UNIT-1

1. Define cybercrime and explain its core characteristics, highlighting why it is considered a global threat.

Definition of Cybercrime

Cybercrime refers to illegal activities carried out using computers, computer networks, or the internet, where digital technology acts as a tool, target, or medium for committing the crime.

Examples of cybercrime include:

- Hacking
- Online fraud
- Identity theft
- Phishing attacks
- Cyber stalking

Core Characteristics of Cybercrime

1. Technology-Dependent Nature

Cybercrime is completely dependent on Information and Communication Technology (ICT). Criminals use advanced tools, software, and techniques such as malware, spyware, and hacking programs.

2. Borderless in Nature

Cybercrime has no geographical boundaries.

An attacker sitting in one country can easily target victims in another country through the internet.

3. Anonymity of Offenders

Cybercriminals often hide their identities using:

- Virtual Private Networks (VPNs)
- Proxy servers
- Fake IP addresses
- Dark web platforms

This makes tracing and identifying offenders difficult.

4. High Speed and Automation

Cybercrimes can be executed at very high speed and can affect thousands of systems within seconds due to automation.

Example: Worm attacks, Distributed Denial of Service (DDoS) attacks.

5. Financial and Data Loss

Cybercrime causes significant financial losses, theft of sensitive data, and damage to organizational reputation.

Example: Banking frauds, credit card theft, data breaches.

6. Wide Range of Victims

Victims of cybercrime include:

- Individuals
- Businesses
- Government organizations
- Critical infrastructure systems

No sector is completely safe from cyber threats.

Why Cybercrime Is Considered a Global Threat

1. It affects both developed and developing countries.
2. It poses a serious threat to national security through cyber terrorism and espionage.
3. It causes huge economic losses worldwide every year.
4. Differences in cyber laws across countries make investigation and prosecution difficult.
5. Rapid growth of technologies like AI, IoT, and cloud computing has increased cyber vulnerabilities.

2 Provide a detailed overview of Social Engineering, describing its life cycle from investigation to exit.

Social Engineering is a non-technical cyber attack technique in which an attacker manipulates, influences, or deceives individuals into revealing confidential information such as passwords, PINs, or sensitive organizational data.

Instead of exploiting system vulnerabilities, it exploits human psychology.

Social Engineering Life Cycle

The social engineering attack follows a systematic life cycle, starting from information gathering and ending with exit.

1. Investigation (Information Gathering)

In this phase, the attacker collects detailed information about the target using open-source intelligence (OSINT).

Sources include:

- Social media platforms
- Company websites
- Public records
- Emails, blogs, and forums

Purpose:

To understand the target’s role, behavior, interests, and weaknesses.

2. Planning (Preparation)

Based on collected data, the attacker designs a strategy and attack scenario.

Activities include:

- Choosing attack type (phishing, pretexting, baiting)
- Creating fake identities or profiles
- Drafting convincing emails or messages

Goal:

To make the attack look legitimate and trustworthy.

3. Approach (Interaction with Victim)

The attacker establishes direct contact with the victim through:

- Emails
- Phone calls
- Social media
- Messaging apps

The attacker builds trust using authority, urgency, fear, or curiosity.

Example:

Pretending to be an IT support executive.

4. Exploitation (Manipulation)

In this phase, the victim is psychologically manipulated to perform an action, such as:

- Sharing login credentials
- Clicking malicious links
- Downloading infected attachments

This is the core phase where the actual breach occurs.

5. Execution (Attack Accomplishment)

The attacker uses the obtained information to:

- Gain unauthorized system access
- Steal sensitive data
- Commit financial fraud
- Install malware

This phase converts deception into actual damage.

6. Exit (Covering Tracks)

After completing the attack, the attacker safely exits by:

- Deleting traces
- Disabling logs
- Closing fake accounts
- Avoiding suspicion

The goal is to remain undetected and prevent investigation.

3 Discuss the Nature and Scope of Cyber Crime in the modern era, explaining why it is an "uncontrollable evil".

Cyber crime refers to criminal activities carried out using computers, digital devices, networks, and the internet. In the modern digital era, rapid technological growth has increased dependence on cyberspace, which has simultaneously expanded the nature and scope of cyber crime. Due to its complex, borderless, and evolving nature, cyber crime is often described as an "uncontrollable evil."

Nature of Cyber Crime

The nature of cyber crime describes its basic characteristics and behavior:

1. Technology-Oriented

Cyber crime is completely dependent on advanced technologies such as computers, mobile devices, cloud computing, and the internet.

2. Borderless and Global

Cyber crimes do not have geographical boundaries.
An offender can operate from one country and target victims across the world.

3. Anonymous and Hidden

Cyber criminals can hide their identity using:

- Fake profiles
- VPNs and proxy servers
- Dark web platforms

This anonymity makes detection and punishment difficult.

4. Rapid and Dynamic

Cyber crimes are committed at high speed and keep changing with new technologies. As security improves, criminals develop new attack techniques.

5. Low Risk, High Reward

Compared to traditional crimes, cyber crime involves:

- Low physical risk
- High financial gain
- Lesser chances of immediate arrest

Scope of Cyber Crime

The scope of cyber crime refers to how widely it affects individuals, organizations, and nations:

1. Crimes Against Individuals

- Identity theft
- Cyber stalking
- Online harassment
- Phishing and financial fraud

2. Crimes Against Organizations

- Data breaches
- Corporate espionage
- Ransomware attacks
- Intellectual property theft

3. Crimes Against Government and Nation

- Cyber terrorism
- Cyber espionage
- Attacks on critical infrastructure
- Election interference

4. Expanding Digital Platforms

The scope of cyber crime has expanded due to:

- Social media
- E-commerce
- Online banking
- Cloud services
- IoT devices

Why Cyber Crime Is Considered an "Uncontrollable Evil"?

Cybercrime is called an uncontrollable evil due to the following reasons:

1. Rapid Technological Advancement

Technology grows faster than laws and security systems, giving criminals an advantage.

2. Lack of Global Uniform Laws

Different countries have different cyber laws, making international investigation and prosecution difficult.

3. Difficulty in Detection and Attribution

Tracing attackers across multiple networks and countries is highly complex.

4. Human Factor

Humans are the weakest link in security.
Even strong technical systems can fail due to lack of awareness or negligence.

5. Increasing Dependence on Cyberspace

Modern life depends heavily on digital systems, making complete elimination of cyber crime impractical.

4 Describe the different types of Phishing attacks, including spear phishing, whaling, and angler phishing.

Phishing is a type of social engineering attack in which attackers trick users into revealing sensitive information such as usernames, passwords, credit card details, or OTPs by pretending to be a legitimate and trustworthy entity.

Phishing attacks are carried out through emails, messages, phone calls, and social media platforms.

Different Types of Phishing Attack

1. Email Phishing

This is the most common type of phishing attack.

- Attackers send fraudulent emails that appear to come from trusted organizations like banks, companies, or service providers.
- The email usually contains a malicious link or attachment.

Example:

An email claiming “Your bank account is suspended—verify immediately.”

2. Spear Phishing

Spear phishing is a targeted phishing attack aimed at a specific individual or organization.

- The attacker performs prior research on the victim.
- Emails are personalized using names, job roles, or company details.
- Makes the attack more convincing and harder to detect.

Example:

An email sent to an employee pretending to be the company’s HR manager.

3. Whaling

Whaling is a specialized form of spear phishing that targets high-profile individuals.

- Targets include CEOs, CFOs, directors, and senior executives.
- Focuses on financial transactions, confidential data, or legal documents.
- Uses formal language and professional-looking messages.

Example:

A fake email requesting urgent wire transfer approval from the CEO.

4. Smishing (SMS Phishing)

This phishing attack is carried out through SMS or text messages.

- Messages contain malicious links or fake offers.
- Often creates urgency like account suspension or prize winnings.

Example:

“Your account is blocked. Click here to reactivate.”

5. Vishing (Voice Phishing)

Vishing uses phone calls or voice messages.

- Attackers impersonate bank officials, customer care, or government authorities.
- Victims are tricked into sharing OTPs, PINs, or account details.

Example:
A call claiming suspicious activity in your bank account.

6. Angler Phishing

Angler phishing occurs on social media platforms.

- Attackers impersonate customer support accounts of popular brands.
- They respond to users' complaints or queries with fake help links.
- Exploits public trust in social media customer service.

Example:
A fake Twitter support account asking users to "verify account details."

7. Clone Phishing

In this attack, a legitimate email is copied and resent with a malicious link or attachment replacing the original one.

- Appears familiar to the victim.
- Often claims to be an updated or corrected version of a previous email.

