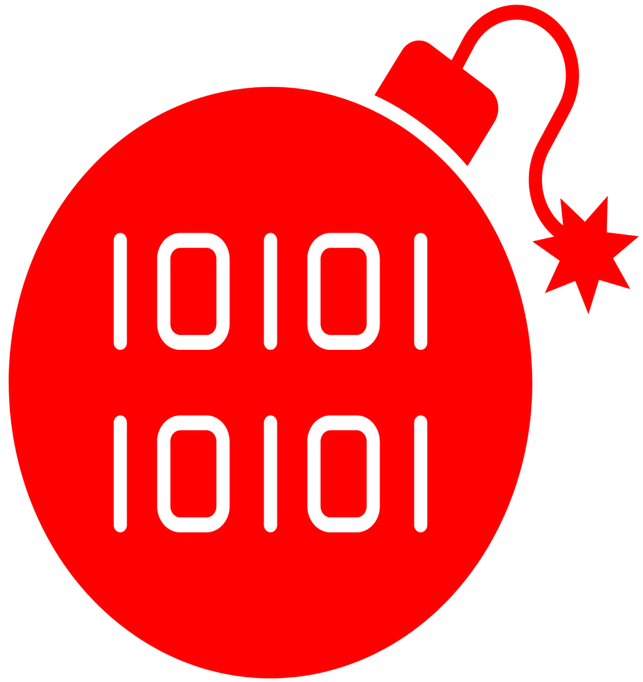
CYBER THREATS

Threat

- A circumstance or event that has the potential to exploit vulnerabilities and to adversely impact organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.



Cyber Security

- Cyber Security, refers to the practice of protecting computer systems, networks, devices, and data from unauthorized access, attacks, damage, disruption, or theft, and **ensuring the confidentiality, integrity, and availability** of digital information and services

Cyber Security

- The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation

Cyber Security

- Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

Cyber Security

- Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

Cyber Threats

- Cyber threats refer to malicious activities or actions that **aim to compromise the confidentiality, integrity, or availability** of digital information, systems, or networks.
- A cyber threat is something that may or may not happen, but **has the potential to cause serious damage**. Cyber threats can lead to attacks on computer systems, networks and more.

Cyber Threats

- Compromise
  - Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred

Cyber Threats

- Evolving Landscape of cyber threats
  - Sophistication of Attack Techniques
  - Proliferation of Ransomware
  - IoT and OT Security Concerns
  - Rise of Supply Chain Attacks
  - Targeting of Critical Infrastructure.
  - Weaponization of Artificial Intelligence (AI)
  - Social Engineering and Phishing
  - Cloud Security Risks
  - Exploitation of Social Media Platforms

Cyber Threats

- Why to understand cyber threats
  - Risk Mitigation
  - Protection of Sensitive Information
  - Preservation of Trust and Reputation
  - Regulatory Requirements
  - Business Continuity
  - Protection of Critical Infrastructure

Cyber Threats

- Types
  - Malware
  - Social Engineering / Phishing
  - Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks
  - Insider Threats
  - Man-in-the-Middle (MitM)

Cyber Threats

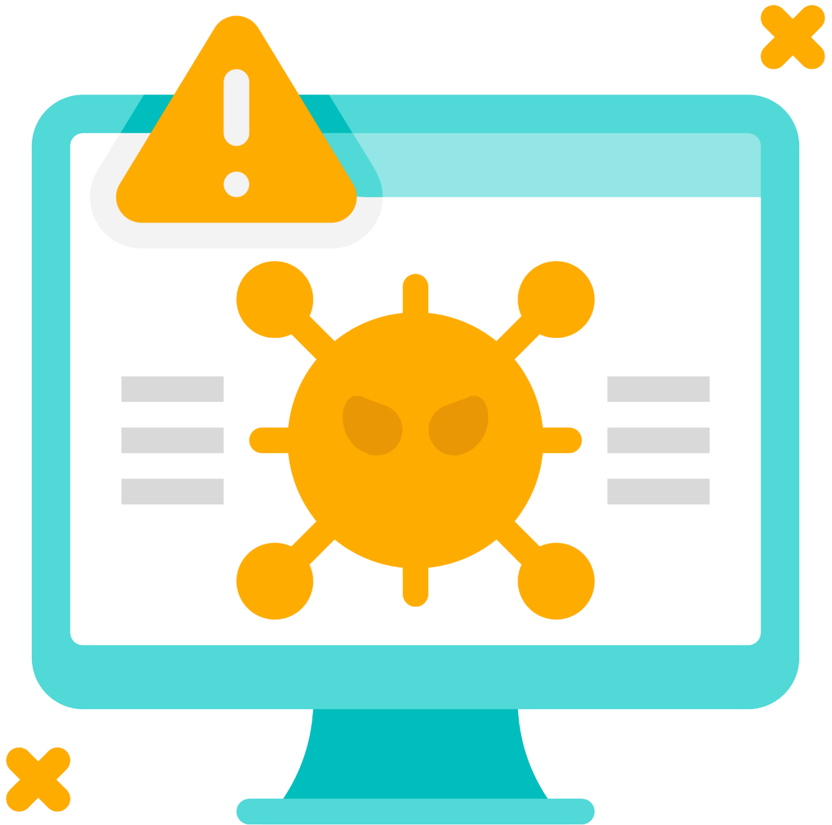
- Types
  - Zero-Day Exploits
  - IoT (Internet of Things) Threats
  - Advanced Persistent Threats (APTs)
  - Physical Threats
  - Policy-Based Threats
  - Social Media Manipulation

Cyber Threats

- Malware. Threats that involve the use of malicious software to compromise systems or steal data.
- Software that compromises the operation of a system by performing an unauthorized function or process. (CNSSI 4009, NIST SP 800-83)

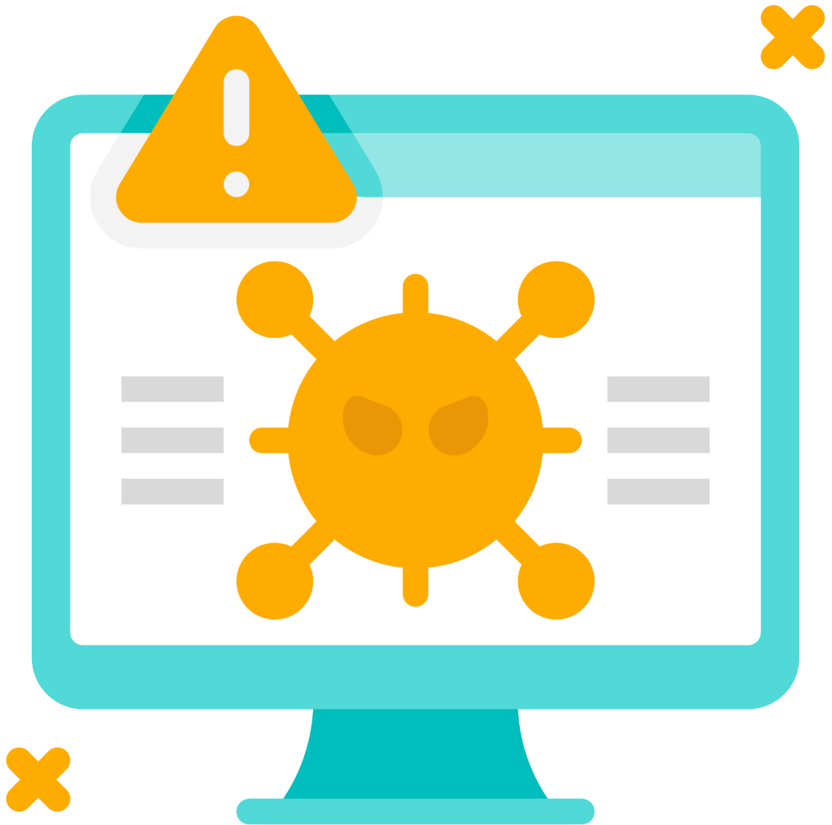
Cyber Threats

- Malware
  - Viruses: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.



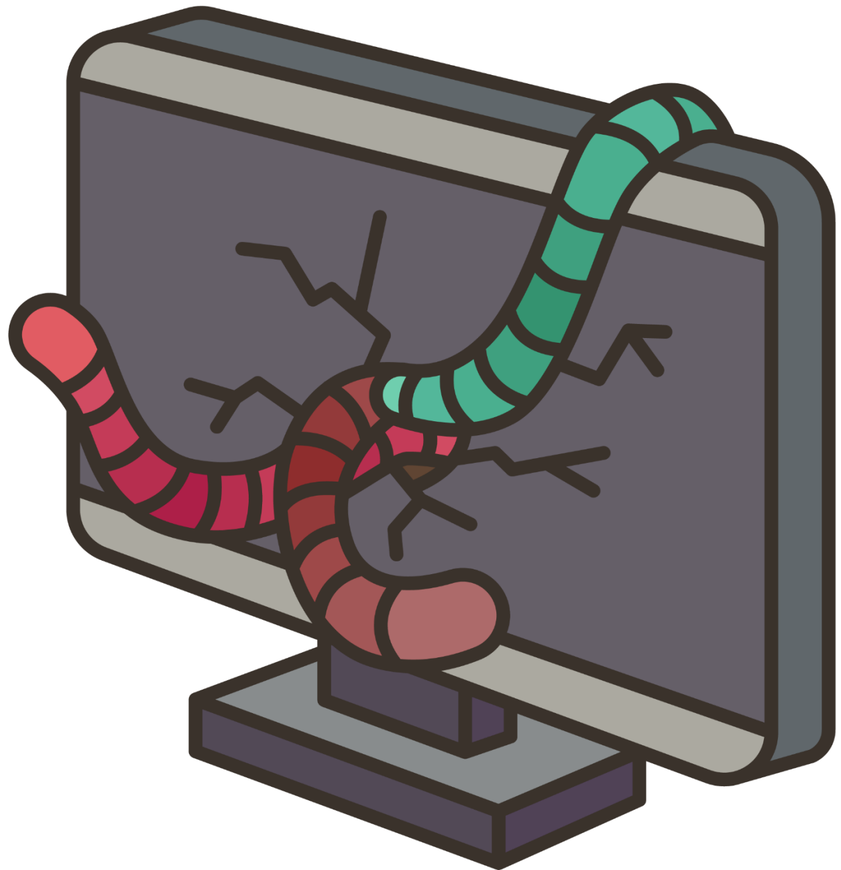
Cyber Threats

- Malware
  - Viruses: Viruses attach themselves to legitimate programs and replicate when those programs are executed. They can spread through infected files, email attachments, or removable storage devices. Viruses can cause damage by corrupting or deleting files, stealing data, or disrupting system operations.



