote servers, where log-in information--including your passwords--can be extracted and used.

A keylogger is a tool that captures and records a user's keystrokes. It can record instant messages, email, passwords and any other information you type at any time using your keyboard. Keyloggers can be hardware or software.

Spyware is any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge or permission. Spyware is a kind of malware that secretly gathers information about a person or organization and relays this data to other parties.

There are two common types of keyloggers. Software and Hardware keyloggers.

- Software Keyloggers.
- Hardware Keyloggers.
- Spear Phishing.
- Drive-by-Downloads.
- Trojan Horse.
- 2-Step Verification.
- Install Anti Malware Software.
- Use Key Encryption Software.

Spyware is mostly classified into four types: adware, system monitors, tracking including web tracking, and trojans; examples of other notorious types include digital rights management capabilities that "phone home", keyloggers, rootkits, and web beacons.

Keystroke logging, often called keylogging, is the practice of noting (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that such actions are being monitored.

Keystroke logger or keylogger is quicker and easier way of capturing the passwords and monitoring the victims' IT savvy behavior. It can be classified as software keylogger and hardware keylogger.

1. Software Keyloggers

Software keyloggers are software programs installed on the computer systems which usually are located between the OS and the keyboard hardware, and every keystroke is recorded. Software keyloggers are installed on a computer system by Trojans or viruses without the knowledge of the user. Cybercriminals always install such tools on the insecure computer systems available in public places and can obtain the required information about the victim very easily. A keylogger

usually consists of two files that get installed in the same directory: a dynamic link library (DLL) file and an EXEcutable (EXE) file that installs the DLL file and triggers it to work. DLL does all the recording of keystrokes.

2. Hardware Keyloggers

To install these keylogers, physical access to the computer system is required. Hardware keyloggers are small hardware devices. These are connected to the PC and/or to the keyboard and save every keystroke into a file or in the memory of the hardware device. Cybercriminals install such devices on ATM machines to capture ATM Cards'PINs. Each keypress on the keyboard of the ATM gets registered by these keyloggers These keyloggers look like an integrated part of such systems; hence, bank customers are unaware of their presence.

3. Antikeylogger

Antikeylogger is a tool that can detect the keylogger installed on the computer system and also can remove the tool.

Advantages of using antikeylogger are as follows:

- Firewalls cannot detect the installations of keyloggers on the systems; hence, antikeyloggers can detect installations of keylogger.
- This software does not require regular updates of signature bases to work effectively such as other antivirus and antispy programs if not updated, it does not serve the purpose, which makes the users at risk.
- Prevents Internet banking frauds. Passwords can be easily gained with the help of installing keyloggers.
- It prevents ID theft
- It secures E-Mail and instant messaging/chatting.

4. Spywares

Spyware is a type of malware, that is installed on computers which collects information about users without their knowledge. The presence of Spyware is typically hidden, from the user, it is secretly installed on the user's personal computer. Sometimes, however, Spywares such as keyloggers are installed by the owner of a shared, corporate or public computer on purpose to secretly monitor other users.

It is clearly understood from the term Spyware that it secretly monitors the user. The features and functions of such Spywares are beyond simple monitoring. Spyware programs collect personal information about the victim, such as the Internet surfing habits/patterns and websites visited. The Spyware can also redirect

Internet surfing activities by installing another stealth utility on the users' computer system. Spyware may also have an ability to change computer settings, which may result in slowing of the Internet connection speeds and slowing of response time that may result into user complaining about the Internet speed connection with Internet Service Providers (ISP).

To overcome the emergence of Spywares that proved to be troublesome for the normal user, anti-Spyware softwares are available in the market. Installation of anti-Spyware has become a common element nowadays from computer security practices perspective.

STEGANOGRAPHY

Steganography is the practice of hiding a secret message inside of (or even on top of) something that is not secret. It is a form of covert communication and can involve the use of any medium to hide messages. It's not a form of cryptography, because it doesn't involve scrambling data or using a key.

Steganography works by hiding information in a way that doesn't arouse suspicion. One of the most popular techniques is 'least significant bit (LSB) steganography. In this type of steganography, the information hider embeds the secret information in the least significant bits of a media file.

Steganography Examples

Playing an audio track backwards to reveal a secret message. Playing a video at a faster frame rate (FPS) to reveal a hidden image. Embedding a message in the red, green, or blue channel of an RGB image. Hiding information within a file header or metadata.

The purpose of steganography is covert communication—to hide the existence of a message from a third party. Knowledge of steganography is of increasing importance to individuals in the law enforcement, intelligence, and military communities.

SQL Injection

An SQL injection is a type of cyber-attack in which a hacker uses a piece of SQL (Structured Query Language) code to manipulate a database and gain access to potentially valuable information. ... Prime examples include notable attacks against Sony Pictures and Microsoft among others.

SQL injection (SQLi) is a type of cyberattack against web applications that use SQL databases such as IBM Db2, Oracle, MySQL, and MariaDB. As the name suggests, the attack involves the injection of malicious SQL statements to interfere with the queries sent by a web application to its database.

Using SQL injection, a hacker will try to enter a specifically crafted SQL commands into a form field instead of the expected information. The intent is to secure a response from the database that will help the hacker understand the database construction, such as table names.

DoS and DDoS Attack

A denial-of-service (DoS) attack floods a server with traffic, making a website or resource unavailable. A distributed denial-of-service (DDoS) attack is a DoS attack that uses multiple computers or machines to flood a targeted resource.

A DoS attack is a denial of service attack where a computer is used to flood a server with TCP and UDP packets. A DDoS attack is where multiple systems target a single system with a DoS attack. The targeted network is then bombarded with packets from multiple locations. All DDoS = DoS but not all DoS = DDoS

What types of resources are targeted by such DoS attacks? Prevents the authorized use of networks, systems, or applications with the help of resources such as memory, bandwidth, CPU, system resources, network connectivity, and disk space.

There are three main types of DoS attacks:

- Application-layer Flood. In this attack type, an attacker simply floods the service with requests from a spoofed IP address in an attempt to slow or crash the service, illustrated in . ...
- Distributed Denial of Service Attacks (DDoS) ...
- Unintended Denial of Service Attacks.
    - . DOS Attack :
      A DOS attack is a denial of service attack, in this attack a computer sends massive amount of traffic to a victims computer and shuts it down.Dos attack is a online attack which is used to make the website unavailable for its users when done on a website. This attack make the server of a website down which is connected to internet by sending a large number of traffic to it.
    - **2.** DDOS Attack **:**
      In ddos attack means distributed denial of service in this attack dos attacks are done from many different locations using many systems.
    - Attention reader! Don’t stop learning now. Get hold of all the important CS Theory concepts for SDE interviews with the **CS Theory Course** at a student-friendly price and become industry ready.