5 Explain the three major categories of cybercrime: crimes against people, property, and government.

Cybercrime can be broadly classified based on the target affected by the crime. In cyberspace, crimes are mainly committed against people, property, and government. Each category involves different types of illegal activities that exploit digital technologies and networks.

1. Crimes Against People

Crimes against people involve harm to individuals by violating their privacy, dignity, or financial security through cyberspace.

Key Types:

- Cyber stalking – Online harassment, threats, or monitoring of individuals
- Cyber bullying – Harassing or humiliating individuals through digital platforms
- Identity theft – Stealing personal information for fraudulent use
- Email spoofing & phishing – Cheating users to obtain sensitive data
- Online defamation – Spreading false information to damage reputation

Impact:

- Mental and emotional distress
- Financial loss
- Loss of privacy and trust

2. Crimes Against Property
Crimes against property target digital or intellectual property belonging to individuals or organizations.
Key Types:

- Hacking and unauthorized access to systems and networks
- Data theft and data breaches
- Malware attacks (viruses, worms, ransomware)
- Software piracy – Illegal copying or distribution of software
- Intellectual property theft – Stealing trade secrets or copyrighted content

Impact:

- Economic loss
- Business disruption
- Damage to reputation and competitiveness

3. Crimes Against Government
Crimes against government involve attacks on government systems, data, and national security.
Key Types:

- Cyber terrorism – Using cyberspace to create fear or disrupt public services
- Cyber espionage – Stealing confidential government information
- Attacks on critical infrastructure (power grids, defense systems)
- Website defacement of government portals
- Election interference and data manipulation

Impact:

- Threat to national security
- Disruption of public services
- Loss of public trust in governance

6 Compare and contrast Hacking and Cracking as defined under crimes against people.

In cybercrime studies, hacking and cracking are often confused, but they differ in intention, legality, and impact. When performed with malicious intent, both can fall under crimes against people because they violate privacy, security, and trust of individuals.

Hacking vs Cracking

Basis	Hacking	Cracking
Definition	Hacking is the act of gaining unauthorized access to a computer system or network, sometimes for learning, testing, or security analysis.	Cracking is the act of breaking into systems with malicious intent to steal, damage, or misuse data.

Intent	May be ethical or unethical, depending on purpose.	Always malicious and illegal.
Legality	Ethical hacking can be legal with permission.	Cracking is always illegal.
Purpose	To identify vulnerabilities, improve security, or gain knowledge.	To steal data, cause damage, commit fraud, or disrupt systems.
Impact on People	Minimal harm when done ethically; unethical hacking may cause privacy issues.	Causes direct harm such as data theft, identity theft, and financial loss.
Skill Usage	Uses technical skills for analysis and problem-solving.	Uses technical skills for exploitation and destruction.
Examples	Penetration testing, vulnerability assessment.	Password cracking, ransomware attacks, data destruction.

Hacking as a Crime Against People

When hacking is performed without authorization, it becomes a crime against people by:

- Violating personal privacy
- Accessing confidential information
- Causing emotional distress and loss of trust

Cracking as a Crime Against People

Cracking directly targets individuals by:

- Stealing personal and financial data
- Destroying or altering information
- Causing financial and psychological harm

7 Detail Cryptocurrency Crime and explain Cyber Terrorism as defined by I4C.

1. Cryptocurrency Crime

Meaning:

Cryptocurrency crime refers to illegal activities carried out using cryptocurrencies such as Bitcoin and other digital currencies. These crimes exploit features like decentralization, anonymity, and lack of regulation in cryptocurrency systems.

Common Types of Cryptocurrency Crimes

1. **Cryptocurrency Fraud**
   - Fake investment schemes
   - Ponzi and pyramid schemes
   - Promises of high returns

2. **Money Laundering**
    - Converting illegal money into cryptocurrency to hide its origin
    - Difficult to trace due to anonymous wallets
3. **Ransomware Attacks**
    - Victims' data is encrypted
    - Ransom demanded in cryptocurrency
4. **Dark Web Transactions**
    - Buying and selling drugs, weapons, or illegal services using crypto
5. **Crypto Wallet Hacking**
    - Stealing private keys
    - Unauthorized transfer of digital assets

Why Cryptocurrency Crimes Are Rising

- Anonymous transactions
- No central authority
- Cross-border usability
- Limited legal control

2. Cyber Terrorism (As Defined by I4C)

Definition

According to Indian Cyber Crime Coordination Centre (I4C),Cyber Terrorism is the use of cyberspace and digital technologies to carry out terrorist activities with the intention to threaten national security, spread fear among the public, disrupt essential services, or influence government decisions.

Key Characteristics of Cyber Terrorism

1. Use of Cyberspace as a Weapon
    - Computers, networks, and the internet are used to launch attacks.
2. Threat to National Security
    - Targets government systems, defense networks, and critical infrastructure.
3. Psychological Impact
    - Creates fear, panic, and insecurity among citizens.
4. Political or Ideological Motive
    - Aimed at influencing government policies or promoting extremist ideologies.

Examples of Cyber Terrorism

- Attacks on power grids, transport systems, or communication networks
- Hacking government or military websites
- Spreading extremist propaganda online
- Coordinated cyber attacks during national emergencies

Difference Between Cryptocurrency Crime and Cyber Terrorism

Aspect	Cryptocurrency Crime	Cyber Terrorism
Main Objective	Financial gain	Fear, disruption, ideology
Target	Individuals, investors, businesses	Government, nation, public
Tools Used	Cryptocurrencies, wallets, exchanges	Networks, malware, cyber weapons
Impact	Economic loss	National security threat

8 Analyze Malware as a cybercrime tool, describing common types.

Malware (Malicious Software) is any software intentionally designed to damage, disrupt, steal data, or gain unauthorized access to computer systems and networks. It is one of the most powerful and widely used cybercrime tools, enabling attackers to automate attacks, exploit system vulnerabilities, and cause large-scale damage.
Malware is commonly delivered through email attachments, malicious links, infected websites, USB drives, and software downloads.

Why Malware Is a Powerful Cybercrime Tool

- Operates silently without user knowledge
- Can spread automatically across networks
- Enables data theft, financial fraud, spying, and system destruction
- Difficult to detect without proper security tools

Common Types of Malware

1. Virus

A virus attaches itself to legitimate files or programs and spreads when the infected file is executed.

Characteristics:

- Requires human action to spread
- Corrupts or deletes data
- Slows down system performance

Example: File-infecting viruses.

2. Worm

A worm is a self-replicating malware that spreads automatically through networks without user interaction.

Characteristics:

- Consumes network bandwidth
- Can cause system crashes
- Spreads very rapidly

Example: Network worms.

3. Trojan Horse

A Trojan disguises itself as legitimate software but performs malicious actions once installed.
Characteristics:

- Does not self-replicate
- Creates backdoors
- Enables unauthorized access

Example: Fake antivirus software.

4. Ransomware

Ransomware encrypts victim's files and demands payment (usually in cryptocurrency) to restore access.
Characteristics:

- Causes data unavailability
- Leads to financial loss
- Often targets organizations

Example: WannaCry-type attacks.

5. Spyware

Spyware secretly monitors user activities and collects sensitive information.
Characteristics:

- Tracks browsing behavior
- Steals passwords and personal data
- Runs in background

Example: Surveillance software.

6. Keylogger

A keylogger records every keystroke made by the user.
Characteristics:

- Captures passwords, PINs, OTPs
- Used for identity theft and banking fraud
- Can be hardware or software-based

7. Adware

Adware displays unwanted advertisements on the user's system.
Characteristics:

- Slows down system
- May redirect to malicious websites
- Sometimes bundled with free software

8. Botnet

A botnet is a network of infected computers controlled remotely by an attacker.

Characteristics:

- Used for DDoS attacks
- Sends spam emails
- Launches coordinated cyber attacks

Impact of Malware

- Financial loss
- Data theft and privacy violation
- Business disruption
- National security threats

9 Explain cybercrime and discuss its key characteristics with suitable examples.

Cybercrime refers to any illegal activity carried out using computers, digital devices, computer networks, or the internet. In cybercrime, technology may act as a tool, target, or medium for committing the offence. With the rapid growth of digitalization, cybercrime has become one of the most serious challenges in the modern world.

Definition of Cybercrime

Cybercrime is defined as any unlawful act where a computer, network, or digital system is involved, either to attack data, steal information, or cause harm to individuals, organizations, or governments.

Examples:

- Hacking
- Phishing
- Online banking fraud
- Identity theft
- Cyber stalking

Key Characteristics of Cybercrime

1. Technology-Based Crime

Cybercrime heavily depends on Information and Communication Technology (ICT) such as computers, smartphones, and the internet.

Example:

Using malware to steal data from a computer system.

2. Borderless Nature

Cybercrime has no geographical boundaries.