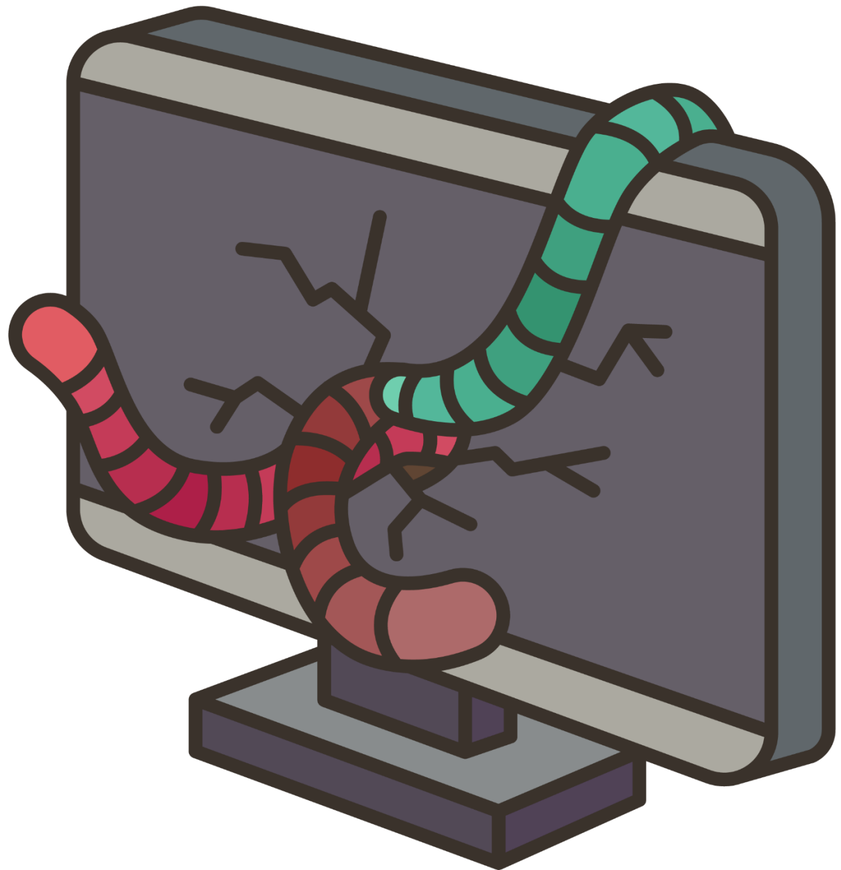
Cyber Threats

- Malware
  - Worms: Worms are standalone malware programs that replicate and spread across networks without requiring human interaction



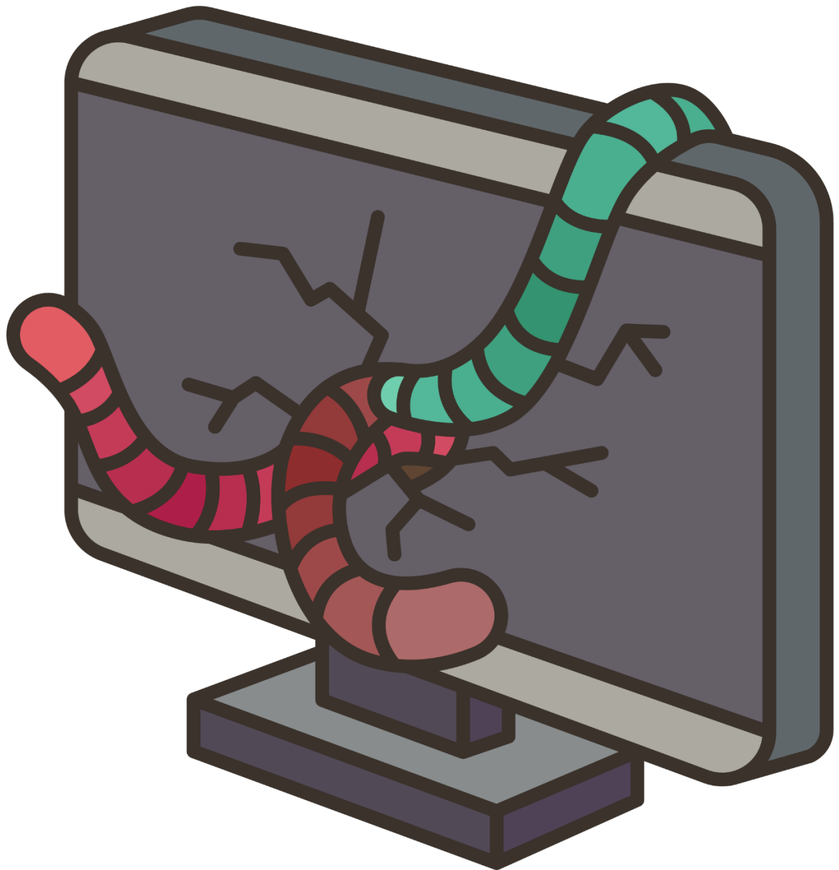
Cyber Threats

- Malware
  - Worms: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself..



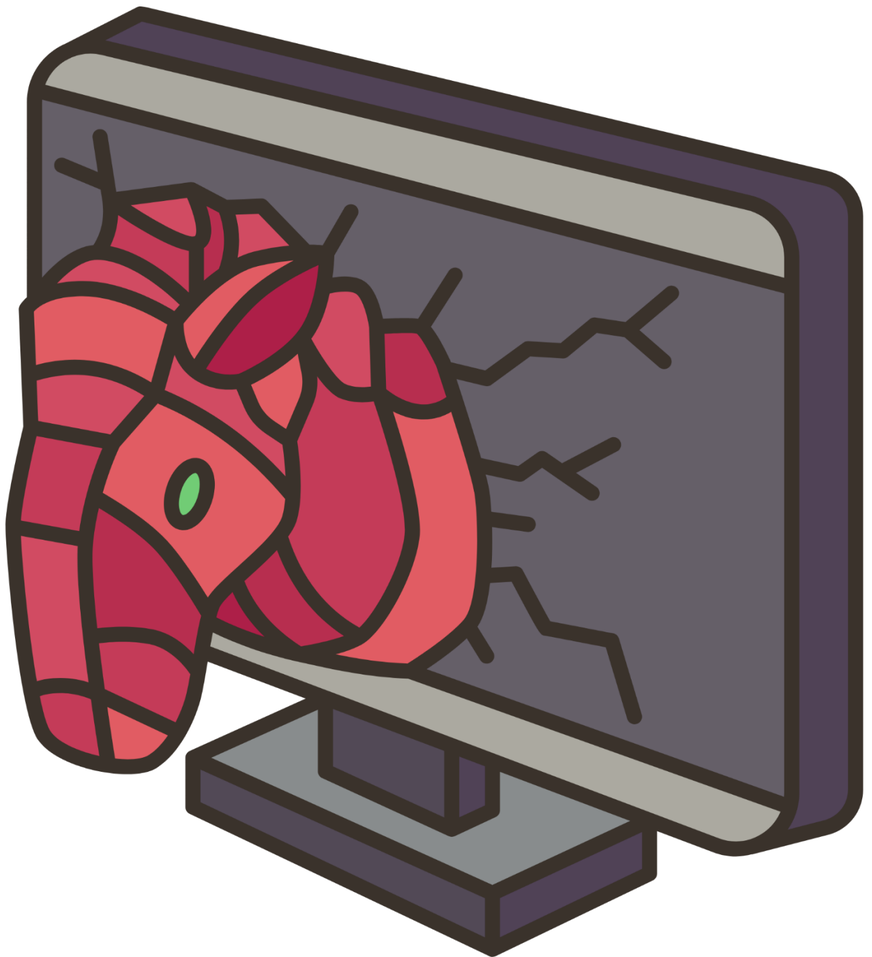
Cyber Threats

- Malware
  - Worms: . They exploit vulnerabilities in network protocols or operating systems to propagate and can cause network congestion, system slowdowns, or service disruptions.



