اونيۏرسيتي مليسيا ڤهڠ السلطان عبدالله
UNIVERSITI MALAYSIA PAHANG
AL-SULTAN ABDULLAH

Faculty of Computing
Fakulti Komputeran

Data & Network Security

Chapter 4 - Threats and Attacks

Outline

4.1 Attacker’s goals, capabilities, and motivations

4.2 Malware

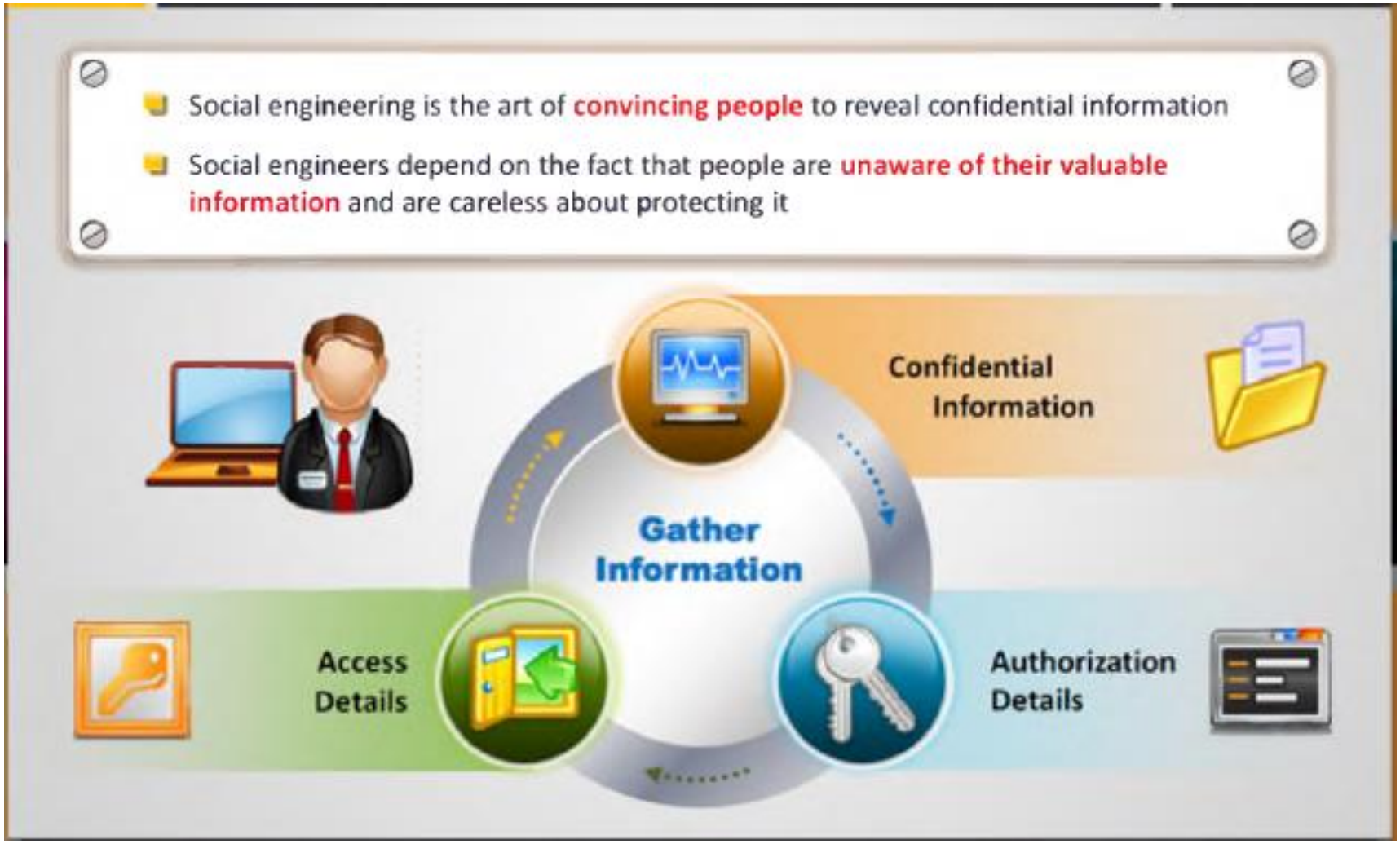
4.3 Social engineering

4.4 Network specific threats and attack types

Sub-topic 4.3

Social engineering

Social engineering



Behaviours vulnerable to attacks

I. Human nature of trust is the basis of any social engineering attack

II. Ignorance about social engineering and its effects among the workforce makes the organization an easy target

III. Social engineers might threaten severe losses in case of non- compliance with their request

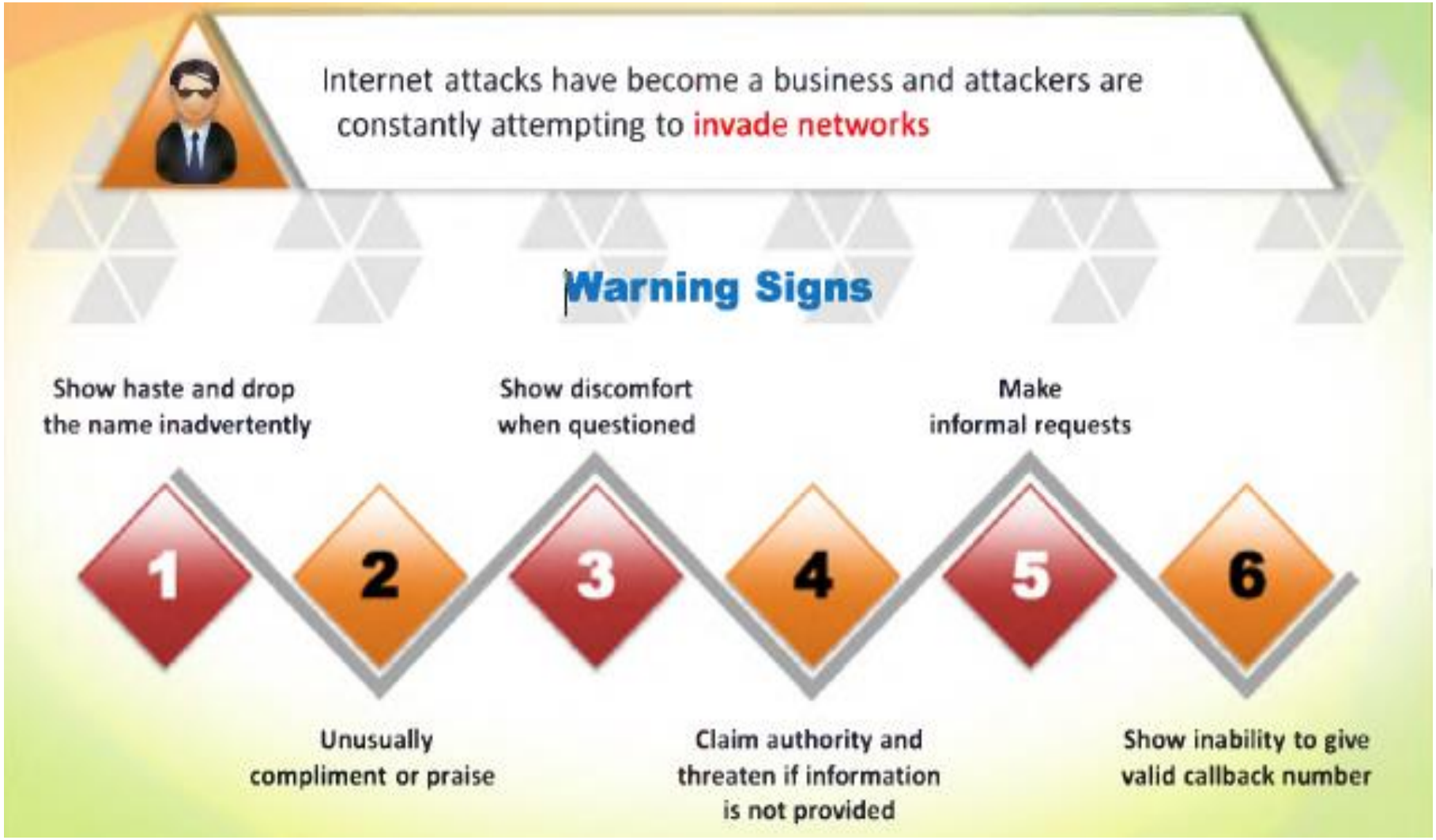
IV. Social engineers lure the targets to divulge information by promising something for nothing

V. Targets are asked for help and they comply out of a sense of moral obligation

Factors that make companies vulnerable to attacks

Why is social engineering effective?

Warning signs of an attack



Phases in a social engineering attack

1

Research on Target Company

Dumpster diving, websites, employees, tour company, etc.