An attacker from one country can target victims in another country easily.

Example:

An international hacker stealing data from an Indian company.

3. Anonymity of Criminals
Cybercriminals can hide their identity using:

- Fake accounts
- VPNs and proxy servers
- Dark web platforms

Example:
A phishing attacker using a fake email address and IP masking.

4. High Speed and Automation
Cybercrimes can be committed very quickly and on a large scale using automated tools.
Example:
A worm spreading to thousands of systems within minutes.

5. Huge Financial and Data Loss
Cybercrime often results in:

- Financial loss
- Theft of sensitive personal or business data
- Damage to reputation

Example:
Online banking fraud or credit card theft.

6. Wide Range of Victims
Cybercrime affects:

- Individuals
- Businesses
- Government organizations

Example:
Cyber attacks on government websites or online harassment of individuals.

7. Difficulty in Detection and Investigation
Due to advanced techniques and cross-border nature, investigation and prosecution are complex.
Example:
Tracing the source of a ransomware attack involving multiple countries.

10 Describe the nature and scope of cybercrime in the modern digital era.

Cybercrime refers to criminal activities committed using computers, digital devices, networks, and the internet. In the modern digital era, rapid growth of technologies such as cloud computing, mobile devices, social media, artificial intelligence, and the Internet of Things (IoT) has expanded both the nature and scope of cybercrime, making it more complex and widespread.

Nature of Cybercrime

The nature of cybercrime describes its fundamental characteristics:

1. Technology-Driven

Cybercrime depends entirely on digital technology and cyberspace. Criminals use computers, smartphones, software tools, and networks to commit offences.

2. Borderless and Global

Cybercrime has no geographical boundaries.
An attacker in one country can target victims in multiple countries at the same time.

3. Anonymous in Nature

Cybercriminals can hide their identity using:

- Fake profiles
- VPNs and proxy servers
- Encrypted communication
- Dark web platforms

This anonymity makes detection difficult.

4. Rapid and Dynamic

Cybercrime evolves very quickly. As new technologies emerge, new cyber-attack techniques also develop.

5. Low Risk, High Reward

Cybercrime often involves low physical risk and high financial or strategic gain, encouraging more offenders.

Scope of Cybercrime

The scope of cybercrime explains how widely it affects society:

1. Crimes Against Individuals

- Identity theft
- Cyber stalking and bullying
- Online fraud
- Phishing and scams

2. Crimes Against Organizations

- Data breaches
- Ransomware attacks
- Corporate espionage
- Intellectual property theft

3. Crimes Against Government and Nation

- Cyber terrorism
- Cyber espionage
- Attacks on critical infrastructure
- Defacement of government websites

4. Expansion Due to Digital Platforms

The scope has widened due to:

- Online banking and e-commerce
- Social media platforms
- Cloud computing
- IoT devices and smart systems

5. Economic and Social Impact

Cybercrime causes:

- Massive financial losses
- Loss of trust in digital systems
- Threats to national security

11 Explain social engineering and analyze its life cycle stages.

Social Engineering is a cybercrime technique in which attackers manipulate human behavior to trick individuals into revealing confidential information such as passwords, PINs, OTPs, or sensitive organizational data.

Instead of exploiting technical vulnerabilities, social engineering exploits the human factor, which is often the weakest link in security systems.

Meaning of Social Engineering

Social engineering can be defined as the art of deceiving people into performing actions or disclosing information that compromises security. Attackers use psychological tactics like trust, fear, urgency, authority, and curiosity to achieve their goals.

Examples:

- Phishing emails
- Fake technical support calls
- Impersonation on social media

Life Cycle Stages of Social Engineering

Social engineering attacks usually follow a structured life cycle, from planning to exit.

1. Investigation (Information Gathering)

This is the initial stage where the attacker collects information about the target.
Sources include:

- Social media profiles
- Company websites
- Public records
- Online forums and emails

Purpose:

To understand the victim's role, habits, interests, and weaknesses.

2. Planning and Preparation

Using the collected information, the attacker plans the attack strategy.
Activities include:

- Selecting the attack type (phishing, pretexting, baiting)
- Creating fake identities or accounts
- Drafting convincing messages or scripts

Goal:

To make the attack appear legitimate and trustworthy.

3. Approach (Initial Contact)

The attacker establishes contact with the victim through:

- Email
- Phone calls
- SMS
- Social media platforms

Psychological techniques such as authority, urgency, or fear are used to gain trust.

4. Exploitation (Manipulation)

In this stage, the attacker convinces the victim to take a specific action, such as:

- Sharing login credentials
- Clicking malicious links
- Downloading infected attachments

This is the most critical stage, where the actual compromise occurs.

5. Execution

The attacker uses the obtained information to:

- Gain unauthorized system access
- Steal sensitive data
- Commit financial fraud
- Install malware

The objective of the attack is fully achieved in this stage.

6. Exit (Covering Tracks)

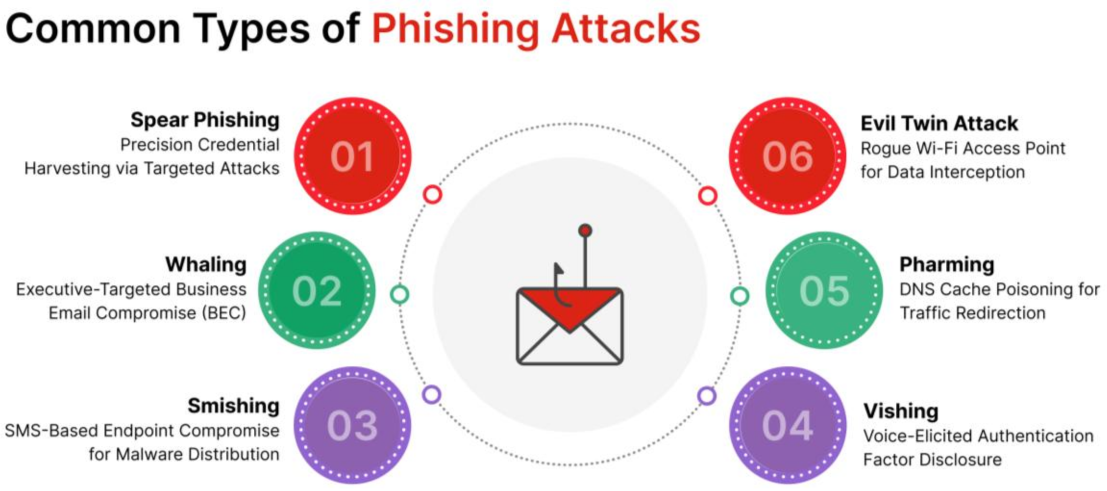
After completing the attack, the attacker exits safely by:

- Deleting evidence
- Closing fake accounts
- Avoiding detection

The aim is to remain undetected and prevent investigation.

12 Discuss various types of phishing attacks and their impact on users.

Phishing is a type of social engineering cyber-attack in which attackers impersonate trusted entities to trick users into revealing sensitive information such as usernames, passwords, bank details, credit card numbers, or OTPs. Phishing attacks are widely used because they exploit human trust and lack of awareness rather than technical vulnerabilities.


Common Types of Phishing Attacks
Spear Phishing
Precision Credential Harvesting via Targeted Attacks
01
Whaling
Executive-Targeted Business Email Compromise (BEC)
02
Smishing
SMS-Based Endpoint Compromise for Malware Distribution
03
Evil Twin Attack
Rogue Wi-Fi Access Point for Data Interception
06
Pharming
DNS Cache Poisoning for Traffic Redirection
05
Vishing
Voice-Elicited Authentication Factor Disclosure
04

Types of Phishing Attacks

1. Email Phishing

This is the most common form of phishing.

- Fraudulent emails appear to come from banks, companies, or service providers.
- Messages contain malicious links or attachments.

Example:

Fake email asking users to “verify account details immediately.”

2. Spear Phishing

Spear phishing is a targeted attack aimed at a specific individual or organization.

- Attackers use personal information like name, designation, or company details.
- Highly convincing and difficult to detect.

Example:

An email sent to an employee pretending to be from HR or management.

3. Whaling

Whaling targets high-level executives such as CEOs, CFOs, or directors.

- Focuses on large financial transactions or sensitive company data.
- Uses professional and urgent communication.

Example:

A fake email requesting urgent approval for fund transfer.

4. Smishing (SMS Phishing)

Smishing uses text messages (SMS) to deceive users.

- Messages include fake offers, alerts, or warnings.
- Often include malicious links.

Example:

"Your account is blocked. Click here to reactivate."

5. Vishing (Voice Phishing)

Vishing is carried out using phone calls or voice messages.

- Attackers impersonate bank officials or customer care agents.
- Victims are tricked into sharing OTPs or PINs.

