

Cyber Security (SO692)

LEARNING OUTCOME-01

Learners will be able to analyse investment scams and frauds on the internet and configure web browser security settings.

Key Elements

- a) Discuss various types of scams and frauds on the internet.
- b) *Create a plan to protect computer networks from fraudulent activities and data theft on the internet.*
- c) Configure privacy settings for web browsers.
- d) *State legislation relevant to cyber-crimes.*

LEARNING OUTCOME-02

Learners will be able to illustrate an attack, denial of service attack, malware and spyware.

Key Elements

- a) Select the common tools to identify denial of service attack.
- b) *Discuss different types of virus, malware and spyware.*
- c) Build a network secured from malware and spyware.
- d) Select software tools to secure network from malware and spyware.

LEARNING OUTCOME-03

Learners will be able to gain advanced knowledge of methodologies used by hackers and apply tools and techniques to protect computer networks from hackers.

Key Elements

- a) Select hacking tools to protect networked computers.
- b) *Analyse different cryptography methods that can be used to prevent attacks and protect the network and analyse basic methodologies used by hackers.*
- c) Select appropriate cryptographic methodology to secure the network.

LEARNING OUTCOME - 04

Learners will be able apply computer security technology to build a secure network

Key Elements

- a) Select an appropriate firewall for the computer network.
- b) Test the functions of software scanners.
- c) Identify intrusion detection systems to solve the security issues in computer networks.

LEARNING OUTCOME-05

Learners will be able create security policies for users and administrators of computer networks.

Key Elements

- a) *Discuss the importance of security policies for users.*
- b) Create security policies for networked users.
- c) Analyse and improve existing security policies to meet prevalent industry standards.

LEARNING OUTCOME-06

Learners will be able use vulnerability scanning tools and implement security in networks.

Key Elements

- a) Select vulnerability scanning tools to detect and resolve security problems.
- b) Evaluate security concerns in computer networks.
- c) Detect the hacker's presence and footprint on the network.

Delivery

Timeframe	Total Teaching Days per week	Total Teaching Hours per week	Self-Study Hours per week
9 weeks	4	20	13.5

Assessment Type

Assessments	Assignment 1	50% (Learning Outcomes 1,2,3)
	Assignment 2	50% (Learning Outcomes 4,5,6)

Classroom Rules



Class Schedule



- SO692- Cyber Security
- Classes: 8:30am-2:00pm



Breakdown of Timings



- **First Session : 8:30am - 11:30am**
- **Break Time : 11:30am-12:00pm**
- **Second Session : 12:00pm - 2:00p**

BREAK TIME



Attendance



- Attendance is checked at 8:30 – 11:30am
- Once student comes **between 8:30am-11:30am**, you are marked **LATE**
- If student comes **after 8:50am**, you are marked **ABSENT**

Right Conduct

- Put **mobile in silent mode** and **Don't use in the class room**
- **Respect others**



Right Conduct (cont'd)

- **Put chairs under the table after the class** to make room tidy
- **Put all rubbish into the bin** to make room clean at all times.
- **No eating in the classroom**



Cyber Security (SO692)

What is Cyber Security?

CIA (Confidentiality, Integrity and Availability)

Cybersecurity is the protection of internet-connected systems from cyber attacks including

- hardware,
- software and
- data.

In a computing, **security** comprises **cybersecurity** and physical **security** -- both are used by enterprises to protect against unauthorized access to datacenter and other computerized systems.

Cyber Attacks

Classification of Cyber Crimes:

- Insider/Internal Attack,
- Outsider/External Attack

Reasons for Cyber Crimes:

- Money,
- Revenge,
- Fun,
- Recognition,
- Anonymity,
- Cyber Espionage

Types Of Cyber Attacks

1. Device Compromise
2. Service Disruption
3. Data Exfiltration
4. Bad Data Injection
5. Advanced Persistent Threat (APT)

Types Of Cyber Attacks

- Device Compromise
 - *Goal: To obtain total control of a device.*
 - Requirements:
 - Root credentials
 - Privilege escalation exploit
 - Powers Granted:
 - Arbitrary execution on compromised device
 - Network foothold
 - Ability to carry out other types of cyber attacks!



