Security Awareness Training Program

PRESENTATION BY KODHAI UDAY (TEAM 8.2)

What is this program and why do we need it?

What?

- To increase the understanding of cyber threats
- To understand the security risks associated with one's actions
- To empower common people and employees be safer and more secure online
- Manage and mitigate organizational risk
- To identify cyber attacks
- To help fight or prevent information security breaches

Why?

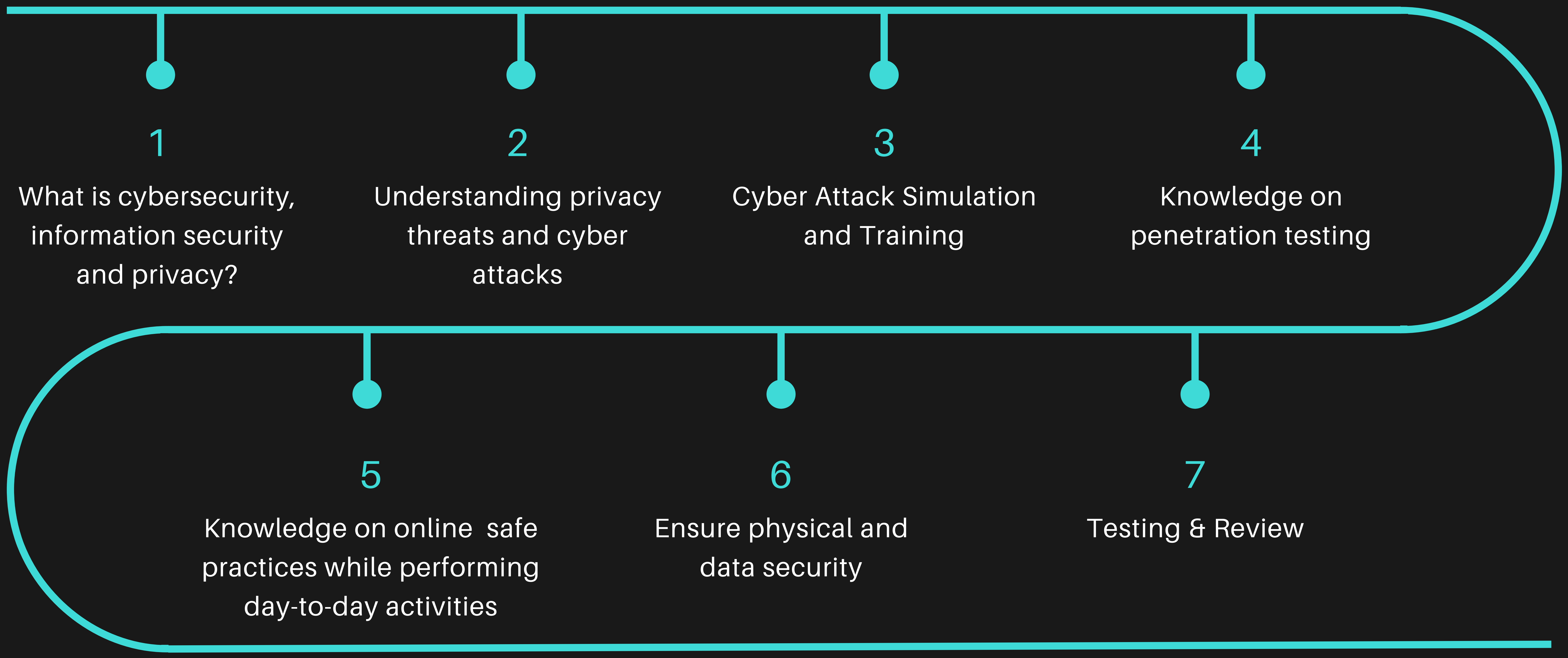
- Data breaches are expensive and need to be secured properly
- Human errors may cause security breaches and so this program helps address these errors committed while performing day-to-day tasks

How do we do this?