2

Select Victim

Identify the frustrated employees of the target company

3

Develop Relationship

Develop relationship with the selected employees

4

Exploit the Relationship

Collect sensitive account information, financial information, and current technologies

Impact on the organization

Common Targets of Social Engineering

CEH

- Receptionists and Help Desk Personnel
- Technical Support Executives
- System Administrators
- Vendors of the Target Organization
- Users and Clients

Method: type of social engineering

Human-based social engineering: Eavesdropping and shoulder surfing

Eavesdropping

- Eavesdropping or unauthorized listening of conversations or reading of messages
- Interception of any form such as audio, video, or written
- It can also be done using communication channels such as telephone lines, email, instant messaging, etc.

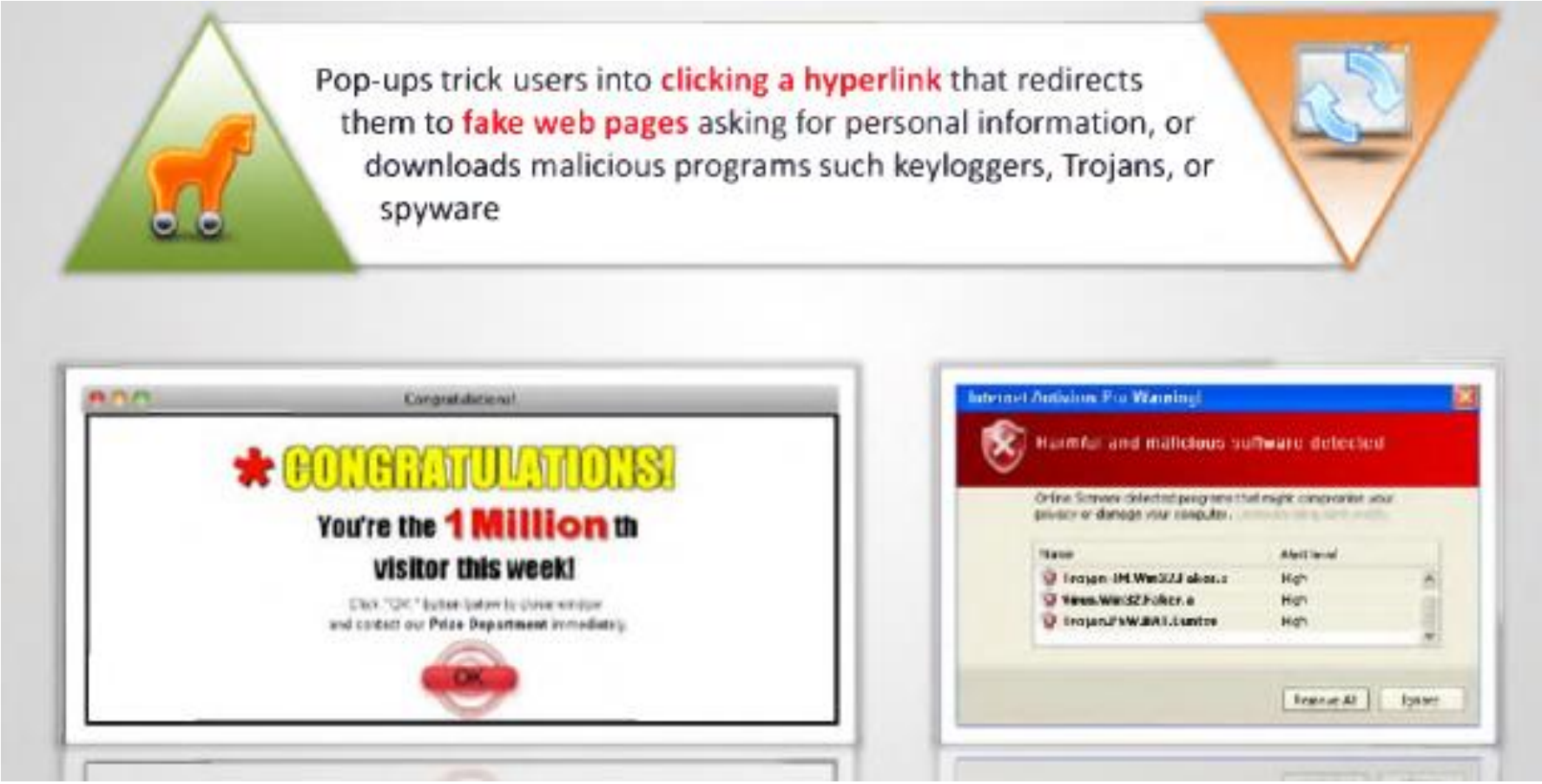
Shoulder Surfing

- Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.
- Shoulder surfing can also be done form a longer distance with the aid of vision enhancing devices such as binoculars to obtain sensitive information

Human-based social engineering: Dumpster diving

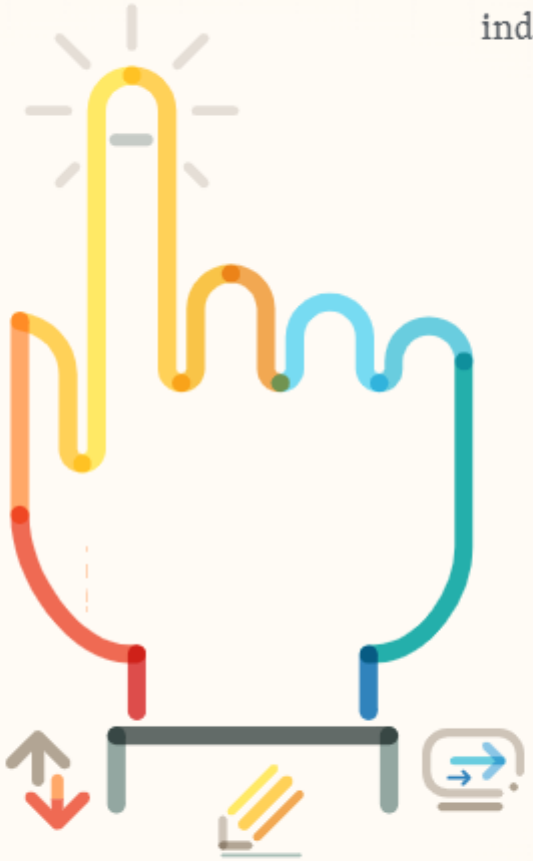
Computer-based social engineering

Computer-based social engineering: Pop-Ups



Often posing as a request for data from a trusted third party, phishing attacks are sent via email and ask users to click on a link and enter their personal data.

It often **involves psychological manipulation**, invoking urgency or fear, fooling unsuspecting individuals into handing over confidential information.

