PHISHING ATTACK

ELAJMI YOUSSEF

INTRODUCTION

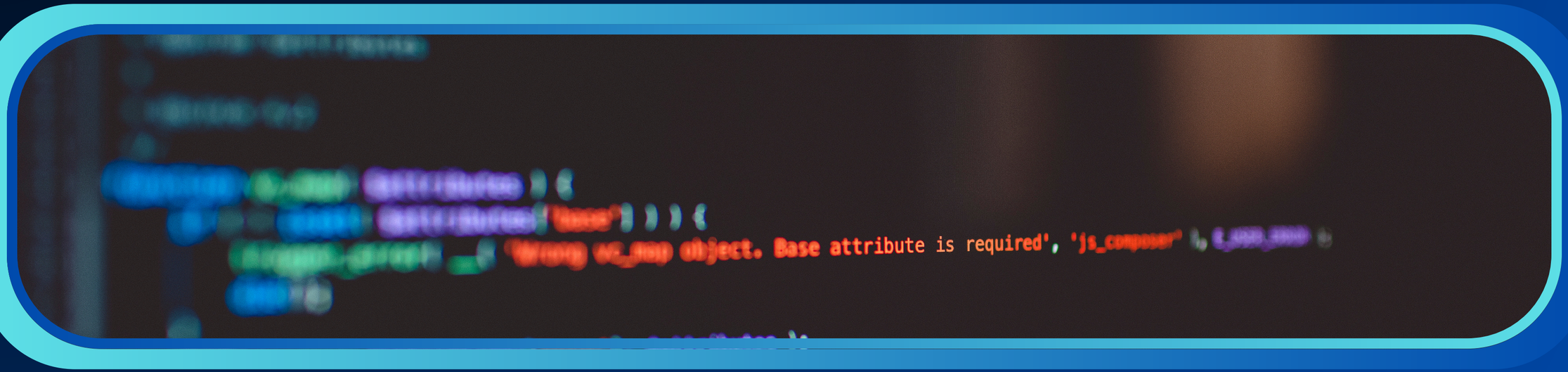
PHISHING

Phishing is a type of cyberattack where malicious actors deceive individuals into revealing sensitive information or taking actions that compromise their security.

WHY DO HACKERS USE PHISHING?

They aim to:

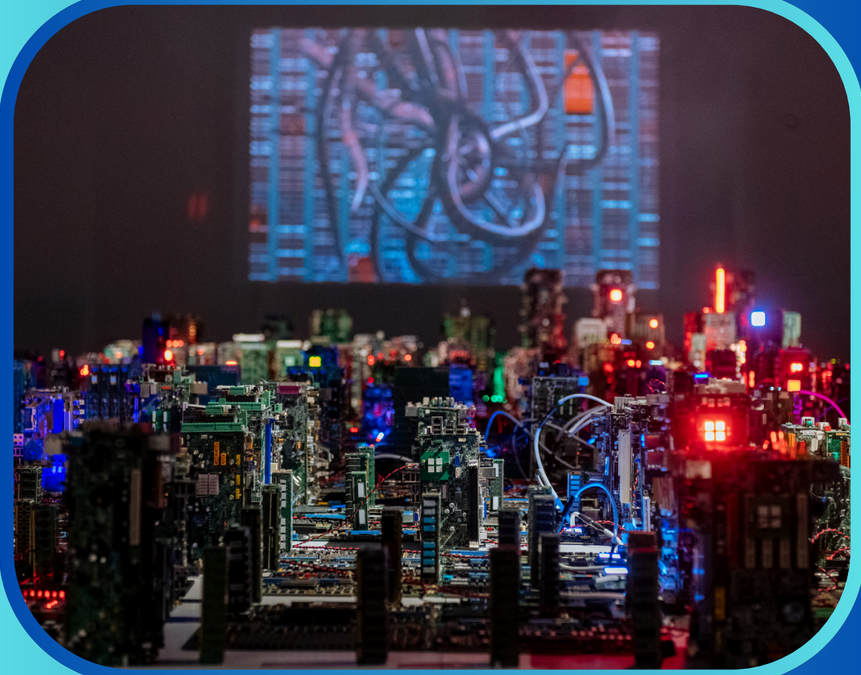
- Steal login credentials
- Get financial access
- Infect your device with malware
- Gain control of your accounts or systems



HOW TO SPOT A PHISHING ATTEMPT

Be careful with:

- Generic greetings (“Dear user”)
- Strange or urgent messages (“Click now or lose access”)
- Misspelled words or weird formatting
- Links that don’t match the real website (hover to check)
- Unexpected attachments



TRICKS USED BY ATTACKERS

Phishers play with your emotions:

- **Fear**: “Your account is at risk!”
- **Curiosity**: “You won a prize!”
- **Authority**: “IT support needs access.”
- **Urgency:** “Act immediately or lose everything!”