Types Of Cyber Attacks

- Service Disruption
 - Goal: To prevent a device from performing its duties.
 - Requirements:
 - LOTS of computing power
 - Powers Granted:
 - Consequences of the device failing to do its job
 - Device downtime?
 - Revenue loss?
 - Public attention/shaming?
 - System failure?



Types Of Cyber Attacks

- Data Exfiltration
 - *Goal: To steal sensitive information from a target.*
 - Requirements:
 - Access (legit or otherwise) to device storing data
 - Powers Granted:
 - Arbitrary Data Operations!
 - Reconnaissance
 - IP Theft
 - Expose private information



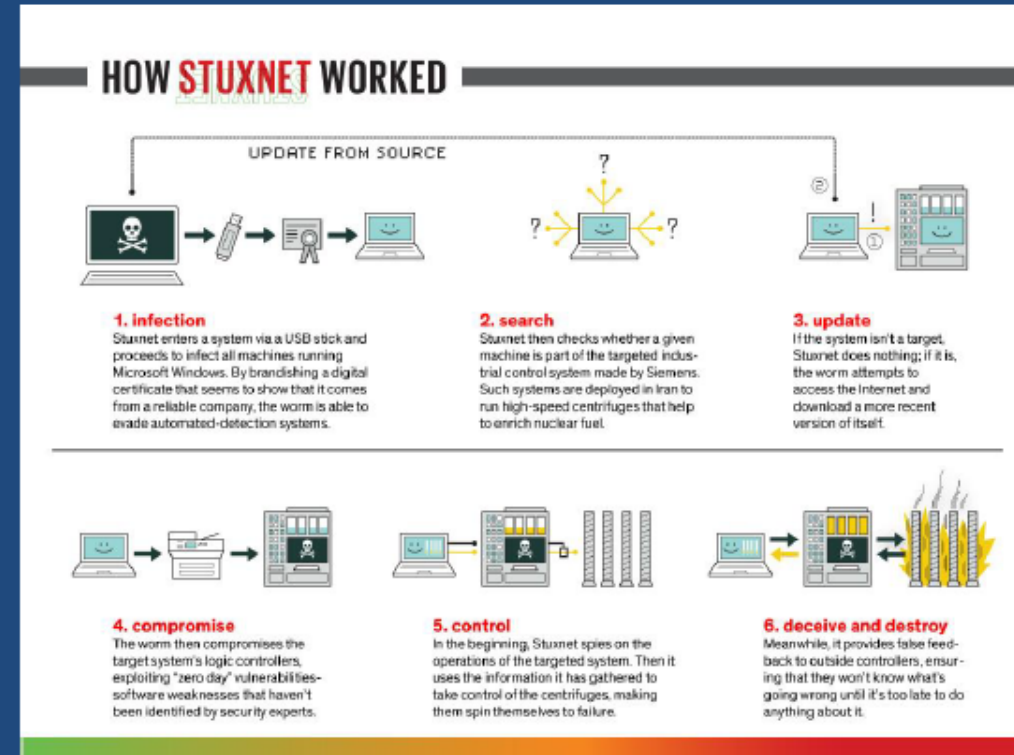
Types Of Cyber Attacks

- Bad Data Injection
 - *Goal: To submit incorrect data to a system without detection.*
 - Requirements:
 - Access (legit or otherwise) to device storing data
 - Powers Granted
 - Determine the state of data-driven services!
 - Real-world consequences, potentially catastrophic



Types Of Cyber Attacks

- Advanced Persistent Threat (APT)
 - *Goal: To gain extended access to a device.*
 - Requirements:
 - Time, patience, resources
 - Extensive target knowledge
 - Powers Granted:
 - Long-term reconnaissance
 - Ability to act on target quickly
 - Complete and invisible control of systems!