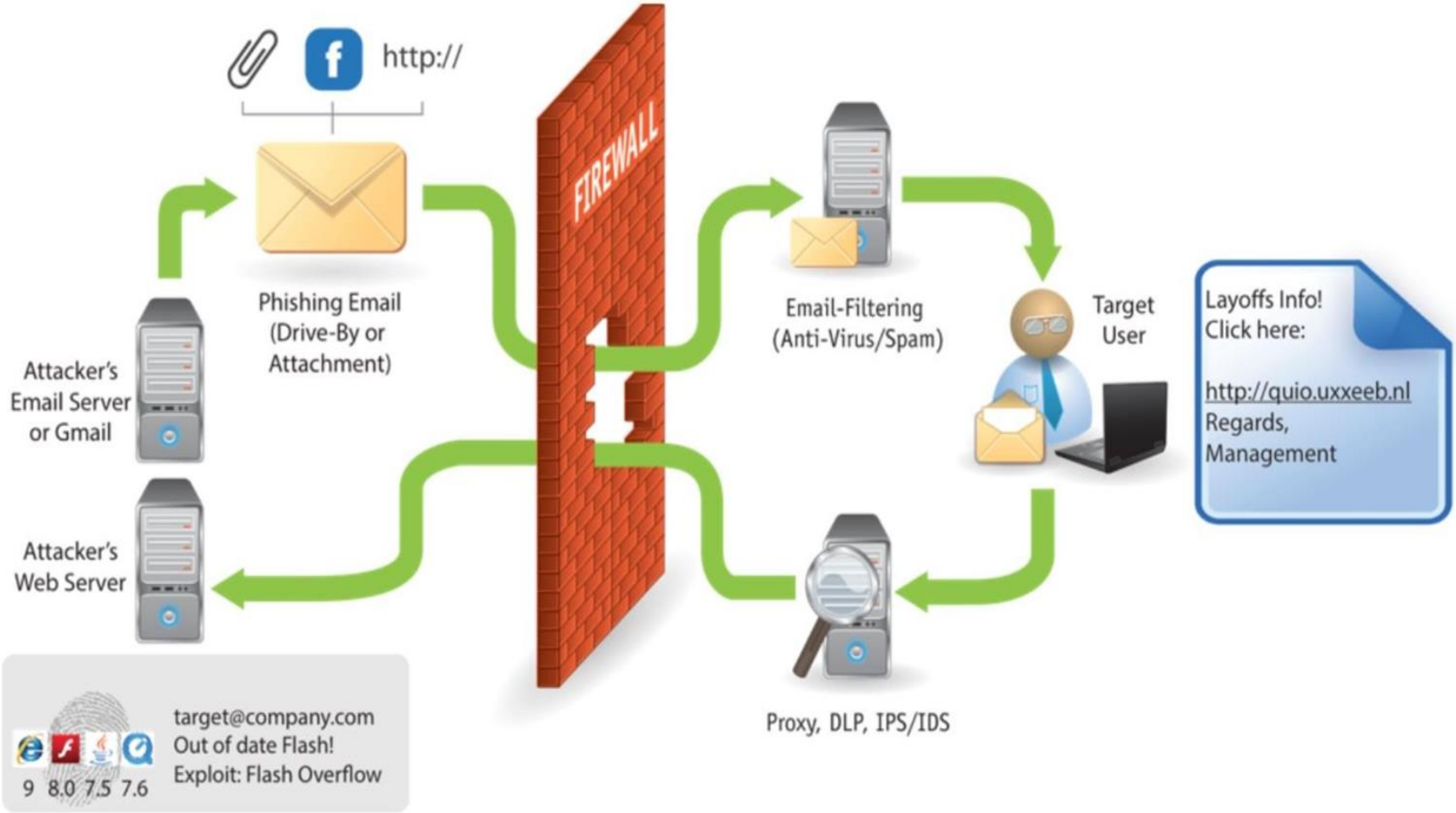


Phishing emails have become sophisticated and often look just like legitimate requests for information. Second, phishing technology is now being licensed out to cybercriminals.

Phishing emails are six times more likely to be clicked than regular consumer marketing emails.

Phishing Attacks

How phishing works?

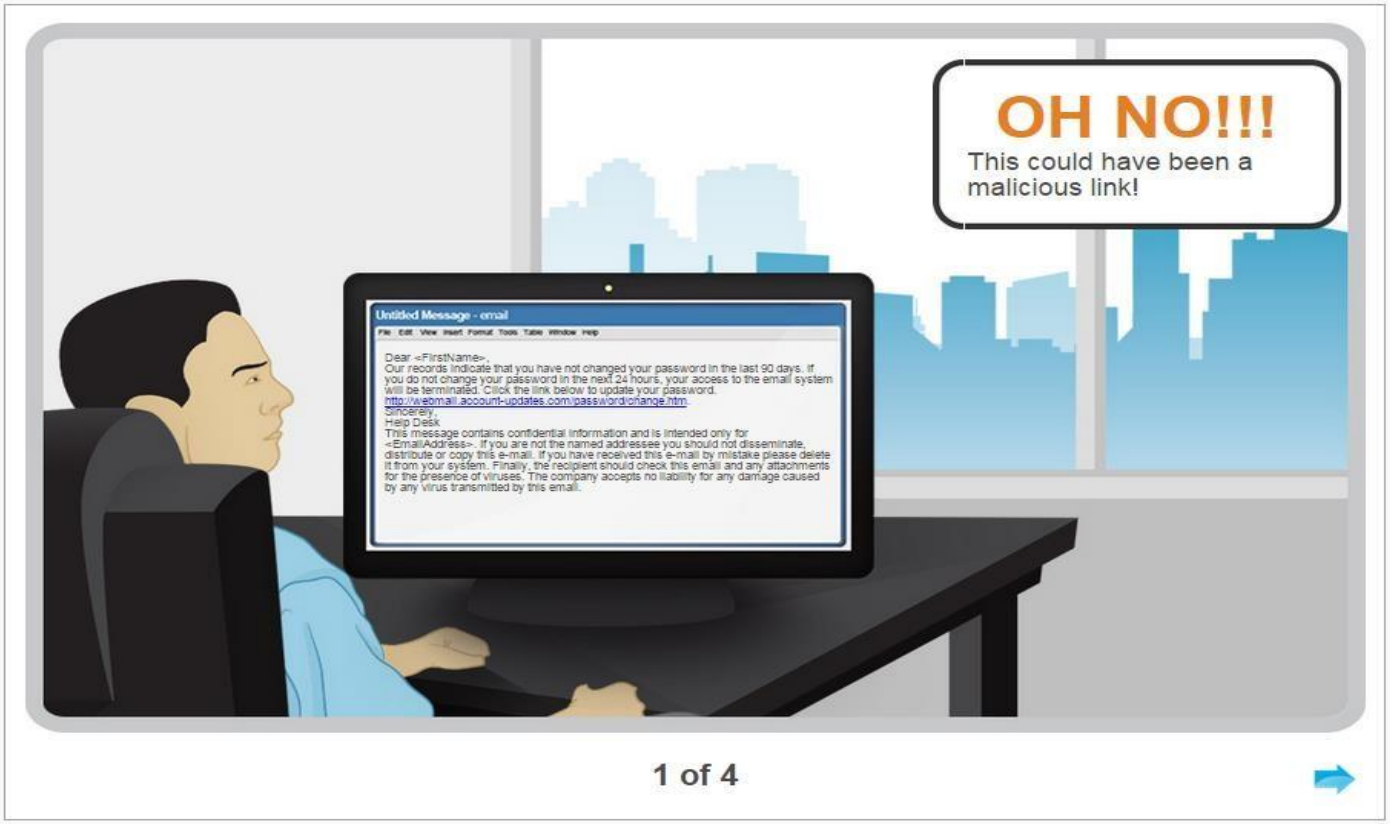


What makes phishing work?

- Phishing uses tactics that motivate a response - greed, fear, ambition, curiosity
- Sometimes simple is dangerous - shipping notifications, funny pictures
- Employees don’t really know better
- Deception is key - look-alike URLs, obfuscated file attachment names
- Includes a “call to action” (e.g. “Open this now!”, “Click here now!”)
- Employees are conditioned to both trust email and be responsive

Teachable moment

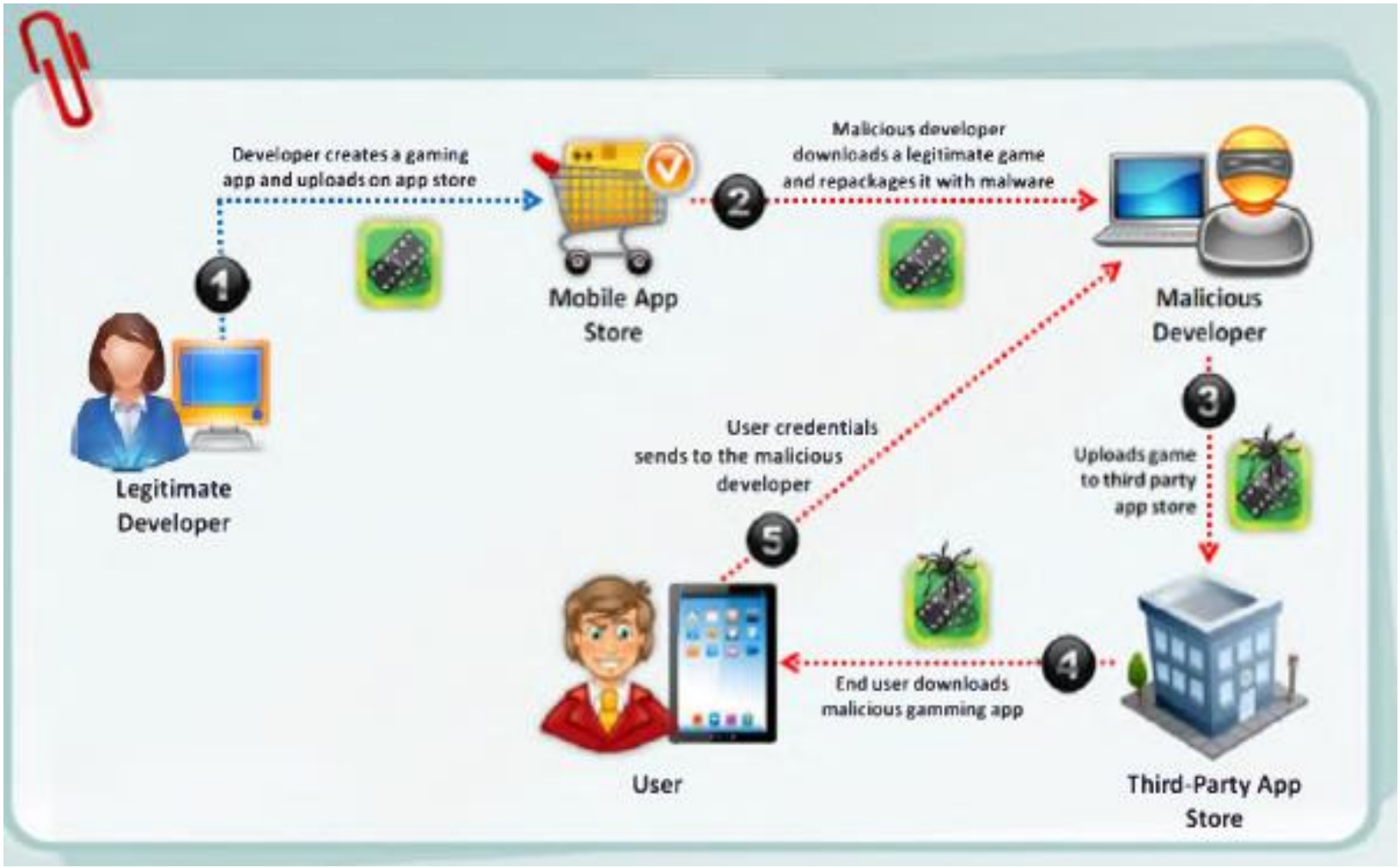
Oops! The email you just responded to was a fake phishing email. Don't worry! It was sent to you to help you learn how to avoid real attacks. Please do not share your experience with colleagues, so they can learn too.