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victims system.	In DDos multiple system attacks the victims system..
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple location.
Dos attack is slower as compared to ddos.	DDos attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and

DOS	DDOS
	attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDos attack Bots are used to attack at the same time.
DOS Attcaks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks

Password Cracking

Password cracking is the process of attempting to gain Unauthorized access to restricted systems using common passwords or algorithms that guess passwords. In other words, it's an art of obtaining the correct password that gives access to a system protected by an authentication method.

Password cracking refers to various measures used to discover computer passwords. This is usually accomplished by recovering passwords from data stored in, or transported from, a computer system. Password cracking is done by either repeatedly guessing the password, usually through a computer algorithm in which the computer tries numerous combinations until the password is successfully discovered.

Password cracking can be done for several reasons, but the most malicious reason is in order to gain unauthorized access to a computer without the computer owner's awareness. This results in cybercrime such as stealing passwords for the purpose of accessing banking information.

Other, nonmalicious, reasons for password cracking occur when someone has misplaced or forgotten a password. Another example of nonmalicious password cracking may take place if a system

Chapter No. - 4

Cyber Crime and Cybe Security – The legal Perspective

Cybercrime and legal landscape around the world

Cybercrime is a crime done with the misuse of information technology for unauthorized or illegal access, electronic fraud; like deletion, alteration, interception, concealment of data, forgery etc. Cybercrime is an international crime as it has been affected by the worldwide revolution in information and communication

Cybercrime is a growing concern to countries at all levels of developments and affects both, buyers and sellers.

While 154 countries (79 per cent) have enacted cybercrime legislation, the pattern varies by region: Europe has the highest adoption rate (93 per cent) and Asia and the Pacific the lowest (55 per cent).

The evolving cybercrime landscape and resulting skills gaps are a significant challenge for law enforcement agencies and prosecutors, especially for cross-border enforcement.

List of Top 3 Countries with the highest rate of Cybercrime (source: BusinessWeek/Symantec)

1. United States of America. Share of malicious computer activity: 23%
2. China. Share of malicious computer activity: 9%
3. Germany. Share of malicious computer activity: 6%

China–United States cooperation is one of the most striking progress recently, because they are the top two source countries of cybercrime.

Need of Cyber Law

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-

governance and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum.

In today's highly digitalized world, almost everyone is affected by cyber law. For example:

- Almost all transactions in shares are in demat form.
- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit/debit cards for shopping.
- Most people are using email, phones and SMS messages for communication.
- Even in "non-cyber crime" cases, important evidence is found in computers/cell phones eg: in cases of murder, divorce, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.
- Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common.
- Digital signatures and e-contracts are fast replacing conventional method of transacting business.

Technology is never a disputed issue but for whom and at what cost has been the issue in the ambit of governance. The cyber revolution holds the promise of quickly reaching the masses as opposed to the earlier technologies, which had a trickle-down effect. Such a promise and potential can only be realized with an appropriate legal regime based on a given socio-economic matrix.

Need for Cyber Law in India

Cyber-law is important in a country like India where the internet is used to a large extent. The law is enacted to save people and organizations from cybercrime and other internet-related crimes. It protects the privacy of every individual and

organization. Before the enactment of Cyber-law, no specific law existed in India to deal with cybercrime. As per rules and regulations of the Cyber-law, a person who commits cybercrime is liable to get punishment. If anyone violates and breaks the provisions of the law, then it allows another person or organization to take legal action against that person.

Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.

- The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on17th October 2000.

Information Technology Act, 2000

Enacted by	Parliament of India
Enacted	9 June 2000
Assented to	9 June 2000
Signed	9 May 2000

The Information Technology Act, 2000 provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.

Objectives of the Act

The Information Technology Act, 2000 provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.

This also involves the use of alternatives to a paper-based method of communication and information storage to facilitate the electronic filing of documents with the Government agencies.

Further, this act amended the Indian Penal Code 1860, the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891, and the Reserve Bank of India Act 1934.

The objectives of the Act are as follows:

i. Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.

ii. Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication

iii. Facilitate the electronic filing of documents with Government agencies and also departments

iv. Facilitate the electronic storage of data

v. Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions

vi. Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Features of the Information Technology Act, 2000

i. All electronic contracts made through secure electronic channels are legally valid.
ii. Legal recognition for digital signatures.
iii. Security measures for electronic records and also digital signatures are in place
iv. A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized

v. Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.
vi. An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court
vii. Digital Signatures will use an asymmetric cryptosystem and also a hash function
viii. Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.
ix. The Act applies to offences or contraventions committed outside India
x. Senior police officers and other officers can enter any public place and search and arrest without warrant
xi. Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

Amendments in Indian IT act

A major amendment was made in 2008. It introduced Section 66A which penalized sending "offensive messages". It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource".

According to a recent Ministry of Communication & Information Technology news release, the Information Technology (Amendment) Act, 2008 has come into effect in India from October 27, 2009. The Act has received mixed responses. While some are happy about the Indian government's attempt to curtail usage of the internet for terrorist activities, others feel that the surveillance powers received by government are prone to misuse.

The Information Technology (Amendment) 2008 Act has been debated since it was passed by the Indian Parliament in December 2008, about a month after the terrorist attacks in Mumbai. Certain sections like Section 69 which provides

authority to the Indian government for interception, monitoring, decryption and blocking electronic data traffic have come under major criticism. "The Act has provided Indian government with the power of surveillance, monitoring and blocking data traffic. The new powers under the amendment act tend to give Indian government a texture and color of being a surveillance state,"

Cyber Crime and Punishment in India:-

Penalties under Cyber Crimes:-

a) Section 43 and 66 –

Section 43 and 66 of the IT Act punishes a person committing data theft, transmitting virus into a system, hacking, destroying data, or denying access to the network to an authorized person with maximum imprisonment up to 3 years or a fine of rupees 5 lacs or both. At the same time data theft is also punishable under Section 378 and Section 424 of IPC with maximum imprisonment of 3 years or fine or both; and imprisonment of 2 years or fine or both respectively. Denying access to an authorized person or damaging a computer system is penalized under Section 426 of IPC with imprisonment of up to 3 months or fine or both.

