

# SPPU-BE-COMP-CONTENT – KSKA Git

## CSDF UNIT 1 – PYQ Answers

➤ OCT – 2022

Q1)

a) Define cybercrime. Explain types of cybercrime. [5]

Cybercrime refers to **criminal activities carried out using computers, digital devices, or the internet**. These crimes are intended to harm individuals, steal data, damage systems, or disrupt services

### Types of Cybercrime:

Cybercrimes can be categorized based on the target or the nature of the crime:

#### 1. Crime Against Individuals:

These crimes target a person's personal data, online presence, or privacy.

**Examples include:** Identity theft, cyberstalking, email spoofing, and online harassment.

#### 2. Crime Against Property:

These involve damaging or stealing digital property or data.

**Examples include:** Hacking bank accounts, ransomware attacks, software piracy, and data breaches.

#### 3. Crime Against Organizations or Governments:

These attacks are aimed at disrupting services or stealing sensitive information from institutions.

**Examples include:** Cyber terrorism, DDoS attacks, cyber espionage, and website defacement.

#### 4. Cyber Extortion:

The attacker threatens to cause harm (like data leaks or service disruption) unless a ransom is paid.

**Examples include:** Ransomware demanding cryptocurrency or blackmail via hacked data.

#### 5. Drug Trafficking & Illegal Trade via Dark Web:

Criminals use the dark web to conduct illegal trade anonymously.

**Examples include:** Selling drugs, weapons, or fake documents using hidden marketplaces.

### b) Explain the process of security risk analysis. [5]

Security Risk Analysis is the process of **identifying, analyzing, evaluating, and addressing** risks that could compromise the **confidentiality, integrity, or availability (CIA)** of an organization's data and systems.



#### 1. Identify

- Identify **assets** that need protection, such as data, hardware, software, and networks.
- Also recognize **threats** (e.g., hackers, malware) and **vulnerabilities** (e.g., weak passwords, outdated systems).

*Example:* Customer database may be exposed due to an unpatched system.

#### 2. Analyze

- Analyze how likely a threat is to exploit a vulnerability.
- Consider **risk levels** using methods like **risk matrices** or **risk scoring** (Low / Medium / High).

*Example:* High chance of ransomware if antivirus is outdated.

#### 3. Evaluate

- Evaluate and **prioritize risks** based on business impact.
- Decide which risks are most urgent and which can be monitored.

## SPPU-BE-COMP-CONTENT – KSKA Git

*Example:* Data breach risk is ranked high due to sensitive information involved.

### 4. Address

- Select a **risk response strategy**:
  - Accept – if risk is minor,
  - Mitigate – apply controls to reduce risk,
  - Transfer – buy insurance or outsource,
  - Avoid – change operations to remove risk.

*Example:* Implementing a firewall to block unauthorized access.

### c) Give the reasons behind the need for information security. [5]

**Information Security** refers to the practice of protecting digital information from unauthorized access, use, disclosure, disruption, modification, or destruction.

#### Reasons for the Need of Information Security:

##### 1. Protect Confidential Data

- Sensitive data like customer records, financial details, and intellectual property must be protected from unauthorized access.
- Example: Prevent data leaks or identity theft.

##### 2. Ensure Data Integrity

- Information must remain accurate and unaltered during storage or transmission.
- Example: Prevent tampering or corruption of files in databases.

##### 3. Maintain Availability of Services

- Systems and data must be accessible to authorized users when needed.
- Example: Prevent DoS (Denial of Service) attacks that shut down systems.

##### 4. Prevent Cyber Attacks and Breaches

- Rising threats like malware, ransomware, and phishing require strong security controls.
- Example: Avoid financial and reputational loss due to hacking.

## SPPU-BE-COMP-CONTENT – KSKA Git

### 5. Compliance with Legal and Regulatory Requirements

- Organizations must follow cybersecurity laws like IT Act, GDPR, HIPAA, etc.
- Example: Avoid penalties and legal issues due to non-compliance.

### 6. Build Trust and Reputation

- A secure environment improves customer trust and brand reputation.
- Example: A company known for data leaks will lose customers.

## Q2

### a) Explain different threats to Information System. [5 Marks]

**Information System Threats** are potential dangers that can compromise the **confidentiality, integrity, or availability** of data, systems, or networks.

#### Different Types of Threats to Information Systems:

##### 1. Malware (Malicious Software)

- Includes viruses, worms, Trojans, ransomware, spyware, etc.
- These programs can **steal data, damage systems, or lock files** for ransom.

*Example:* Ransomware encrypts user files and demands payment.