Example:

A call claiming suspicious activity in a bank account.

6. Angler Phishing

Angler phishing occurs on social media platforms.

- Attackers create fake customer support accounts.
- They respond to user complaints with malicious links.

Example:

Fake support account on Twitter asking users to "verify details."

7. Clone Phishing

A legitimate email is copied and resent with a malicious attachment or link replacing the original.

- Appears familiar and trustworthy to the victim.

Impact of Phishing Attacks on Users

1. Financial Loss – Unauthorized transactions and fraud
2. Identity Theft – Misuse of personal and official information
3. Privacy Violation – Exposure of confidential data
4. Emotional Stress – Fear, anxiety, and loss of trust
5. Account Compromise – Loss of email, social media, or banking accounts
6. Organizational Damage – Data breaches and reputation loss

13 Explain crimes against people with reference to hacking and cyberstalking.

Crimes against people in cyberspace are offences that directly harm individuals by violating their privacy, security, dignity, or mental peace. Among the various cyber offences, hacking and cyberstalking are two important crimes that seriously affect individuals in the digital environment.

1. Hacking (as a Crime Against People)

Hacking refers to unauthorized access to computer systems, networks, or digital accounts with the intention of viewing, stealing, modifying, or misusing personal information.
When hacking is done without permission and with malicious intent, it becomes a crime against people.

How Hacking Affects Individuals

- Unauthorized access to personal emails and social media accounts
- Theft of personal and financial data
- Violation of privacy
- Identity theft and impersonation

Example

A hacker gaining illegal access to an individual's email account and using personal data for fraud or blackmail.

2. Cyberstalking

Cyberstalking is the act of repeatedly harassing, threatening, or monitoring an individual using digital technologies such as social media, emails, messaging apps, or online forums.

Forms of Cyberstalking

- Sending threatening or abusive messages
- Spreading false information online
- Monitoring online activities continuously
- Creating fake profiles to harass the victim

Impact on Victims

- Psychological trauma and fear
- Emotional distress and anxiety
- Loss of personal safety and privacy
- Damage to reputation

Example

Repeated harassment of a person through social media messages and fake accounts.

Why These Are Crimes Against People

Both hacking and cyberstalking:

- Directly target individual victims
- Violate personal privacy and security
- Cause emotional, psychological, and financial harm

14 Compare crimes against property and crimes against government with examples.

Cybercrimes can be classified based on the target affected by the offence. Two important categories are crimes against property and crimes against government. While crimes against property mainly cause economic and data loss, crimes against government threaten national security and public stability.

Crimes Against Property

Crimes against property refer to cyber offences that target digital assets, data, software, or intellectual property belonging to individuals or organizations.

Major Types

- Hacking and unauthorized access to systems
- Data theft and data breaches
- Ransomware and malware attacks
- Software piracy
- Intellectual property theft

Examples

- Stealing customer data from a company database
- Ransomware attack encrypting an organization's files
- Illegal copying and distribution of licensed software

Impact

- Financial loss
- Business disruption
- Loss of confidential data
- Damage to organizational reputation

Crimes Against Government

Crimes against government are cyber offences that target government systems, data, services, and national interests.

Major Types

- Cyber terrorism
- Cyber espionage
- Attacks on critical infrastructure (power, transport, defense)
- Defacement of government websites
- Election interference

Examples

- Hacking a government portal and defacing its website
- Cyber attacks on power grids or defense networks
- Stealing confidential government or military data

Impact

- Threat to national security
- Disruption of public services
- Loss of public trust
- Political and social instability

15 Analyze malware as a cybercrime tool and explain its common variants.

Malware (Malicious Software) refers to any software intentionally designed to harm, disrupt, spy on, steal data from, or gain unauthorized access to computer systems and networks. Malware is one of the most effective and widely used tools in cybercrime, as it allows attackers to automate attacks, operate secretly, and target a large number of victims simultaneously.

Cybercriminals use malware for activities such as data theft, financial fraud, ransomware attacks, espionage, and system sabotage.

Why Malware Is an Effective Cybercrime Tool

- Operates silently without the user's knowledge
- Can spread automatically across systems and networks
- Enables large-scale attacks with minimal effort
- Difficult to detect without proper security software

Common Variants of Malware

1. Virus

A virus is a malicious program that attaches itself to legitimate files or programs and spreads when the infected file is executed.

Characteristics:

- Requires user action to spread
- Corrupts or deletes files
- Slows down system performance

Example: File-infecting virus damaging documents.

2. Worm

A worm is a self-replicating malware that spreads automatically through networks without user interaction.

Characteristics:

- Consumes network bandwidth
- Spreads very rapidly
- Can cause system crashes

Example: Network worms spreading via email or shared networks.

3. Trojan Horse

A Trojan Horse disguises itself as legitimate software but performs malicious actions in the background once installed.

Characteristics:

- Does not self-replicate
- Creates backdoors for attackers
- Allows unauthorized access

Example: Fake antivirus software.

4. Ransomware
Ransomware encrypts the victim’s data and demands a ransom (usually in cryptocurrency) to restore access.
Characteristics:

- Causes data unavailability
- Leads to financial loss
- Commonly targets organizations

Example: Encrypting company files and demanding payment.

5. Spyware
Spyware secretly monitors user activity and collects sensitive information.
Characteristics:

- Tracks browsing behavior
- Steals passwords and personal data
- Operates in the background

Example: Monitoring keystrokes and online activity.

6. Keylogger
A keylogger records every keystroke typed by the user.
Characteristics:

- Captures passwords, PINs, OTPs
- Used in banking and identity theft
- Can be hardware or software-based

7. Adware
Adware displays unwanted advertisements and may redirect users to malicious websites.
Characteristics:

- Degrades system performance
- Often bundled with free software

8. Botnet
A botnet is a network of infected computers controlled remotely by an attacker.
Characteristics:

- Used for DDoS attacks
- Sends spam emails
- Launches coordinated cyber attacks

Impact of Malware

- Financial loss
- Data theft and privacy violation
- Business and service disruption
- Threats to national security

16 Examine why cybercrime is considered an uncontrollable global threat.

Cybercrime has emerged as one of the most serious threats in the modern digital era. It involves criminal activities carried out using computers, networks, and the internet. Cybercrime is often described as an “uncontrollable global threat” because of its borderless nature, rapid growth, anonymity, and continuous evolution with technology

Reasons Why Cybercrime Is an Uncontrollable Global Threat

1. Borderless Nature of Cyberspace
Cybercrime has no geographical boundaries.Attackers can operate from one country and target victims across multiple countries simultaneously.
Impact:
International cooperation becomes difficult due to jurisdictional and legal issues.

2. Anonymity of Cybercriminals
Cybercriminals hide their identity using:

- VPNs and proxy servers
- Encrypted communication
- Dark web platforms

Impact:
Tracing and identifying offenders is extremely difficult.

3. Rapid Technological Advancement
Technology evolves faster than laws and security mechanisms.

- New tools like AI, IoT, and cloud computing create new vulnerabilities.
- Criminals quickly adapt to new technologies.

4. Lack of Uniform Global Cyber Laws
Different countries have different cyber laws, policies, and enforcement mechanisms.
Impact:

- Extradition is difficult
- Punishment is inconsistent
- Criminals exploit legal loopholes

5. High Speed and Automation of Attacks
Cyber attacks can be:

- Executed within seconds
- Automated to target thousands of systems

Example:
Worm attacks, ransomware campaigns, DDoS attacks.

6. Low Risk and High Reward

Cybercrime involves:

- Low physical risk
- High financial and data-related gains
- Reduced chances of immediate arrest

This attracts more offenders worldwide.

7. Human Factor (Weakest Link)

Even with advanced security systems, human error such as:

- Clicking malicious links
- Sharing credentials
- Lack of awareness

continues to enable cybercrime.

8. Increasing Dependence on Digital Systems

Modern society depends heavily on:

- Online banking
- E-commerce
- Digital governance
- Cloud and smart systems

This dependence makes complete elimination of cybercrime impractical.

Global Impact of Cybercrime

- Massive financial losses worldwide
- Identity theft and privacy violations
- Threats to national security

2 MARKS UNIT-1

1. What is the definition of Cybercrime Investigation?

Cybercrime investigation is the process of identifying, collecting, analyzing, and presenting digital evidence to detect and prosecute crimes committed using computers and the internet.

2. Briefly explain DDoS attacks.

A DDoS (Distributed Denial of Service) attack is an attack where multiple systems flood a target server or network with traffic, making it unavailable to legitimate users.

3. What is Cyber Stalking?

Cyberstalking is the act of repeatedly harassing, threatening, or monitoring a person using digital platforms such as social media, emails, or messages.