Mobile-based social engineering: Apps malicious publishing

- Attackers create **malicious apps** with attractive features and **similar names** to that of popular apps, and publish them on major **app stores**
- Unaware **users download these apps** and get infected by malware that sends **credentials to attackers**

Mobile-based social engineering: Repackaging legitimate apps

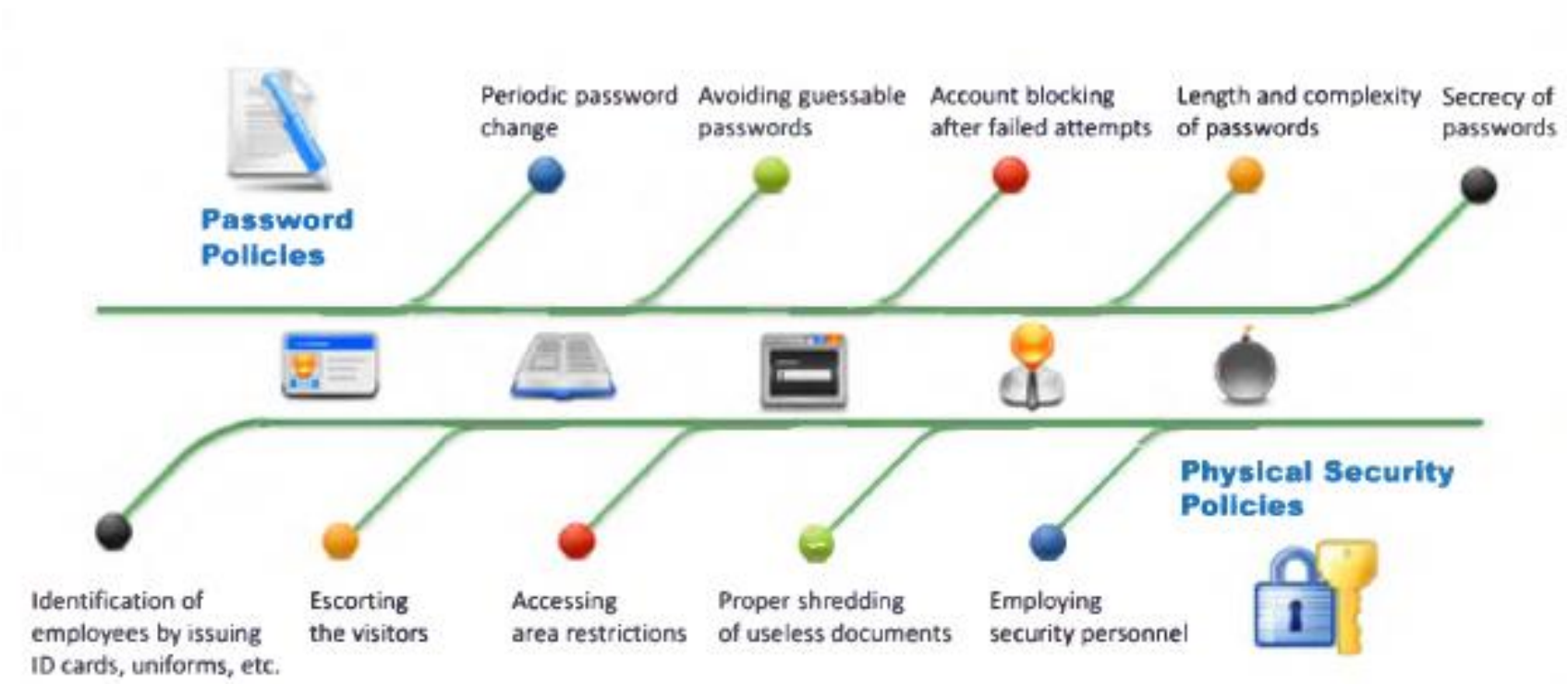


Common social engineering targets and defence strategies

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, Ingratiation, etc.	Employee training, best practices and checklists for using passwords Escort all guests
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, employee training
Machine room/ Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment

Social engineering: Countermeasures

- Good policies and procedures are ineffective if they are not taught and reinforced by the employees
- After receiving training, employees should sign a statement acknowledging that they understand the policies