Top Cyber Attacks

- ☐ Denial-of-service (DoS)& distributed denial-of-service (DDoS) attacks
- ☐ Man-in-the-middle (MitM) attack
- ☐ Phishing and spear phishing attacks
- ☐ Drive-by attack
- ☐ Password attack
- ☐ SQL injection attack
- ☐ Cross-site scripting (XSS) attack
- ☐ Eavesdropping attack
- ☐ Birthday attack
- ☐ Malware attack

Dos/DDoS

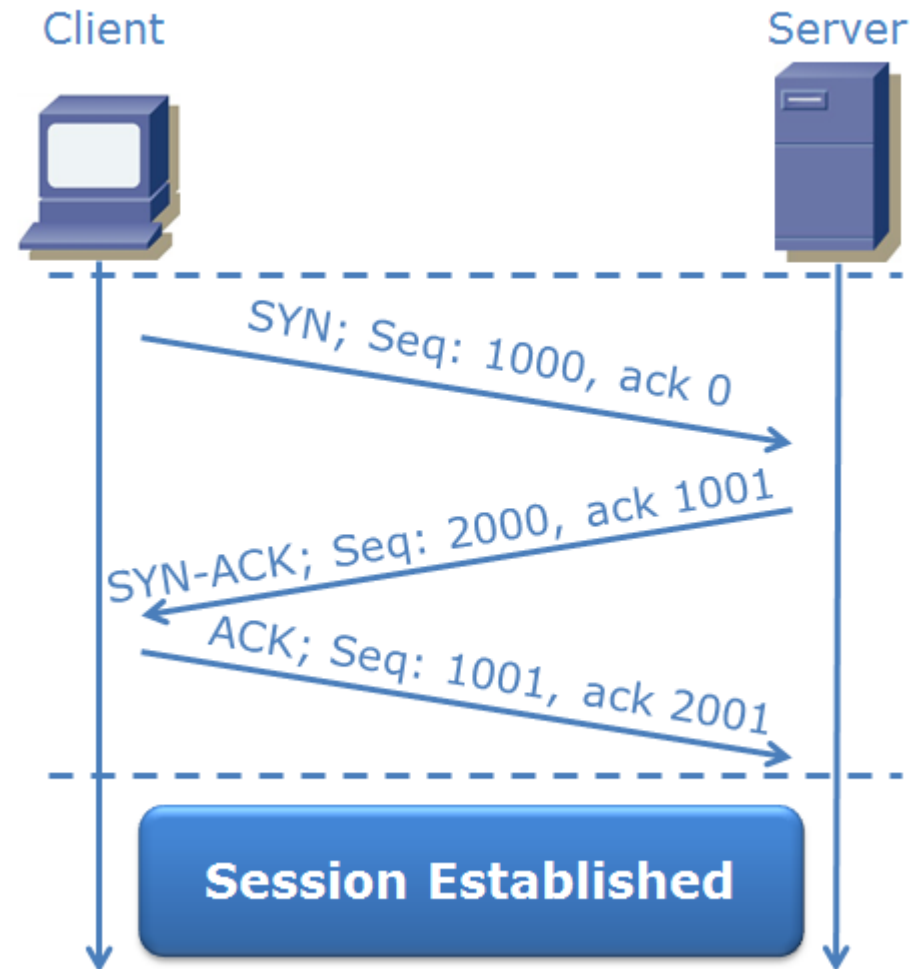
- ❑ A denial-of-service attack overwhelms/Exhausts a system's resources so that it cannot respond to service requests.
- ❑ A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.
- ❑ Another purpose of a DoS attack can be to take a system offline so that a different kind of attack can be launched. One common example is session hijacking.