4. Define Identity Theft.

Identity theft is the illegal use of another person's personal information such as name, Aadhaar, bank details, or passwords for fraud or crime.

5. What are Botnets?

Botnets are networks of compromised computers (bots) controlled remotely by an attacker to perform activities like spam, DDoS attacks, or data theft.

6. Explain Honey Trap in Social Engineering.

A honey trap is a social engineering technique where an attacker uses fake emotional or romantic relationships to manipulate victims into sharing sensitive information.

7. What is Cyber Squatting?

Cyber squatting is the act of registering domain names similar to famous brands or trademarks with the intention of selling them at high prices or misleading users.

8. Define Cryptojacking.

Cryptojacking is the unauthorized use of a victim's computer or device to mine cryptocurrency without their knowledge or consent.

9. Define Cybercrime.

Cybercrime is any illegal activity carried out using computers, networks, or the internet where technology is used as a tool or target.

10. What is Social Engineering?

Social engineering is a technique where attackers manipulate people psychologically to trick them into revealing confidential information.

11. Define Phishing.

Phishing is a cyber attack where fake emails, messages, or websites are used to steal sensitive information like passwords or bank details.

12. What is Cyberstalking?

Cyberstalking is the use of electronic communication to harass, threaten, or intimidate a person repeatedly.

13. Define Malware.

Malware is malicious software designed to damage, disrupt, spy on, or gain unauthorized access to computer systems.

14. What are Botnets?

Botnets are groups of infected devices controlled by a cybercriminal to carry out large-scale cyber attacks.

15. Define Identity Theft.

Identity theft is the fraudulent use of another person’s identity or personal data for illegal activities.

16. What is Cryptojacking?

Cryptojacking is the secret mining of cryptocurrency using someone else’s system resources without permission.

10 MARKS UNIT-2

1 Examine risks of unauthorized access and long-term company damage.

Unauthorized access refers to gaining entry into a computer system, network, or data without permission. In the modern digital era, unauthorized access is a serious cyber threat that can cause immediate losses as well as long-term damage to organizations. Even a single security breach can have lasting consequences for a company.

Risks of Unauthorized Access

1. Data Theft and Data Breaches

Attackers may steal:

- Customer personal data
- Financial records
- Trade secrets
- Intellectual property

Risk:

Loss of sensitive data can lead to legal issues and loss of customer trust.

2. Financial Loss

Unauthorized access can result in:

- Direct theft of money
- Fraudulent transactions
- Cost of system recovery and investigation

Example:

Attackers accessing banking systems or payment gateways.

3. Loss of Confidentiality

Confidential business information such as:

- Business strategies
- Client databases
- Research data

can be exposed or sold to competitors.

4. System Damage and Operational Disruption

Attackers may:

- Delete or modify data
- Install malware or ransomware
- Shut down critical systems

Impact:

Business operations may come to a halt.

5. Legal and Regulatory Consequences
Companies may face:

- Heavy fines
- Lawsuits
- Regulatory penalties

especially if customer data protection laws are violated.

Long-Term Damage to Companies

1. Loss of Reputation and Brand Image
A cyber breach damages public trust.

- Customers may lose confidence
- Brand value may decline

Rebuilding reputation takes years.

2. Loss of Customers and Business Opportunities
Customers may switch to competitors due to fear of data misuse.

- Reduced customer base
- Loss of future contracts

3. Competitive Disadvantage
Stolen intellectual property or business plans can give competitors an unfair advantage.

4. Increased Security and Compliance Costs
After a breach, companies must invest heavily in:

- Advanced security infrastructure
- Cyber audits
- Employee training

5. Long-Term Financial Instability
Repeated or major cyber incidents can lead to:

- Reduced profits
- Lower investor confidence
- Decline in market value

2 Discuss tips to detect and prevent unauthorized access.

Unauthorized access occurs when an individual gains access to a computer system, network, or data without permission. Detecting and preventing unauthorized access is essential to protect confidential data, system integrity, and organizational reputation. This can be achieved through a combination of technical controls, monitoring mechanisms, and user awareness.

Tips to Detect Unauthorized Access

1. Log Monitoring and Audit Trails

- Regularly monitor system logs and access records
- Identify unusual login times, locations, or failed login attempts

Benefit:
Helps in early detection of suspicious activities.

2. Intrusion Detection Systems (IDS)

- IDS monitors network traffic for abnormal behavior
- Alerts administrators about possible intrusions

3. Account Activity Alerts

- Enable alerts for:
    - Multiple failed login attempts
    - Password changes
    - New device logins

4. Regular Security Audits

- Conduct periodic vulnerability assessments
- Identify weak points in systems and networks

5. Behavioral Analysis

- Detect unusual user behavior such as:
    - Accessing sensitive files unnecessarily
    - Sudden data downloads

Tips to Prevent Unauthorized Access

1. Strong Password Policy

- Use complex passwords (mix of letters, numbers, symbols)
- Avoid reuse of passwords
- Change passwords periodically

2. Multi-Factor Authentication (MFA)

- Require additional verification such as:
  - OTP
  - Biometric authentication
  - Security tokens

3. Access Control and Least Privilege

- Grant users only the access they need
- Remove access immediately when roles change

4. Firewalls and Network Security

- Use firewalls to block unauthorized traffic
- Secure Wi-Fi networks with strong encryption

5. Regular Software Updates

- Patch operating systems and applications regularly
- Fix known vulnerabilities that attackers exploit

6. Antivirus and Anti-Malware Tools

- Install and update security software
- Detect and remove malicious programs

7. User Awareness and Training

- Educate users about:
  - Phishing emails
  - Suspicious links
  - Safe login practices

3 Explain Computer Intrusions and misuse techniques.

Computer intrusion refers to unauthorized access into a computer system, network, or digital resource with the intention to view, steal, modify, or disrupt data and services. Intrusions are a major part of cybercrime and are often followed by misuse of systems, causing financial loss, privacy violation, and operational damage.

Computer Intrusions

A computer intrusion occurs when an attacker bypasses security mechanisms such as passwords, firewalls, or authentication controls to gain illegal access to a system.

Objectives of Intrusion

- Steal sensitive data
- Modify or delete information
- Install malware
- Disrupt services
- Gain control of systems

Common Computer Intrusion Techniques

1. Password Attacks

Attackers attempt to crack passwords using:

- Brute force attacks (trying all combinations)
- Dictionary attacks (using common words/password lists)

Impact: Unauthorized account access.

2. Malware-Based Intrusion

Malicious software is used to gain access or control.

Examples:

- Trojans creating backdoors
- Keyloggers stealing credentials
- Spyware monitoring activities

3. Phishing and Social Engineering

Attackers trick users into revealing login credentials.

Example:

Fake emails or websites asking users to "verify account details".

4. Exploiting Software Vulnerabilities

Attackers exploit:

- Unpatched software
- Weak system configurations

Example:

Using known OS or application flaws to enter systems.

5. Network-Based Attacks

Intrusions through networks using:

- Packet sniffing
- Man-in-the-Middle (MITM) attacks
- IP spoofing

Computer Misuse Techniques

Computer misuse refers to improper or illegal use of computer systems after gaining access.

1. Data Theft and Data Manipulation

- Stealing confidential files
- Altering records or databases

2. Unauthorized Resource Usage

- Using systems for illegal activities
- Mining cryptocurrency using company resources

3. Installation of Backdoors

- Creating hidden access points
- Allowing repeated unauthorized entry

4. Spreading Malware

- Using compromised systems to spread viruses, worms, or ransomware

5. Denial of Service (DoS) Attacks

- Overloading systems to make services unavailable to legitimate users

Impact of Intrusions and Misuse

- Financial loss
- Loss of data integrity and confidentiality
- Business disruption
- Legal and reputational damage

4 Define white-collar crime with examples.

Definition of White-Collar Crime

White-collar crime refers to non-violent, financially motivated crimes committed by individuals, businesses, or government professionals during the course of their occupation or professional activities.

These crimes are usually committed by educated and respectable persons who misuse their position, authority, or trust for personal or organizational gain.

The term was first introduced by sociologist Edwin H. Sutherland.

Key Characteristics of White-Collar Crime

- Non-violent in nature
- Committed for financial or professional gain
- Involves deception, fraud, or breach of trust
- Difficult to detect and investigate
- Causes huge economic loss

Examples of White-Collar Crimes

1. Fraud

Deliberate deception to gain unlawful benefit.

Example:

Bank fraud, insurance fraud, financial statement manipulation.

2. Embezzlement

Misappropriation of money or assets by a person entrusted with them.

Example:

An employee diverting company funds to a personal account.

3. Insider Trading
Illegal buying or selling of shares using confidential, non-public information.
Example:
A company executive trading stocks before public announcement.