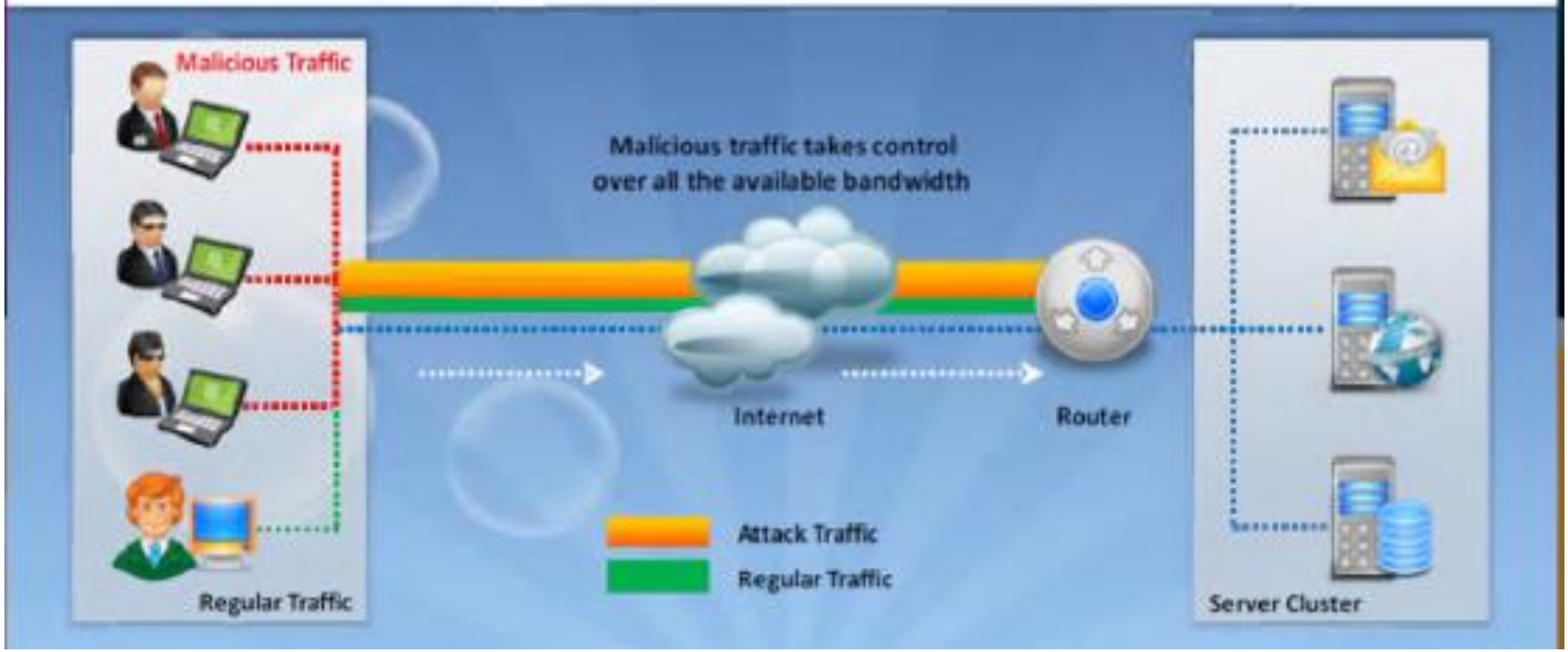


Sub-topic 4.4

Network specific threats and attack types

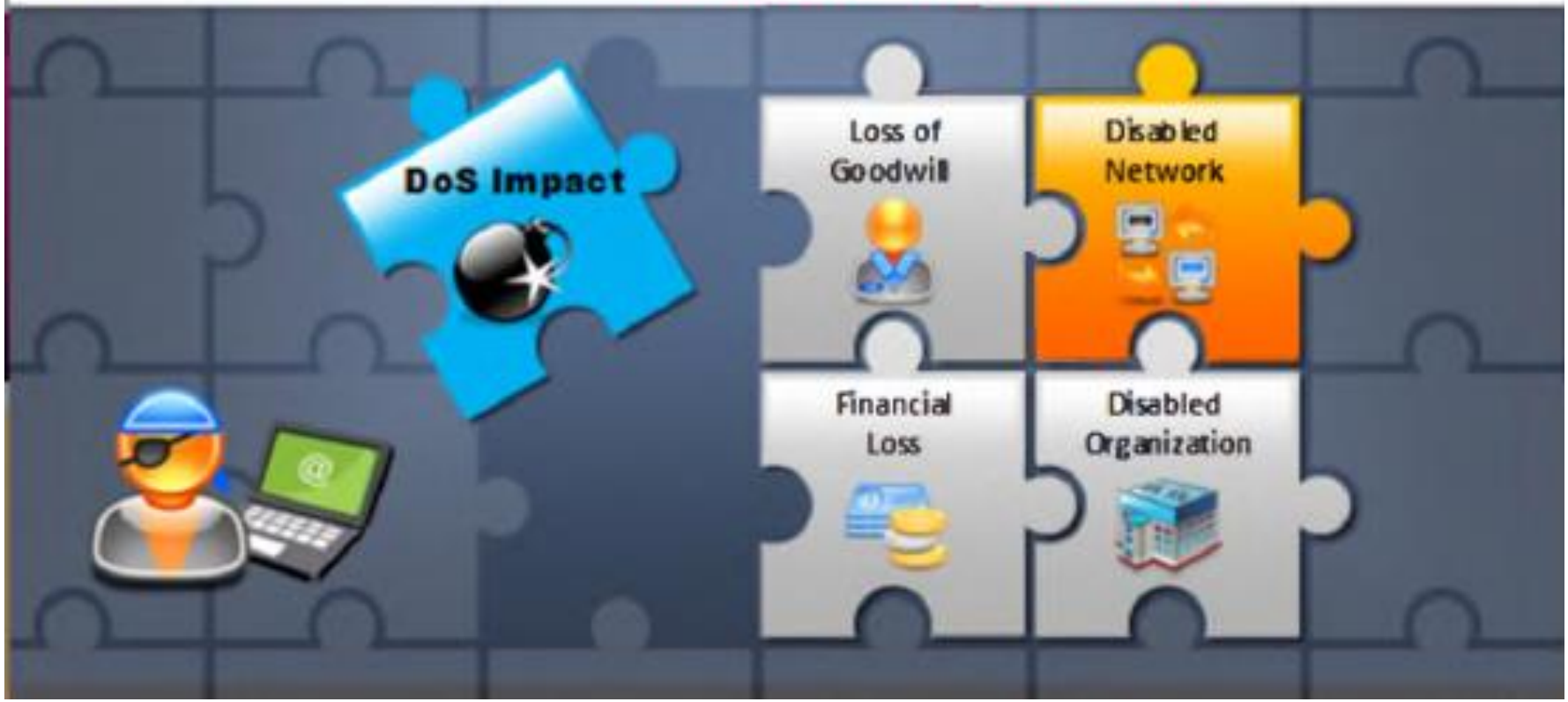
Network-specific threats and attack types: DoS

- Denial of Service (DoS) is an attack on a computer or network that **reduces, restricts** or **prevents legitimate** of its resources
- In a DoS attack, attackers flood a victim system with **non-legitimate service requests or traffic** to overload its resources

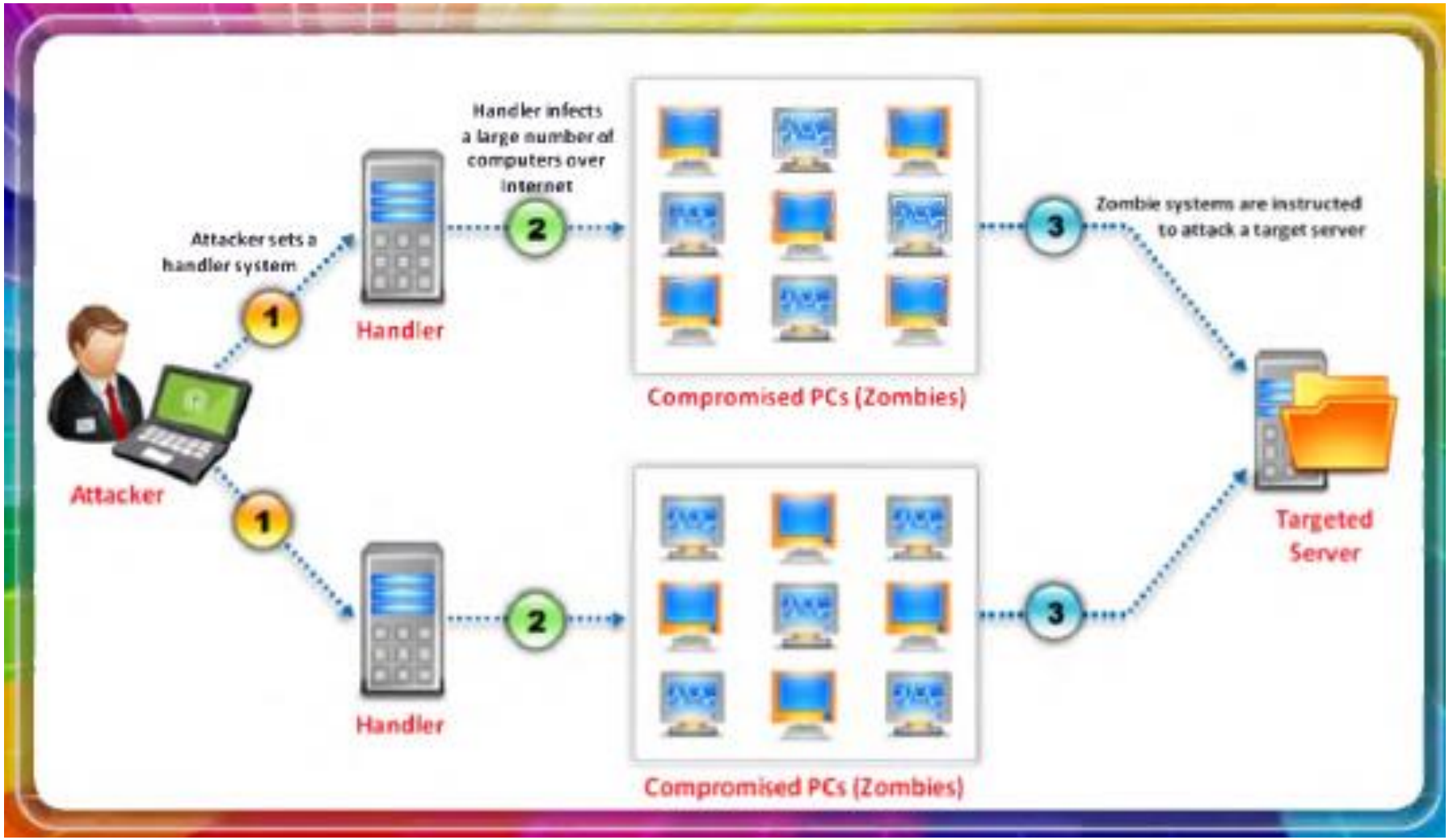


Network-specific threats and attack types: DDoS

- A distributed denial-of-service (DDoS) attack involves a **multitude of compromised systems** attacking a single target, thereby causing denial of service for users of the targeted system
- To launch a DDoS attack, an attacker **uses botnets** and **attacks a single system**