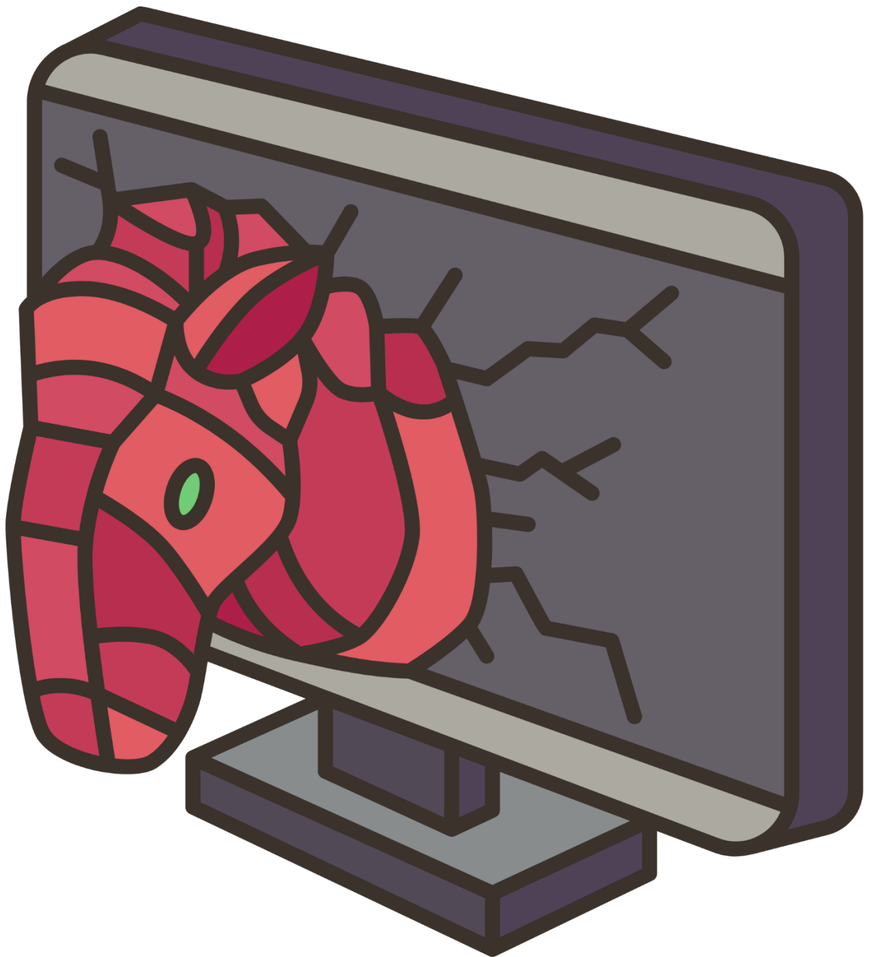
Cyber Threats

- Malware
  - Trojans: A type of malware that conceals its true content to fool a user into thinking it's a harmless file..



Cyber Threats

- Malware
  - Trojans:. Trojans pretend as legitimate software to trick users into downloading and executing them. Once installed, Trojans can perform various malicious actions, such as stealing sensitive information, creating backdoors for remote access, or downloading additional malware.



Cyber Threats

- Malware
  - Ransomware: a malware designed to deny a user or organization access to files on their computer

Cyber Threats

- Malware
  - Ransomware: Ransomware encrypts files or entire systems and demands payment (usually in cryptocurrency) for the decryption key.

Cyber Threats

- Malware
  - Ransomware: It can spread through malicious email attachments or compromised websites. Ransomware attacks can cause significant data loss, and operational disruptions

Cyber Threats

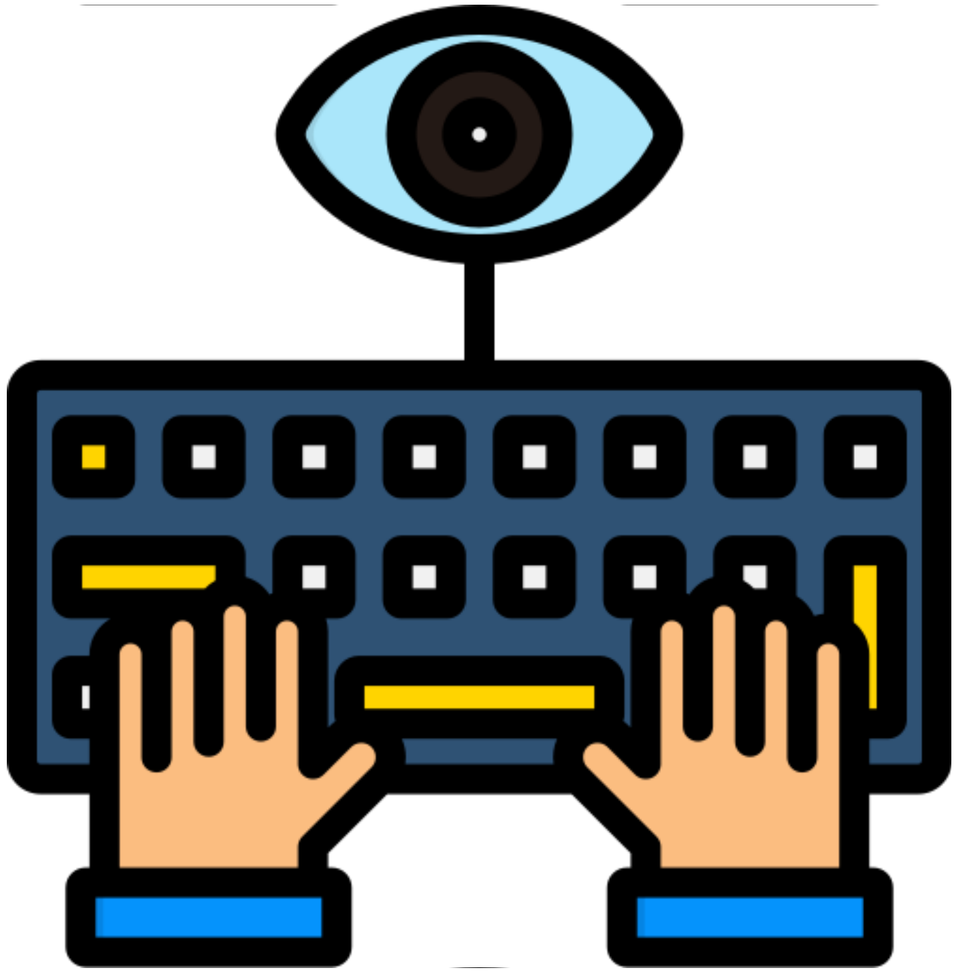
- Malware
  - Spyware: Software that is secretly installed into an information system without the knowledge of the system user or owner.

Cyber Threats

- Malware
  - Spyware: Spyware secretly monitors and gathers information about a user's activities, such as web browsing habits, keystrokes, or login credentials. It can be used for targeted advertising, identity theft, or espionage purposes

