PHISHING AWARENESS TRAINING

YAMAN DAHIYA

CODE ALPHA CYBERSECURITY INTERNSHIP – TASK 2

WHAT IS PHISHING?

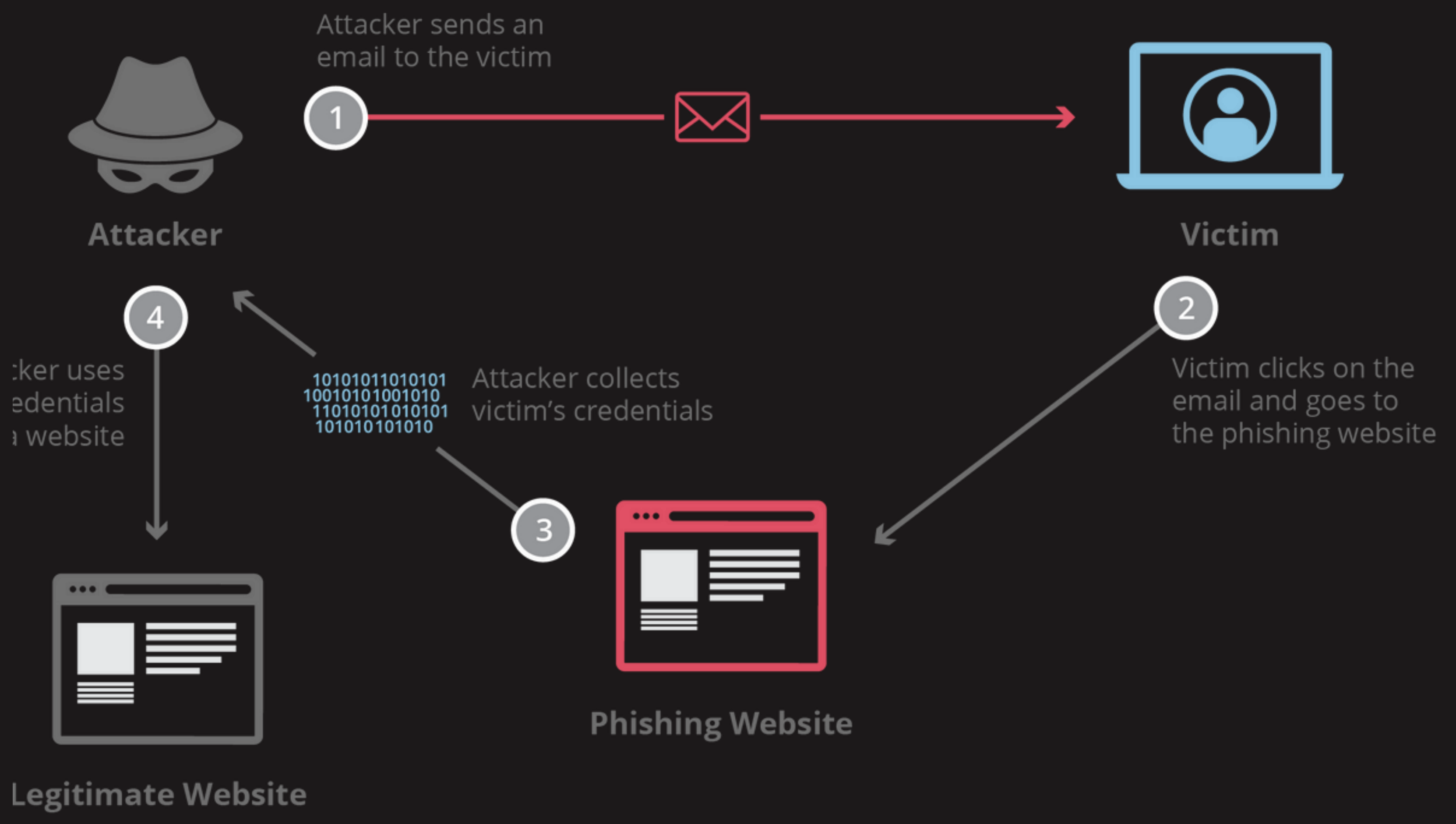
Phishing attempts involve deceiving individuals through emails, text messages, phone calls, or even social media to reveal sensitive data.

This data can include passwords, credit card numbers, bank account details, and personal information.

Attackers often masquerade as legitimate entities like banks, credit card companies, or popular online services.

HOW PHISHING WORKS?

- Email Delivery: Attackers send emails disguised as legitimate sources, often using familiar logos and language.
- Clicking the Bait: The email contains a link or attachment that, when clicked, triggers the next step.
- Fake Website: The link leads to a fraudulent website designed to mimic the real website, duplicating its look and feel.
- Information Sharing: Unaware of the deception, the victim enters their login credentials, personal details, or financial information on the fake site.
- Data Theft: The attacker successfully captures the entered information for malicious purposes.