They know how to manipulate trust — so stay alert!

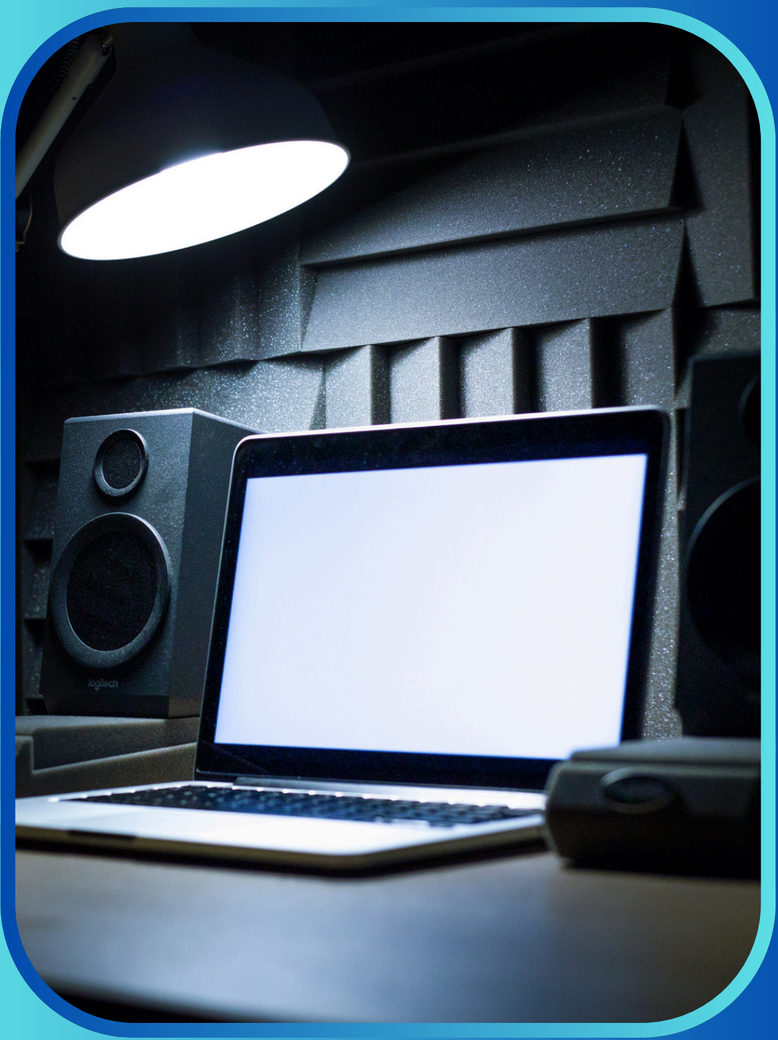
HOW TO STAY SAFE

Stay Safe

- Don’t click on unknown links
- Double-check the sender’s email
- Use two-factor authentication (2FA)
- Report suspicious emails
- Never share passwords

REAL PHISHING EXAMPLES

- Fake Amazon emails with invoice links
- Imitation PayPal or bank websites
- SMS messages asking you to “confirm delivery”
- Emails from fake “support teams” with urgent requests



QUIZ AND ANSWERS

QUESTION 1

You receive an email from security-update@microsoft-support.co asking you to download a file to “fix a critical issue”

Is this a phishing attempt?

(Yes / No)

QUESTION 2

You visit a website that looks like your bank’s site, but the URL starts with http:// instead of https://.

Is this safe?

(Yes / No)

CORRECT ANSWER – QUESTION 1

You receive an email from security-update@microsoft-support.co asking you to download a file to “fix a critical issue”

Is this a phishing attempt?

✅ Yes :

- The email address is suspicious (not the official Microsoft domain).
- Unsolicited attachments from unknown sources are common phishing methods.
- Unsolicited attachments from unknown sources are common phishing methods.

CORRECT ANSWER – QUESTION 2

You visit a website that looks like your bank’s site, but the URL starts with http:// instead of https://.

Is this safe?

❌ No, it’s not safe

- A missing “https” means the site is not encrypted.
- Legitimate banking websites always use secure connections.
- This could be a fake or compromised website.

CONCLUSION

Phishing attacks are everywhere — but with the right knowledge, you can recognize and stop them.

🔐 **Stay careful. Stay secure. Stay smart.**

THANK YOU

ELAJMI YOUSSEF