Dos/DDoS

Most common DoS/DDoS attacks are:

- ☐ TCP SYN flood attack,
- ☐ Teardrop attack,
- ☐ Smurf attack,
- ☐ Ping-of-death attack and
- ☐ Botnets

TCP SYN flood attack,



TCP SYN flood attack,

- ❑ An attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake.
- ❑ This causes the target system to time out while waiting for the response from the attacker's device, which makes the system crash or become unusable when the connection queue fills up

TCP SYN flood attack,

There are a few countermeasures to a TCP SYN flood attack:

- ✓ Place servers behind a firewall configured to stop inbound SYN packets.
- ✓ Increase the size of the connection queue and decrease the timeout on open connections.

Smurf Attack

This attack involves using IP spoofing and the ICMP to saturate a target network with traffic.

- ❑ Attacker (Spoof Victim Address say 10.0.0.10) -----> ICMP echo to Broadcast Address (say 10.255.255.255).
- ❑ This request would go to all IPs in the range, with all the responses going back to 10.0.0.10, overwhelming the network.
- ❑ This process is repeatable, and can be automated to generate huge amounts of network congestion

Smurf Attack

This attack involves using IP spoofing and the ICMP to saturate a target network with traffic.

- ❑ Attacker (Spoof Victim Address say 10.0.0.10) -----> ICMP echo to Broadcast Address (say 10.255.255.255).
- ❑ This request would go to all IPs in the range, with all the responses going back to 10.0.0.10, overwhelming the network.
- ❑ This process is repeatable, and can be automated to generate huge amounts of network congestion

Ping of Death Attack

- ❑ This type of attack uses IP packets to 'ping' a target system with an IP size over the maximum of 65,535 bytes.
- ❑ IP packets of this size are not allowed, so attacker fragments the IP packet.
- ❑ Once the target system reassembles the packet, it can experience buffer overflows and other crashes.

Ping of death attacks can be blocked by using a firewall that will check fragmented IP packets for maximum size.

Botnets Attack

- ❑ In Botnets ,millions of systems are infected with malware under hacker control in order to carry out DDoS attacks.
- ❑ These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities.
- ❑ These DDoS attacks are difficult to trace because botnets are located in differing geographic locations

Botnets Attack

Can be mitigated by:

- ☐ Black hole filtering, which drops undesirable traffic before it enters a protected network.
- ☐ When a DDoS attack is detected, the BGP (Border Gateway Protocol) host should send routing updates to ISP routers so that they route all traffic heading to victim servers to a null0 interface at the next hop.

Man-in-the-Middle (MiTM)

A MitM attack occurs when a hacker inserts itself between the communications of a client and a server.