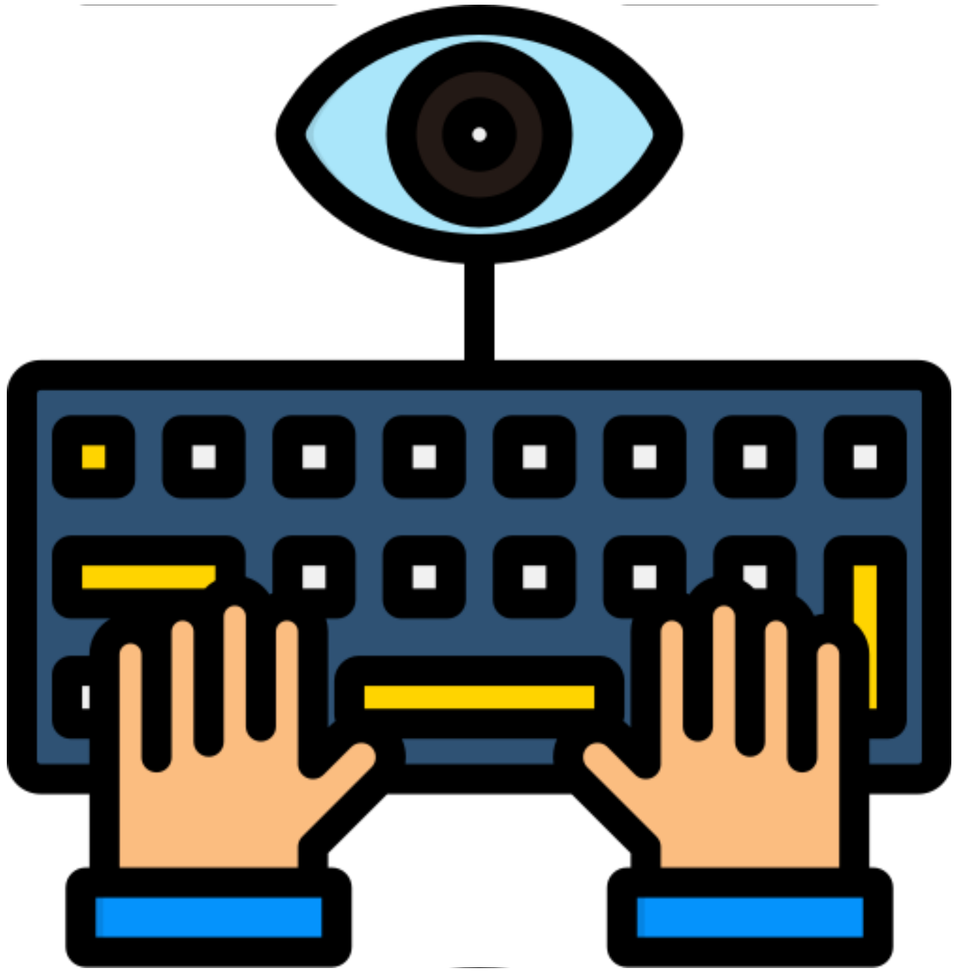
Cyber Threats

- Malware
  - Keyloggers: A tool that record what a person types on a device



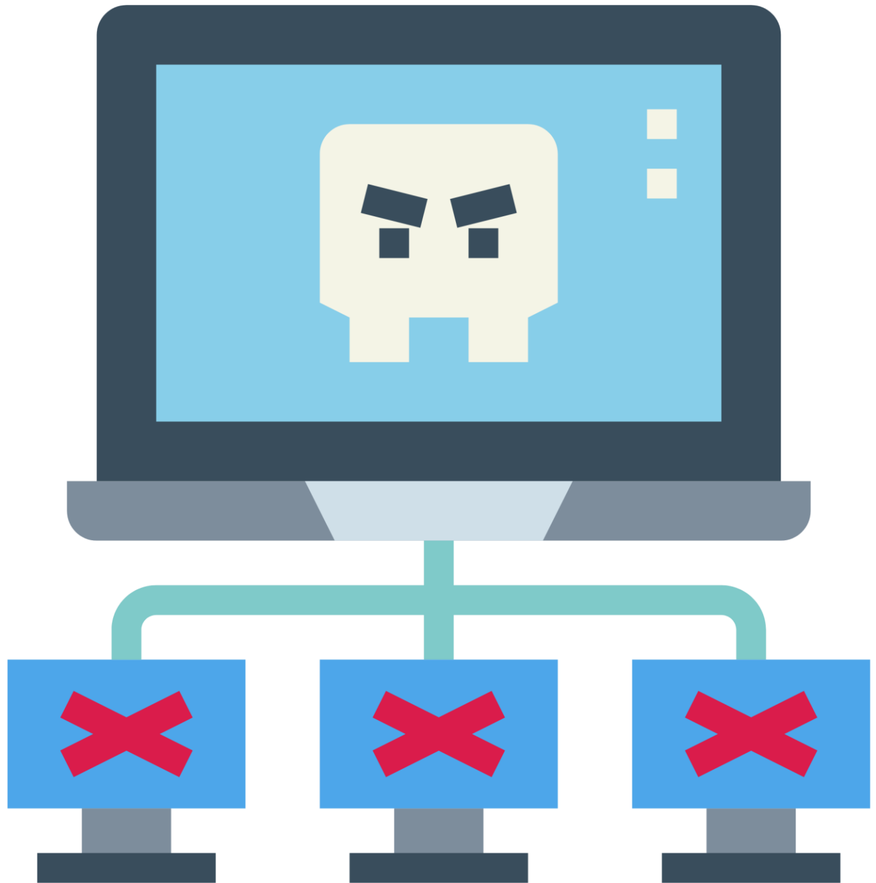
Cyber Threats

- Malware
  - Keyloggers: Keyloggers record keystrokes typed by users and can capture sensitive information such as passwords, credit card numbers, or personal messages. They can be deployed as standalone malware or as components of other malicious software



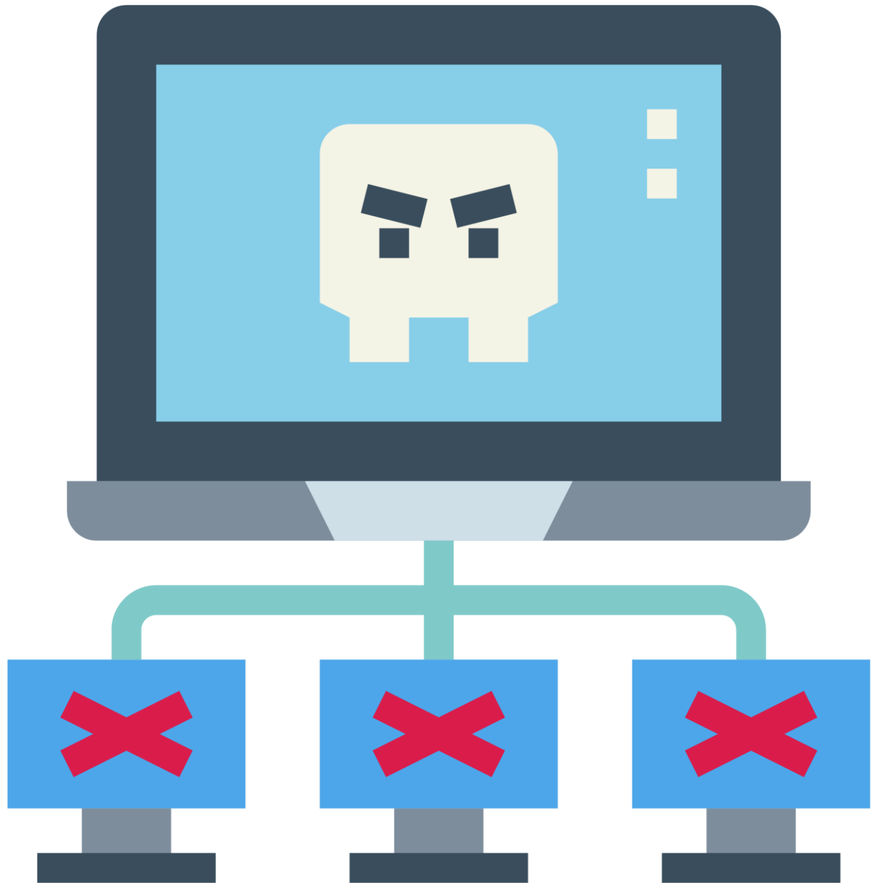
Cyber Threats

- Malware
  - Bot: A computer connected to the Internet that has been secretly compromised with malicious logic to perform activities under the command and control of a remote administrator.
  - Botnet: A collection of computers compromised by malicious code and controlled across a network.



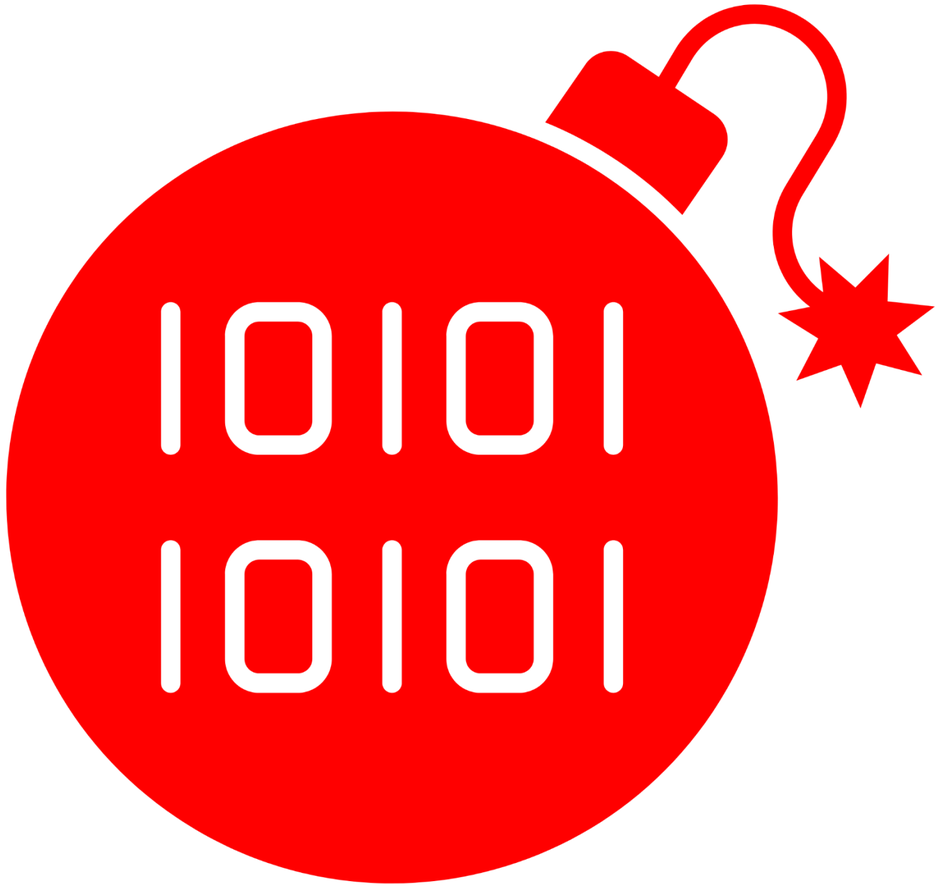
Cyber Threats

- Malware
  - Botnets: These are networks of compromised computers (bots) controlled by a central command-and-control server. Botnets can be used to carry out various malicious activities, including distributed denial-of-service (DDoS) attacks, spam campaigns, or cryptocurrency mining.