- Through conducting detailed training courses (such as this one)
- Providing knowledge about vulnerabilities and cyber attacks
- Simulations of attacks for more understanding
- Risk assessment reports need to be performed
- Every person, employee and employer should be aware of these threats and vulnerabilities including safe-keeping and protection techniques.

Security Awareness Training Program

Roadmap



1
What is cybersecurity, information security and privacy?

2
Understanding privacy threats and cyber attacks

3
Cyber Attack Simulation and Training

4
Knowledge on penetration testing

5
Knowledge on online safe practices while performing day-to-day activities

6
Ensure physical and data security

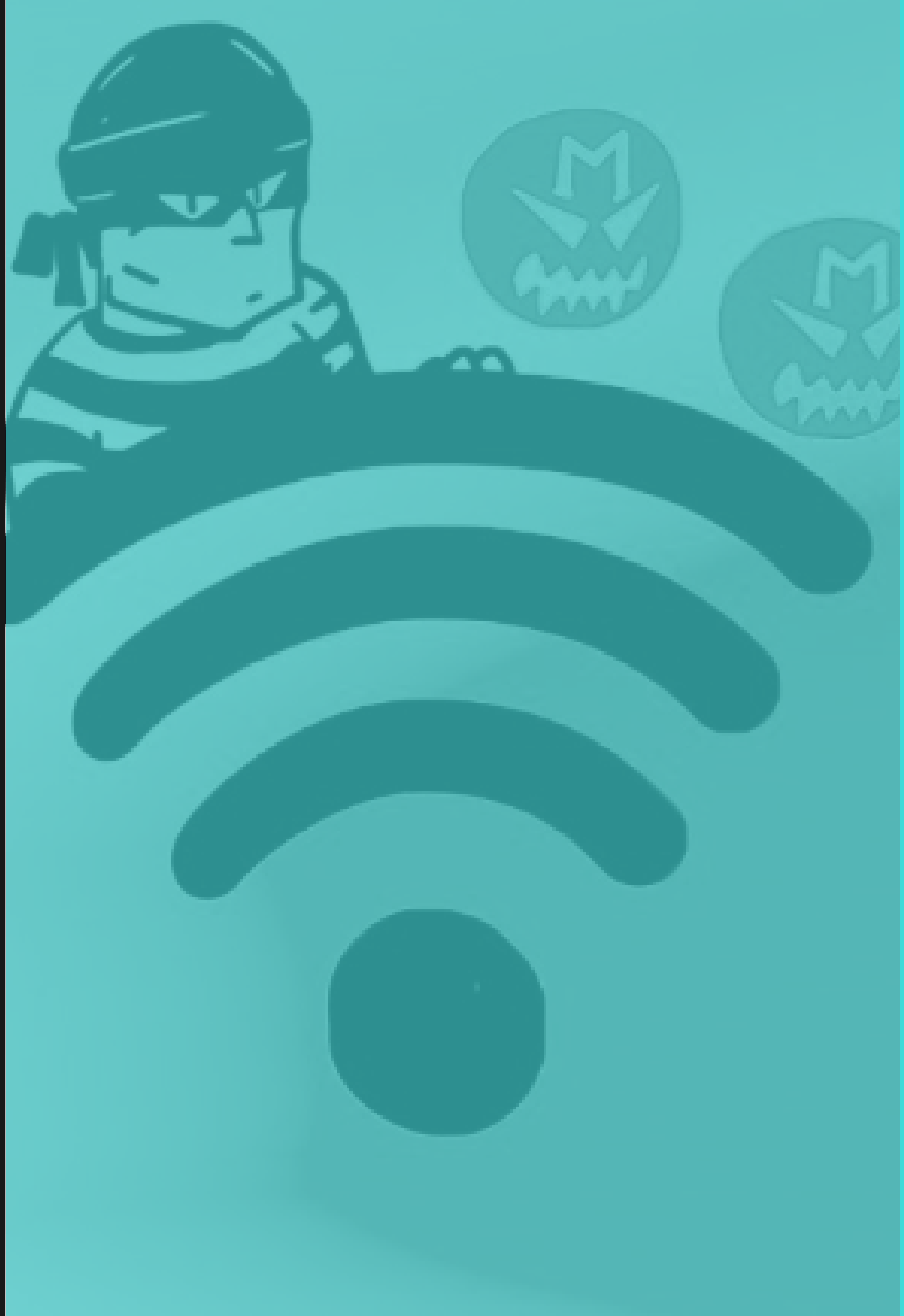
7
Testing & Review

Some key topics include:

- Password management
- Privacy
- Email/phishing security
- Web/internet security
- Physical and office security
- Social Media Usage
- Social Engineering
- Public Wi-fi safety
- Guidance on working remotely
- SQL Injection

Public Wifi Safety

- Hackers lurking in the background of public wifi.
- Hacker position himself between the victim and the connection point.
- Necessary to use a remote access sytem (like a VPN) to protect the user's network.



Public Wifi Safety

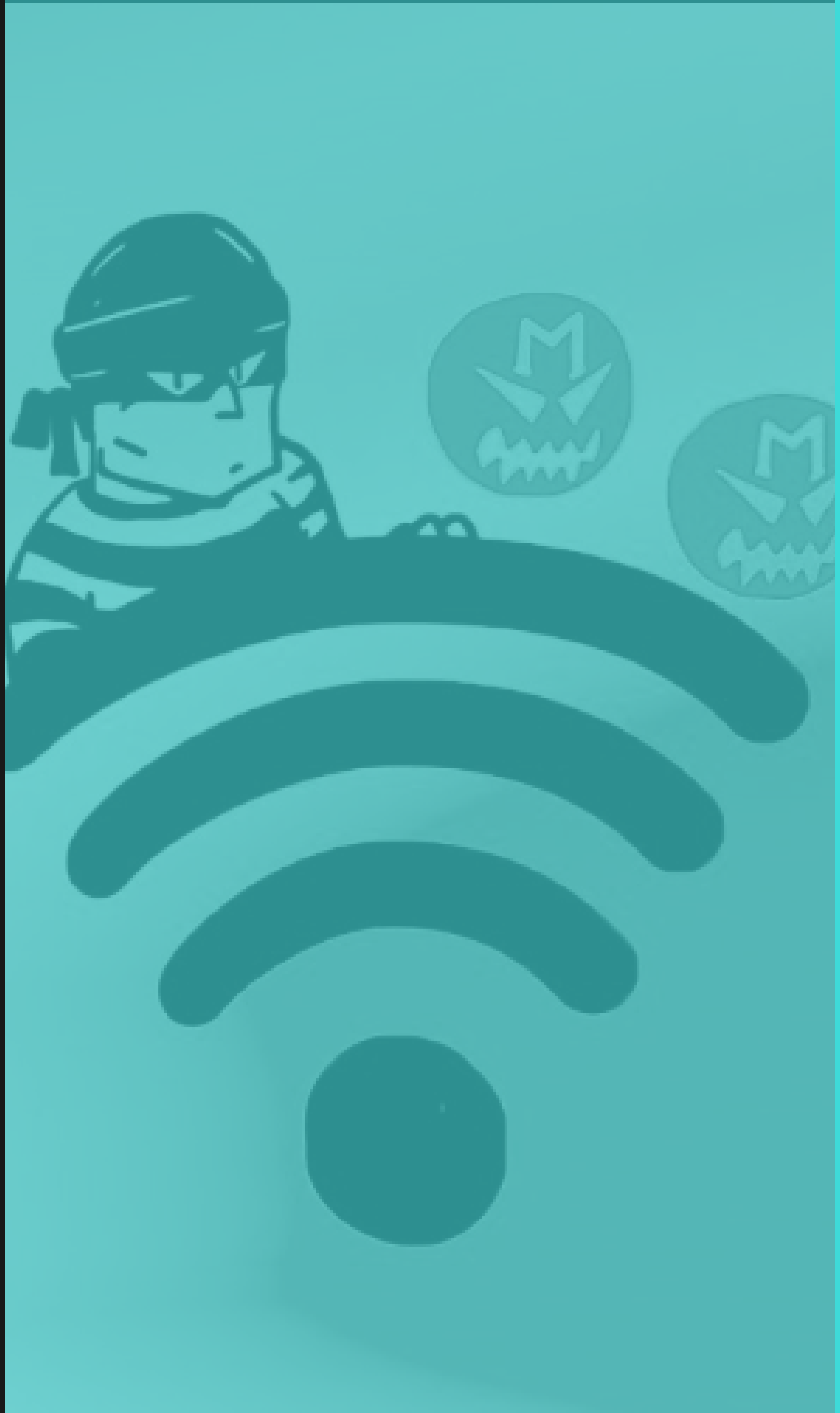
Different threats possible through using public wifi:

-Man in the Middle Attack: A third party intercepts communication between two participants.

-Fake Wifi Connections (Malicious Hotspots): Setting up fake access points with similar names to trick the victim into connecting to the wrong network.

-Packet Sniffing: Transmission of data packets through an unencrypted network that can be read by free softwares like wireshark.

-Sidejacking: Obtaining information via packet sniffing. Can even bypass some level of encryption.



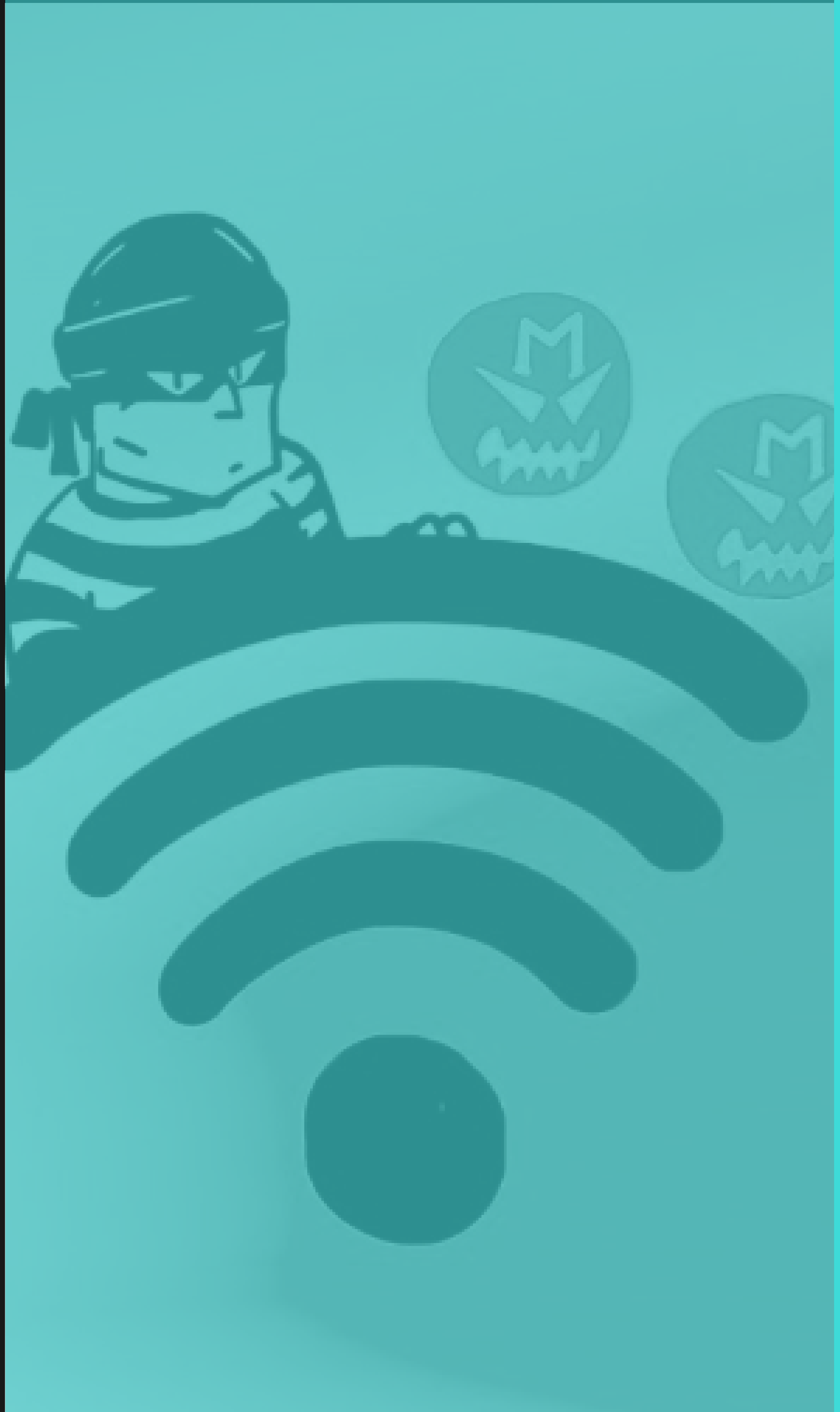
Public Wifi Safety

Protection:

- Using a Virtual Private Network (VPN): will reroute the traffic through a private, encrypted network.

- Enable 2-factor authentication: To help keep your account safer drom cyber attacks.

- Bluetooth Monitoring: Can be vulnerable to identity thefts due to intermediate access points. Data can be accessed via bluetooth and hence it should be constantly monitored.



Email/Phishing Attacks

Attackers send fraudulent mails with malicious links to lure and trick the victims into opening.

These mails are usually disguised as though they are from a legit trusted sender.

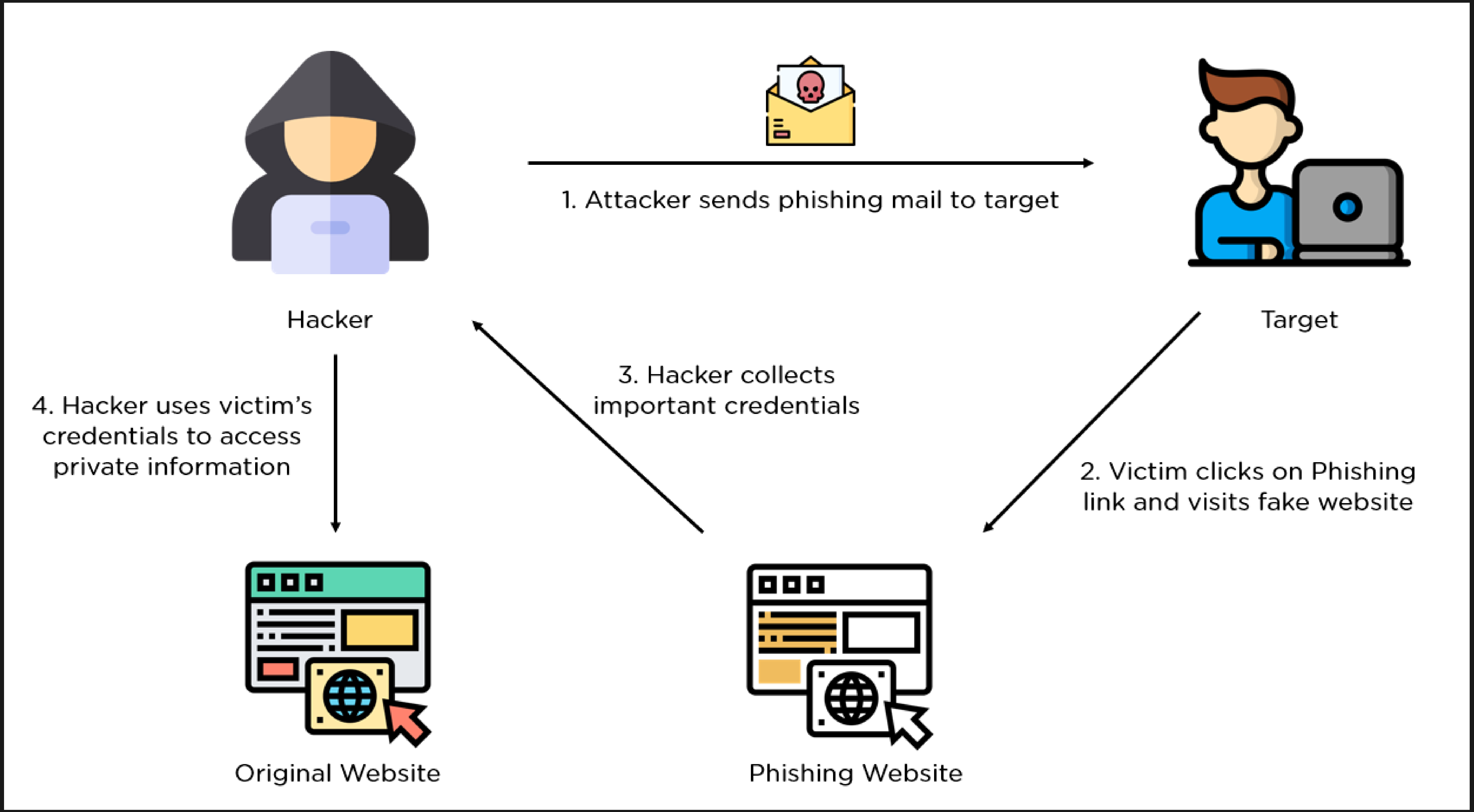
The goal is usually:

- to steal sensitive information like login credentials and passwords of victims by tricking them.
- or to download malware into the victim's computer through the links in the mail.

Protection:

- User Education: Ability to differentiate and recognize a phishing mail.
- Network security technologies (Access Control, malware protection, user behavior monitoring, web security) can be implemented.

Email Phishing Attacks



1. Attacker sends phishing mail to target

2. Victim clicks on Phishing link and visits fake website

3. Hacker collects important credentials

4. Hacker uses victim's credentials to access private information

SQL Injection

A web hacking technique. Placement of malicious code in SQL statements through web page input.

Allows attackers to interfere with the queries made by applications to their databases, resulting in leaking sensitive information or even destroying the database.

Through SQL injection, one can:

- Retrieve hidden data: Modify a query to return additional information
- UNION attack: To retrieve data from different database tables
- Examine the database: Extract information about the database
- Subvert application logic: Applications logic can be interfered by modifying a query

Detecting SQL Injection Vulnerability

Can be detected manually by testing against every entry point in the specific application:

- Submitting specific syntax that calculates the base value of the entry point and to a different value and checking for differences in the results
- Submitting boolean conditions and checking for differences in the results
- Submitting payloads (that trigger time delays) and checking for differences in the time taken to provide results
- Submitting a single quote character and checking for errors or anomalies
- SQL injections can in be in different parts of hte query

⋆First Order SQL Injection
⋆Second Order SQL Injection

SQL Injection Vulnerability Prevention

Usage of parameterized queries (prepared statements) instead of string concatenation
Example:
Vulnerable Query: String query = "SELECT * FROM xxx WHERE attrib = ' "+ input + " ' ";
Statement statement = connection.createStatement();

Re-written Query: PreparedStatement statement = connection.prepareStatement
("SELECT * FROM products WHERE category = ?"); statement.
setString(1, input);

Denial of Service Attacks

What?

To shut down a network or machine, making it inaccessible to the intended users.

How?

By flooding the target with traffic by providing numerous requests continuously or by sending information that triggers a crash.