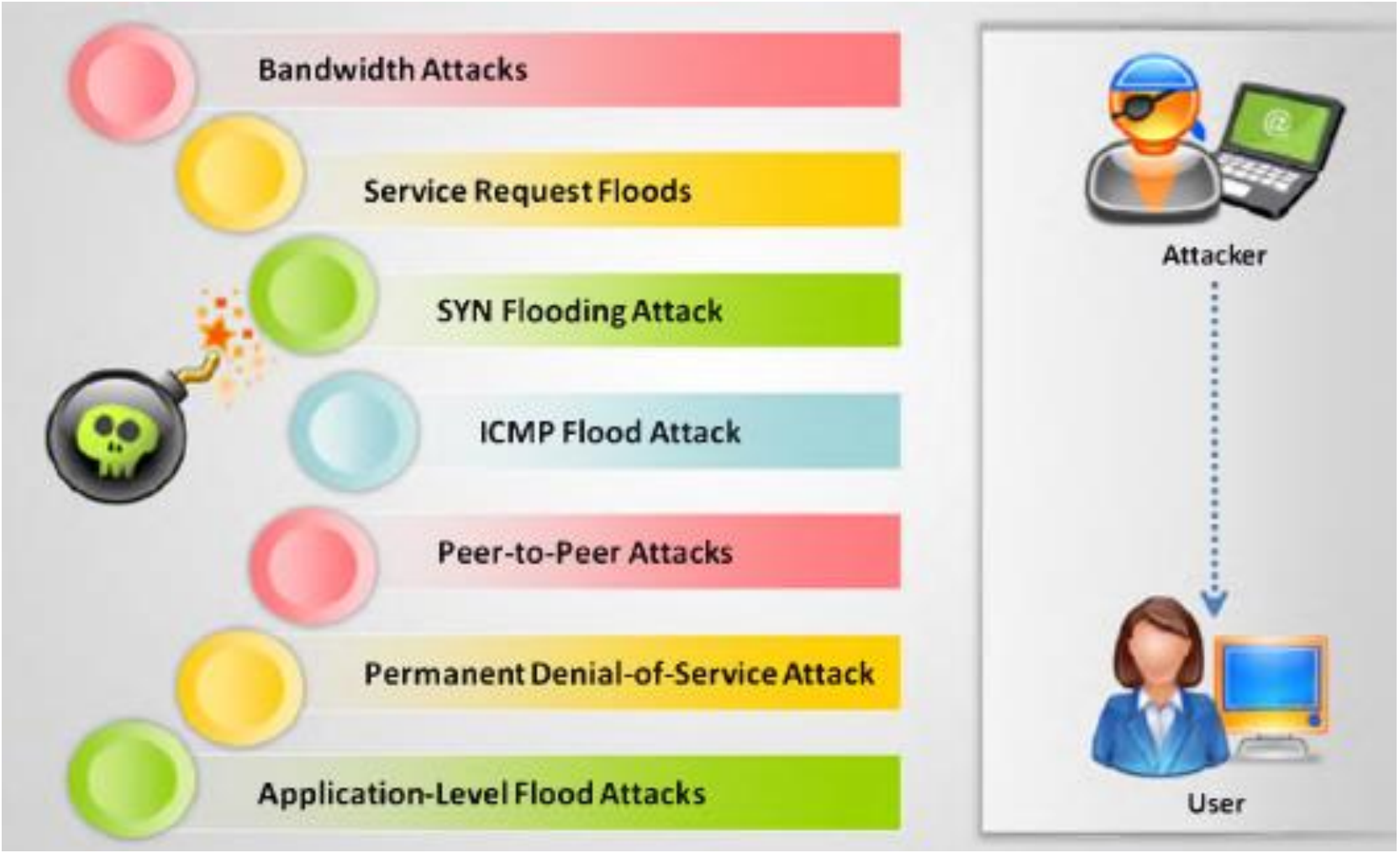


Network-specific threats and attack types: DDoS



Symptoms of a DoS attack

DoS attack techniques



Permanent denial-of-service attack

Phlashing

Permanent DoS, also known as **phlashing**, refers to attacks that cause irreversible damage to system hardware

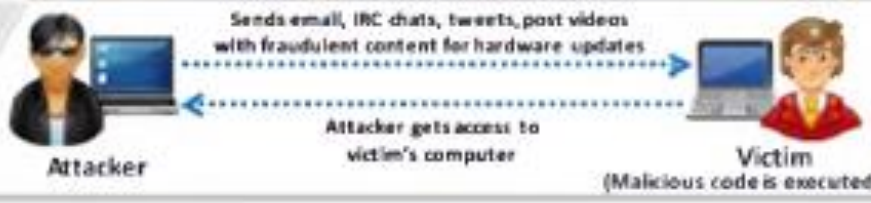
Sabotage

Unlike other DoS attacks, it **sabotages** the **system hardware**, requiring the victim to replace or reinstall the hardware

Bricking a system method

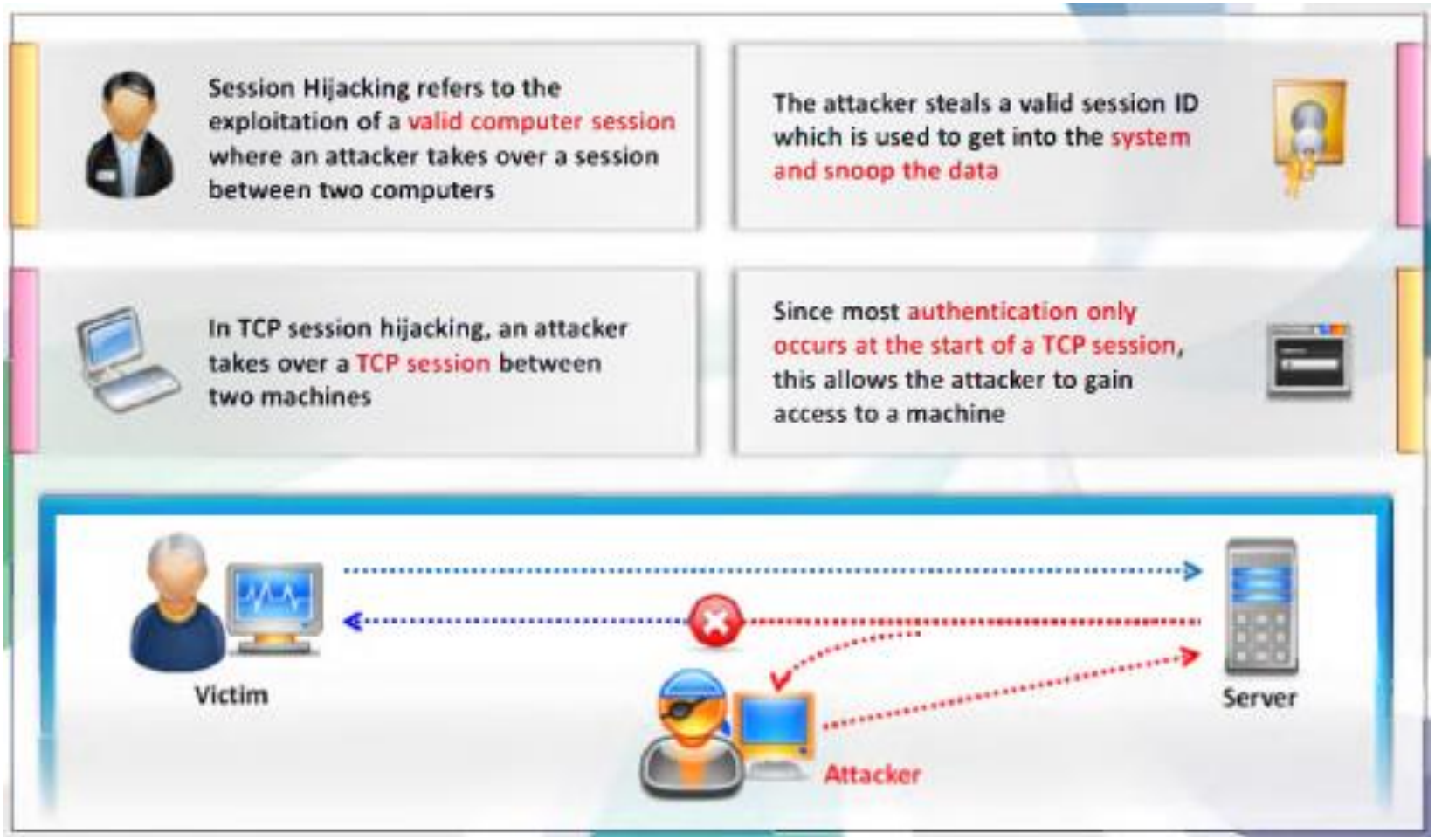
1. This attack is carried out using a method known as **"bricking a system"**
2. Using this method, attackers send **fraudulent hardware updates** to the victims