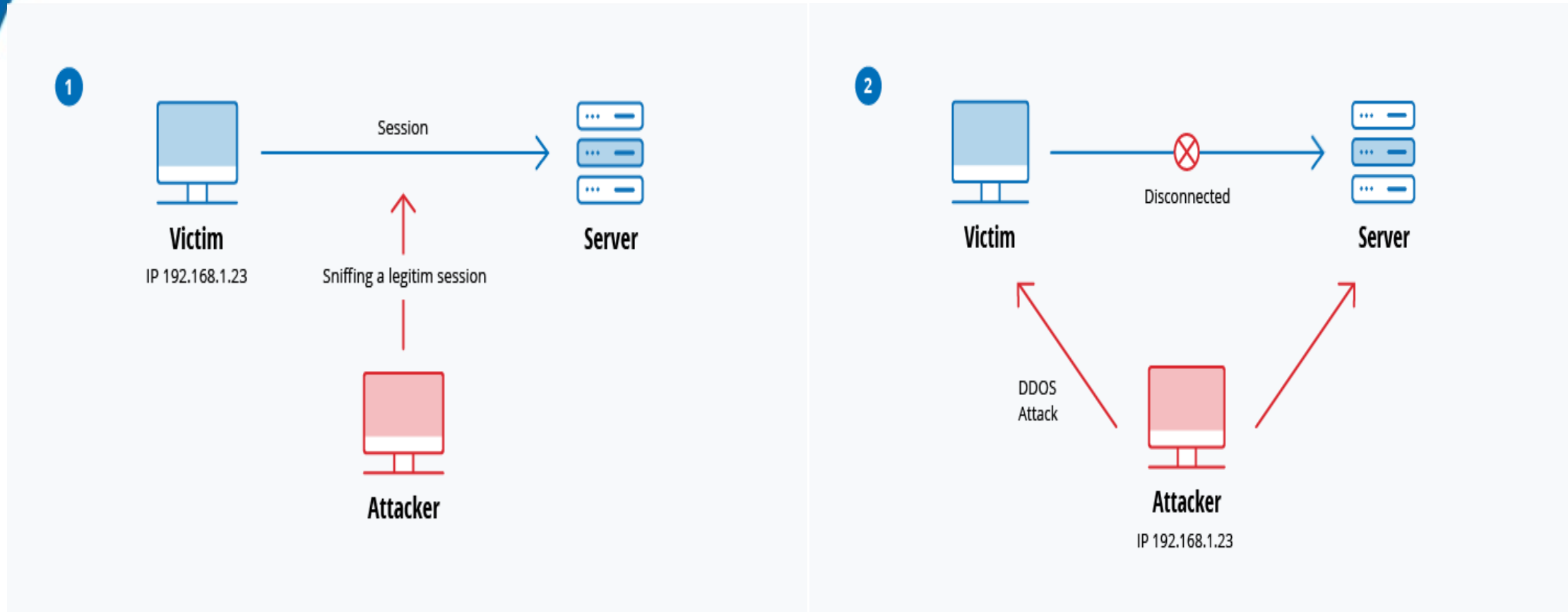
Common MitM attack are:

- ☐ Session Hijacking
- ☐ IP Spoofing
- ☐ Replay

Session Hijacking (MiTM)

- ✓ A client connects to a server.
- ✓ The attacker's computer gains control of the client.
- ✓ The attacker's computer disconnects the client from the server.
- ✓ The attacker's computer replaces the client's IP address with its own IP address and spoofs the client's sequence numbers.
- ✓ The attacker's computer continues dialog with the server and the server believes it is still communicating with the client.

Session Hijacking (MiTM)



Phishing Attack

Phishing – Cybercriminal attempts to steal personal and financial information.

- ✓ Designed to trick you into clicking a link or providing personal or financial information
- ✓ Often in the form of emails and websites
- ✓ May appear to come from legitimate companies, organizations or known individuals
- ✓ Take advantage of natural disasters, epidemics, health scares, political elections or timely events

Phishing Attack

Common Baiting Tactics are:

- ☐ **Notification from a help desk or system administrator**
Asks you to take action to resolve an issue with your account (e.g., email account has reached its storage limit), which often includes clicking on a link and providing requested information.
- ☐ **Advertisement for immediate weight loss, hair growth or fitness**
Allure you to click on a link that will infect your computer or mobile device with malware or viruses.

Phishing Attack

Common Baiting Tactics are:

- ☐ **Attachment labeled “invoice” or “shipping order”**
Contains malware that can infect your computer or mobile device if opened.
- ☐ **Notification from what appears to be a credit card company**
Indicates someone has made an unauthorized transaction on your account. If you click the link to log in to verify the transaction, your username and password are collected by the scammer.
- ☐ **Fake account on a social media site**
Mimics a legitimate person, business or organization. May also appear in the form of an online game, quiz or survey designed to collect information from your account.

