Understanding Phishing: How to Recognize and Avoid Cyber Threats

A Guide to Protecting Yourself Online

CodeAlpha Cybersecurity Intern

Othmane Bougnar

1Realised on February 15th 2025

Summary

01 What is Phishing?

02 Common Types of Phishing Attacks

03 How Phishing Works

04 How to Identify Phishing Emails

05 How to Protect Yourself from Phishing

06 What to Do If You Fall for a Phishing Attack

07 Conclusion

01 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)

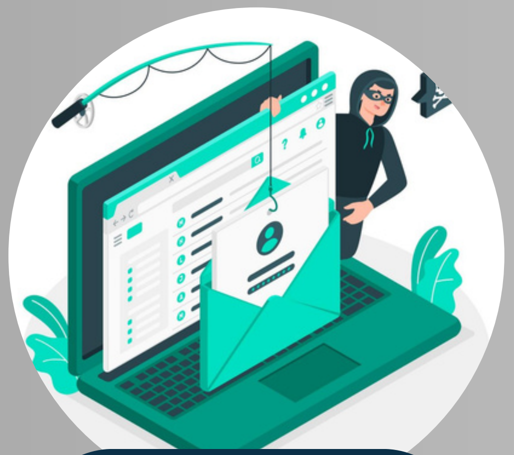
03 How Phishing Works

The Bait

- Attackers send fake emails, messages, or create fake websites that look legitimate.
- Example: A fake email from "PayPal" saying, "Your account has been compromised."

The Hook

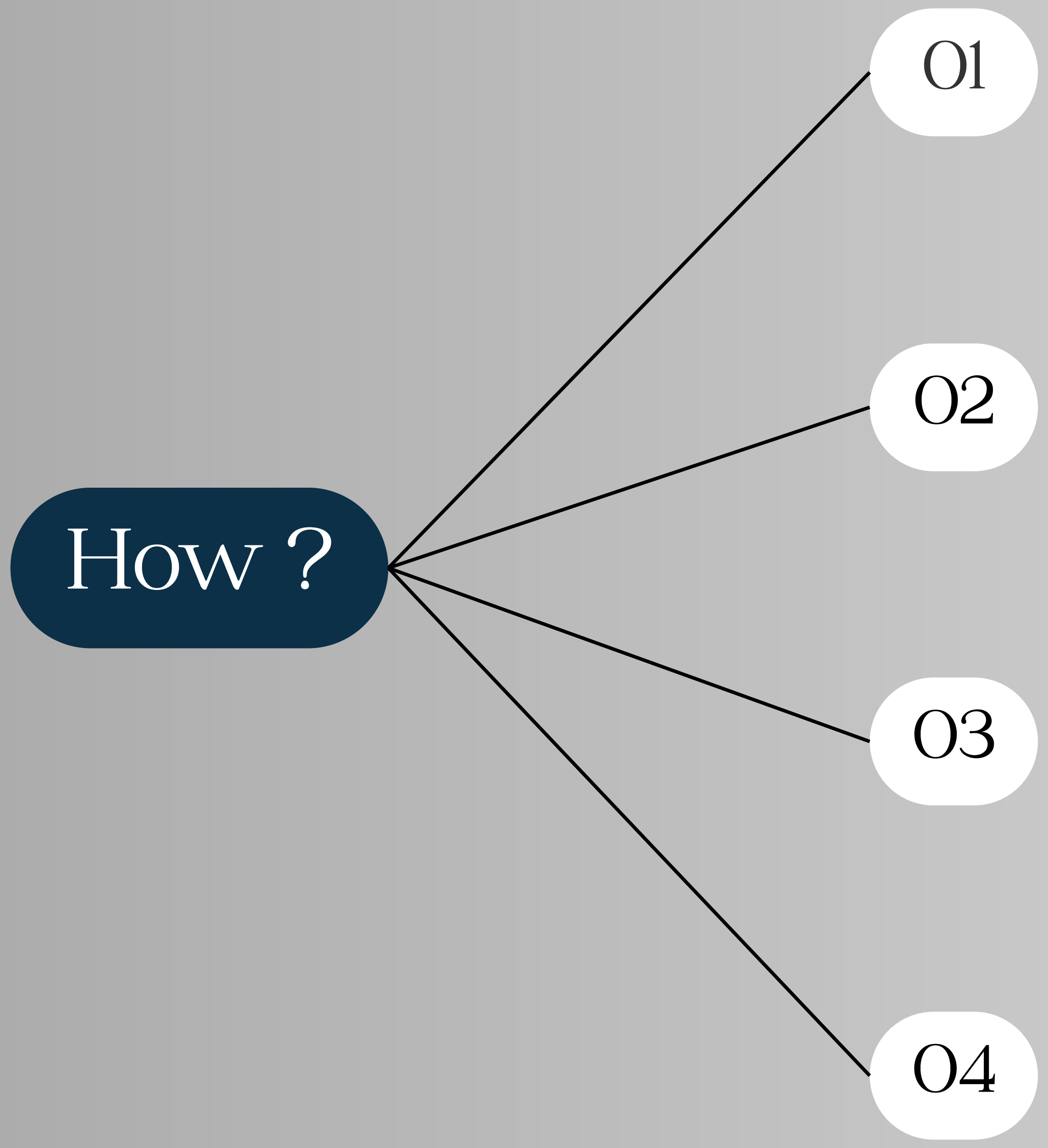
- The message contains a link to a fake website or asks for sensitive information.
- Example: "Click here to secure your account."



The Catch

- Victims enter their information (e.g., passwords, credit card numbers) on the fake website.
- Attackers steal this information and use it for malicious purposes.

04 How to Identify Phishing Emails


How ?

01 Check the Sender's Email Address:

- Look for misspellings or unusual domains (e.g., "support@paypa1.com" instead of "support@paypal.com").

02 Look for Generic Greetings:

- Phishing emails often use generic greetings like "Dear Customer" instead of your name.

03 Watch for Urgent or Threatening Language:

- Phishing emails often create a sense of urgency (e.g., "Your account will be locked!").

04 Hover Over Links Before Clicking:

- Hover over links to see the actual URL. If it looks suspicious, don't click it.

05 How to Protect Yourself from Phishing

01

Use strong, unique passwords – Consider a password manager to store them securely.

02

Look for HTTPS – Secure sites start with "https://" and often show a padlock icon

03

Avoid entering personal info on pop-ups – Legitimate sites don’t ask for sensitive info via pop-ups.

04

Verify with the company – Contact the company directly if you get an unexpected request.

06 What to Do If You Fall for a Phishing Attack

01

- Change Your Passwords Immediately
- If you entered your credentials, change your password for that account and any others using the same password.

02

- Contact the Affected Company or Service
- Notify the bank, email provider, or any service that was impersonated.
- They may help secure your account and prevent further fraud.

03

- Scan for Malware
- If you downloaded an attachment or clicked a malicious link, run a full antivirus scan on your device.

04

- Educate Yourself to Prevent Future Attacks
- Learn to spot phishing attempts and be extra cautious with links and emails.

07 Conclusion

Phishing attacks are a serious cybersecurity threat that can lead to financial loss, identity theft, and compromised personal data. Cybercriminals use deceptive emails, messages, and fake websites to trick individuals into revealing sensitive information. However, by staying vigilant, using strong security measures, and being cautious with unsolicited messages, you can significantly reduce the risk of falling victim to phishing. If you ever suspect a phishing attempt, avoid clicking links, verify the sender's identity, and report the incident immediately. Awareness and proactive security habits are the best defense against these evolving threats. Stay informed, stay cautious, and protect your digital identity.

THANK YOU !