##### 2. Phishing Attacks

- Fraudulent emails or messages trick users into revealing sensitive information like passwords or bank details.
- Often appear to be from legitimate sources.

*Example:* Fake bank email asking you to “verify your account.”

##### 3. Insider Threats

- Current or former employees, contractors, or business partners who misuse access to cause harm.
- May be **intentional** (revenge, fraud) or **unintentional** (human error).

*Example:* Employee leaking customer data to competitors.

#### 4. Denial of Service (DoS/DDoS) Attacks

- Flooding a server or network with excessive traffic to make it unavailable.
- Aimed at **disrupting services** and causing business loss.

*Example:* Online banking system crashes due to DDoS attack.

#### 5. Social Engineering

- Manipulating people to disclose confidential information or perform risky actions.
- Exploits **human psychology** rather than technical flaws.

*Example:* Someone calls pretending to be IT support and asks for your login password.

#### b) What do you mean by Cyber extortion, Drug trafficking? [5]

##### 1. Cyber Extortion:

- **Definition:**  
Cyber extortion is a type of cybercrime where an attacker **demands money or other favors** from a victim by threatening to launch an attack, release stolen data, or cause harm to the digital infrastructure.
- **Common Methods:**
  - **Ransomware:** Encrypts files and demands payment for decryption.
  - **Doxxing threats:** Leaking personal or sensitive info unless paid.
  - **DDoS-for-ransom:** Threatening or launching a DDoS attack unless payment is made.
- **Example:**  
An attacker locks a hospital's medical records and demands ₹10 lakhs in cryptocurrency to restore access.

##### 2. Drug Trafficking (via Cyberspace):

- **Definition:**  
Drug trafficking in the context of cybercrime refers to **illegally buying, selling, or distributing narcotics** through **online platforms**, especially the **dark web** using encrypted tools and anonymous networks.
- **Common Platforms and Methods:**
  - **Dark Web markets** (e.g., Silk Road-type platforms).

## SPPU-BE-COMP-CONTENT – KSKA Git

- Use of **cryptocurrencies** like Bitcoin for anonymous transactions.
- Hidden services using **Tor** browser and end-to-end encryption.
- **Example:**  
An individual purchases illegal drugs using a dark web marketplace and makes payment via Bitcoin to avoid being traced.

### c) Describe in detail about Cyber Crime against an Individual and Organization. [5]

#### 1. Cyber Crime Against an Individual:

These crimes are targeted directly at **individual persons** with the intent to **harm, defame, harass, or steal personal data**.

##### Common Types:

- **Identity Theft:** Stealing someone's personal data like Aadhar number, PAN, bank credentials, etc., to commit fraud.
- **Cyberstalking:** Repeated online harassment or threats via email, social media, etc.
- **Phishing:** Tricking individuals into revealing confidential information through fake emails or websites.
- **Email Spoofing:** Sending emails that appear to be from trusted sources to mislead victims.

##### Example:

A hacker sends a fake job offer email to collect personal and banking details from the victim.

#### 2. Cyber Crime Against an Organization:

These crimes are aimed at **companies, institutions, or government bodies**, often to steal data, disrupt operations, or demand ransom.

##### Common Types:

- **Hacking & Data Breaches:** Unauthorized access to servers to steal company secrets, customer data, or intellectual property.
- **Ransomware Attacks:** Encrypting the organization's data and demanding payment to restore access.
- **Denial of Service (DoS) Attacks:** Crashing servers or websites by flooding them with traffic.
- **Insider Threats:** Employees or former staff leaking or misusing sensitive data.

**Example:** A ransomware attack locks all files in a hospital's server, halting patient care and demanding payment in cryptocurrency.

➤ SEP 2023

Q1)

a) What are different threats to information system? Explain any two in details. [7]

**Threats to Information Systems** are potential events or actions that can cause **harm to data, software, hardware, or networks**, affecting the **confidentiality, integrity, or availability (CIA)** of the system.

**List of Different Threats to Information Systems:**

1. Malware (Viruses, Worms, Trojans, Ransomware)
2. Phishing Attacks
3. Insider Threats
4. Denial of Service (DoS/DDoS) Attacks
5. Social Engineering
6. Data Breaches
7. Man-in-the-Middle Attacks
8. SQL Injection
9. Password Attacks
10. Zero-Day Exploits

## 1. Malware (Malicious Software):

- Malware refers to **malicious programs** designed to damage, steal, or disrupt systems or data.
- Types include:
  - **Viruses:** Attach themselves to files and spread.
  - **Worms:** Self-replicating programs that spread across networks.
  - **Trojans:** Disguise as legitimate software but give unauthorized access.
  - **Ransomware:** Encrypts files and demands payment for decryption.