66E - Tampering with computer source documents is a punishable offence under Section 65 of the IT Act. Section 66E provides the punishment for violation of privacy. It states that if any person captures, publishes, or distributes an image of a private area of a person without his/her consent has committed a breach of privacy and is punishable with imprisonment up to 3 years or a fine up to 2 lacs or both.

66F

Section 66F covers a crucial matter which is cyber terrorism and prescribes punishment for the same. It provides the acts which constitute cyber terrorism like denial of access or penetrating through a network or transmitting virus/malware utilizing which he is likely to cause death or injury to any person, which is all done with the purpose to threat the integrity, sovereignty, unity, and security of India or create terror in the minds of its citizen.

66B and 66 C

Section 66B of the IT Act and Section 411 of IPC deal with the offense of dishonestly receiving stolen computer resources or devices. Section 66C of the IT Act prescribes punishment for identity theft and states that any person who uses the identity credentials of a person for fraud or in a dishonest manner is liable for punishment with imprisonment up to 3 years and a fine up to Rupees 3 lacs. Cheating by personation using a computer resource is punishable under Section 66D of the IT Act. Similar provisions for these offenses are given under IPC under Section 419, 463, 465, and 468. IT Act not only punishes persons but corporate as well if they fail to implement and maintain a reasonable and diligent mechanism to protect the sensitive data of any person in their possession. Such a body corporate is liable to pay compensation to the aggrieved person who has suffered a loss due to the negligence of the corporation.

Apart from the provisions for punishment, the IT Act also empowers the Central Government to issue directions to block access of any information on an intermediary or computer resource for the public, if it feels necessary in the interest of the State. It can also intercept, decrypt or monitor such information.

Date – 10 Dec 2021

Cyber Crime and Punishment in India:-

The IT Act 2000 w1as mainly to ensure legal recognition of e-commerce within India. Due to this most provisions are mainly concerned with establishing digital certification processes within the country. Cybercrime as a term was not defined in the act. It only delved with few instances of computer-related crimes. These acts as defined in Chapter XI of the Act are:

1. **Section 43**– Illegal access, the introduction of the virus, denial of services, causing damage and manipulating computer accounts.
2. **Section 65**– Tampering, destroying and concealing computer code.
3. **Section 66**– Acts of hacking leading to wrongful loss or damage.
4. **Section 67**– Acts related to publishing, transmission or causing publication of obscene/ lascivious in nature.

Punishment in Section 65 and 66 is three years or fine up to two lakh rupees or both. For Section 67 the first time offenders can be punished up to 5 years with a fine up to one lakhs of rupees. A subsequent offense can lead to ten years of punishment and fine up to two lakhs of rupees.

Salient Features Of Information Technology Amendment Act

Information Technology Act Amendment which came into force after Presidential assent in February 2009 has the following salient features:

- **Liability of body corporate towards Sensitive Personal Data-**New amendment was brought in changes in Section 43 of IT Act 2000 in which for the first time anybody corporate which deals with sensitive personal information does not have adequate controls resulting in wrongful loss or wrongful gain to any person is liable to pay damages to that person to the tune of five crores.
- **Introduction of virus, manipulating accounts, denial of services etc made punishable-**Section 66 has been amended to include offenses punishable as per section 43 which has also been amended to include offenses as listed above; punishment may lead to imprisonment which may extend to three years or with fine which may extend to five lakh rupees or with both. This is a change from an earlier position where the introduction of

the virus, manipulating someone's account has been made punishable with imprisonment for the first time.

- **Phishing and Spam-** While this has not been mentioned specifically but this can be interpreted in the provisions mentioned here in Section 66 A. Through this section sending of menacing (frightening), annoying messages and also misleading information about the origin of the message has become punishable with imprisonment up to three years and fine.
- **Stolen Computer resource or communication device –** Newly added **Section 66B** has been introduced to tackle with acts of dishonestly receiving and retaining any stolen computer resource. This has also been made punishable with three years or fine of one lakh rupees or both.
- **Misuse of Digital Signature-Section 66C.** Dishonest use of somebody else's digital signature has been made punishable with imprisonment which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.
- **Cheating-**Cheating using computer resource has been made punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee (**Section 66D**).
- **Cyber terrorism-** The newly introduced **Section 66F** talks about acts of cyber terror which threatens the unity, integrity or sovereignty of India or strike terror in the people or any section of the people include
- **Child Pornography**– Newly introduced **Section 67 B** attempts to address the issue of child pornography. Through this section it has made the publication or transmission of material in any electronic form which depicts children engaged in sexually explicit act or conduct, anyone who creates, facilitates or records these acts and images punishable with imprisonment of

five years and fine which may extend up to ten lakhs in first offence and seven years and fine of ten lakhs on subsequent offence.

Digital Signature

A digital signature is a way to identify yourself online. Just like passports, driving licenses, and PAN cards allow you to prove your identity offline, digital signatures let you prove your identity online. To do this, you need a digital signature certificate and that lets you sign documents digitally.

Digital signatures work by proving that a digital message or document was not modified—intentionally or unintentionally—from the time it was signed. Digital signatures do this by generating a unique hash of the message or document and encrypting it using the sender's private key.

You can use digital signature certificates to e-file your income tax returns, for a Registrar of Companies e-filing, online auctions (such as e-tenders), and to sign documents such as PDFs

Digital signatures were given legal status in India, by Information Technology (IT ACT 2000) in the year 2000. It granted e-signatures on electronic documents, the same legal status as the handwritten signatures on physical documents.

The IT Act, 2000 introduced the concept of digital signatures under Sec. 2(1)(p) as authentication of any electronic record by a subscriber, i.e., a person in whose name the Digital Signature Certificate' (DSC) is issued,by means of an electronic method or procedure in accordance with the provisions of Sec. 3

Chapter No. - 5

Cyber Forensics

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The terms digital forensics and cyber forensics are often used as synonyms for computer forensics.

What Is Cyber Forensics?

Cyber forensics in the simplest words means investigating, gathering, and analyzing information from a computer device which can then be transformed into hardware proof to be presented in the court regarding the crime in question.

The purpose of cyber forensics is the forensically-sound investigation of digital media with the intent to: identify, preserve, recover, analyze, present facts, and opinions; concerning the digital information.

