MASUMI JAIN

UNDERSTANDING PHISHING: HOW TO RECOGNIZE AND AVOID CYBER THREATS

A Guide to Protecting Yourself Online

CodeAlpha Cybersecurity Intern

WHAT IS PHISHING ?

Phishing is a type of cyber attack where attackers trick individuals into revealing sensitive information (e.g., passwords, credit card numbers) by pretending to be a trustworthy entity. Phishing attacks often use email, but they can also occur via text messages (smishing) or phone calls (vishing).

1.How Phishing Works: Attackers send fake emails, messages, or create fake websites that look legitimate. They lure victims into clicking malicious links, downloading harmful attachments, or entering sensitive information.

2.Common Goals of Phishing: Stealing login credentials (e.g., usernames and passwords). Gaining access to bank accounts or credit card information. Installing malware on the victim's device.

3.Why It's Dangerous: Phishing attacks are highly effective because they exploit human psychology (e.g., fear, urgency, or curiosity). They can lead to identity theft, financial loss, or data breaches

02 Common Types of Phishing Attacks

1

Email Phishing

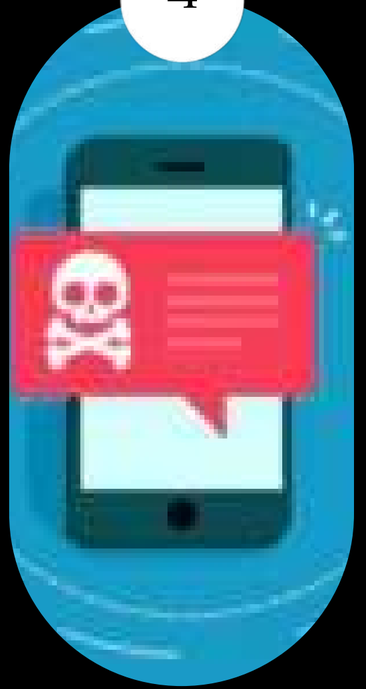
2

Spear Phishing

3

Whaling

4



Smishing (SMS Phishing)

HOW PHISHING WORKS

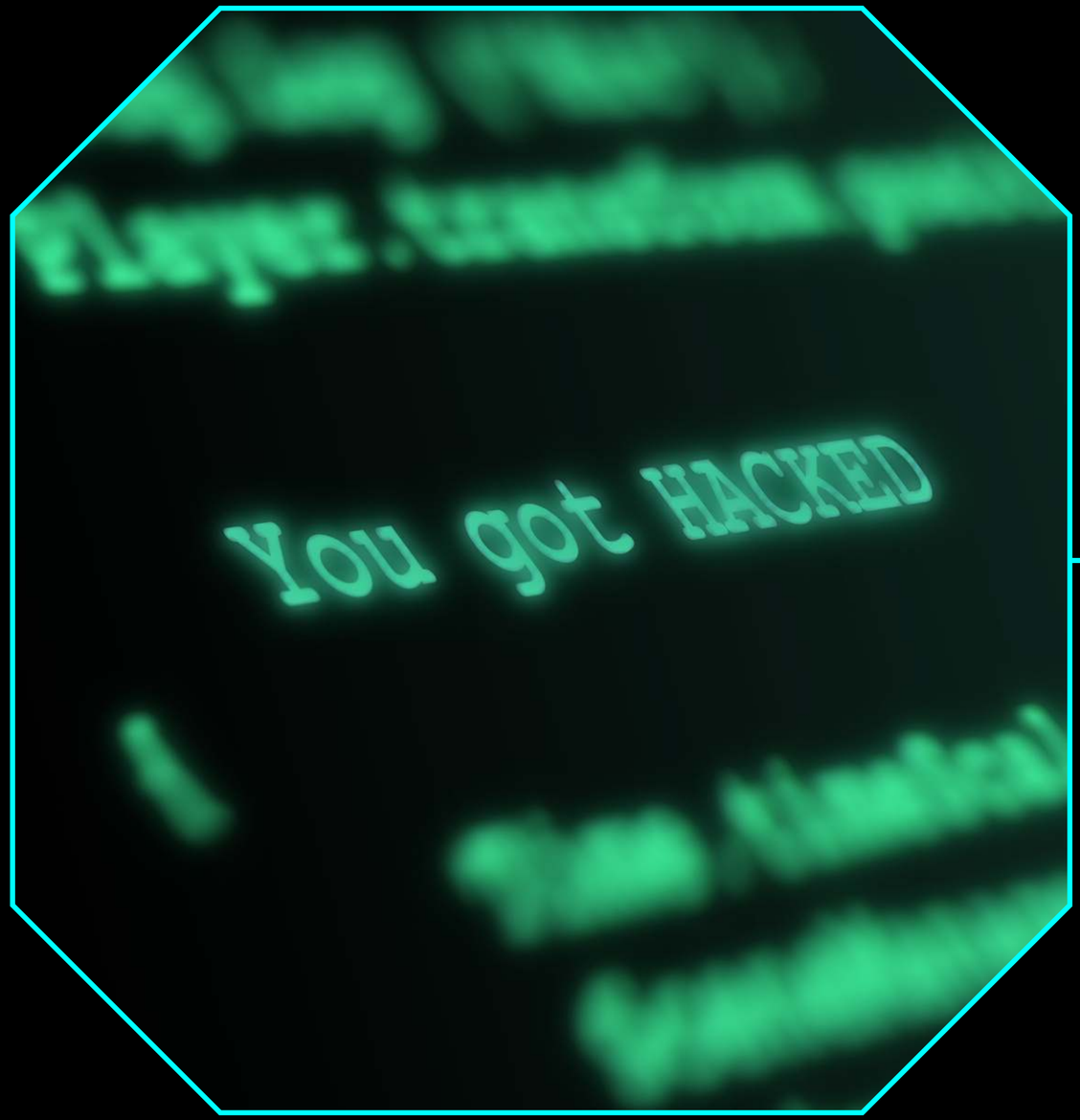
Phishing uses deceptive messages, like emails or texts, pretending to be from trusted entities. These messages create urgency or fear, prompting you to click malicious links or open attachments. These actions lead to fake websites or malware downloads, ultimately stealing your sensitive information, such as passwords or financial details.