Phishing Attack

How to Detect a Phishing Scam

- ✓ Spelling errors (e.g., “pessward”), lack of punctuation or poor grammar
- ✓ Hyperlinked URL differs from the one displayed, or it is hidden
- ✓ Threatening language that calls for immediate action
- ✓ Requests for personal information
- ✓ Announcement indicating you won a prize or lottery
- ✓ Requests for donations

Phishing Attack - Detect



NDSU IT-HELPDESK <ndsu-it-helpdask@gmail.com>
URGENT MESSAGE

Inbox

Attention,

Your password expires in 2 weeks. Reset your Password below via the ACCOUNT
MANAGEMENT PAGE>

Click on CHANGE-PASSWORD <http://publicidadefectiva.net/owa/update.html>

If Password is not changed in the next 2 hours your next log-in access will be denied.

If you find any difficulties to changind your password please contact the ITS-helpdesk.

Regards,
ITS Helpdesk.

Phishing Attack - Detect



NDSU IT-HELPDESK <ndsu-it-helpdesk@gmail.com>

URGENT MESSAGE



Is the name of the staff mailing list correct?

Inbox

Attention,

Your password expires in 1 hour
MANAGEMENT PAGE>



Use the "hover" technique.

Does the displayed URL match the actual URL?

Click on CHANGE-PASSWORD <http://publicidadefectiva.net/owa/update.html>

If Password is not changed in the next 2 hours your next log-in access will be denied.

If you find any difficulties to changing your password please contact the ITS-helpdesk.

Regards,
ITS Helpdesk.

Examine the spelling, grammar and punctuation.

Phishing Attack - Detect

ndsu.edu

HOME WHERE TO BUY

WEBMASTER ADMINISTRATOR

User name

Email Address

Pessward

Confirm Pessward

Submit

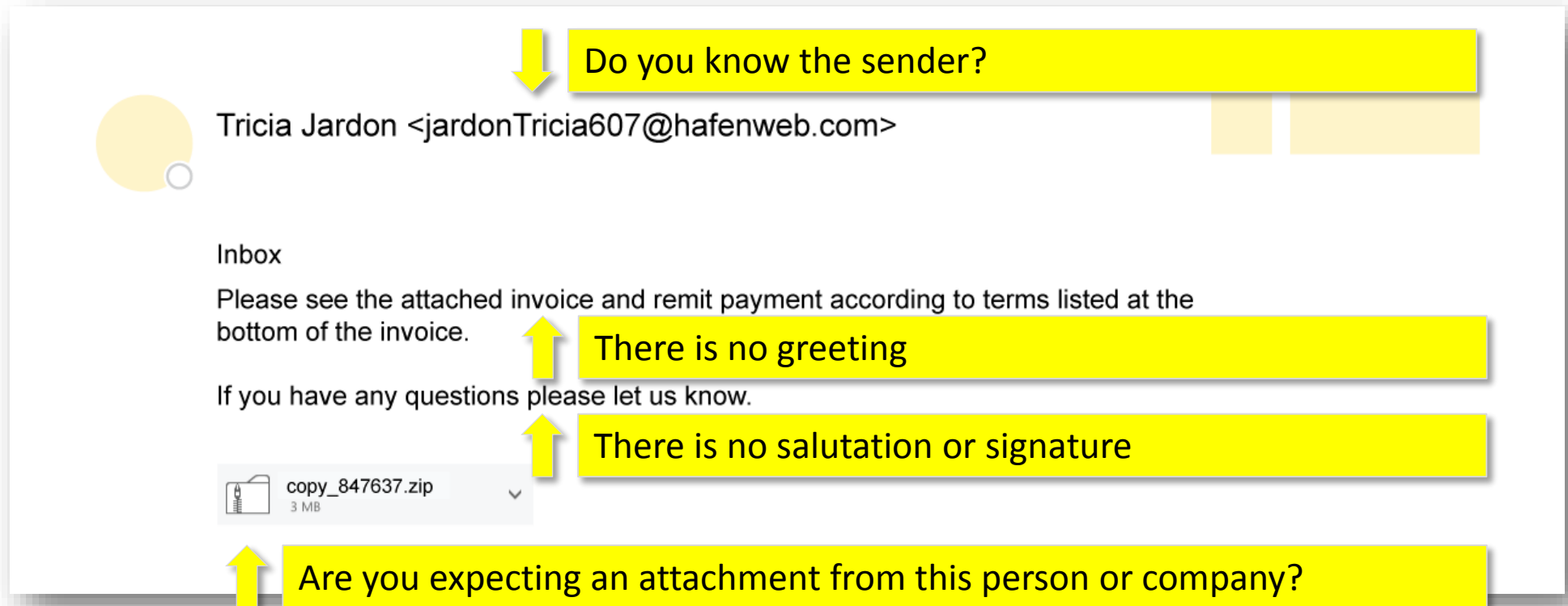
Examine the login page – is the logo familiar?