Digital Forensics

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.

Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

Why do we need digital forensics?

Digital forensics can help identify what was stolen, and help trace whether the information was copied or distributed. Some hackers may intentionally destroy data in order to harm their targets. In other cases, valuable data may be accidentally damaged due to interference from hackers or the software that hackers use.

What is the Purpose of Digital Forensics?

The most common use of digital forensics is to support or refuse a hypothesis in a criminal or civil court.

History of Digital forensics

Here, are important landmarks from the history of Digital Forensics:

- Hans Gross (1847 -1915): First use of scientific study to head criminal investigations
- FBI (1932): Set up a lab to offer forensics services to all field agents and other law authorities across the USA.
- In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- Francis Galton (1982 – 1911): Conducted first recorded study of fingerprints
- In 1992, the term Computer Forensics was used in academic literature.
- 1995 International Organization on Computer Evidence (IOCE) was formed.
- In 2000, the First FBI Regional Computer Forensic Laboratory established.
- In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called "Best practices for Computer Forensics".
- In 2010, Simson Garfinkel identified issues facing digital investigations.

Types of Digital Forensics

Three types of digital forensics are:

Disk Forensics:

It deals with extracting data from storage media by searching active, modified, or deleted files.

Network Forensics:

It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

Wireless Forensics:

It is a division of network forensics. The main aim of wireless forensics is to offers the tools need to collect and analyze the data from wireless network traffic.

Database Forensics:

It is a branch of digital forensics relating to the study and examination of databases and their related metadata.

Malware Forensics:

This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

Email Forensics

Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

Memory Forensics:

It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

Mobile Phone Forensics:

It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

Need of computer forensics

Here are the essential objectives of using Computer forensics:

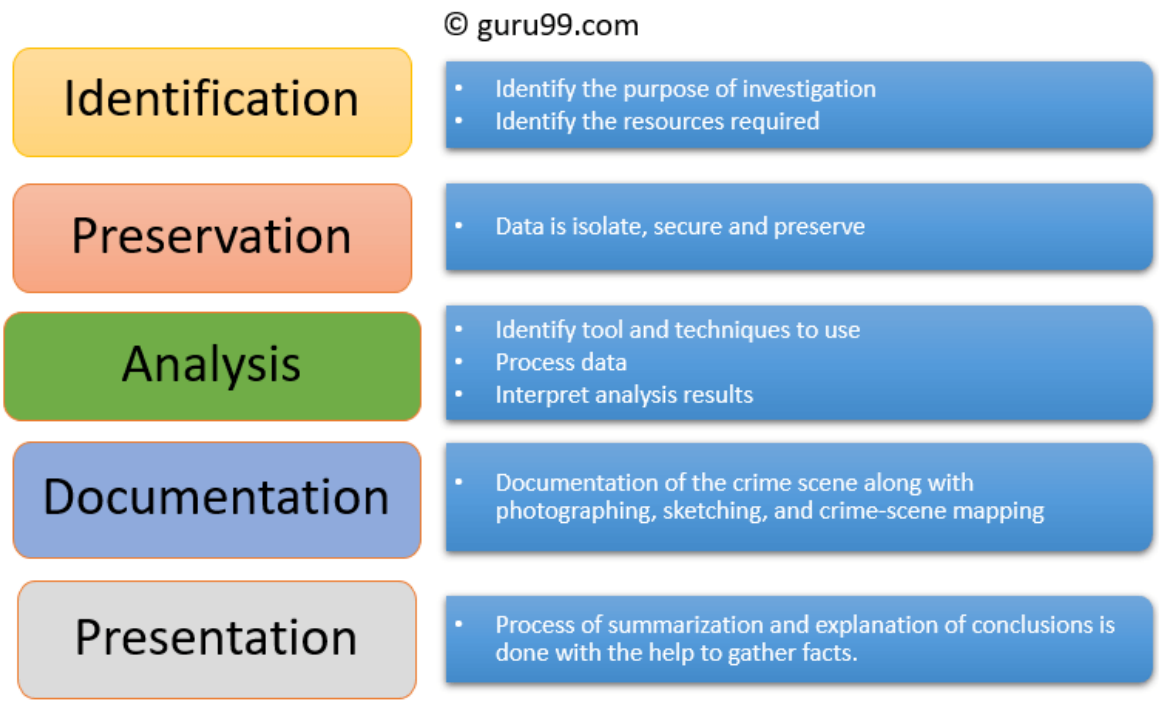
- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
- It helps to postulate the motive behind the crime and identity of the main culprit.

- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.
- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim
- Producing a computer forensic report which offers a complete report on the investigation process.
- Preserving the evidence by following the chain of custody.

Process of Digital forensics

Digital forensics entails the following steps:

- Identification
- Preservation
- Analysis
- Documentation
- Presentation



Identification

It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).

Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

Preservation

In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

Analysis

In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

Documentation

In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

Presentation

In this last step, the process of summarization and explanation of conclusions is done.

However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

Example Uses of Digital Forensics

In recent time, commercial organizations have used digital forensics in following a type of cases:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Inappropriate use of the Internet and email in the workplace

- Forgeries related matters

Advantages of Digital forensics

Here, are pros/benefits of Digital forensics

- To ensure the integrity of the computer system.
- To produce evidence in the court, which can lead to the punishment of the culprit (criminal).
- It helps the companies to capture important information if their computer systems or networks are compromised.
- Efficiently tracks down cybercriminals from anywhere in the world.
- Helps to protect the organization's money and valuable time.
- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

Disadvantages of Digital Forensics

Here, are major drawbacks of using Digital Forensic

- Digital evidence accepted into court. However, it is must be proved that there is no tampering
- Producing electronic records and storing them is an extremely costly affair
- Legal practitioners must have extensive computer knowledge
- Need to produce authentic and convincing evidence
- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.
- Lack of technical knowledge by the investigating officer might not offer the desired result

Forensic Analysis of Email

Email forensics is the study of source and content of email as evidence to identify the actual sender and recipient of a message along with some other information such as date/time of transmission and intention of sender. It involves investigating metadata, port scanning as well as keyword searching.

Some of the common techniques which can be used for email forensic investigation are

- Header Analysis
- Server investigation
- Network Device Investigation
- Sender Mailer Fingerprints
- Software Embedded Identifiers

Aid4Mail Forensic is e-mail investigation software for forensic analysis, e-discovery, and litigation support. it's an e-mail migration and conversion tool, which supports various mail formats including Outlook (PST, MSG files), Windows Live Mail, Thunderbird, Eudora, and mbox.

