ICT Skilling for Schools

Introduction to Cybersecurity

ICT in Education

07th May 2025

Outline

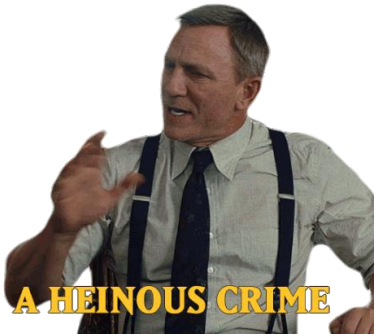
- Introduction
- Cyber Crimes
- Cyber Security Principles
- Vulnerabilities

Cyber Crime

Cyber crimes are, as the name implies, crimes committed using computers, phones or the internet.

Some types of cyber crime include:

- Illegal interception of data.
- System interferences.
- Copyrights infringements
- Sale of illegal items



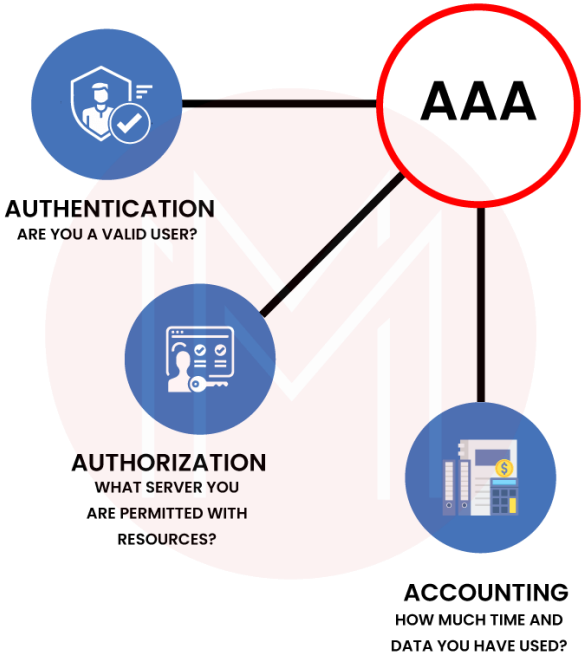
Cyber Security

- Cyber security refers to technologies, processes and practices involved in protecting individuals and organisations from cyber crime.

- It is designed to protect integrity of networks, computers, programs and data from attack, damage or unauthorised access.

Cyber Security Principles

There are six key principles in cyber security



Cybersecurity Principle Definitions

Confidentiality

A set of rules that limit access or place restrictions on certain type of information

Integrity

Assurance that the information is trustworthy and accurate

Availability

The guarantee of reliable access to the information by authorized people

Cybersecurity Principle Definitions

Authorisation

Process of determining what an authenticated user is allowed to do.

Authentication

Process of verifying the identity of a user, system or device before access to resources

Accountability

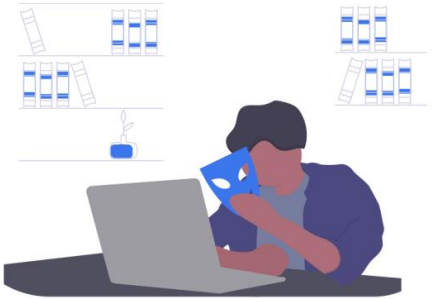
Process of recording and tracking user activities on a system

Cyber Threat

- A cyber threat is any malicious act that attempts to gain access to a computer network without authorisation or permission from the owners.
- It refers to the wide range of malicious activities that can damage or disrupt a computer system, a network or the information it contain.
- Most common cyber threats: social engineered trojans, unpatched software, phishing, network worms etc.