### **Example:**

WannaCry ransomware affected thousands of systems globally by locking files and demanding ransom in Bitcoin.

## 2. Phishing Attacks:

## SPPU-BE-COMP-CONTENT – KSKA Git

- Phishing is a **social engineering technique** used to trick individuals into revealing personal or sensitive information.
- It usually involves fake emails, websites, or messages that appear to come from trusted sources.
- Victims may unknowingly provide login credentials, credit card details, or install malware.

### *Example:*

An email pretending to be from a bank asks the user to “verify” account info via a fake link that captures their login credentials.

### **b) List different types of cybercrime. Explain any two in detail [8]**

**Cybercrime** refers to any illegal activity involving computers, digital devices, or networks, either as a **target** or a **tool** to commit the crime.

#### **List of Different Types of Cybercrime:**

1. Hacking
2. Identity Theft
3. Cyberstalking
4. Phishing
5. Cyber Extortion
6. Ransomware Attacks
7. Online Drug Trafficking
8. Cyber Terrorism
9. Financial Fraud
10. Cyberbullying

#### **Explanation of Any Two in Detail:**

##### **1. Identity Theft:**

- In identity theft, a criminal **steals personal information** such as name, Aadhar number, PAN, credit card number, or login credentials to impersonate someone.
- This information is then used to **access bank accounts, commit fraud, or make illegal purchases.**
- It can result in **financial loss**, reputation damage, and legal issues for the victim.

### *Example:*

A fraudster uses someone's credit card details to make unauthorized online purchases.

##### **2. Ransomware Attack:**

- Ransomware is a type of malware that **encrypts the victim's data** and demands payment (usually in cryptocurrency) to restore access.



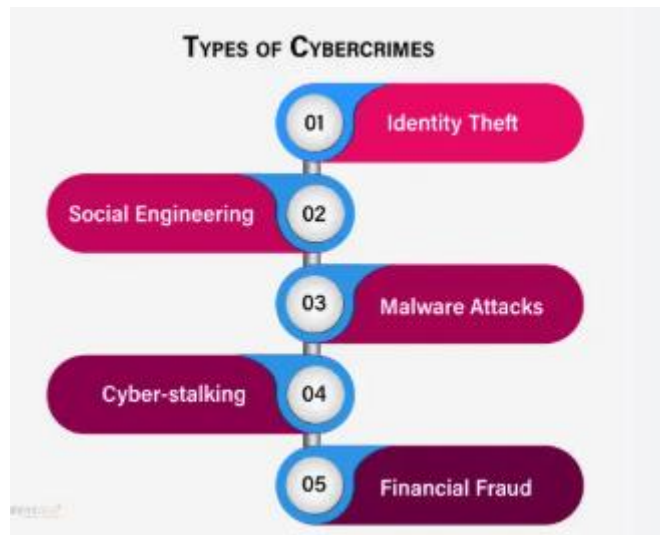
## SPPU-BE-COMP-CONTENT – KSKA Git

- It affects individuals, companies, and even governments, disrupting operations and causing massive losses.
- Paying the ransom doesn't guarantee data recovery and may encourage further attacks.

*Example:*

In 2017, the **WannaCry ransomware** attack impacted healthcare systems, banks, and companies across 150+ countries.

Cybercrimes are becoming more advanced and widespread. It is essential to stay aware, adopt **cybersecurity practices**, and follow **legal frameworks** to protect individuals and organizations from these threats.



### Q2

#### a) Elaborate the process of risk analysis in cyber security [7]

**Risk analysis in cybersecurity** is the process of **identifying potential threats, vulnerabilities, and the impact of cyber incidents** on assets, and then **evaluating the likelihood and consequences** to determine the level of risk.

#### Steps in Risk Analysis Process:

##### 1. Identify Assets

- Recognize critical digital assets like data, systems, hardware, and applications.
- Example: Customer database, payment gateway, internal network.

##### 2. Identify Threats

## SPPU-BE-COMP-CONTENT – KSKA Git

- Determine possible threats that can harm the system.
- Examples: Malware, phishing, ransomware, insider attacks.

### 3. Identify Vulnerabilities

- Find weaknesses that can be exploited by threats.
- Examples: Outdated software, weak passwords, unpatched systems.

### 4. Determine Likelihood of Exploitation

- Assess how likely each threat is to exploit a specific vulnerability.
- Often rated as **Low / Medium / High**.

### 5. Determine Impact

- Evaluate the **business or operational impact** if the threat is successful.
- Consider **financial loss, data leakage, service disruption**, legal implications.