Digital Evidence and Cyber Forensics

Digital evidence can be any sort of digital file from an electronic source. This includes email, text messages, instant messages, files and documents extracted from hard drives, electronic financial transactions, audio files, video files.

Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events.

Digital Forensic Life Cycle

There are many type of Cyber crimes taking place in the digital world, it is important for the investigator to collect, analyze, store and present the evidence in such a manner that court will believe in such digital evidences and give appropriate punishment to the Cyber criminal.

The steps in a digital forensics follow an life cycle approach and consists of following steps

- Requirement Analysis – This preliminary step we should check our technological feasibility. Then investigator has to determine how we can protect the stored data from misuse and tampering that is known as chain of custody, that means investigator has to prove that nobody has alter or tampered the evidential data after it has been collected by him.
- Retrieval of Data – It is most crucial to identify the source and destination media. Generally the suspected computer or server storage is worked as a source media and data available on that is taken on to the other media for further investigation. So the investigator should has knowledge of different kind of storage devices, and how the data of that storage device is taken in to own storage devices without loss and alteration of the data, which can be further use as legal evidence in the court.
- Reliability – It is also vital to determine that, how much authenticated the data is? Therefore, the image we have created must be identical to original data. To check the originality of the data we should create the hashes of original data before we create the image. Immediately after creating the image, create the hash of image data. These two hashes must be match and if

they don't match then it shows something wrong happened with the imaging process and thus data is unreliable. That is suggested to use any complex algorithm to build the hash of the data like MD5 or SHA-1, which is very difficult to spoof.

- Review of Evidence – After getting all the data from the suspected resources it is most important things that how we get the data that can consider as evidence in the court of law. We require proper chain of evidence that can't be challenge from the opposing party and that is only possible if all the evidence is relevant to the case. After collecting the large set of information it is important to extract the evidence data from media, therefore some tools like Forensic Tool Kit and EnCase are used for the analysis of collected information from the suspected computer. For Linux environment Coronor's Toolkit is used for evidence collection and analysis. The analysis of the physical media layer of abstraction, which translates a custom storage layout and contents to a standard interface, IDE or SCSI for example. The boundary layer is the bytes of the media. Examples include a hard disk, compact flash, and memory chips. The analysis of this layer includes processing the custom layout and even recovering deleted data after it has been overwritten
- Representation of Evidence – Here due to lots of uncertainty in the validity and acceptability in the digital evidence it is equally important to represent the evidence in such a form that can be understood by the court. For many types of digital data records or logging data for processes it is obvious that they can potentially be relevant as digital evidence in the case of disputes. But sometimes court will not accept the same data as valid evidence because of the improper representation of the digital evidence.

- Repository of Data – After the successful investigation it is also equally important that how you can archive the data in repository for future use. First important thing is to determine what are the data that can be useful for future use and how long we have to store that data. So, in the legal procedure, the completed case may be re-open in future or opponent may go for appeal or revision in the higher court. Since it is very difficult to store all the data related to the case in the repository, investigator has to find that; what are the important datasets that can be useful for the future use and only those data is stored in the repository. Therefore, the removal of the data from the repository are depend on the likelihood of the case will be appealed.

Challenges in Computer Forensics

High speed and volumes

Issues related to acquiring, storing, and processing large amounts of data for forensic purposes have been causing problems for at least a decade, and are now exacerbated by the availability and widespread marketing of digital information.

“The availability of gigabit class links and multimedia-rich contents accounts for an explosion in the volume of data to be stored and processed for collecting clues or detecting incidents. This is of particular relevance in the case of live network analysis, as the investigator might not be able to capture and store all the necessary traffic,”

Explosion of complexity

Evidence is no longer confined within a single host but, rather, is scattered among different physical or virtual locations, such as online social networks, cloud resources, and personal network–attached storage units. For this reason, more expertise, tools, and time are needed to completely and correctly reconstruct evidence. Partially automating some tasks has been highly criticized by the digital investigation community, because it could quickly deteriorate the quality of the investigation.

"The technological advances in and proliferation of novel services account for a dramatic increase in the complexity that forensics professionals must manage," say the authors.

Development of standards

"Despite technological advances, files are still the most popular digital artifacts to be collected, categorized, and analyzed. Thus, the research community has tried to agree on standard formats, schema, and ontologies—but without much success," the authors say.

They add that investigations of cutting-edge cybercrimes might require processing information in a collaborative manner or using outsourced storage and computation. Therefore, a core step for the digital forensics community will be the development of proper standard formats and abstractions.

Privacy-preserving investigations

Nowadays, people bring into cyberspace many aspects of their lives, primarily through online social networks or social media sites. Unfortunately, collecting

information to reconstruct and locate an attack can severely violate users' privacy and is linked to other hurdles when cloud computing is involved.

Legitimacy

Modern infrastructures are becoming complex and virtualized, often shifting their complexity at the border (such as in fog computing) or delegating some duties to third parties (such as in platform-as-a-service frameworks).

Thus, say the authors, "an important challenge for modern digital forensics will be executing investigations legally, for instance, without violating laws in borderless scenarios."

Rise of antiforensics techniques

Defensive measures encompass encryption, obfuscation, and cloaking techniques, including information hiding.

Cooperation among international jurisdictions notwithstanding, investigating cybercrime and collecting evidence is essential in building airtight cases for law enforcement. For that, security experts need the best tools to investigate.

Unit No – 6

Cyber Security : Organizational Implications

Cost of cyber crime and IPR issues

Nowadays, cyber crimes do not only restrict itself to fraud, cyber bullying, identity thefts but also infringement (violation) of copyrights and trademarks of various business and other organizations. Intellectual Property Rights (IPR) and Cyber Laws cannot be separated, and online content must be protected.

Online content needs to be protected and hence Intellectual Property Rights and Cyber laws cannot be separated. In cyberspace, sometimes one person makes a profit by using another person's creation without the owner's consent. This is a violation of privacy, and it is protected by IPR.

What are web threats for organizations

Threats refer to negative influences which not only hamper the productivity of an organization but also bring a bad name to it.

A web threat is any threat that uses the World Wide Web to facilitate cybercrime. Web threats use multiple types of malware and fraud, all of which utilize HTTP , but may also employ other protocols and components, such as links in email or malware attachments or on servers that access the Web.