4. Tax Evasion
Illegally avoiding payment of taxes by hiding income or falsifying records.
Example:
Showing false expenses to reduce taxable income.

5. Bribery and Corruption
Offering or accepting illegal gratification to influence decisions.
Example:
A government official accepting a bribe to approve a contract.

6. Corporate Espionage
Stealing trade secrets or confidential business information.
Example:
An employee selling competitor's business strategies.

7. Cyber White-Collar Crimes
White-collar crimes committed using computers and the internet.
Examples:

- Online banking fraud
- Identity theft
- Credit card fraud

Impact of White-Collar Crime

- Huge financial and economic loss
- Loss of public trust
- Damage to business reputation
- Negative impact on economic growth

5 Discuss viruses and malicious code.

Viruses and malicious code are forms of malware (malicious software) designed to damage computer systems, disrupt operations, steal data, or gain unauthorized access. They are widely used as cybercrime tools and pose serious threats to individuals, organizations, and governments in the digital era.

Computer Viruses

A computer virus is a type of malicious code that attaches itself to a legitimate program or file and spreads when the infected program is executed. It requires human action to activate and propagate.

Characteristics of Viruses

- Attaches to host files or programs
- Replicates itself
- Activates when the host file is executed
- Can corrupt, modify, or delete data

Types of Computer Viruses

1. File Infector Virus
   - Attaches to executable files (.exe, .com)
2. Boot Sector Virus
   - Infects the boot sector of storage devices
3. Macro Virus
   - Infects documents like Word or Excel files
4. Polymorphic Virus
   - Changes its code to avoid detection

Impact of Viruses

- System slowdown
- Data corruption or loss
- Frequent system crashes

Malicious Code

Malicious code refers to any unauthorized program or script intentionally designed to cause harm to a system, network, or data. Viruses are a type of malicious code, but malicious code also includes other threats.

Common Types of Malicious Code

1. Worms

- Self-replicating malware
- Spreads automatically through networks
- Does not require user action

Impact: Network congestion, system crashes

2. Trojan Horse

- Disguises itself as legitimate software
- Creates backdoors for attackers

Impact: Unauthorized access, data theft

3. Ransomware

- Encrypts user data
- Demands ransom for decryption

Impact: Financial loss, data unavailability

4. Spyware

- Secretly monitors user activity
- Collects sensitive information

Impact: Privacy violation, identity theft

5. Logic Bomb

- Malicious code triggered by a specific condition or time

Impact: Sudden system failure or data destruction

6. Backdoors

- Hidden access points bypassing authentication

Impact: Repeated unauthorized access

Prevention Measures

- Install updated antivirus software
- Avoid downloading unknown files
- Keep OS and applications updated
- Use firewalls and access controls
- User awareness and training

6 Compare Hacker vs Cracker traits.

In cybersecurity, hackers and crackers both possess strong technical skills, but they differ greatly in intention, ethics, and impact. While hackers may work to improve security, crackers misuse their skills for illegal and harmful activities. Understanding their traits helps in clearly distinguishing between ethical and criminal behavior in cyberspace.

Hacker vs Cracker: Trait Comparison

Aspect / Trait	**Hacker**	**Cracker**
Basic Meaning	A person who explores computer systems to understand and improve them	A person who breaks into systems with malicious intent
Intent	Learning, security testing, or system improvement	Stealing, damaging, or misusing data
Ethical Nature	Can be ethical (white-hat) or authorized	Always unethical and illegal
Permission	Often works with authorization	Works without permission

Goal	Identify vulnerabilities and strengthen security	Exploit vulnerabilities for personal gain
Impact on Users	Helps protect users and systems	Causes financial, data, and privacy loss
Legal Status	Legal when authorized	Always illegal
Techniques Used	Penetration testing, vulnerability analysis	Password cracking, malware injection
Skill Usage	Constructive and defensive	Destructive and offensive
Reputation	Respected security professional	Considered a cyber criminal

Examples

- Hacker:
  A certified ethical hacker testing a company's network to find security weaknesses.
- Cracker:
  A cyber criminal breaking into bank servers to steal customer data.

7 Detail impact of Software Piracy.

Software piracy refers to the illegal copying, distribution, installation, or use of software without proper authorization or license. It is a major form of cybercrime and intellectual property violation that affects software developers, businesses, governments, and end users in the modern digital era.

Impact of Software Piracy

1. Financial Loss to Software Developers

- Developers lose revenue due to illegal copies
- Reduced return on investment for research and development

Impact:
Discourages innovation and development of quality software.

2. Economic Loss to the Nation

- Loss of tax revenue
- Negative impact on IT industry growth

Impact:
Affects national economy and employment opportunities.

3. Legal Consequences

- Users and organizations may face:
  - Heavy fines
  - Legal actions
  - Criminal penalties

Impact:
Creates legal and compliance risks for businesses.

4. Security Risks

Pirated software often contains:

- Malware
- Viruses
- Spyware or backdoors

Impact:

Leads to data theft, system damage, and cyber attacks.

5. Lack of Updates and Support

- No access to official updates or patches
- No technical support from vendors

Impact:

Systems remain vulnerable to known security flaws.

6. Damage to Business Reputation

- Use of pirated software reflects unethical practices
- Loss of trust among customers and partners

Impact:

Harms brand image and professional credibility.

7. Reduced Quality and Reliability

- Pirated software may be unstable or incomplete
- Higher chances of crashes and data loss

Impact:

Decreases productivity and operational efficiency.

8. Impact on Employment

- Reduced revenue affects job creation
- Layoffs in software and IT sectors

Impact:

Increases unemployment and skill underutilization.

9. Encouragement of Other Cybercrimes

- Piracy supports underground cybercrime markets
- Often linked with malware distribution and fraud

Impact:

Increases overall cybercrime ecosystem.

10. Ethical and Moral Impact

- Promotes unethical behavior
- Disrespects intellectual property rights

Impact:

Weakens respect for law and digital ethics.

8 Identify law enforcement roles in cybercrime.

Law enforcement agencies play a crucial role in preventing, detecting, investigating, and prosecuting cybercrime. With the rapid increase in digital crimes such as hacking, fraud, identity theft, and cyber terrorism, law enforcement has expanded its functions to include technical, legal, and international coordination roles.
Key Roles of Law Enforcement in Cybercrime

1. Prevention of Cybercrime

- Conduct cyber awareness programs for the public
- Educate users about phishing, online fraud, and safe internet practices
- Issue advisories and warnings about new cyber threats

Purpose:
Reduce cybercrime by improving public awareness.

2. Detection and Monitoring

- Monitor cyberspace for suspicious activities
- Track online frauds, illegal websites, and cyber threats
- Use cyber surveillance and threat intelligence tools

Purpose:
Early identification of cyber offences.

3. Investigation of Cybercrimes

- Register cybercrime complaints and FIRs
- Identify attackers through IP tracking, log analysis, and digital trails
- Collect technical and electronic evidence

Purpose:
Find offenders and understand the crime mechanism.

4. Digital Forensics

- Seize and examine digital devices (computers, mobiles, servers)
- Recover deleted data and analyze malware
- Maintain chain of custody for electronic evidence

Purpose:
Produce legally admissible digital evidence in courts.

5. Enforcement of Cyber Laws

- Enforce laws such as:
    - Information Technology Act
    - Cybercrime-related IPC sections
- Take action against offenders through arrests and prosecution

Purpose:
Ensure legal accountability and punishment.

6. Coordination with Other Agencies

- Coordinate with:
  - Banks and financial institutions
  - Internet Service Providers (ISPs)
  - CERTs and cybersecurity agencies

Purpose:
Speedy response and effective investigation.

7. International Cooperation

- Work with foreign law enforcement agencies
- Share intelligence and evidence
- Handle cross-border cybercrime cases

Purpose:
Address the borderless nature of cybercrime.

8. Cybercrime Reporting and Support

- Provide platforms for reporting cybercrime
- Assist victims in recovery and legal procedures

Purpose:
Support victims and improve reporting mechanisms.

9. Capacity Building and Training

- Train police officers in:
  - Cyber investigation techniques
  - Digital forensics
  - Emerging technologies

Purpose:
Strengthen law enforcement capabilities.

9 Explain unauthorized access and discuss its risks.

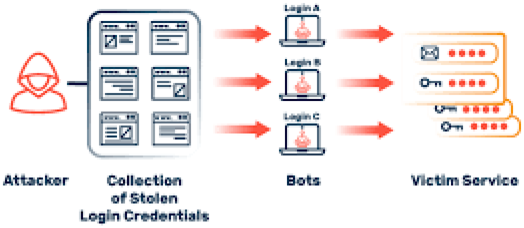
Unauthorized access refers to the act of gaining entry into a computer system, network, application, or data without permission of the owner or authorized user. It is a common cybercrime and often acts as the first step for many other cyber attacks such as data theft, fraud, and malware installation.