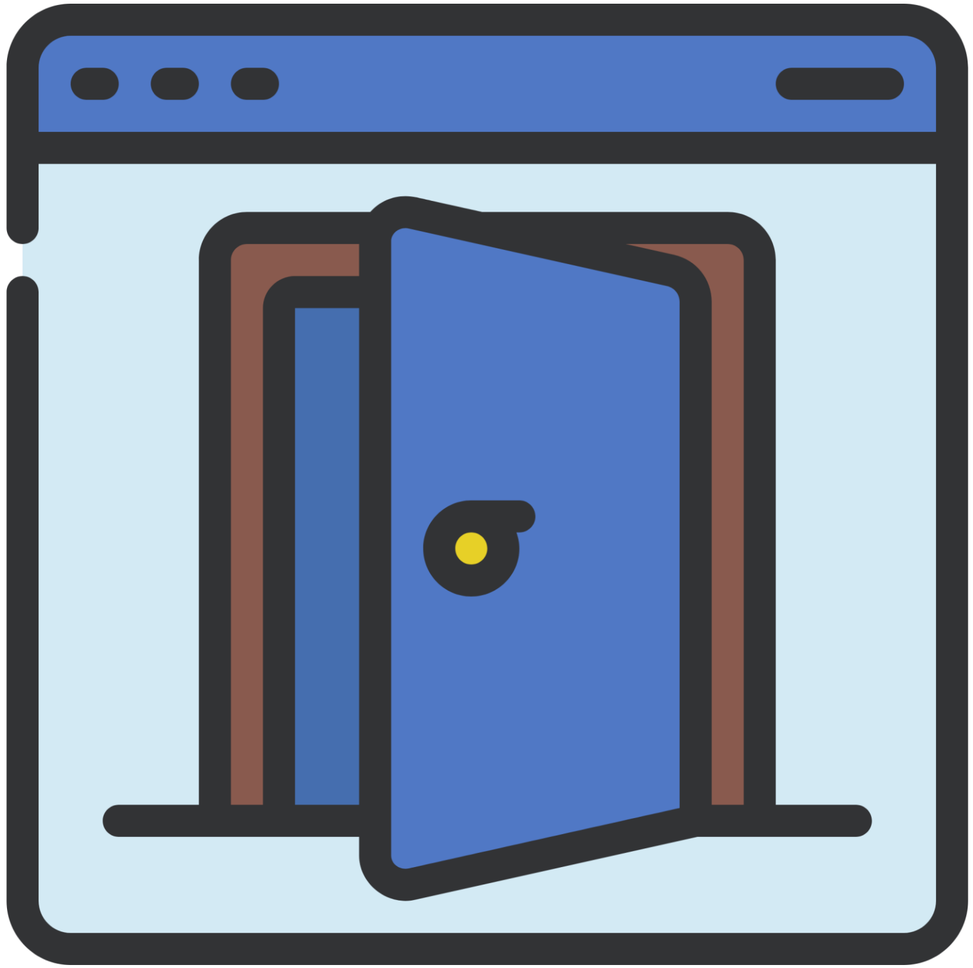
Cyber Threats

- Malware
  - Logic Bombs: Triggers malicious code when specific conditions are met



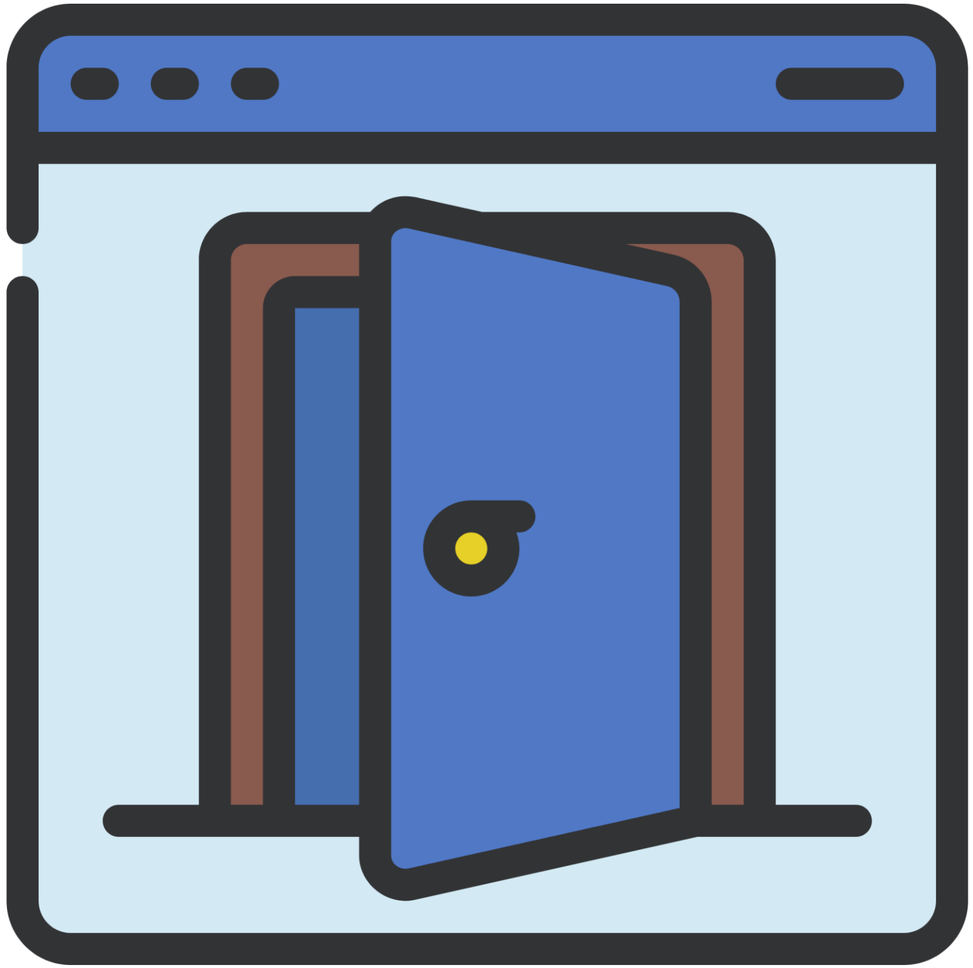
Cyber Threats

- Malware
  - Backdoors: An undocumented way of gaining access to computer system. A backdoor is a potential security risk.



Cyber Threats

- Malware
  - Backdoors: It refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access on a computer system, network, or software application.

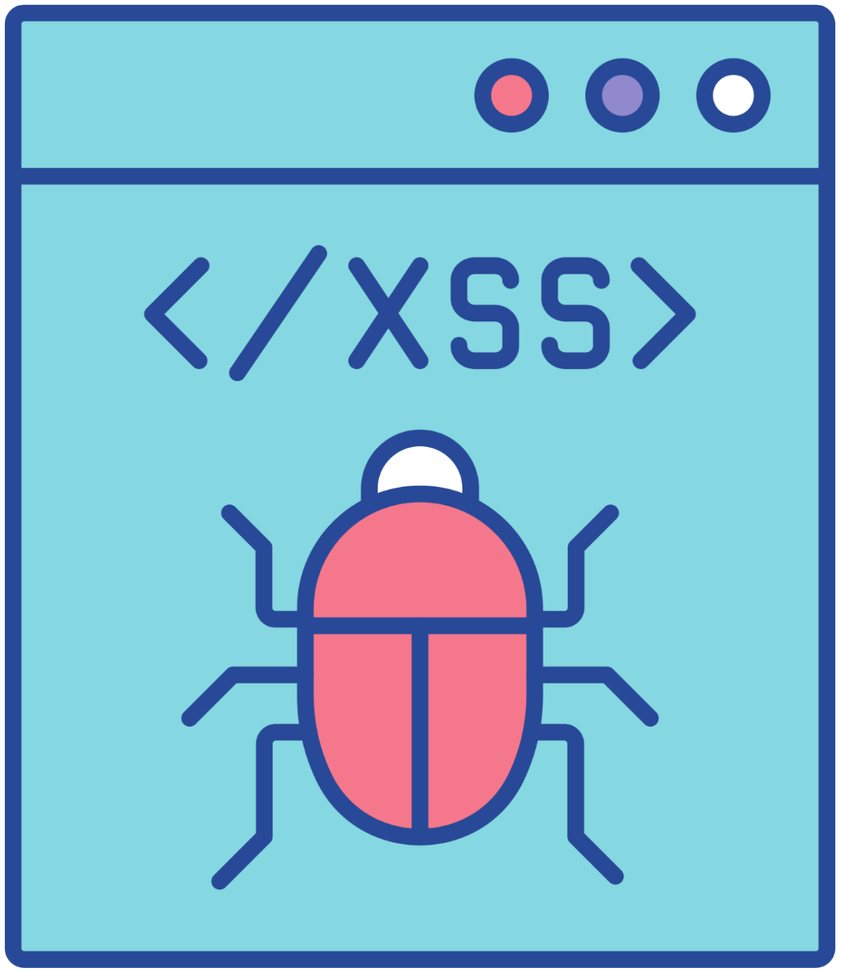


Cyber Threats

- Malware
  - SQL Injection: injects malicious code into database to extract or modify data. In computing, SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution

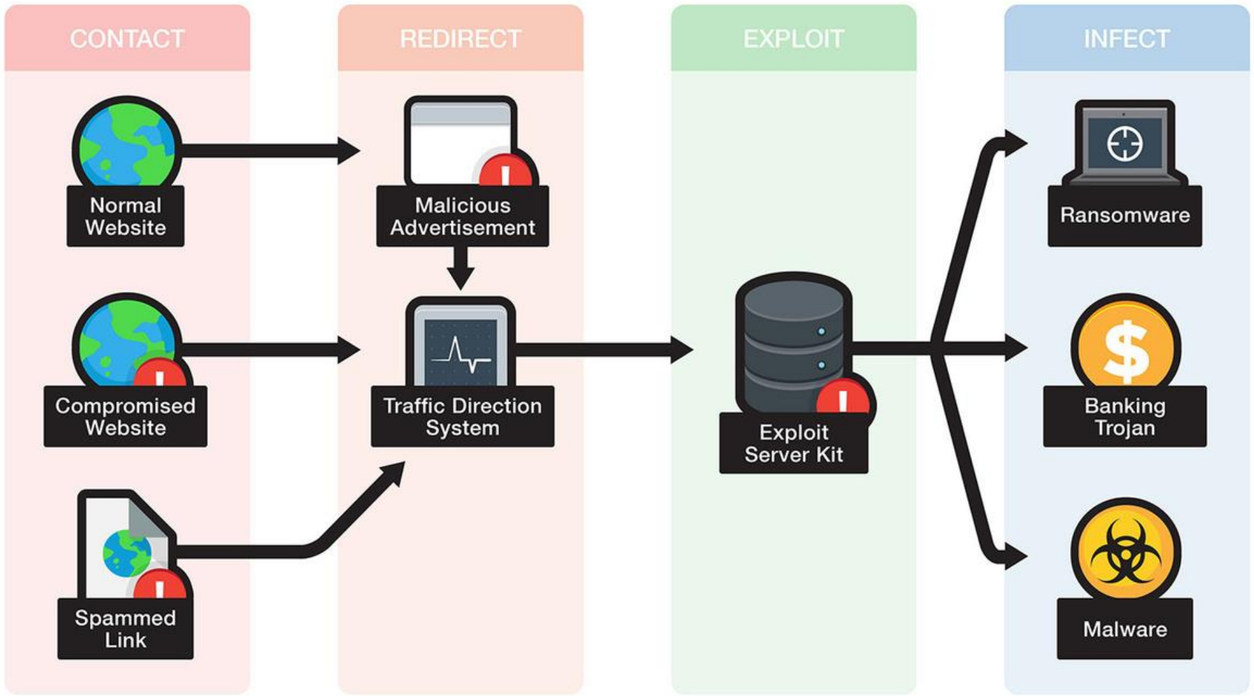
Cyber Threats

- Malware
  - Cross-Site Scripting (XSS): injects malicious code into website to steal data or take control.



Cyber Threats

- Malware
  - Exploit Kits: Automated tools that exploit vulnerabilities in a software.



Cyber Threats

- Malware
  - Banking Malware: Targets online banking and financial transactions.

Cyber Threats

- Root user: A privileged user that is authorized (and therefore, trusted) to have access to perform system control, monitoring, administration functions, or security-relevant functions that ordinary users are not authorized to perform..

Cyber Threats

- Malware
  - Rootkit: A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root level access to the host through covert means.

Cyber Threats

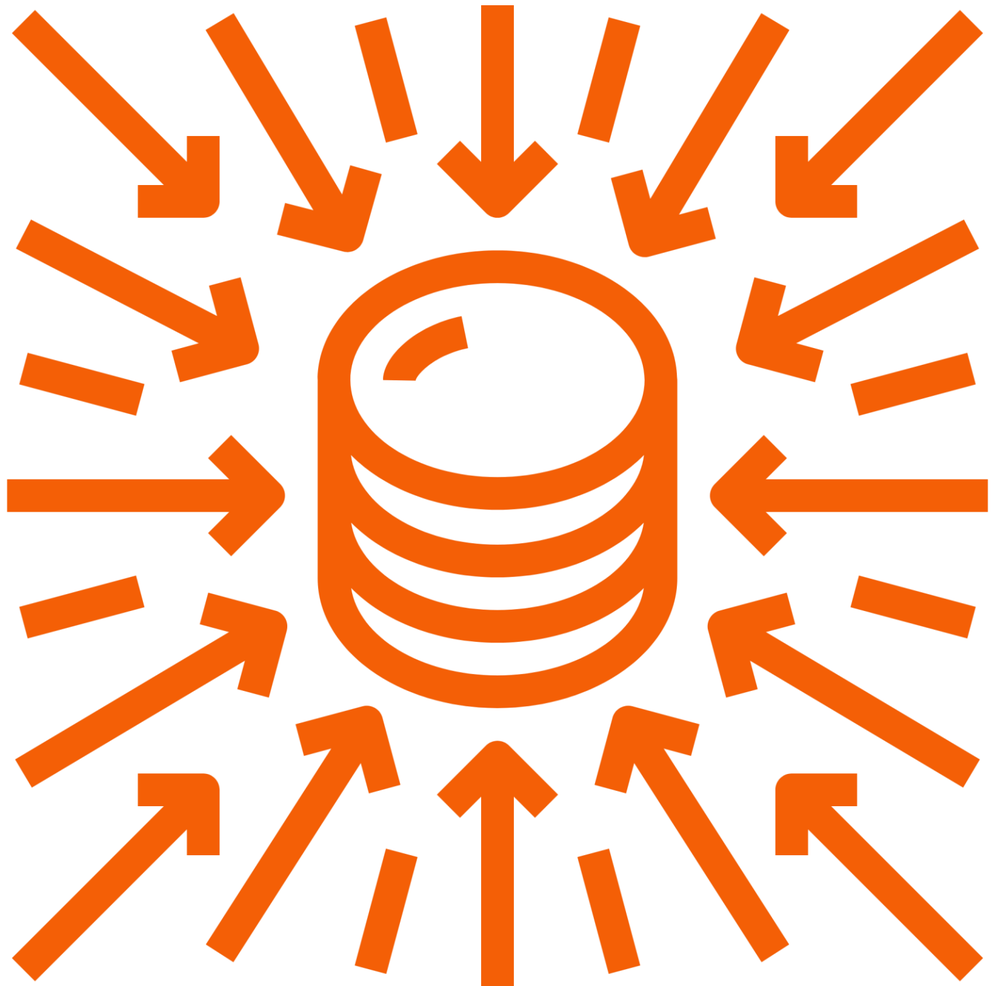
- Social Engineering / Phishing:
  - An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Cyber Threats

- Social Engineering / Phishing:
  - Social engineering refers to the manipulation of individuals into divulging confidential information through psychological manipulation rather than technical means. Phishing involves the use of deceptive emails, messages, or websites to trick individuals

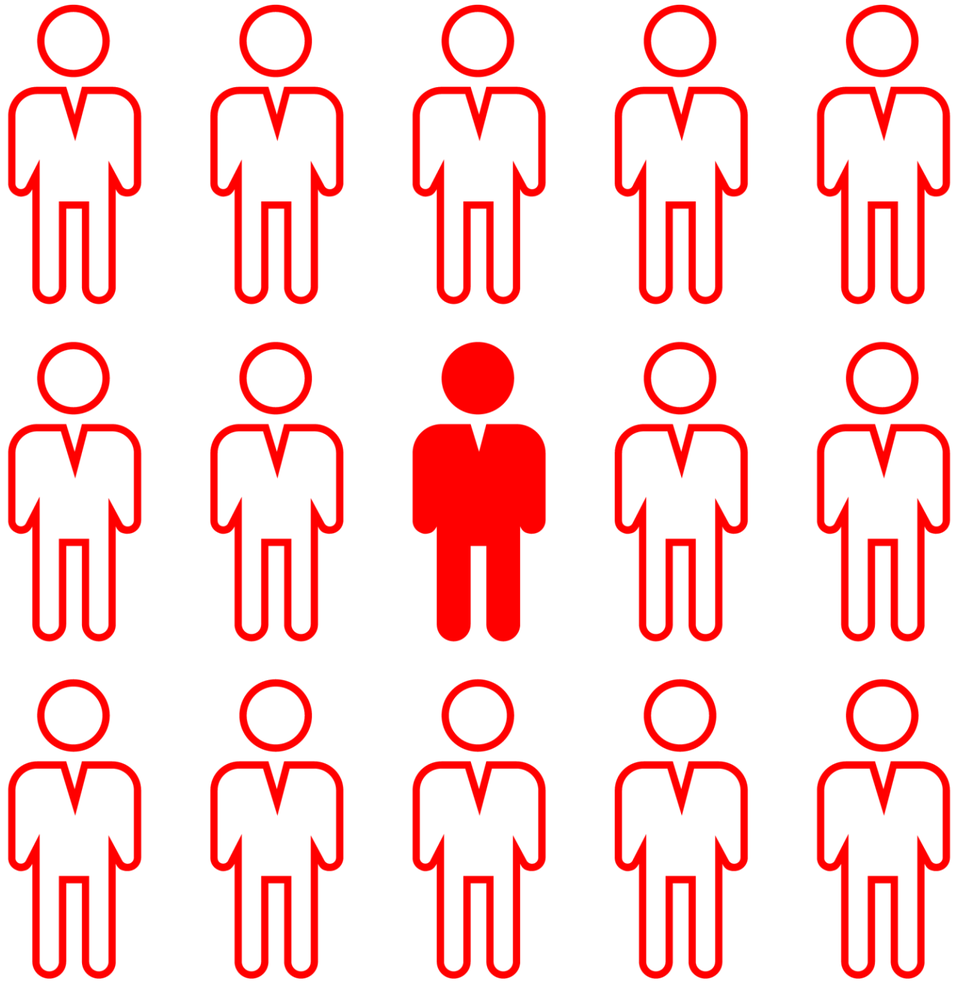
Cyber Threats

- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)
  - Aim is to disable a targeted device/app by overwhelming it with a flood of traffic. In a DoS attack, a single source and in a DDoS attack, multiple compromised devices (botnet) are used.