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
:ker uses
edentials
ı website
10101011010101
10010101001010
11010101010101
101010101010
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

TYPES OF PHISHING

Phishing attacks come in different forms

1

SPEAR PHISHING

Targets a specific individual or organization with personalized emails based on their information.

2

VISHING

Uses phone calls to impersonate legitimate companies, tricking victims into revealing personal details.

3

SMISHING

Leverages text messages with urgent tones and malicious links to deceive victims.

4

WHALING

Aims for high-profile individuals or organizations like CEOs or executives, often using a combination of tactics.

RED FLAGS

Red flags in phishing attempts are warning signs or indicators that help individuals identify potential scams. Some common read flags in phishing include:

1. Urgent or threatening language
2. Suspicious sender information
3. Requests for personal information
4. Misspellings or grammatical errors
5. Suspicious links or attachments
6. Generic greetings
7. Too good to be true

01 URGENT OR THREATENING LANGUAGE

Phishing attempts often create a sense of urgency or use threatening language to prompt immediate action. Phases like "urgent action required," "account suspended," or "your account will be deleted" may indicate a phishing attempt.

02 SUSPICIOUS SENDER INFORMATION

Check the sender's email address or social media profile. Phishing emails or messages often use generic or suspicious email addresses that do not match the legitimate entity they claim to represent.

03 REQUESTS FOR PERSONAL INFORMATION

Legitimate organizations do not request personal information, such as usernames, passwords, or credit card numbers, via email, social media, or other online means. Be cautious of any request for personal information.

04 MISSPELLINGS OR GRAMMATICAL ERRORS

Phishing emails or messages may contain misspellings, grammatical errors, or awkward phrasing. Legitimate organizations usually have professional communications and do not contain obvious errors.

05 SUSPICIOUS LINKS OR ATTACHMENTS

Be cautious of links or attachments in emails or messages from unknown or untrusted sources. Hover over links to check their actual destinations, and do not click on suspicious links or download attachments that you were not expecting.

06 GENERIC GREETINGS

Phishing emails may use generic greetings like "Dear Customer" instead of addressing you by your name. Legitimate organizations often personalize their communications with your name or other relevant information.

07 TOO GOOD TO BE TRUE

Phishing attempts may lure individuals with enticing offers, such as winning a prize or getting a huge discount. If an offer seems too good to be true, it may be a phishing attempt.

SOCIAL ENGINEERING TACTICS

Social engineering relies on manipulation and deception to trick individuals into revealing personal information or taking specific actions.

- Pretexting: Attackers create a fictitious scenario to gain trust and extract information.
- Quid pro quo: The attacker offers something in return for information or assistance, often exploiting a sense of obligation or urgency.
- Tailgating: Gaining unauthorized access by following closely behind someone with authorized access.
- Baiting: The attacker presents tempting information or opportunities to lure victims into compromising their security.

HOW TO PROTECT YOURSELF FROM PHISHING?

- Be cautious with emails: Don't click on links or open attachments from unknown senders, even if they look legitimate.
- Verify information: If an email claims to be from a legitimate source, contact them directly using a verified phone number or website to confirm its authenticity.
- Beware of urgency: Don't rush into any action based on urgent requests in emails. Take your time, verify information, and consider the legitimacy of the sender's message.
- Use strong passwords: Use complex and unique passwords for all your online accounts. Consider using a password manager to help you create and manage strong passwords.
- Enable multi-factor authentication (MFA): Activate MFA whenever available. This adds an extra layer of security by requiring a second verification step beyond your password.

WHAT TO DO IF YOU FALL VICTIM TO PHISHING?

- Change your passwords: Immediately change your passwords for all online accounts that you think might have been compromised.
- Contact your financial institutions: If you suspect you've shared financial information, immediately contact your bank or credit card company to report the incident and take necessary steps to protect your accounts.
- Report the phishing attempt: Help protect others. Report the phishing attempt to the appropriate authorities, such as your email provider or the Anti-Phishing Working Group (APWG).
- Seek professional help: If you suspect you have downloaded malware or compromised your device, consider seeking assistance from a computer security professional to help you clean your system and ensure its security.

CONCLUSION

Phishing attacks are a constant threat, but by understanding their tactics and implementing these simple safety measures, you can significantly reduce your risk.

- Stay informed: Keep yourself updated on the latest phishing scams and tactics.
- Be cautious: Don't click on suspicious links or open unexpected attachments.
- Verify information: Always double-check information before acting on any request, no matter how urgent it seems.
- Report suspicious activity: Help protect others by reporting phishing attempts to the appropriate authorities.

THINK BEFORE YOU CLICK!

PROTECT YOURSELF FROM PHISHING

Don't share your personal information online!