Process

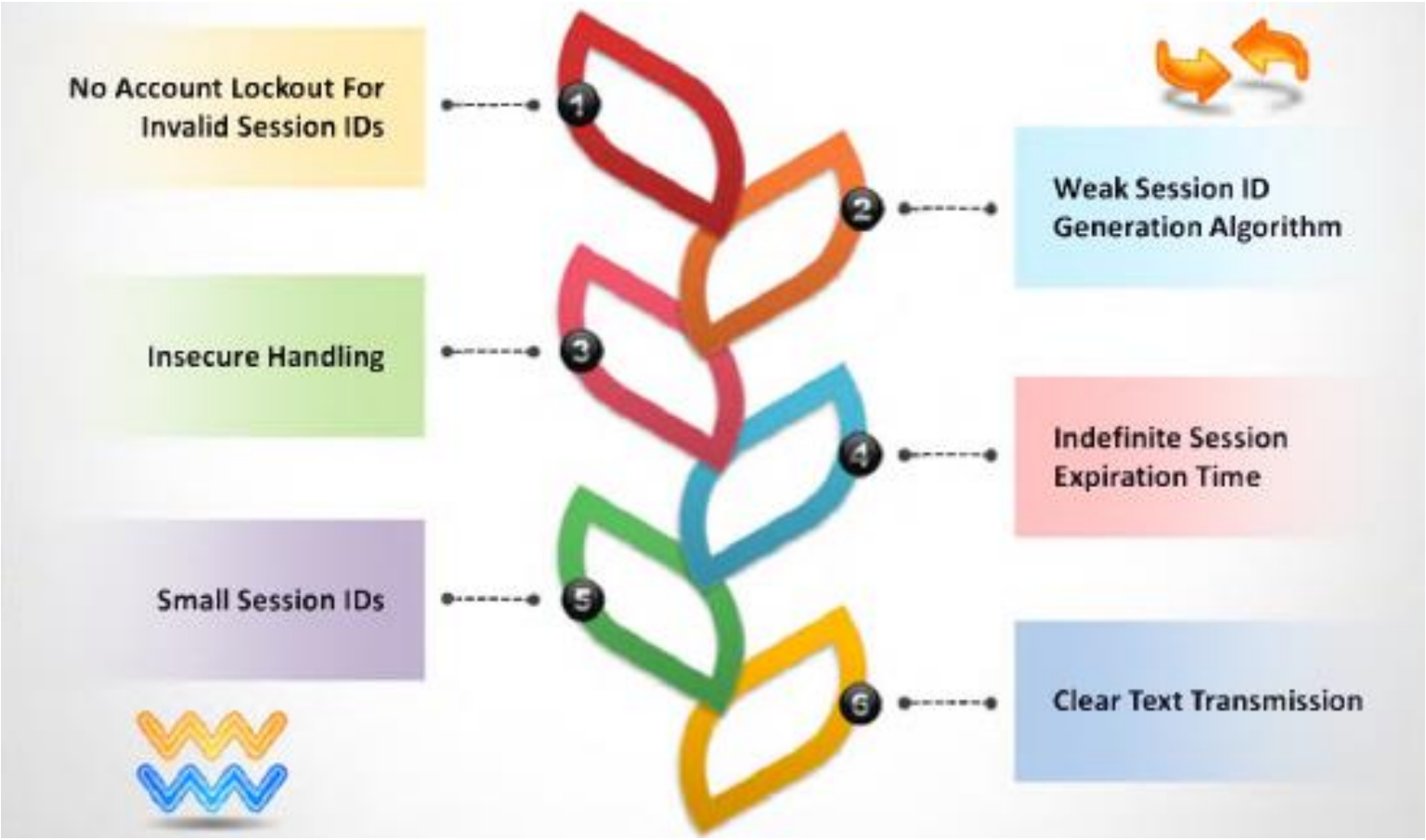


DoS/DDoS countermeasure strategies

Network-specific threats and attack types: Session hijacking



Why session hijacking is successful?



Spoofing vs. Hijacking

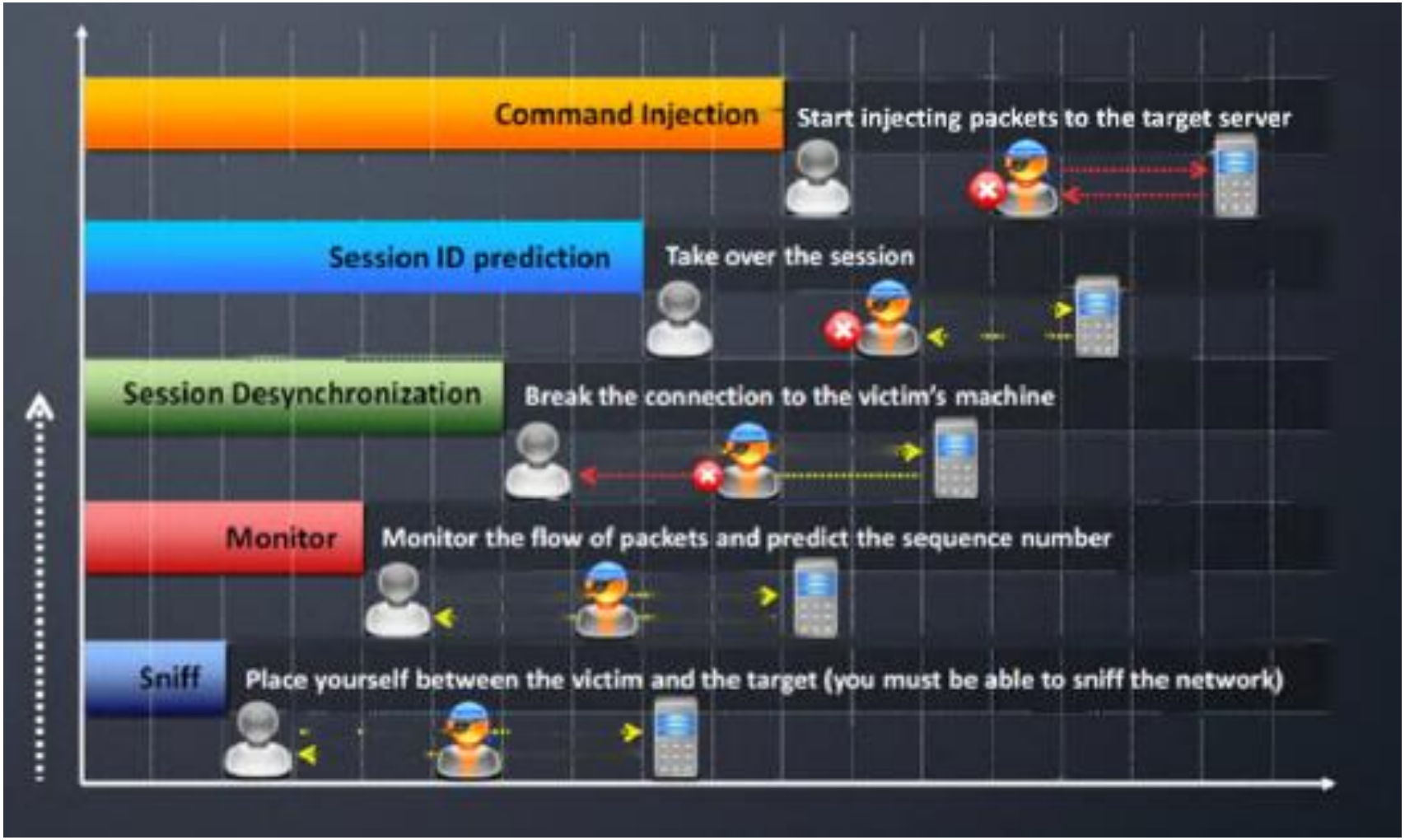
Spoofing Attack

- Attacker pretends to be another user or machine (victim) to gain access
- Attacker does not take over an existing active session. Instead he initiates a new session using the victim's stolen credentials

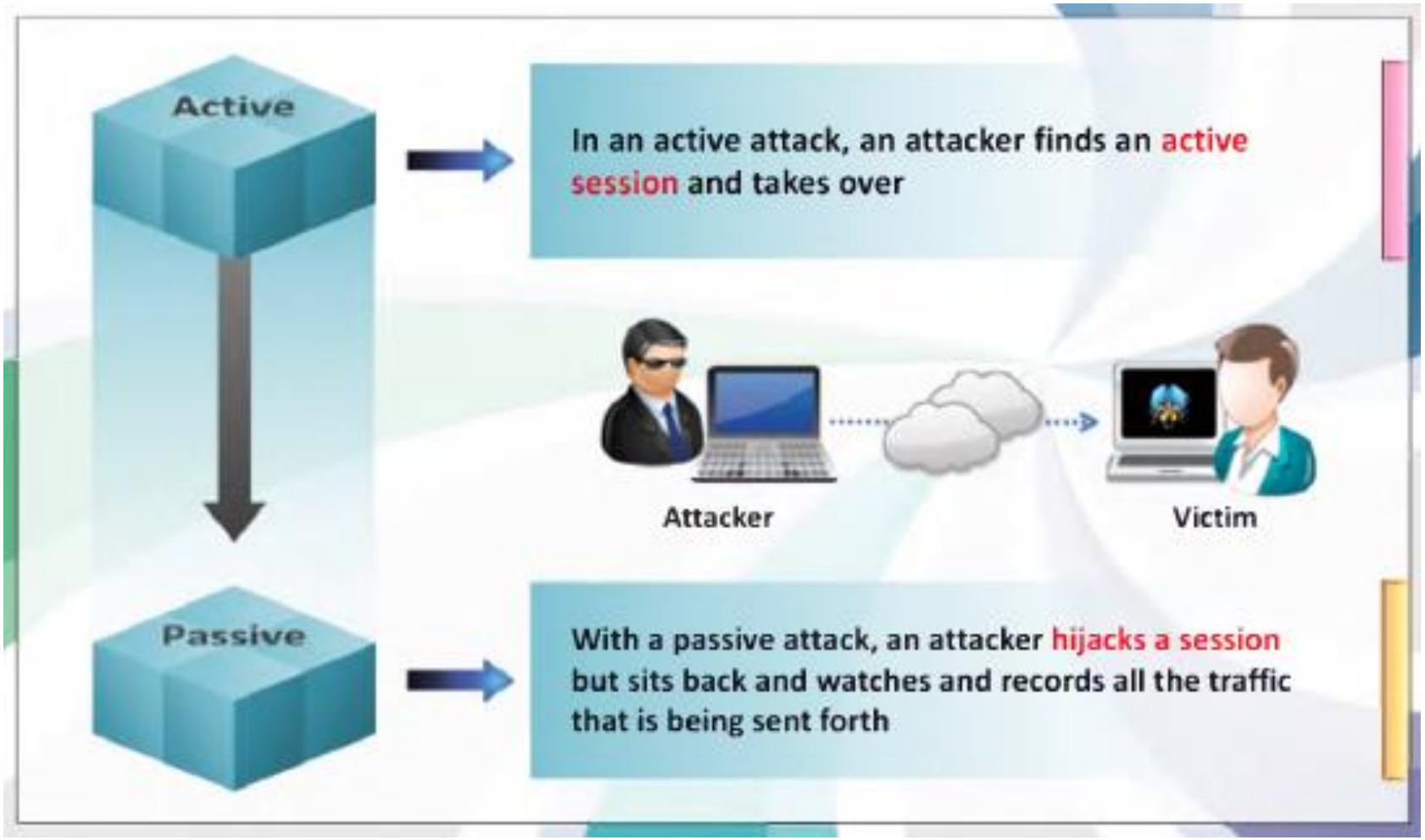
Hijacking

- Session hijacking is the process of taking over an existing active session
- Attacker relies on the legitimate user to make a connection and authenticate