### 6. Calculate Risk Level

- Combine likelihood and impact to **assign a risk score** or priority.
- Can use tools like **risk matrix, heat maps**, or **quantitative risk models**.

### 7. Prepare for Risk Response

- After risk levels are understood, the organization can plan actions like mitigation, acceptance, transfer, or avoidance.

## b) Write short note on : [8]

### i) Cyber extortion

### ii) Drug trafficking

#### i) Cyber Extortion

- **Definition:**  
Cyber extortion is a type of cybercrime where an attacker threatens to **damage, steal, or release sensitive data** or **disrupt services** unless a ransom is paid.
- **Common Methods:**
  - **Ransomware attacks:** Encrypts files and demands payment to decrypt them.

## SPPU-BE-COMP-CONTENT – KSKA Git

- **Threatening data leaks:** Hackers demand money in exchange for not leaking private or corporate data.
- **DDoS for ransom:** Attackers threaten to crash systems unless paid.
- **Impact:**  
Can cause **financial loss**, **reputation damage**, and **business disruption**.
- **Example:**  
The WannaCry ransomware attack locked files on computers worldwide and demanded ransom in cryptocurrency.

### ii) Drug Trafficking (via Cyberspace)

- **Definition:**  
Cyber-enabled drug trafficking involves the **illegal buying and selling of drugs using the internet**, especially the **dark web**, and anonymous payment methods.
- **How it Works:**
  - Carried out using **encrypted websites** on the dark web.
  - **Cryptocurrencies** (like Bitcoin) are used to hide the buyer's/seller's identity.
  - **Tor networks** allow untraceable browsing.
- **Impact:**  
It poses a threat to **public safety**, enables **global crime syndicates**, and is hard to trace for law enforcement.
- **Example:**  
Darknet marketplaces like Silk Road were used for large-scale illegal drug sales before being shut down by the FBI.

### ➤ SEP -2024

#### Q1

#### a) What is Cybercrime? How to prevent it? [5]

Cybercrime refers to any **illegal activity involving computers, digital devices, or the internet**, either as a **tool**, **target**, or both.  
It includes offenses like **hacking, phishing, identity theft, cyberstalking, ransomware attacks**, and more.

#### Prevention of Cybercrime (Point-wise):

## SPPU-BE-COMP-CONTENT – KSKA Git

### 1. Use Strong Passwords

- Use complex, unique passwords for all accounts.
- Change passwords regularly and avoid sharing them.

### 2. Install and Update Antivirus & Firewalls

- Protect systems with updated antivirus software and firewalls.
- Keeps malware and unauthorized access in check.

### 3. Enable Two-Factor Authentication (2FA)

- Adds an extra security layer to login processes.
- Prevents access even if password is stolen.

### 4. Avoid Clicking Unknown Links or Attachments

- Be cautious of suspicious emails or websites.
- Prevents phishing, ransomware, and spyware attacks.

### 5. Regular Data Backup

- Keep backups of important data in secure locations.
- Helps in recovery after ransomware or data loss incidents.

### 6. Awareness & Training

- Users should be educated about cyber threats and safe practices.
- Avoids human errors which are a major cause of cyber incidents.

Cybercrime is a growing threat in today's digital world. **Awareness, technology, and safe online behavior** are the best ways to prevent it.

### b) What is the Need for Information Security? [5]

**Information Security** is the practice of protecting **data, systems, and networks** from unauthorized access, misuse, modification, or destruction.

Its main objective is to preserve the **Confidentiality, Integrity, and Availability (CIA)** of information.



### Need for Information Security :

#### 1. Protection of Sensitive Data

- Prevents unauthorized access to personal, financial, or business-critical information
- *Example:* Protects customer credit card details from hackers.

#### 2. Maintain Data Integrity

- Ensures that data is accurate and not altered by unauthorized parties.
- *Example:* Prevents tampering with medical records or financial reports.

#### 3. Ensure Availability of Services

- Systems and data must be available to authorized users when needed.
- *Example:* Avoids service disruption due to cyberattacks like DoS.

#### 4. Prevent Cyber Threats and Attacks

- Shields systems from malware, phishing, ransomware, and hacking attempts.
- *Example:* Protects company networks from ransomware that locks files.

### 5. Legal Compliance and Reputation Management

- Helps organizations comply with laws like IT Act, GDPR, etc., and maintain trust.
- *Example:* Avoids penalties and maintains customer confidence.

Information security is essential in today's digital age to **protect data, build trust, ensure business continuity**, and stay legally compliant.

#### c) What are the Types of Cyber Criminals? [5]

**Cyber criminals** are individuals or groups who **use technology and the internet to commit illegal acts**, such as stealing data, damaging systems, or conducting fraud.