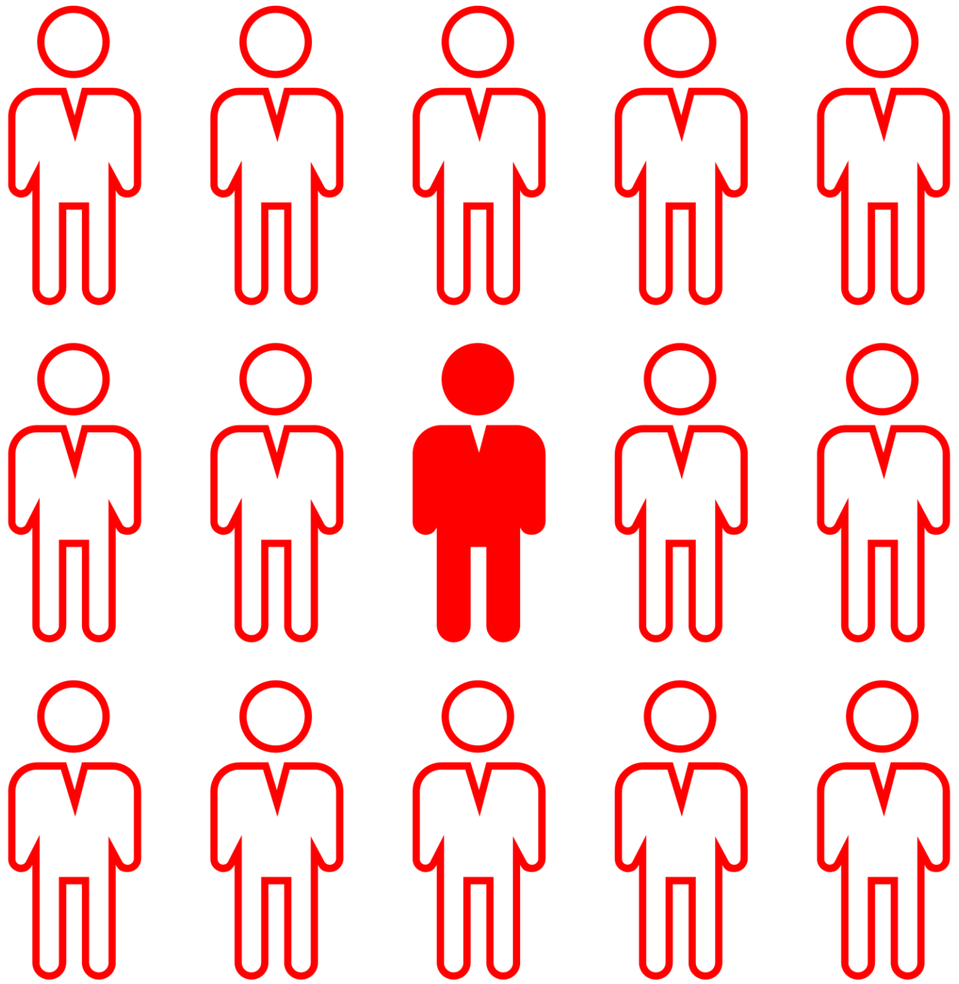
Cyber Threats

- Insider.
  - Any person with authorized access to any organizational resource, to include personnel, facilities, information, equipment, networks, or systems



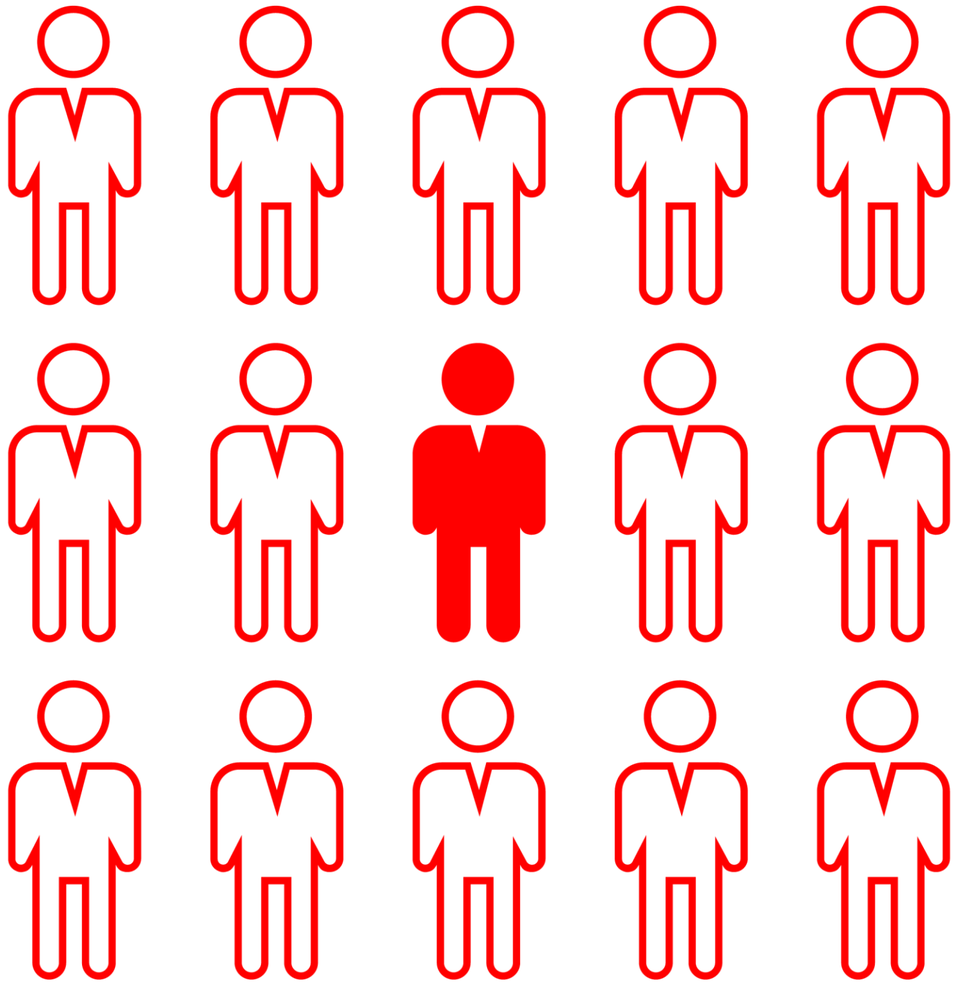
Cyber Threats

- Insider Threat.
  - In this threat that an insider will use her/his authorized access, to do harm to the security of organizational operations and assets, individuals, other organizations, and the Nation. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information



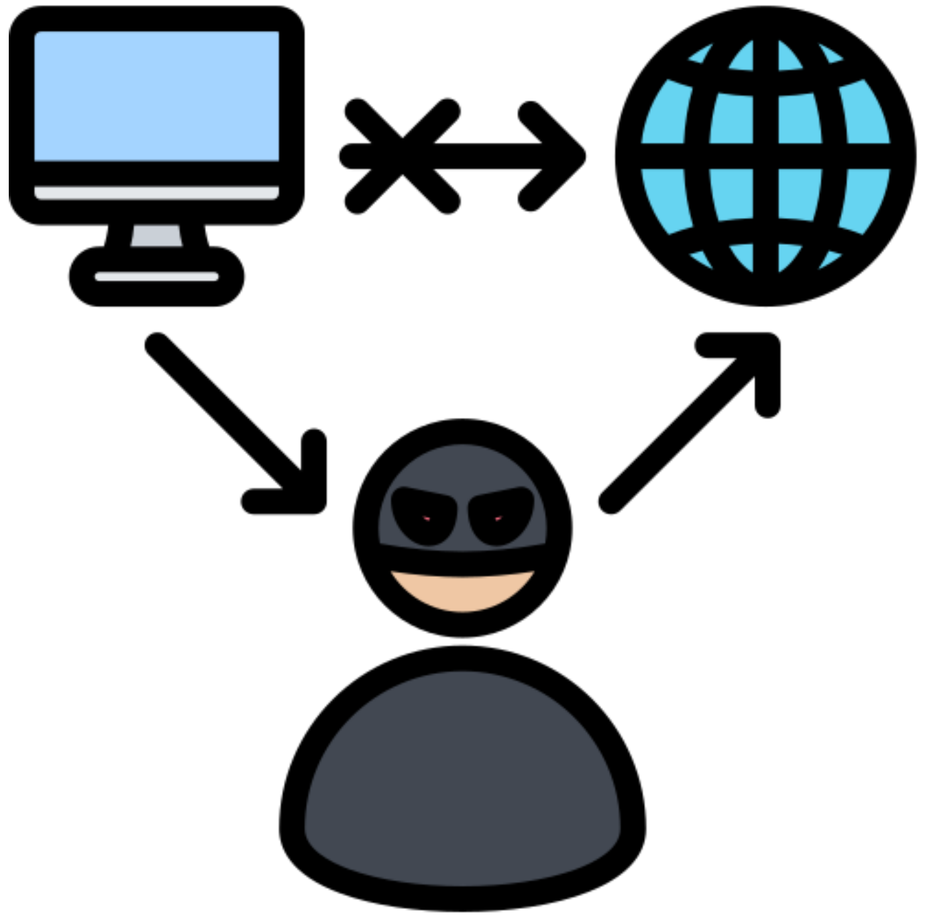
Cyber Threats

- Insider Threats.
  - It originate from within an organization, typically involving current or former employees, contractors, business partners, or other individuals with authorized access to the organization's systems, networks, or data