Look at the subtitles on the logo, is anything unusual?

Who is requesting this information?
Is it someone who would normally request it?

Check for spelling errors

Phishing Attack - Detect



The screenshot shows an email from Tricia Jardon with a subject line 'Inbox'. The body text asks for payment and includes a zip file attachment. Four yellow callout boxes with arrows point to specific elements: 'Do you know the sender?' points to the sender's name and email; 'There is no greeting' points to the start of the body text; 'There is no salutation or signature' points to the end of the body text; and 'Are you expecting an attachment from this person or company?' points to the zip file attachment.

↓ Do you know the sender?

Tricia Jardon <jardonTricia607@hafenweb.com>

Inbox

Please see the attached invoice and remit payment according to terms listed at the bottom of the invoice.

↑ There is no greeting

If you have any questions please let us know.

↑ There is no salutation or signature

copy_847637.zip
3 MB

↑ Are you expecting an attachment from this person or company?

Drive-by Attack

Drive-by download attacks are a common method of spreading malware. In Drive-by Attack

- ☐ Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages.
- ☐ This script might install malware directly onto the computer of someone who visits the site,
- ☐ It might re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window.

Password Attack

Passwords are the most commonly used mechanism to authenticate users to an information system.

- ❑ **Brute-force** - guessing by using a random approach
- ❑ **Dictionary attack** - a dictionary of common passwords