Cyber Threat

Phishing



Insider threats

Denial of Service

Malware

Ransomware

Sources of Cyber Threats

Cyber threats can come from a wide variety of sources, some notable examples include:

- National governments
- Terrorists
- Industrial secret agents
- Rogue employees
- Hackers
- Business competitors
- Organization insiders

Cyber Threat Classifications

Threats can be classified by multiple criteria:

1. Attacker's resources
2. Attacker's organization
3. Attacker's funding

On basis of these criteria, threats are of 3 types:

1. Unstructured threats
2. Structured threats
3. Highly structured threats

Cyber Threats Classifications

Unstructured

Resources: Individual or small group
Organization: Little to no
Funding: Negligible
Attack: Easy to detect and make use of freely available cyber attack tool.

Exploitation based on documented vulnerabilities.

Structured

Resources: Well trained individual or group
Organization: Well planned
Funding: Available
Attack: Against particular individual or organisation

Exploitation based on information gathering.

Highly structured

Resources: Extensive resources
Organization: Extensive
Funding: Negligible
Attack: Long term attack on a particular machine

Exploitation with multiple methods: technical, social and insider help

Cyber Threat Classifications

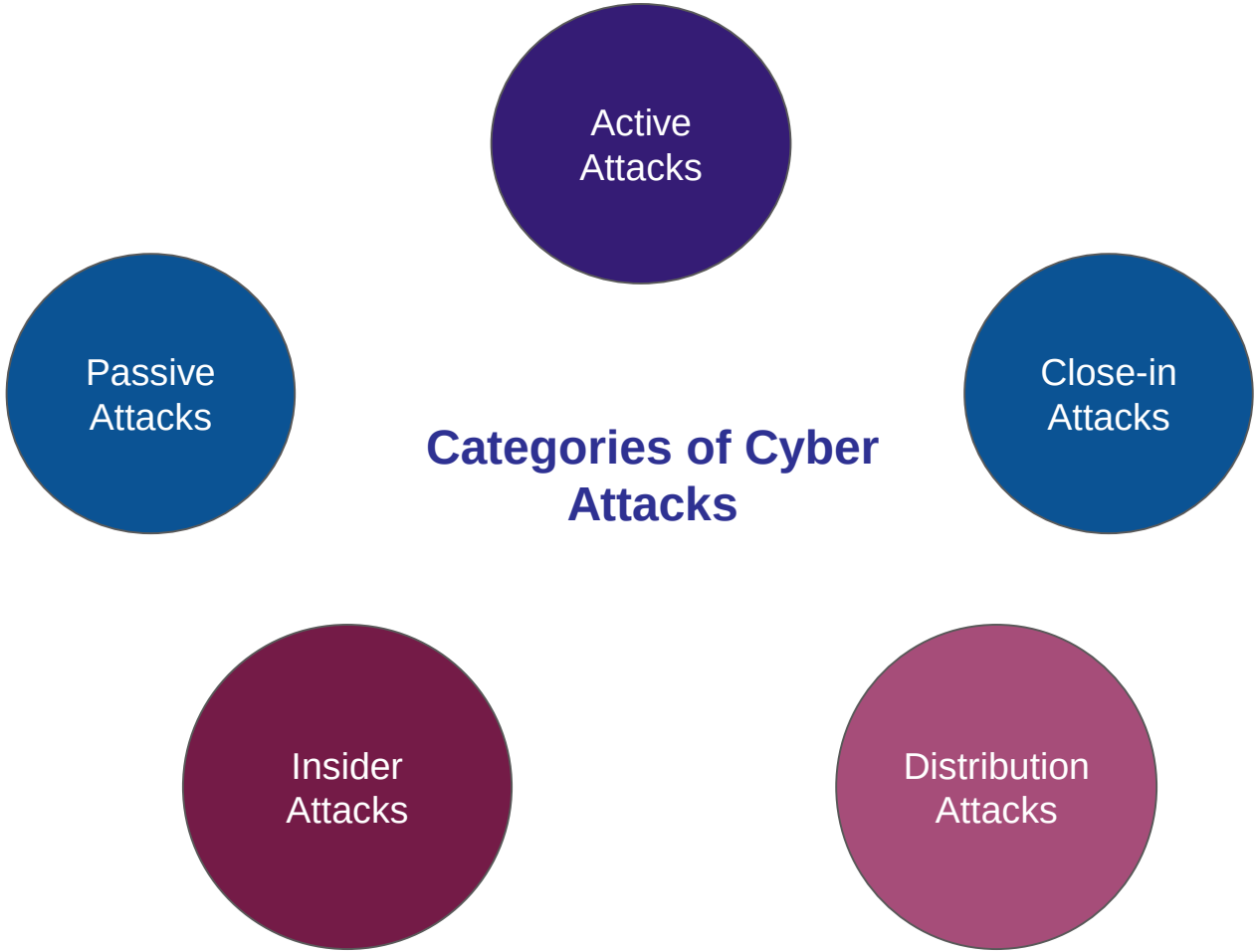
How people think they get hacked:

How they actually get hacked:

Motives, Goals and Objectives of Cyber Attacks

- Disrupt business continuity
- Perform information theft
- Manipulating data
- Create fear and chaos by disrupting critical infrastructures.
- Bring financial loss to the target
- Propage religious or political beliefs.
- Achieve a state's military objectives
- Demand Ransom

Attacks = Motive (Goal)+Method+Vulnerability


Active Attacks
Passive Attacks
Close-in Attacks
Categories of Cyber Attacks
Insider Attacks
Distribution Attacks

Types of Cyber Attacks

Advanced Persistent Threat (APT):
A network attack in which an unauthorised person gains access to network and stays there undetected for a long period of time.

Backdoor:
Method of bypassing normal authentication and gaining access in OS or application.

Types of Cyber Attacks

Buffer Overflow:
An exploit that takes advantage of the program that is waiting for a user's input.

Man-in-the-middle Attack:
This attack intercepts and relays messages between two parties who are communication directly with each other.

Denial of Service Attack:
An attack where the attackers attempt to prevent the authorised users from accessing the service.

Impacts of Cyber Attacks

A successful cyber attack can cause major damage to organisations or systems, as well as to business reputation and consumer trust.

Some potential results include:

1. Financial loss.
2. Reputational damage.
3. Legal consequences.

Common Types of Malicious Code

Virus:
Malicious software program, when it is executed, it replicates itself by modifying other computer programs and inserting its own code.

Network worm:
Standalone malware which replicates itself in order to spread to other computers.

Trojan Horse:
A program that claims to free your computer from viruses but instead introduces viruses onto your system.

Vulnerability

A cyber security term that refers to a flaw in a system that can leave it open to attack.

Vulnerability is the composition of three elements:

1. A flaw in system
2. Access of attacker to that flaw.
3. Capability of attacker to exploit the flaw

Classification of Vulnerabilities

Vulnerabilities are classified according to the asset:

1. Hardware.
2. Software.
3. Network.
4. Personal.
5. Physical site.
6. Organizational.

Classification of Vulnerabilities

Some of the vulnerability in the system occur due to:

1. Missing patches.
2. Cleartext credentials.
3. Using unencrypted channels.
4. RF Emanation.

Common Passwords

- 123456789
- qwerty
- password
- 123456
- qwerty123
- iloveyou
- aaaaaa
- 888888
- liverpool
- chocolate
- xxx
- football
- princess
- michael
- computer
- samsung
- superman
- master
- admin
- test1
- love123
- passw0rd

Simple Steps to Stay Secure

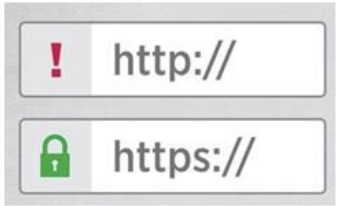
- Creating strong passwords
- Using multi-factor authentication (MFA)
- Software updates & patch management
- Recognizing phishing attempts
- Safe browsing habits:visit secure sites,avoid clicking suspicious ads or pop-ups.

Simple Steps to Stay Secure

LastPass •••|

bitwarden

KeePassXC



THE END

Discussion