Web-based threats, or online threats, are a category of cyber security risks that may cause an undesirable event or action via the internet. Web threats are made possible by end-user vulnerabilities, web service developers/operators, or web services themselves.

Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential information/data, theft of network resources, damaged brand/personal reputation, and erosion of consumer confidence in e-commerce and online banking.

Cloud security challenges

Cloud security breaches and incidents still occur even as security technologies improve and service providers fix their networks. People can attack network hosts and web apps as fast as they can be refreshed. Cloud administrators should test

their environments and have the latest security audits and reports. Take care when adopting new technologies, such as AI and machine learning, which use many data sources and therefore broaden the range for potential attacks.

Security management

The major public cloud vendors continue to invest in their services and improve cloud security, such as their ability to fend off distributed denial-of-service attacks. Some experts say that today's cloud attacks are far less shocking than on-premises ones because cloud attacks are generally limited to a single misconfigured service, whereas a local attack might devastate an entire infrastructure.

Nevertheless, IT shops must remain attentive to guard against security threats. Google, AWS and Microsoft, among others, do not take full responsibility to keep cloud data safe. Cloud users must understand their shared responsibility in the cloud to protect their data. Cloud security best practices include configuration

management, automated security updates on SaaS, and improved logging and access management. Cloud configurations today are more standard, and standard configurations are easier to secure.

Social Media Marking

Social media marketing is the use of social media platforms to connect with your audience to build your brand, increase sales, and drive website traffic.

The term social media marketing (SMM) refers to the use of social media and social networks to market a company's products and services. Social media marketing provides companies with a way to engage with existing customers and reach new ones while allowing them to promote their desired culture, mission, or tone. Social media marketing has purpose-built data analytics tools that allow marketers to track the success of their efforts.

Social Media Marketing Examples

- Ipsy (3.1m Followers) – Content that makes a connection.
- Loot Crate (714k Followers) – Know your audience.
- Top Vintage (149k Followers) – Love your followers and they'll love you back.

Advantages and Disadvantages of Social Media Marketing (SMM)

Social media marketing campaigns have the advantage of appealing to a broad audience at once. For example, a campaign may appeal to current and prospective customers, employees, bloggers, the media, the general public, and other stakeholders, such as third-party reviewers or trade groups.

But these campaigns can also create obstacles that companies may not have had to deal with otherwise. For example, a viral video claiming that a company's product causes consumers to become ill must be addressed by the company, regardless of whether the claim is true or false. Even if a company can set the message straight, consumers may be less likely to purchase from the company in the future.

Incident Handling

Specifically, an incident response process is a collection of procedures aimed at identifying, investigating and responding to potential security incidents in a way that minimizes impact and supports rapid recovery

Most major incidents can be considered to have four stages:

- Initial response
- Consolidation phase
- Recovery phase
- Restoration of normality.

Security incident management is the process of identifying, managing, recording and analyzing security threats or incidents in real-time. A security incident can be anything from an active threat to an attempted intrusion to a successful compromise or data breach.

Organizational guidelines for internet usage

An internet usage policy is a document used by employers to communicate the acceptable use of technology in the workplace. The document provides rules and guidelines surrounding the organization's expectations of their employees when using the internet and other company-provided devices.

It is important for a business to have an internet usage policy in place that sets and establishes guidelines for employees to follow while using the internet at work. Such a policy should address issues including preventing software piracy, decreasing cyber security threats through malware and spyware, deterring misuse of employer-owned computers and network, and increasing employee productivity.

An internet usage policy should include the following:

- A notification that all aspects of employee use of company-owned equipment can be monitored at any time and without notice.
- A statement of the reasons for the policy.
- A description of what constitutes improper use of employer-owned equipment.
- A description of what constitutes proper employee computer use.
- A statement prohibiting unauthorized encryption of information such as email on business computers.

- A statement notifying employees that violating the policy can lead to disciplinary action.
- A zero-tolerance policy for communication that is offensive, discriminatory, or constitutes harassment.
- Depending on the nature of an employer's business, a statement limiting the use of the internet.

Organizational guidelines for safe computing

1. Keep mobile devices and laptops safe
2. Ensure up-to-date security protection is in place
3. Ensure Windows is updated
4. Limit the use of public WiFi, especially when accessing password-protected resources
5. If you share a computer with others in your household, make sure you log out of any resources you are logged in to and close the browser. This ensures that your session is fully closed, and no one else can log in as you.

Following are some practices to do safe computing:

- Keep Mobile devices and laptops safe

When leaving your computer, lock the screen with a password to safeguard the data on your computer. Also, always lock your doors when leaving the computer unattended.

- Never leave your devices or laptop in the car. It's a best practice to keep work laptops and devices on your person at all times while on the road. The

trunk of your car is not any safer. There may be criminals watching to take advantage of this situation.

- Don't allow family members to use your work devices.
    - If you think of your laptop and mobile devices as work-only assets, it makes it easier to control access to sensitive data. For remote workers, treat your work laptop, mobile device and sensitive data as if you were sitting in a physical office location. This will help you continuously associate your actions with a security-first and data-aware mentality in mind. For example, in a physical office location, your child wouldn't be able to use your work mobile device for games or movies.

- Invest in an antivirus software.
    - If you use your personal laptop for work, it's important to keep your system protected. Scan all attachments that are sent to you. Viruses can lurk in emails from friends and family. If you receive a link in an email from a trusted source, hover over the link using your mouse and look in the bottom bar of your web browser to reveal the true URL and validate that the link is legitimate. This will ensure that you know where you are going on the Internet, and whether or not you want to go there.

- Keep your computer with all the software updated.
    - It is essential the use anti-virus software. Most anti-virus software gives the user the ability to do automatic updates.
    - Ensure that your operating system (e.g W10/OS X) is continuously updated and patched. It is also important to keep other software on

your computer updated. Software updates often include essential bug fixes and security features that address existing vulnerabilities.

- Make sure that the firewall on your computer is enabled. This will help to keep unauthorized people from snooping around your computer when it's connected to the Internet.

- Keep Work Data on Work Computers.
  - Introducing a personal computer to a work network, even remotely, put that networks at risk, and yourself at risk, accepting the potential liability of extensive damages though violations of policy, practices or both. Use remote environment such as Office 365, so you could work online and avoid downloading or synching files or emails to a personal device.

