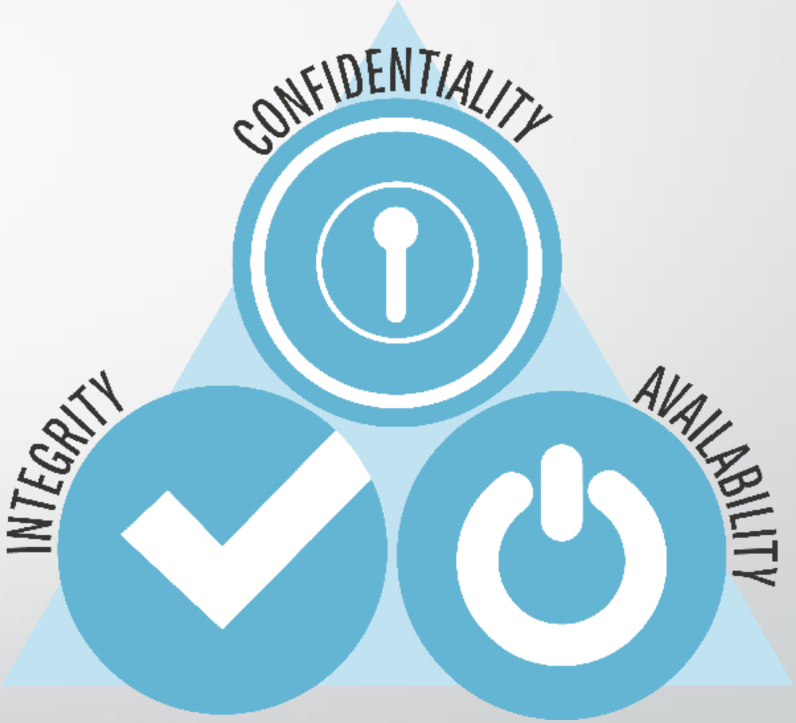
DATA SECURTIY THREATS

Cybersecurity is the protection of internet-connected systems including Hardware, software and Data from cyber attacks.

❖ The key concept of cyber security ?

The cyber security on a whole is very broad term but is based on three fundamental concepts known as "**The CIA triad**"



- **Three fundamental principal of cyber security**

- ✓ Confidentiality
- ✓ Integrity
- ✓ Availability

Availability:- Availability guarantees that systems, applications and data are available to users when they need them. The most common attack that impacts availability is **denial-of-service** in which the attacker interrupts access to information, system, devices or other network resources.

Integrity:- is the ability to ensure that a system and its data has not suffered unauthorized modification. Integrity protection protects not only data, but also **operating systems**, **applications** and **hardware** from being altered by **unauthorized** individuals.

Confidentiality:- ensures that data exchanged is not accessible to unauthorized users. The users could be applications, processes, other **systems** and/or **humans**

What are cyber Threats?

What are Cyber Threats?

Cyber Threats are malicious attacks that damage and steal data which in turn affects the **digital life**

Sources of Cyber Threats:-

- State-sponsored
- Terrorists
- Industrial spies
- Organized crime groups
- Hackers
- Hacktivists

Types of Cyber Threats

Types of cyber Threats

- Phishing attack
- SQL Injection threat
- Man-in-the-middle attack
- Malware
- Zero-day attack
- Cross-site-scripting
- Advanced persistent threats
- Password attack
- Drive by attack

Phishing Attack

Phishing is the technique to steal a user's data from the **internet** or **computer-connected device**.