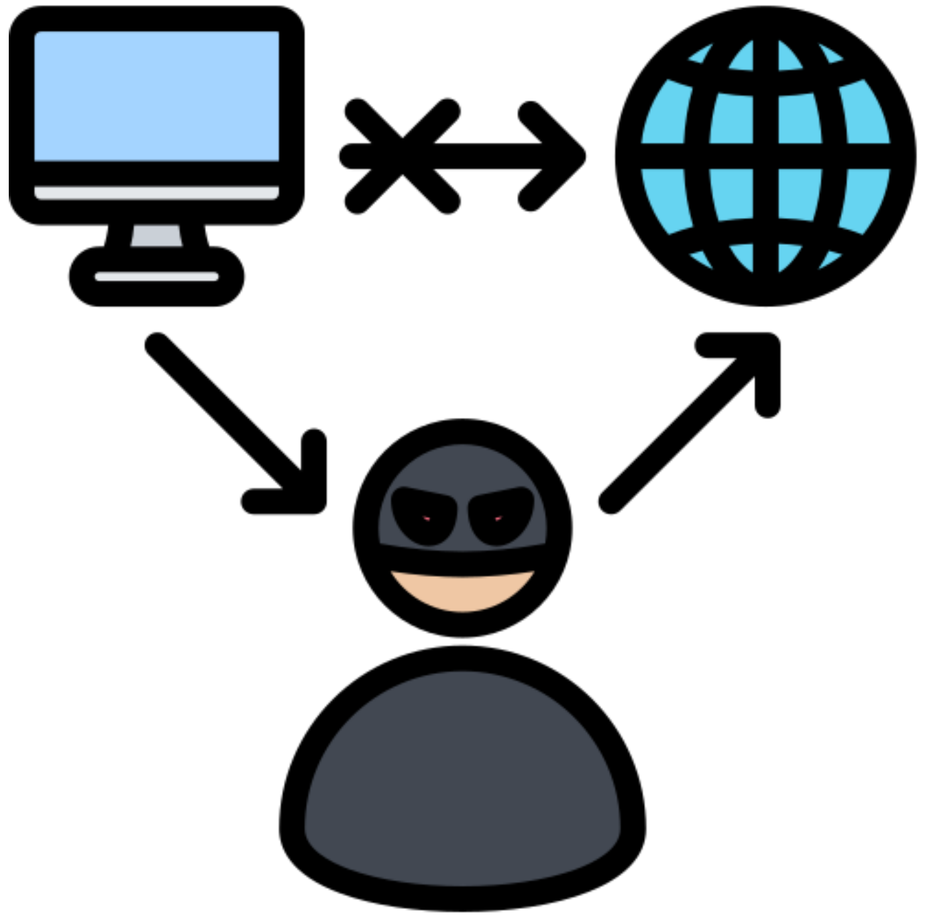
Cyber Threats

- Man-in-the-Middle (MitM) attack.
  - A man-in-the-middle attack is a cyber attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating



Cyber Threats

- Man-in-the-Middle (MitM) attack.
  - An attacker intercepts and alters comm between two parties without their knowledge or consent. The attacker positions themselves between the communicating parties, allowing them to eavesdrop on the communication



Cyber Threats

- Zero-Day Exploits.
  - Zero-day exploits refer to vulnerabilities in software or hardware that are unknown to the vendor or developers and have not yet been patched or fixed. These vulnerabilities are known as "zero-day" because developers had 0 days to fix or mitigate them.

Cyber Threats

- The Internet of Things (IoT)
  - IoT refers to the network of interconnected devices embedded with sensors and software that enable them to collect and exchange data over the internet.
  - Integrating IoT devices with existing IT systems and networks can introduce additional cyber security risks

Cyber Threats

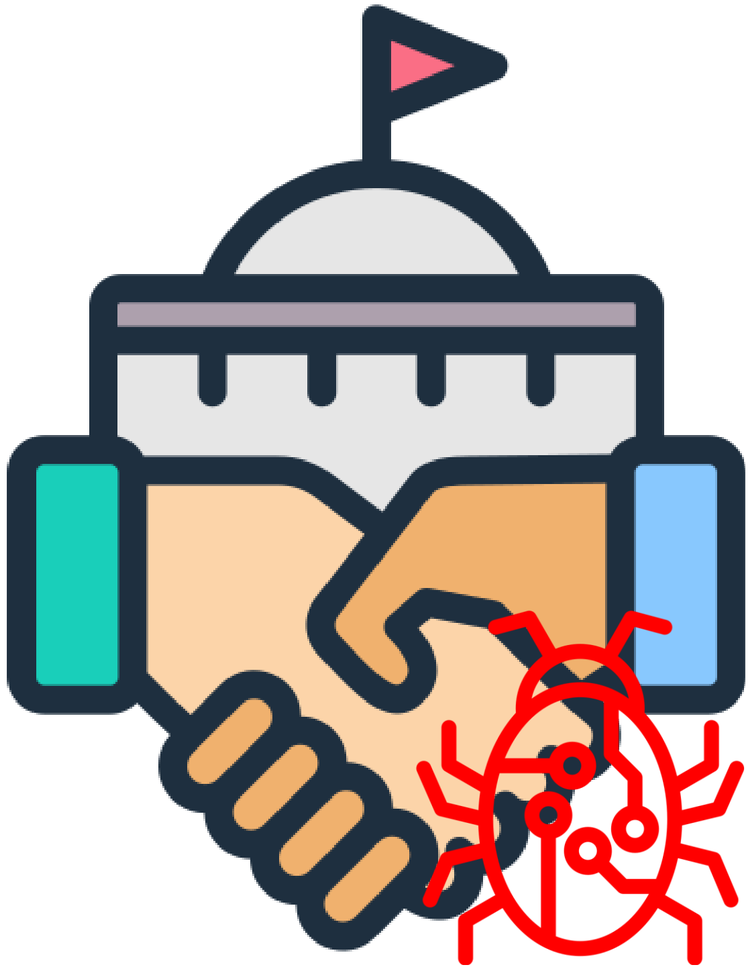
- Advanced Persistent Threats (APTs)
  - APTs are carefully planned and specifically targeted against high-value individuals, organizations, or entities, such as government agencies, multinational corporations, defense contractors, or critical infrastructure sectors. APTs are characterized by their persistence and stealthiness

Cyber Threats

- Advanced Persistent Threats (APTs)
  - APT objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for achieving desired results (such as exfiltration information) repeatedly over an extended period of time

Cyber Threats

- Policy-Based Threats
  - Policy-based threats refer to cyber threats that exploit weaknesses or violations in organizational policies, procedures, or compliance standards to compromise security.

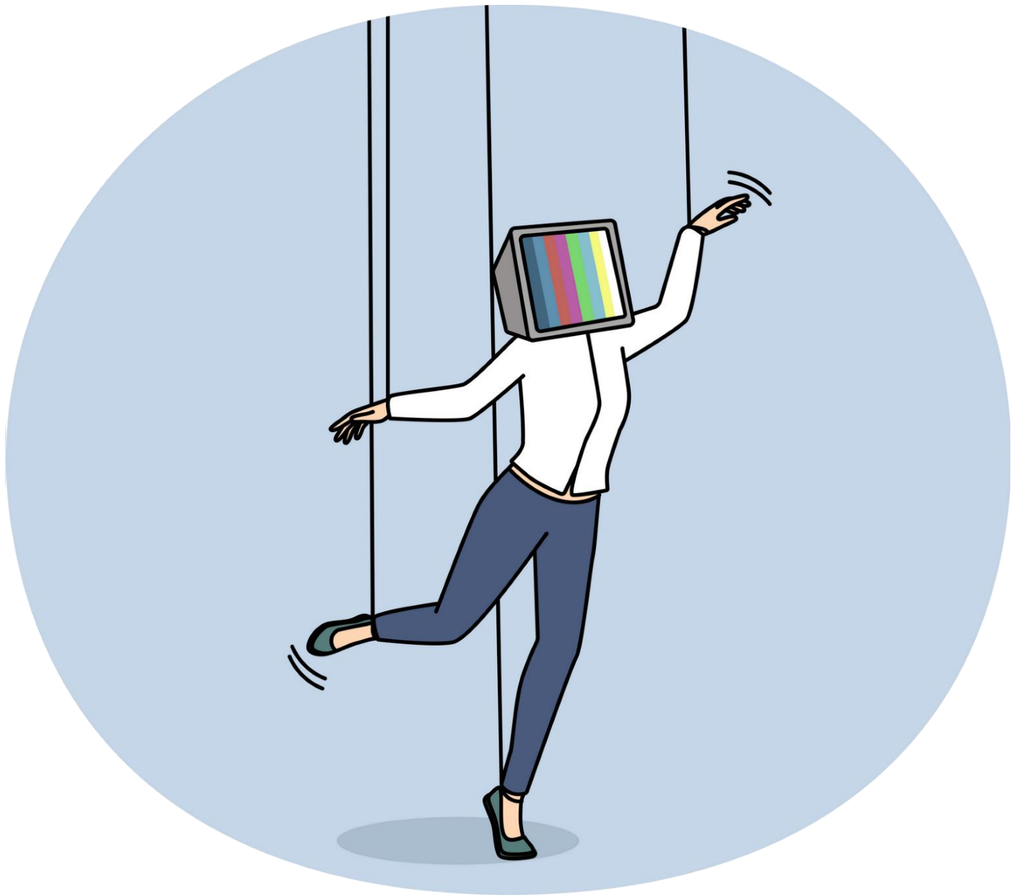


Cyber Threats

- Physical Threats
  - Physical threats refer to cyber security risks and vulnerabilities that arise from physical access to devices, systems, networks, or facilities

Cyber Threats

- Social Media Manipulation
  - Social media manipulation refers to the deliberate use of social media platforms to influence public opinion, spread misinformation, manipulate narratives, or undermine trust in institutions, organizations, or individuals.



Thanks