- Minimize storage of sensitive information.
  - Delete sensitive information whenever you can. Keep it off of your workstation, laptop computer, and other electronic devices if at all possible.
  - Don't keep sensitive information or your only copy of critical data, projects, files, etc. on portable or mobile devices (such as laptop computers, tablets, phones, memory sticks, CDs/DVDs, etc.) unless they are properly protected. These items are extra vulnerable to theft or loss.

- Avoid public Wi-Fi; if necessary, use personal hotspots or some way to encrypt your web connection.
  - Public Wi-Fi introduces significant security risk and should be avoided if possible. If you need to access the internet from a public

Wi-Fi location, you have two essential problems to solve. First, other people have access to that network and, without a firewall between you and them, threat actors can pound away at your computer from across the room. Second, any interested observers on either the current network or any other public networks your data hits between you and your workplace can monitor your traffic as it goes by. It is important to find a way to protect your PC and encrypt your traffic.

- For some use cases, you can also set up encrypted remote connections into a remote desktop or other individual server. Many of these connection types (RDP, HTTPS, SSH) include encryption as part of their service direction and do not require an additional VPN or other encryption service to secure the data in-transit.
- One option is to use a personal hotspot from a dedicated device or your phone. Using a hot spot does eliminate the problem of getting hacked by people on the same public Wi-Fi.
- For many remote access applications, you should use a VPN. VPNs provide a flexible connection to connect to different services (web pages, email, a SQL server, etc.) and can protect your traffic. Keep in mind that VPN services provided for privacy purposes only protect the data to and from the VPN provider, not to the destination so are not suitable for protecting remote access.

- Avoid surfing websites that you don't already know
  - Browsers are quickly becoming one of the larger vulnerabilities in computing. Adware and spyware are written specifically to exploit Chrome, Internet Explorer and Firefox. So try and stick with the websites you trust.

- Only Download files legally.
    - Along with the possibility of significant legal penalties, downloading files from peer-to-peer networks can be harmful to your machine. These downloaded files are sometimes riddled with viruses and spyware.

- Keep personal information safe.
    - Reduce your risk of identity theft. Never share your personal information via email, no matter how official the email looks. Official business that requires personal information should not happen via unsecured email.
    - Also, limit information on social media sites. For many people, birth dates, anniversaries, addresses, phone numbers, and a lot of other personal information can be found on social media sites. Protect yourself from identity theft and other scams by limiting what information you disclose online and who can see that information.

Organizational guidelines for computer usage policy

A computer usage policy is a document that provides employees with guidelines on how to appropriately use company equipment and the internet on your work computer network. This kind of policy can minimize the risk of computer misuse – whether in the university library or a business office.

With such a policy, employees will be aware that browsing specific sites, downloading certain files, and using the computer system for anything other than business purposes is prohibited. It'll also highlight how violation of the policy can lead to termination of employment and other consequences.

This way, you protect your business from various risks like losing or leaking important information and computer files or getting your computers infected with malware.

However, businesses aren't the *only ones* who benefit from such a policy.

1. Prevents Piracy and Security Issues

About 92% of computers with pirated software have malware like Trojan horses, viruses, and worms.

Additionally, if your employees download pirated files or software, your company will be liable and have to pay fines as hefty as $150,000 for every instance of software and other resource piracy.

When you have well-defined rules that prohibit the usage of unlicensed or pirated programs, you can minimize the risk of running into serious security and legal issues like those mentioned above.

2. Minimizes Computer and Network Misuse

There are many ways in which your employees can misuse your computer and information resources.

You can prohibit activities like:

- **Hacking:** Employees using your computer system to gain unauthorized access to data, other computer networks, or user logins.
- **Data misuse:** Illegally revealing or transferring the company's data to personal devices.
- **Copyright infringement:** Copying of intellectual property (software, movies, books) and distributing them on the internet without copyright holder permission.
- **Identity and financial abuses:** Financial frauds and handling stolen credit card information.
- **Cryptocurrency mining:** Using your computer resources and power to mine bitcoins and other cryptocurrencies.
- **Using excessive network bandwidth:** Downloading unnecessary files that might result in bandwidth loss.

3. Helps You Address Employee Privacy Concerns

Privacy-related laws and monitoring rights might differ according to country and state.

That's why it's important to create a straightforward policy about the degree of privacy your employees should expect and your company's monitoring rights in the workplace.

Most employees expect to have personal privacy while working on company-owned computers.

However, according to the *Electronic Communications Privacy Act of 1986,* an employer can monitor employee activity on three occasions:

- **Business exception:** An employer can intercept employee communication when transmitted on company-owned devices during the ordinary course of business.

- **Consent exception:** An employer can monitor communication activities as long as at least one individual agrees.

- **Service provider exception:** An employer can monitor communication on the company's communication system channels. These include email use, voicemail, and other communication software.

Emphasize in the policy that the computers are a company asset and not a device on which they can conduct personal activities.

Including such aspects in your computer usage policy can help your employees understand what expectation of privacy and monitoring they should have, and help them stay away from unproductive internet activities.

What Should You Cover in Your Computer Usage Policy?

A typical computer usage policy structure includes:

1. Overview

This is the introduction to the document. State your company's name and briefly mention the reasons for creating a policy.

2. Scope

State briefly what this document will include – and the people, facilities, and equipment it applies to.

3. Purpose

When you state the purpose of the policy, your employees won't feel like their privacy is aimlessly infringed.

Mention the most important reasons for creating a policy.

Phrase it in a way that your employees can see how this policy will help both the organization and them to be better at their job.

4. Policy

The policy itself can vary depending on your industry and the type of business you're running. But aim to include the following sections which you can customize depending on your needs:

A. A Blanket Statement

Even though you'll have lots of specifics on how your employees should conduct certain procedures, try to include a blanket statement.

This statement should state that your employees can expect to be monitored when using work computers and the business network.

This way, you'll make it clear that they should not expect personal use privacy while using company equipment.

B. What is Appropriate Employee Computer and Internet Usage?

Describe what's included in proper employee computer use and internet access.

This section is specific and should be customized to the nature of your business. For example, many companies prohibit using social media during work hours. However, if you're a social media marketing agency, this isn't feasible.

In this case, you have to specify what their job duties are and the approved activities to carry out those duties. Also, clarify their level of authorization as computer users and what the acceptable use of these communication platforms is.