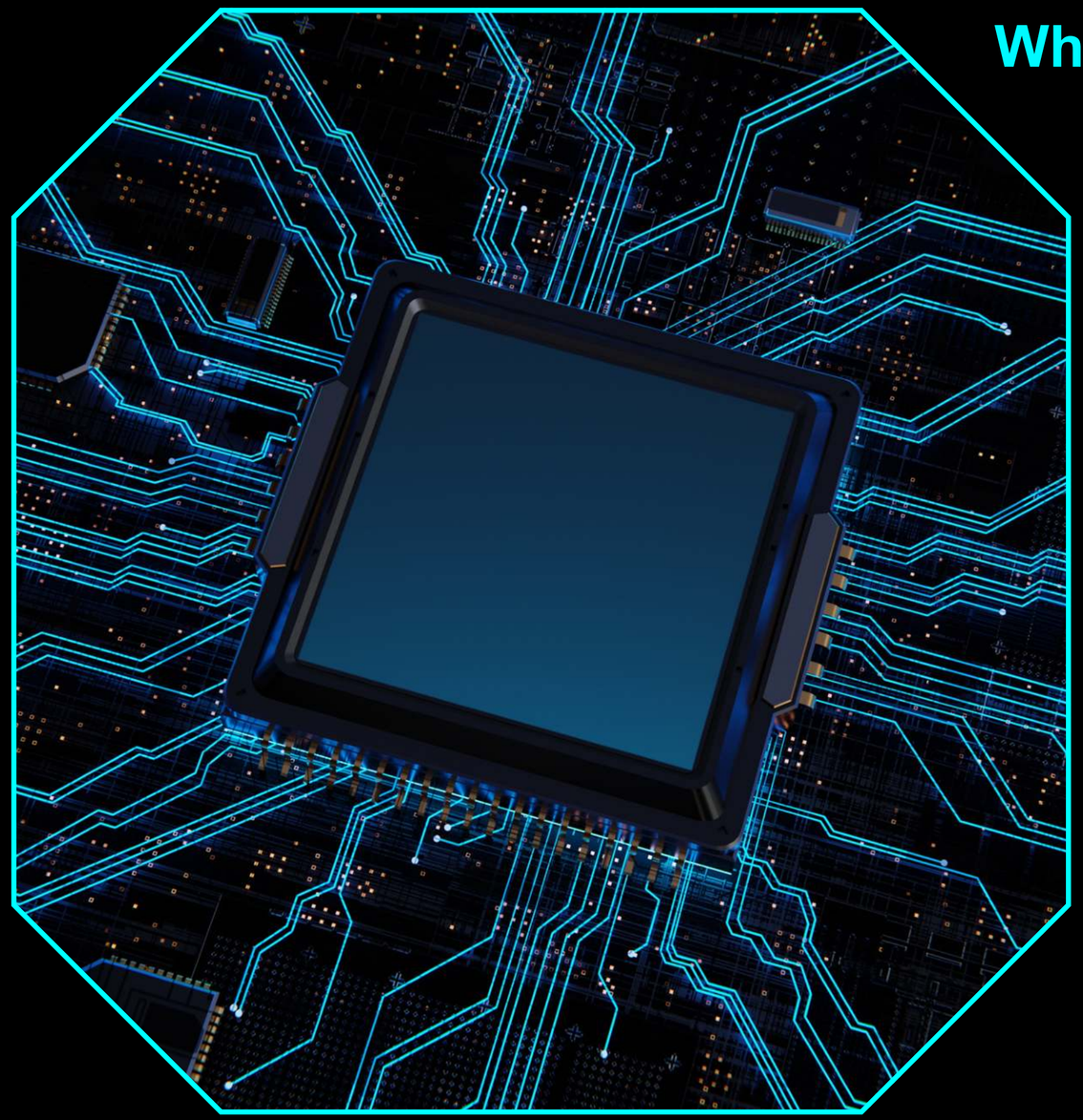
HOW TO IDENTIFY PHISHING EMAILS

- Weird sender address.
- Generic greetings.
- Urgent/scary tone.
- Suspicious links/attachments.
- Poor grammar/spelling.

HOW TO PROTECT YOURSELF FROM PHISHING

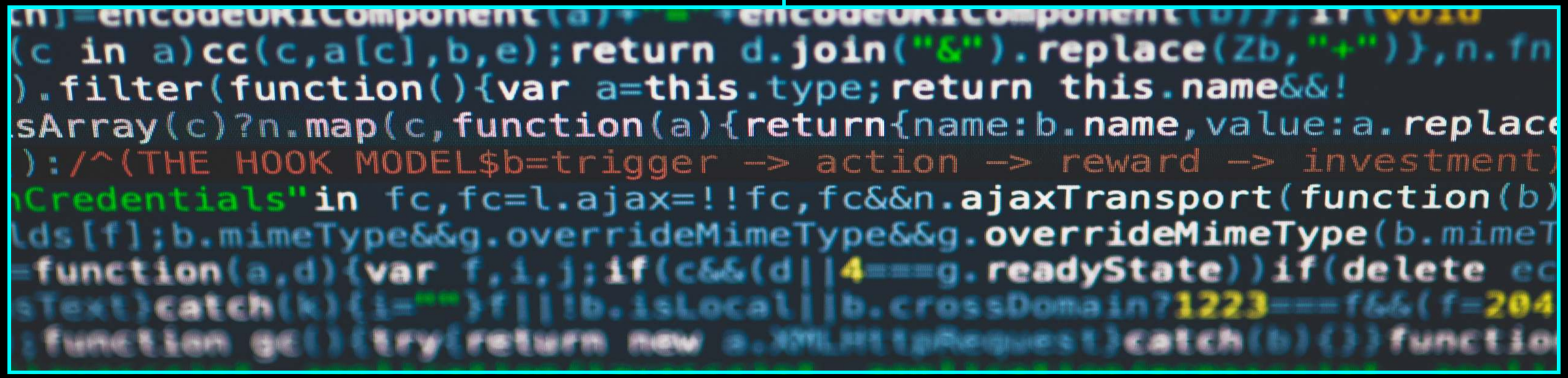
- Be wary: Carefully check sender addresses and links.
- Don't share: Never give personal info via email.
- Verify: Contact senders directly through known channels.
- Strengthen: Use strong passwords and 2FA.
- Update: Keep software current.





What to Do If You Fall for a Phishing Attack?

- If you fall for a phishing attack:
- Immediately change passwords: For all affected accounts.
- Monitor your accounts: Watch for any unauthorized activity.
- Report the incident: To relevant authorities and the affected companies.
- Consider credit monitoring: To detect potential identity theft.
- Disconnect from the internet: If you suspect malware, disconnect to prevent further damage.
- Scan your devices: Use reputable antivirus/anti-malware software to check for and remove any threats.
- Alert your contacts: Inform people who might have received phishing messages from your compromised accounts.



CONCLUSION

Phishing poses a serious threat, but proactive vigilance is key to defense. By consistently verifying information and prioritizing online security, you significantly reduce your risk. Should you encounter a suspicious attempt, promptly report it to authorities. Staying informed about evolving tactics and maintaining safe online practices are essential for minimizing the impact of phishing and safeguarding your digital well-being.

MASUMI JAIN

THANKYOU

CodeAlpha Cybersecurity Intern