Types of Phishing attacks

- Phishing email
- Domain spoofing
- Voice phishing
- SMS phishing

Phishing Attack

Ways to prevent Phishing attack

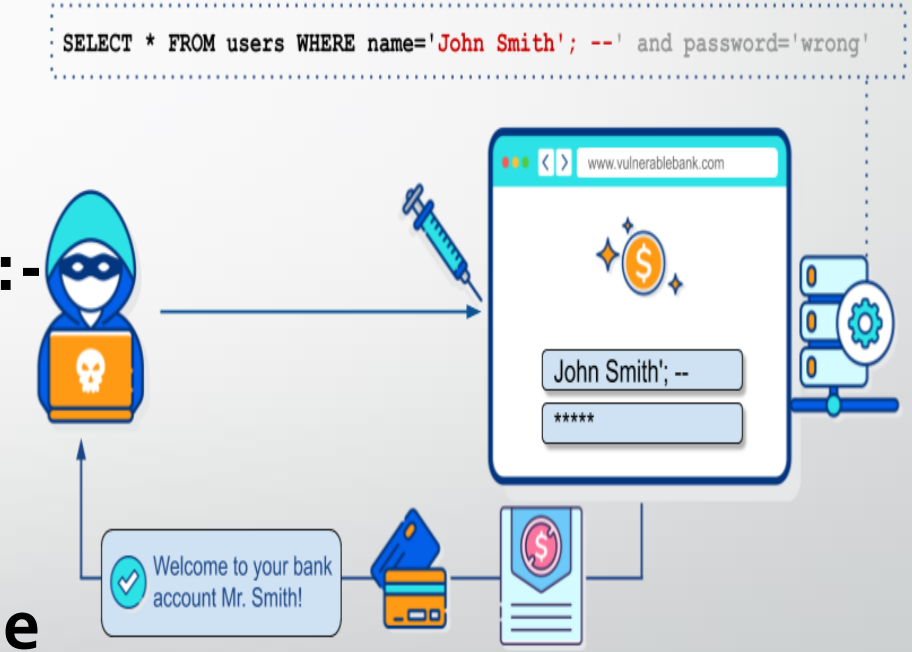
- Know what a phishing scam looks like
- Don’t click on a random **link**
- Get free **anti-phishing** add-ons
- Don’t give your information to an unsecured site
- Change **passwords** regularly
- install **firewall**

SQL injection threat

In the SQL injection threat, the attacker sends a malicious query to the device or a server. The server is then forced to expose sensitive information.

Ways to prevent SQL injection threat:-

- Validate user inputs
- **Sanitize** data by limiting special characters
- Use stored procedures in the **database**
- Establish appropriate **privileges** and **strict**



```
SELECT * FROM users WHERE name='John Smith'; --' and password='wrong'
```

John Smith'; --

*****

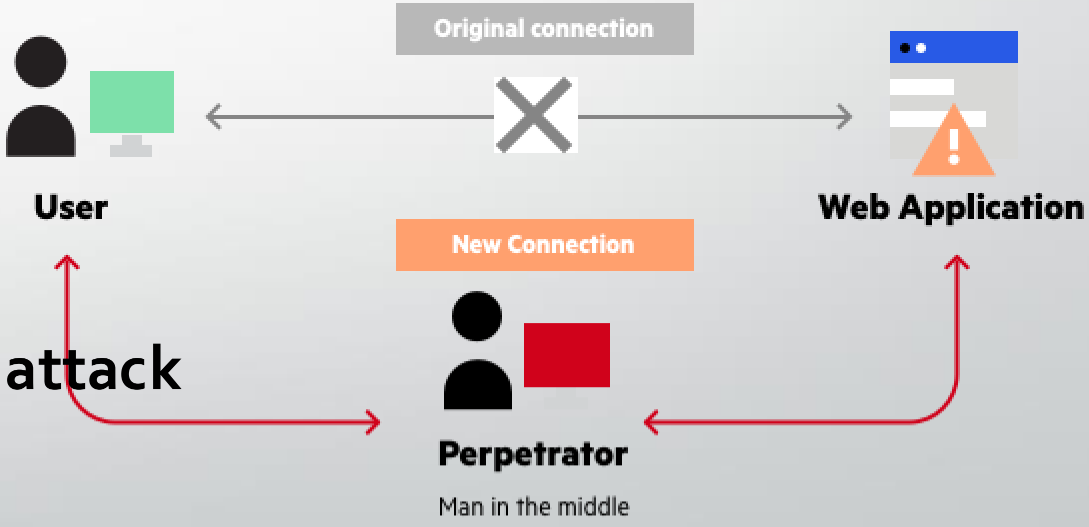
Welcome to your bank account Mr. Smith!

Man-in-the-middle attack

The man-in-the-middle attack is a security breach where cybercriminals place themselves between the **communication system** of a **client** and the **server**.