Session hijacking process



Types of session hijacking



Network-specific threats and attack types: Webserver attack

- Web defacement occurs when an intruder maliciously alters visual appearance of a web page by inserting or substituting provocative and frequently offending data
- Defaced pages exposes visitors to some propaganda or misleading information until the unauthorized change is discovered and corrected

Webserver attack

Most common types of webserver attacks:-

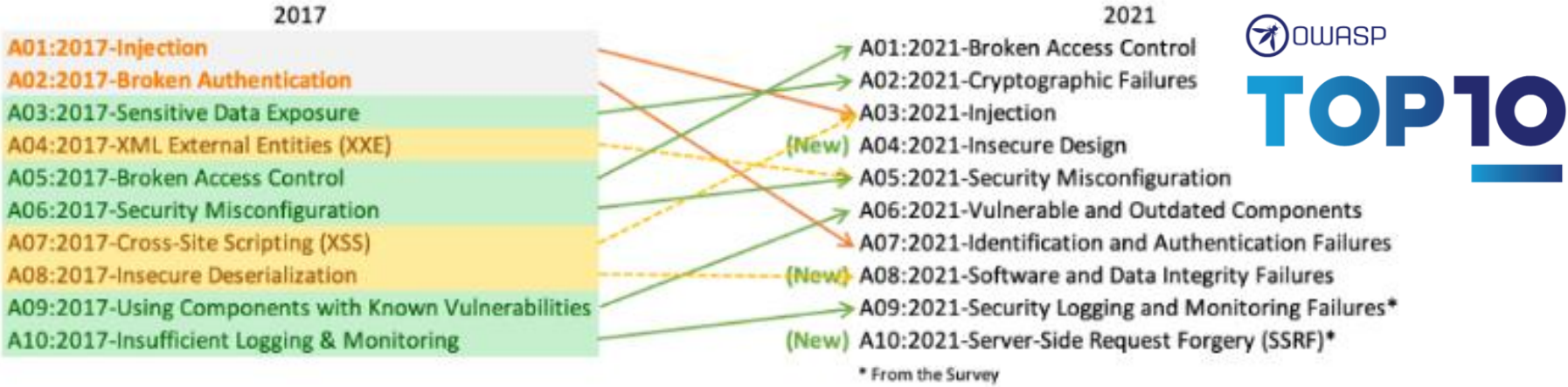
- **Cross-site scripting (XSS).** That involves an attacker uploading a piece of malicious script code onto your website that can then be used to steal data or perform other kinds of mischief. Although this strategy is relatively unsophisticated, it remains quite common and can do significant damage.
- **SQL Injection (SQLI).** This happens when a hacker submits destructive code into an input form. If your systems fail to clean this information, it can be submitted into the database, changing, deleting, or revealing data to the attacker.
- **Path traversal.** Also resulting from improper protection of data that has been inputted, these webserver attacks involve injecting patterns into the webserver hierarchy that allow threat actors to obtain user credentials, databases, configuration files, and other information stored on hard drives.

Webserver attack

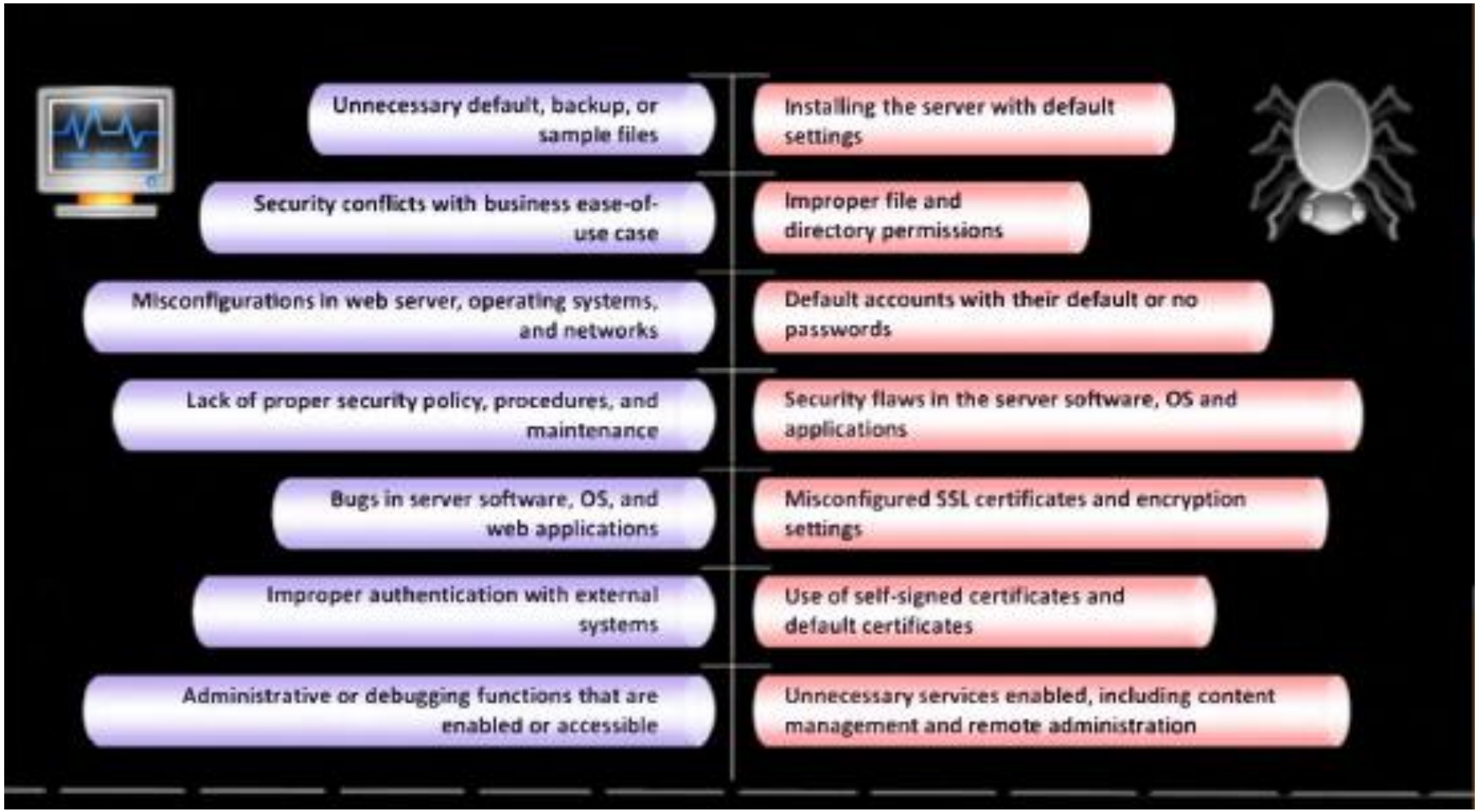
Most common types of webserver attacks:-

- **Local File Inclusion.** This relatively uncommon attack technique involves forcing the web application to execute a file located elsewhere on the system.
- **Distributed Denial of Service (DDoS) attacks.** Such destructive events happen when an attacker bombards the server with requests. In many cases, hackers use a network of compromised computers or bots to mount this offensive. Such actions paralyze your server and prevent legitimate visitors from gaining access to your services.

Web Application Risks – from Open Web Application Security Project (OWASP)



Why webserver compromised



Impact of webserver attack

Summary

- Threat is a possible danger that might exploit a vulnerability to breach security. Meanwhile, the attack is the action to perform the threat that has been identified.
- There are several attack types including malware, social engineering, and network-specific threats and attack types.
- Each attack has a specific aim, objective and motivations.

References

Ethical hacking

https://www.eccouncil.org/malaysia/

CISAM Module

Rocheston Cyberclass