C. What is Inappropriate Employee Computer and Internet Usage?

In this section, try to answer these questions:

- Which activities are considered unauthorized?
- When are employees prone to abuse their access to confidential information?
- In what instances will employees have to be denied their computing privileges?
- On what occasions do they breach security policies and abuse internet use?

- What type of activities are considered illegal and will have law enforcement consequences?

D. Sections on Each Procedural Policy

Here, you can include additional specifications on:

- **Usage:** Computers should not be used for any illegal activities, chain letters (electronic mail spam), or discriminatory communication. You can include more specific usage violations.

- **Monitoring:** Clarifies that employees should not assume their privacy is protected while using the company-owned computer equipment – and that employers have the right to monitor their activities on the computers.

- **Security:** Employees should not engage in activities that jeopardize the security of the computer network system.

- **Copyright:** Employees cannot copy, retrieve, or modify copyrighted materials without the permission of the copyright holder. Violation of this policy can lead to copyright law enforcement for both the individual and the company.

You can expand on each of these sections to include specifics related to your industry and business.

E. Disciplinary Action

In the end, state that violating the policy will lead to disciplinary action. Specify what this action is, the procedure and whether the employee will get a warning beforehand.

Sample Computer Usage Policy

Now, let's take a look at a sample computer policy you can refer to when creating your business's policy:

1. Policy Brief and Purpose

This company computer usage policy outlines the guidelines for properly using its computers, network, and internet.

The aim of this company policy is to avoid inappropriate, illegal, and unauthorized use of the computing equipment and information technology, and to avoid jeopardizing the company's reputation and security.

2. Scope

This computer usage policy applies to all employees and other individuals like partners, volunteers, independent contractors, and those who have access to the company's network and computing facilities.

3. Policy

Proper Computer, Email, and Internet Usage

Employees are expected to use computer devices, the internet, and company computer network to:

- Work on their job responsibilities.
- Do work-related research.
- Use the email system and social media only for work-related purposes.

Employees are expected to:

- Use secure passwords and keep their user ID information private.
- Not connect their personal computers to the company's computer system.
- Not give their computer login information to others or grant them unauthorized access to the company's computer system.

Abuse of Policy and Inappropriate Computer Usage

Employees should not use the company's computers to:

- Send confidential information to unauthorized user accounts.
- Download or upload illegal files or spread illegally copyrighted materials.

- Invade others' privacy, corporate accounts, and email communication.
- Visit unsafe websites that can crash the system or spread a virus in the company's network.
- Engage in hacking activities, steal personal or financial information, mine cryptocurrencies, buy/sell illegal goods.
- Turn off the computer's firewalls or antivirus programs without a system administrator or a manager's permission.

Usage

Electronic media should not be used for transmitting chain letters and other email spam.

The computer devices should only be used for business-related purposes, and employees should not abuse computer data usage limits.

Additionally, network access will be granted to authorized user accounts only.

Monitoring

The company has the right to monitor regularly all electronic communication channels that happen on business computing devices. These include email accounts and other forms of communication and data sharing that occur on work computers.

The company uses this information to increase the efficiency of its operations and improve employee productivity.

Employees should not assume that the communication on these devices is exclusively private and should not use them to transmit private messages or personal data.

Security

Employees should not give their authorized access information to users without proper authorization.

They shouldn't try to obtain other employees' password information, hack into other networks, or engage in other activities that put the company's system security at risk.

Consequences for Being Non-Compliant

Employees who violate this computer usage policy will face disciplinary action.

A warning will follow violations. Depending on the severity of the violation, the employee can face termination of employment or other legal actions.

Examples of severe violations are:

- The usage of computer devices to engage in any sort of illegal activity.
- Activities that spread malware like viruses, worms, and Trojan horses.

- Spreading discriminatory, offensive, or harassing messages. There's a zero-tolerance policy on any kind of harassing and discriminatory communication that can be associated with the company.

Unit No – 7

Cyber Crime – Illustration, Examples and Mini Cases

UIDAI Aadhaar software hacked

A billion Indian Aadhaar card details were leaked in India and this is one of the most massive data breaches that happened in 2018. UIDAI released the official notification about this data breach and mentioned that around 210 Indian Government websites were hacked. This data breach included Aadhar, PAN, bank account IFSC codes, and other personal information of the users and anonymous sellers were selling Aadhaar information for Rs. 500 over Whatsapp. Also, one could get an Aadhaar card printout for just Rs.300.

Mobikwik data breach

The recent data breach at the payment from Mobikwik in India is alarming. According to reports, the data breach affected 3.5 million customers, revealing know-your-customer records including addresses, phone numbers, Aadhaar cards, and PAN cards, among other things. Until recently, the corporation has claimed that no such data breach occurred. Only until the regulator, the Reserve Bank of India (RBI), instructed Mobikwik to immediately perform a forensic audit by a CERT-IN empanelled auditor and submit the findings did the business begin engaging with the appropriate authorities.

ATM system hacked

Around mid-2018 a cyber-attack was launched against Canara bank ATM servers in India. Several bank accounts were emptied of about 20 lakh rupees. According to reports, cybercriminals had access to ATM data for more than 300 individuals, resulting in a total of 50 victims. Skimming devices were used by hackers to collect information from debit cardholders. The value of transactions conducted using stolen information ranged from Rs. 10,000 to Rs. 40,000.

Baazee.com case

In December 2004, the CEO of Baazee.com was arrested after a CD containing inappropriate information was sold on the website. The CD was also available in Delhi's marketplaces. Later, the CEO was released on bail bond. This raised the question of how we should distinguish between Internet Service Providers and Content Providers. The accused bears the burden of proving that he was the Service Provider rather than the Content Provider. It also creates a lot of questions about how police should handle cyber-crime cases, and it necessitates a lot of education.

List of Blackbaud breach victims tops 120

The National Trust in the United Kingdom has joined a growing list of education and charitable organisations whose alumni or contributors' data has been compromised as a result of a two-month-old ransomware attack at US cloud software provider Blackbaud. The Trust, which manages hundreds of vital and

historical sites throughout the UK, including natural landscapes and landmarks, parks, gardens, and stately homes, told BBC that the data of its volunteers and fundraisers had been compromised, but the data on its 5.6 million members was safe. The organisation is investigating and alerting anyone who could be affected. It has also reported the incident to the Information Commissioner's Office, which is currently dealing with a significant number of reports, including Blackbaud's, in accordance with UK data protection laws.