Types of Man-in-the-middle attack

- Session hijacking
- IP spoofing
- Replay

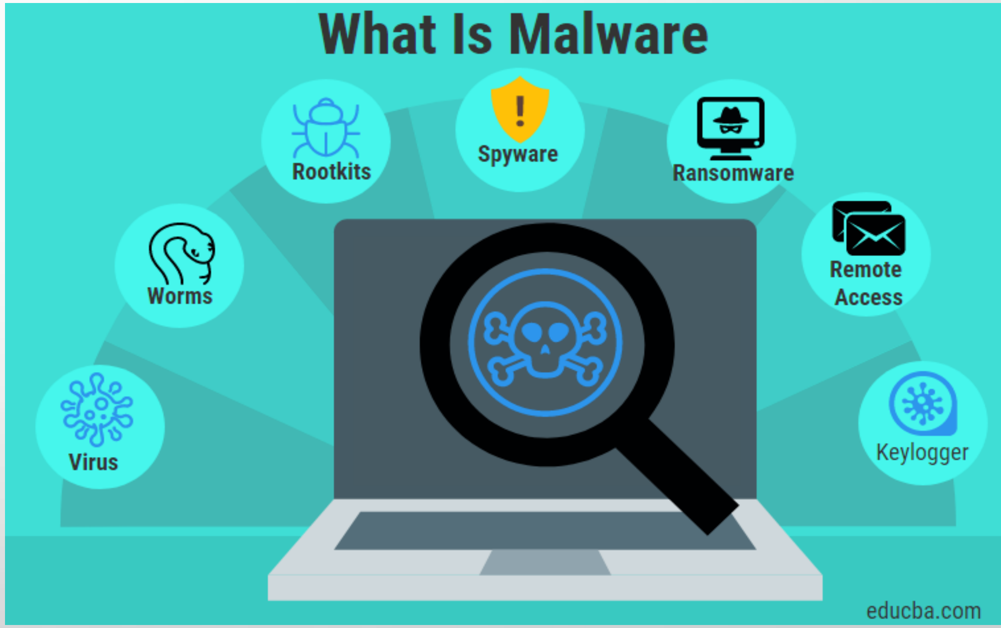


Ways to prevent Man-in-the-middle attack

- Strong router login credentials
- Virtual private network
- Strong encryption on access points
- Force HTTPS Man-in-the-middle attack P

Malware

Malware is a malicious software which gets installed into the system when the user clicks on a dangerous **link** or an **email**.



Types of Malware:-

- Viruses
- Trojans
- Worms
- Ransomware

Ways to prevent Malware:-

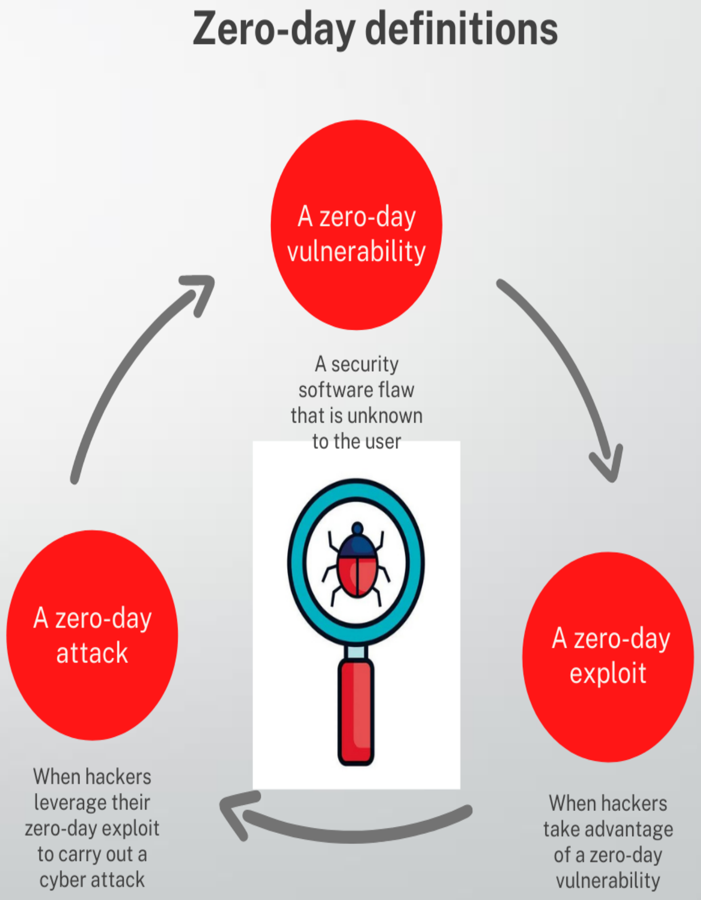
- Regularly update your computer and software
- Be careful while opening unknown email attachments or images

Zero-day-Attack

A zero-day attack is an attack done by hackers when the network, hardware or software **vulnerability** is **announced publicly**.