Meaning of Unauthorized Access

Unauthorized access occurs when a person:

- Logs into a system using stolen or guessed credentials
- Bypasses security controls
- Exploits system vulnerabilities
- Uses another user’s account without consent

Such access violates confidentiality, integrity, and security of information systems.



Risks of Unauthorized Access

1. Data Theft

Attackers may steal:

- Personal information
- Financial records
- Customer databases
- Confidential business data

Risk:

Leads to identity theft, fraud, and loss of privacy.

2. Financial Loss

Unauthorized access can result in:

- Illegal money transfers
- Online banking fraud
- Costly system recovery

Risk:

Direct financial damage to individuals and organizations.

3. Loss of Privacy

Personal emails, photos, and messages may be accessed or misused.

Risk:

Emotional distress, blackmail, and reputational harm.

4. Data Manipulation or Destruction

Attackers may:

- Modify important records
- Delete critical data
- Corrupt databases

Risk:

Loss of data integrity and business disruption.

5. Malware Installation

Unauthorized access allows attackers to install:

- Viruses
- Trojans
- Ransomware
- Spyware

Risk:

Long-term system compromise and repeated attacks.

6. Service Disruption

Critical systems may be shut down or misused.

Risk:

Downtime, reduced productivity, and customer dissatisfaction.

7. Legal and Compliance Issues

Organizations may face:

- Legal action
- Regulatory penalties
- Loss of licenses

Risk:

Failure to protect user data leads to legal consequences.

8. Damage to Reputation

Security breaches reduce trust among:

- Customers
- Partners
- Stakeholders

Risk:

Long-term brand and credibility damage.

10 Analyze long-term damage caused by unauthorized access.

Unauthorized access occurs when an attacker gains entry into a computer system, network, or data without permission. While the immediate effects may include data loss or service disruption, the long-term damage caused by unauthorized access is often more severe and lasting, affecting an organization’s reputation, finances, operations, and trust.

Long-Term Damage of Unauthorized Access

1. Loss of Reputation and Brand Value

Once unauthorized access becomes public:

- Customers lose trust
- Brand image is permanently affected

Long-term effect:
Rebuilding reputation can take years and may never fully recover.

2. Loss of Customer Trust and Loyalty
Customers may fear misuse of their personal data.
Long-term effect:

- Reduced customer base
- Shift of customers to competitors

3. Continuous Financial Loss
Beyond immediate losses, companies face:

- Legal fines and penalties
- Compensation to affected customers
- Increased cybersecurity spending

Long-term effect:
Reduced profitability and financial instability.

4. Legal and Regulatory Consequences
Organizations may face:

- Lawsuits
- Regulatory scrutiny
- Long-term compliance obligations

Long-term effect:
Ongoing legal costs and restrictions on business operations.

5. Competitive Disadvantage
Attackers may steal:

- Trade secrets
- Intellectual property
- Business strategies

Long-term effect:
Loss of market advantage and innovation capability.

6. Operational Disruption
Unauthorized access can permanently affect:

- System reliability
- Data integrity
- Workflow efficiency

Long-term effect:
Reduced productivity and higher operational costs.

7. Increased Cybersecurity Costs

After a breach, companies must invest heavily in:

- Advanced security tools
- Regular audits
- Employee training

Long-term effect:
Higher operational expenditure.

8. Employee Morale and Productivity Impact

Repeated security incidents create:

- Stress
- Fear of blame
- Reduced confidence

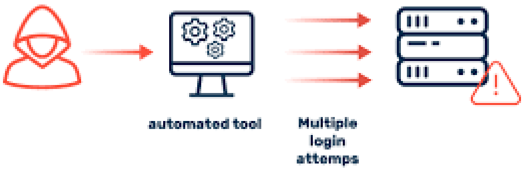
Long-term effect:
Lower employee productivity and higher attrition.

9. Loss of Business Opportunities

Partners and investors may hesitate to collaborate.
Long-term effect:
Missed growth opportunities and reduced market credibility.

11 Explain computer intrusions and intrusion techniques.

Computer intrusion refers to unauthorized access into a computer system, network, or digital resource with the intention to steal data, modify information, disrupt services, or gain control of the system. Intrusions are a major cybercrime threat and often act as the entry point for further misuse, such as malware installation, data theft, or denial-of-service attacks.



Meaning of Computer Intrusion

A computer intrusion occurs when an attacker bypasses security controls like passwords, authentication mechanisms, firewalls, or access permissions to enter a system without authorization.

Objectives of Computer Intrusions

- Steal sensitive or confidential data
- Modify or delete information
- Install malware or backdoors
- Disrupt normal system operations
- Use systems for illegal activities

Common Computer Intrusion Techniques

1. Password Attacks

Attackers try to obtain valid login credentials.
Types:

- Brute force attack – Trying all possible password combinations
- Dictionary attack – Using common passwords or wordlists

Impact:
Unauthorized account access.

2. Phishing and Social Engineering

Attackers deceive users into revealing login details.
Techniques include:

- Fake emails
- Fraudulent websites
- Impersonation messages

Impact:
Credential theft without technical hacking.

3. Malware-Based Intrusion

Malicious software is used to gain access or control.
Examples:

- Trojans creating backdoors
- Keyloggers capturing passwords
- Spyware monitoring activities

4. Exploiting Software Vulnerabilities

Attackers exploit weaknesses in:

- Operating systems
- Applications
- Unpatched software

Example:
Using known security flaws to gain system access.

5. Network-Based Attacks

Intrusions carried out through networks.
Techniques include:

- Packet sniffing – Capturing network data
- Man-in-the-Middle (MITM) – Intercepting communication
- IP spoofing – Faking IP addresses

6. Backdoor Attacks

Attackers install hidden access points to:

- Re-enter systems repeatedly
- Maintain long-term control

7. Insider Attacks

Authorized users misuse their access intentionally or unintentionally.

Examples:

- Employees stealing data
- Sharing passwords

Impact of Computer Intrusions

- Data theft and privacy violation
- Financial loss
- Service disruption
- Legal and reputational damage

12 Describe white-collar crimes with cyber examples.

White-collar crimes are non-violent offences committed for financial or professional gain by individuals who misuse their position, authority, trust, or technical knowledge. In the digital era, many white-collar crimes are committed using computers, networks, and the internet, making them closely linked with cybercrime.

The term *white-collar crime* was introduced by sociologist Edwin H. Sutherland.

Major White-Collar Crimes with Cyber Examples

1. Cyber Fraud

Deliberate deception using digital platforms to gain financial benefit.

Cyber Examples:

- Online banking fraud
- Credit/debit card fraud
- Fake e-commerce websites

Impact: Financial loss to individuals and institutions.

2. Identity Theft

Stealing personal information and using it illegally.

Cyber Examples:

- Using stolen Aadhaar/PAN details for loans
- Creating fake social media or email accounts

Impact: Financial loss and loss of personal reputation.

3. Embezzlement (Digital Form)
Misappropriation of funds using computerized systems.
Cyber Examples:

- Employee transferring company funds through online banking
- Manipulating digital accounting records

Impact: Organizational financial loss.

4. Insider Trading (Using Digital Systems)
Illegal trading of shares using confidential digital information.
Cyber Examples:

- Accessing internal emails or databases for unpublished financial data
- Trading stocks before public announcements

Impact: Market manipulation and unfair advantage.

5. Corporate Espionage
Stealing confidential business information using cyber means.
Cyber Examples:

- Hacking competitor databases
- Stealing trade secrets via malware or email attacks

Impact: Loss of competitive advantage.

6. Tax Evasion Using Technology
Avoiding taxes by manipulating digital records.
Cyber Examples:

- Filing false online tax returns
- Hiding income using digital transactions

Impact: Loss of government revenue.

7. Intellectual Property Theft
Illegal copying or misuse of digital intellectual property.
Cyber Examples:

- Software piracy
- Illegal downloading and distribution of copyrighted content

Impact: Financial loss to creators and companies.

8. Cyber Money Laundering
Using digital platforms to hide illegal money.
Cyber Examples:

- Using online wallets and cryptocurrencies
- Routing money through multiple digital accounts

Impact: Supports organized crime and terrorism.

Impact of Cyber White-Collar Crimes

- Huge economic and financial losses
- Loss of public trust in digital systems
- Legal and regulatory challenges
- Damage to business reputation

13 Discuss viruses and malicious code propagation.

Viruses and malicious code are types of malware designed to damage systems, steal data, disrupt operations, or gain unauthorized access.
Propagation refers to the methods by which viruses and malicious code spread from one system to another. Understanding propagation mechanisms is essential to prevent large-scale cyber infections.