They are categorized based on their **intent, skills, and target**.

#### Types of Cyber Criminals:

##### 1. Hacktivists

- Use hacking to promote **political, social, or ideological agendas**.
- Aim to deface websites, leak data, or disrupt systems for attention or protest.

*Example:* Anonymous group hacking government sites.

##### 2. Script Kiddies

- Inexperienced hackers who use **pre-written tools and scripts** to attack systems just for fun or attention.
- They typically don't understand the inner workings of the tools they use.

*Example:* Teenagers launching a simple DDoS attack using free tools.

##### 3. Cyber Terrorists

- Use cyberattacks to **spread fear, violence, or political unrest**.
- Often target critical infrastructure like power grids, hospitals, or transport systems.

*Example:* Disrupting air traffic control systems or defense databases.

##### 4. Insider Threats

## SPPU-BE-COMP-CONTENT – KSKA Git

- Individuals **within an organization** (employees, contractors) who misuse their access for personal gain or revenge.
- Can cause serious damage because they have authorized access.

*Example:* An employee leaking customer data to a competitor.

### 5. Organized Cybercrime Groups

- Highly skilled groups that operate **like criminal enterprises** for financial gain.
- Conduct large-scale attacks like ransomware, phishing scams, and credit card fraud.

*Example:* International gangs running dark web drug sales and bank frauds.

Understanding the types of cyber criminals helps in designing **targeted cybersecurity strategies** and policies to defend against them.

## Q2

### a) What are the Characteristics of Cyber Crime? [5]

Cybercrime refers to **unlawful acts** involving computers, networks, or digital devices, either as **targets** or **tools**, with the aim to steal, defraud, harm, or disrupt.

#### Key Characteristics of Cyber Crime:

##### 1. Use of Technology

- Cybercrimes are committed using computers, mobile devices, or the internet.
- Criminals often exploit software, networks, or communication channels.

##### 2. Borderless Nature

- Cybercrimes are **not limited by geography** and can be committed remotely across countries.
- Makes **jurisdiction and investigation complex**.

*Example:* A hacker in one country can target users in another country.

##### 3. Anonymity of the Criminal

## SPPU-BE-COMP-CONTENT – KSKA Git

- Cybercriminals often use tools like **VPNs, proxies, dark web, and encryption** to hide their identity.
- Tracking the exact person behind the crime is difficult.

### 4. Speed and Scale

- Cybercrimes can happen **within seconds** and can impact **millions of users** instantly.
- Data breaches, ransomware attacks, or virus spread can scale rapidly.

### 5. Difficulty in Detection and Investigation

- Many cybercrimes remain **undetected for weeks or months**.
- Requires technical expertise and digital forensics to investigate properly.

### 6. Involves Various Victims

- Cybercrime may affect **individuals, organizations, or governments**.
- Victims often suffer **financial loss, data theft, privacy breach, or reputational damage**.

### b) What is Cyber Stalking? How is it Conducted? [5]

Cyberstalking refers to the repeated use of the internet, email, social media, or other digital means to harass, threaten, or intimidate an individual. It is a serious cybercrime that invades a person's privacy and creates fear or emotional distress.

#### How it is conducted:

Cyberstalking is carried out in various ways, including:

1. **Persistent online contact:** Repeatedly sending messages or emails despite no response or rejection.
2. **Monitoring online activity:** Watching the victim's posts, likes, check-ins, or other online behavior.
3. **Following across platforms:** Stalking a person on multiple social media platforms such as Instagram, Facebook, Twitter, etc.
4. **Sending obscene or threatening content:** Sending vulgar, abusive, or sexually explicit messages or images.
5. **Posting harmful content:** Uploading private, obscene, or manipulated images/videos of the victim to harass or defame them.



### Common Methods Used in Cyberstalking :



### c) Define Cyber Terrorism and state its objectives. [5]

Cyber Terrorism is the use of the internet and digital technologies to carry out attacks that cause fear, violence, or disruption with political, religious, or ideological motives. It targets critical infrastructure, government systems, or civilians to create widespread panic or damage.

#### Objectives of Cyber Terrorism:

1. **Cause Panic and Fear:**  
To create terror among people by threatening or attacking national security through cyber means.
2. **Disrupt Critical Infrastructure:**  
To disable or damage essential services like power grids, transportation, communication networks, or hospitals.
3. **Steal or Destroy Sensitive Information:**  
To hack into government or military systems to steal confidential data or destroy critical records.
4. **Financial Damage:**  
To cause economic losses by attacking banks, stock markets, or business systems.
5. **Spread Propaganda:**  
To influence public opinion, spread extremist ideologies, or recruit people through online platforms.