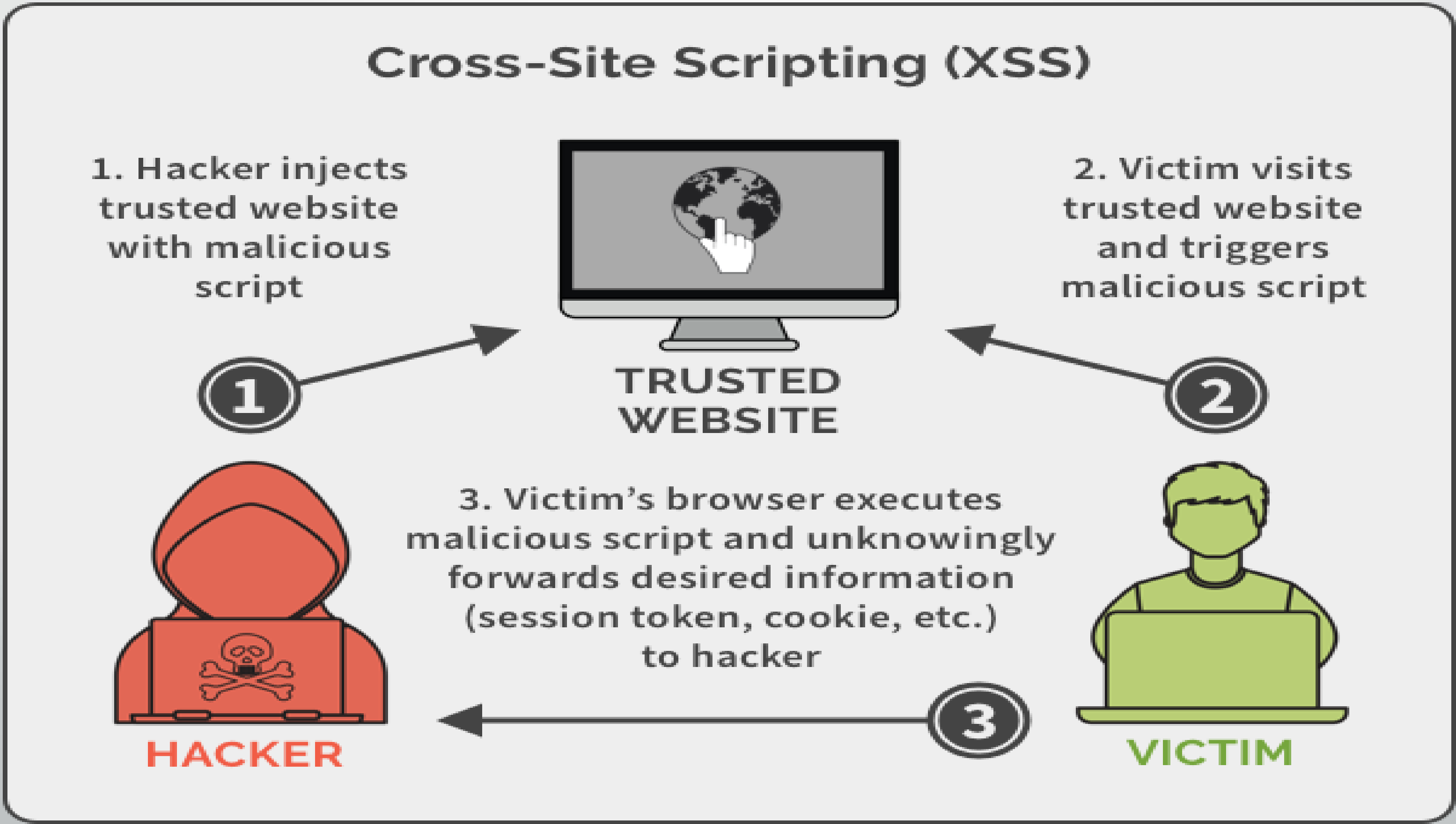
Ways to prevent Zero-day Attack :-

- Use an advanced, proactive email security solution
- Educate users
- Deploy a web application firewall
- Implement network access control Zero-day attack


Zero-day definitions
A zero-day vulnerability
A security software flaw that is unknown to the user
A zero-day exploit
When hackers take advantage of a zero-day vulnerability
A zero-day attack
When hackers leverage their zero-day exploit to carry out a cyber attack

Cross-site scripting

Cross-site scripting is a cyber-attack where an attacker sends **malicious code** to a reputable website



Cross-Site Scripting (XSS)