Computer Viruses

A computer virus is a malicious program that attaches itself to a legitimate file or program and spreads when the infected file is executed.
Viruses generally require human action to propagate.

Virus Propagation Methods

1. **File Execution**
   - Virus attaches to executable files (.exe, .com)
   - Spreads when the user runs the infected file
2. **Email Attachments**
   - Infected attachments sent through emails
   - Virus activates when attachment is opened
3. **Removable Media**
   - USB drives, CDs, external hard disks
   - Virus spreads when infected media is connected
4. **Macro-Based Documents**
   - Infected Word or Excel files
   - Spreads when macros are enabled

Malicious Code:

Malicious code refers to any unauthorized program or script designed to harm systems, networks, or data.
Viruses are one type of malicious code, but others spread automatically without user action.

Propagation of Common Malicious Code

1. Worms

- Self-replicating malware
- Spread automatically through networks

Propagation Method:

- Exploiting network vulnerabilities
- Sending copies through email or shared folders

Impact:

Rapid large-scale infection.

2. Trojan Horses

- Disguised as legitimate software

Propagation Method:

- Free software downloads
- Fake updates or cracked software

Impact:

Creates backdoors and enables repeated access.

3. Ransomware

- Encrypts files and demands ransom

Propagation Method:

- Phishing emails
- Malicious websites
- Exploited vulnerabilities

Impact:

Data unavailability and financial loss.

4. Spyware and Keyloggers

- Secretly monitor user activities

Propagation Method:

- Bundled with free software
- Malicious links and downloads

Impact:

Data theft and privacy violation.

5. Botnets

- Network of infected systems controlled remotely

Propagation Method:

- Malware infection via phishing or vulnerabilities

Impact:

Used for DDoS attacks and spam campaigns.

Impact of Malware Propagation

- Rapid spread across systems and networks
- Large-scale data breaches
- Financial and operational damage
- Threats to national and organizational security

Prevention of Virus and Malware Propagation

- Updated antivirus and anti-malware tools
- Regular system and software updates
- Email filtering and attachment scanning
- Disabling unnecessary macros
- User awareness and safe browsing practices

14 Compare hacking and cracking.

In cybersecurity, hacking and cracking are often confused, but they differ mainly in intent, legality, and impact. Both involve technical skills, yet hacking can be ethical, while cracking is always malicious and illegal.

Hacking vs Cracking

Basis	Hacking	Cracking
Meaning	Gaining access to computer systems or networks to understand, test, or improve security	Breaking into systems illegally to steal, damage, or misuse data
Intent	Can be ethical, educational, or defensive	Always malicious and harmful
Legality	Legal when done with permission (ethical hacking)	Always illegal
Authorization	Usually performed with owner’s consent	Performed without permission
Objective	Identify vulnerabilities and strengthen security	Exploit vulnerabilities for personal gain
Nature	Constructive and preventive	Destructive and offensive
Impact on Users	Helps improve system safety	Causes data loss, privacy violation, and financial damage
Examples	Penetration testing, security audits	Password cracking, data theft, ransomware attacks
Professional Role	Cybersecurity expert or ethical hacker	Cyber criminal

15 Examine impact of software piracy.

Software piracy is the illegal copying, distribution, installation, or use of software without a valid license. In the modern digital era, software piracy is a serious cybercrime that affects software developers, businesses, governments, and end users. Though it may seem harmless, its impact is long-term and wide-ranging.

Major Impacts of Software Piracy

1. Financial Loss to Software Developers

- Loss of revenue due to illegal copies
- Reduced funds for research and development

Impact:
Discourages innovation and quality software development.

2. Economic Loss to the Nation

- Reduction in tax revenue
- Negative impact on IT industry growth

Impact:
Affects national economy and employment opportunities.

3. Legal Consequences

- Piracy is punishable under copyright and cyber laws
- Users and organizations may face:
  - Heavy fines
  - Legal action
  - Criminal penalties

4. Security Risks
Pirated software often contains:

- Malware
- Viruses
- Spyware or backdoors

Impact:
Leads to data theft, system compromise, and cyber attacks.

5. No Updates or Technical Support

- No access to official patches or security updates
- No vendor support

Impact:
Systems remain vulnerable to known security flaws.

6. Damage to Business Reputation

- Use of pirated software reflects unethical practices
- Loss of trust from customers and partners

Impact:
Harms brand value and corporate credibility.

7. Reduced Software Quality and Reliability

- Pirated software may be unstable or incomplete
- Frequent crashes and data loss

Impact:
Decreases productivity and operational efficiency.

8. Impact on Employment

- Reduced revenue affects job creation
- Downsizing in software and IT sectors

Impact:
Increases unemployment and skill underutilization.

9. Encouragement of Other Cybercrimes

- Supports underground cybercrime markets
- Often linked with fraud and malware distribution

Impact:
Strengthens the cybercrime ecosystem.

10. Ethical and Moral Impact

- Violates intellectual property rights
- Promotes unethical digital behavior

Impact:
Weakens respect for law and digital ethics.

16 Discuss law enforcement agencies' role.

Law enforcement agencies play a critical role in preventing, detecting, investigating, and prosecuting cybercrimes. With the rapid growth of digital technologies, their responsibilities have expanded to include technical expertise, digital forensics, legal enforcement, and international cooperation to effectively handle cyber offences.

Key Roles of Law Enforcement Agencies

1. Prevention and Awareness

- Conduct cyber awareness programs for citizens and organizations
- Educate users about phishing, online fraud, identity theft, and safe internet practices
- Issue public alerts and advisories on emerging cyber threats

Objective: Reduce cybercrime through awareness and prevention.

2. Detection and Monitoring

- Monitor cyberspace for suspicious activities and cyber threats
- Track illegal online activities, fake websites, and cyber fraud networks
- Use cyber surveillance and threat intelligence tools

Objective: Early identification of cyber offences.

3. Registration of Complaints

- Receive cybercrime complaints and register FIRs
- Provide online and offline reporting mechanisms for victims

Objective: Ensure timely reporting and legal action.

4. Investigation of Cybercrimes

- Identify offenders using IP tracking, log analysis, and digital trails
- Analyze methods used in cyber attacks
- Collect electronic evidence

Objective: Trace criminals and establish facts of the crime.

5. Digital Forensics

- Seize and examine computers, mobiles, servers, and storage devices
- Recover deleted or encrypted data
- Maintain proper chain of custody of digital evidence

Objective: Produce legally admissible evidence in courts.

6. Enforcement of Cyber Laws

- Enforce cyber laws such as the IT Act and relevant IPC provisions
- Arrest offenders and initiate prosecution

Objective: Ensure punishment and legal accountability.

7. Coordination with Stakeholders

- Coordinate with banks, ISPs, social media platforms, and CERT teams
- Work with cybersecurity experts and private organizations

Objective: Faster response and effective investigation.

8. International Cooperation

- Collaborate with foreign law enforcement agencies
- Share intelligence and evidence in cross-border cybercrime cases

Objective: Address the global and borderless nature of cybercrime.

9. Capacity Building and Training

- Train officers in cyber investigation techniques
- Upgrade skills in digital forensics and emerging technologies

Objective: Strengthen institutional capability.

2 MARKS UNIT-2

1. What is Unauthorized Access?

Unauthorized access is the act of gaining access to a computer system, network, or data without permission of the owner or authorized user.

2. Define Snooping.

Snooping is the act of secretly accessing or monitoring another person's computer data, emails, or files without authorization.

3. What is Bribery in cyber context?

Cyber bribery refers to offering or accepting illegal digital benefits (money, data, favors) to influence decisions or gain unauthorized access using electronic means.

4. Explain Eavesdropping.

Eavesdropping is the act of secretly intercepting and listening to private digital communications such as emails, phone calls, or network data.

5. What is a Trojan Horse?

A Trojan Horse is a type of malware that disguises itself as legitimate software but performs malicious activities once installed.

6. Define Software Piracy.

Software piracy is the illegal copying, distribution, or use of software without a valid license or permission from the owner.

7. What is a Mail Bomb?

A mail bomb is a cyber attack in which a large number of emails are sent to a target to overload and crash their email server.

8. Define Cyberstalking as Obscenity.

Cyberstalking as obscenity refers to using the internet to repeatedly harass, threaten, or send obscene messages or content to a person.

9. Define Eavesdropping.

Eavesdropping is the unauthorized interception of private electronic communications between two or more parties.

10. What is Cyber Obscenity?

Cyber obscenity refers to publishing, transmitting, or viewing obscene or sexually explicit content using digital platforms like the internet.

11. Define White-Collar Crime.

White-collar crime is a non-violent crime committed for financial gain by professionals or officials using their position, trust, or authority.