Popular Flood Attacks: ICMP Flood, SYN Flood, Buffer Overflow Attacks

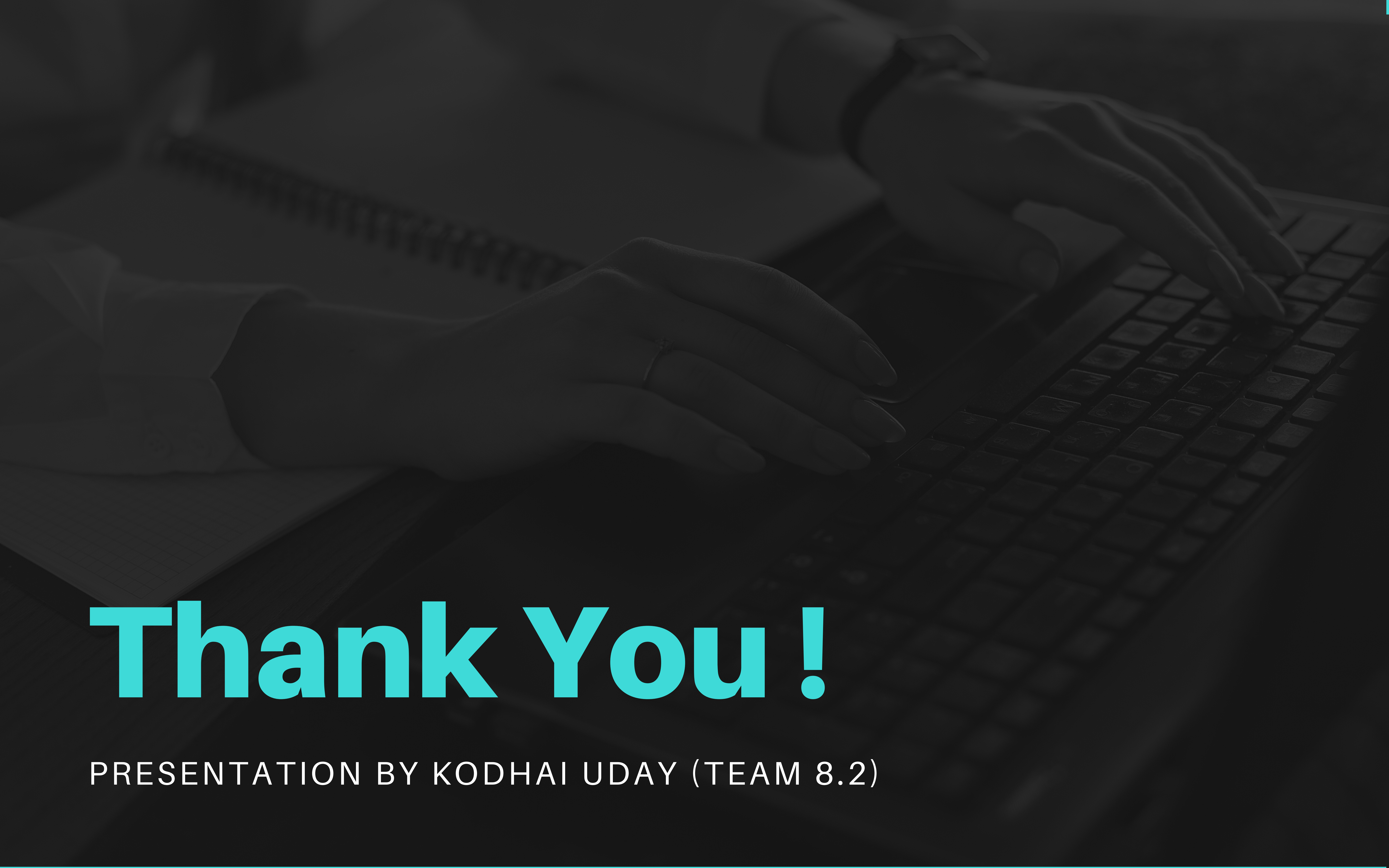
Why?

Attacker might ask for some sort of ransom in return for granting access to the victims again.

Can cause a lot of waste in time.

DoS Attacks Prevention

- Blocking the IP and hence the traffic from suspicious sources.
- Limiting the rate of traffic that can reach a server.
- Traffic distribution among multiple servers (Load balancing)
- Distributing the contents of a website across various locations.
- Network segmentation to smaller pieces.
- Choosing the correct kind of DoS protection solution.



Thank You !

PRESENTATION BY KODHAI UDAY (TEAM 8.2)