1. Hacker injects trusted website with malicious script

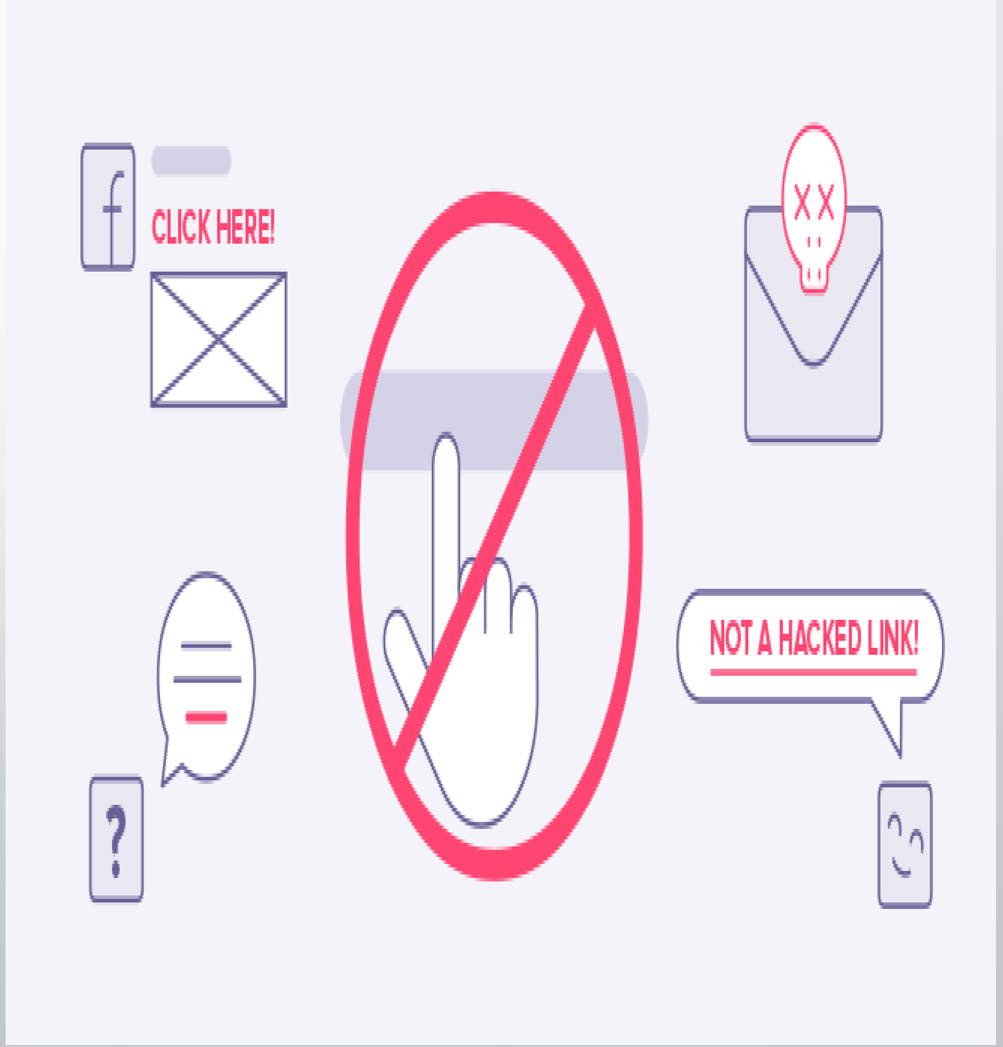
2. Victim visits trusted website and triggers malicious script

3. Victim's browser executes malicious script and unknowingly forwards desired information (session token, cookie, etc.) to hacker

Cross-site scripting

Ways to prevent Cross-site-scripting:-

- Filter input on arrival.
- Encode data on output.
- Use appropriate response headers.
- Content security policy.



Advanced persistent threat

An advanced persistent threat occurs when an attacker gains **unauthorized access** to a system or network and remains **undetected** for a **long duration**.

Ways to prevent Advanced persistent threats:-

- Install a firewall
- Enable a web application firewall
- Install an antivirus
- Implement intrusion prevention systems
- Create a sandboxing environment
- Install a VPN

Password attacks

Password attack is an attempt to **steal** passwords from a user.

Two common techniques used to get user’s password :-

- Brute-force guessing
- Dictionary attack Ways to prevent Password attack
- Use strong password
- Multi-factor authentication

Few other types of cyber threats

- Drive by attack
- Denial of service
- Distributed denial of service
- Eavesdropping attack
- AI-powered attack

Cyber threats and intelligence

Cyber threat intelligence is the amount of data that becomes cyber threat information that is collected, evaluated in the context of its source, and **analyzed** through **rigorous** and **firm tradecraft techniques** by the industry experts.

Thank you