SQL Injection Attack

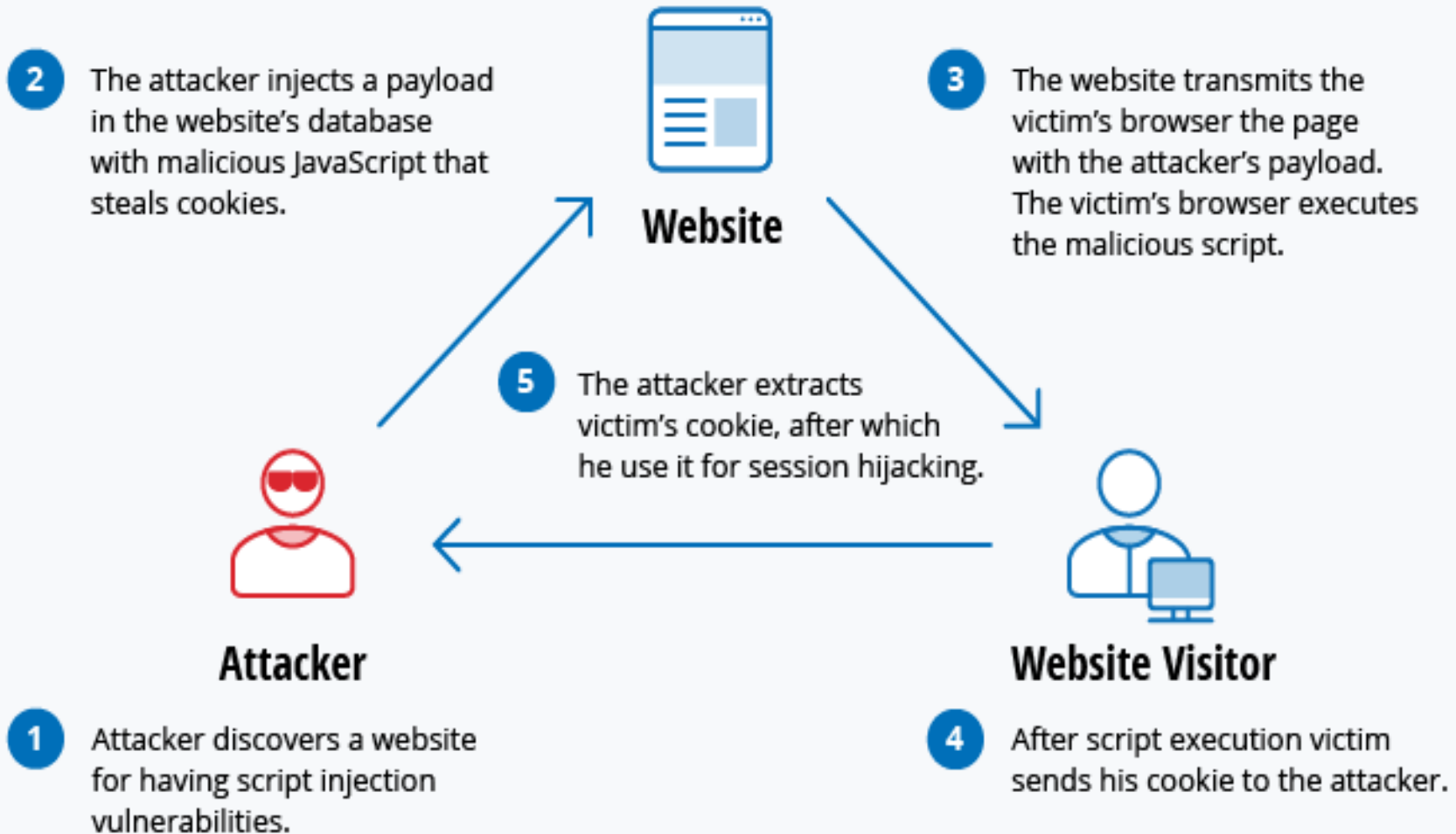
SQL injection has become a common issue with database-driven websites.

- ❑ A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database.

Cross-Site Scripting (XSS) Attack

- ❑ XSS can be taken advantage of within VBScript, ActiveX and Flash, the most widely abused is JavaScript — primarily because JavaScript is supported widely on the web.
- ❑ XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application.
- ❑ Attacker injects a payload with malicious JavaScript into a website's database.
- ❑ When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script.

Cross-Site Scripting (XSS) Attack



Cross-Site Scripting (XSS) Attack

The most dangerous consequences occur when XSS is used to exploit additional vulnerabilities. Such as

- ☐ Log key strokes,
- ☐ Capture screenshots,
- ☐ Discover and collect network information, and
- ☐ Remotely access and control the victim's machine.

Eavesdropping Attack

Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain

- ✓ passwords,
- ✓ credit card numbers and
- ✓ other confidential information

that a user might be sending over the network.

Birthday Attack

- ❑ Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature.
- ❑ A message processed by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message.
- ❑ If an attacker calculates same MD for this message as the user has, he can safely replace the user's message with this.
- ❑ The receiver will not be able to detect the replacement even if he compares MDs.

Malware Attack

Malicious software can be described as unwanted software that is installed in your system without your consent.

Some common malwares are

- ☐ Macro viruses
- ☐ File infectors
- ☐ Trojans
- ☐ Logic bombs
- ☐ Worms
- ☐ Ransomware
- ☐ Adware
- ☐ Spyware

The top-left corner of the slide features abstract geometric shapes in two shades of blue. A darker blue triangle points towards the center, while a lighter blue trapezoidal shape is positioned above it.

Thank You