CODE ALPHA

PHISHING AWARENESS TRAINING

Caution: A Single Click Can Lead to Serious Threats!

Task - 3
Keshav Joshi
26/08/2024

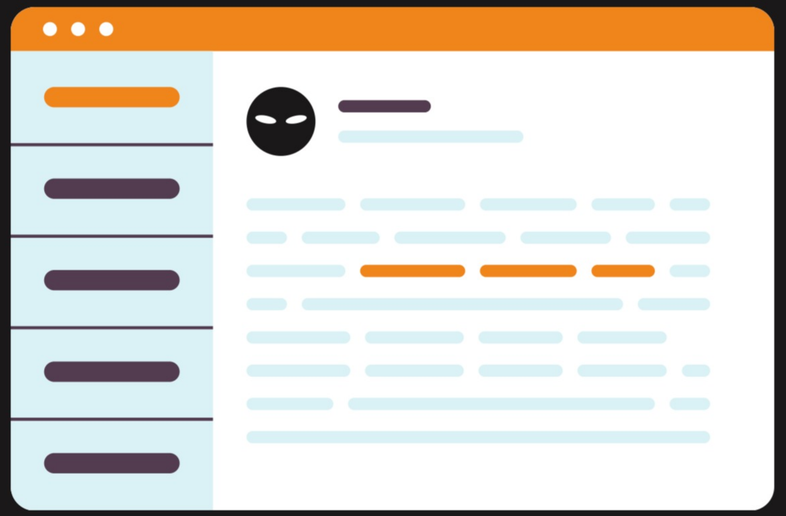
OBJECTIVES

By the end of this lesson, you will be able to:

1. Define phishing and identify common methods used by scammers
2. Recognize red flags in phishing emails, messages, or posts
3. Develop critical thinking skills to discern legitimate requests from potential phishing attempts

WHAT IS PHISHING?

Phishing is when someone tries to trick you into revealing personal information like your password, credit card numbers, or social security number.
Phishing can happen through emails, text messages, or other online platforms.
Phishing is one of the most common and effective forms of cyber attack.



Think of an email or message you received that asked for personal information. What made it suspicious?

CODE ALPHA

TYPES OF PHISHING

Phishing attacks come in different forms

EMAIL PHISHING

Scammers send fake emails pretending to be a trustworthy organization

SMS PHISHING

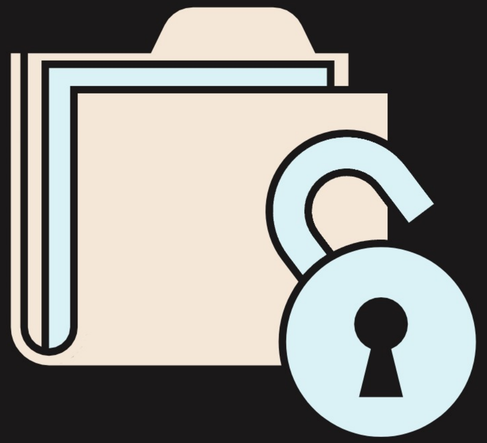
Scammers send text messages with fake links or requests for personal information

SOCIAL MEDIA PHISHING

Scammers create fake profiles or posts to trick you into clicking on links or sharing personal information.

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:



Suspicious emails or messages often create a sense of urgency and ask for personal information.

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

CODE ALPHA

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.

Which of the seven red flags do you think is the hardest to detect? What makes you say that?
Comment down below.

Social **Engineering** Tactics

- What is Social Engineering?
  - Manipulating individuals into divulging confidential information.

- Common Tactics
  - Impersonation: Pretending to be someone you trust.
  - Pretexting: Creating a fabricated scenario to steal information.
  - Baiting: Offering something enticing to trick you into giving information.
  - Tailgating: Following someone into a restricted area without authorization.
  - Quid Pro Quo: Offering a service in exchange for information.

Real-Life Examples of Phishing Attacks

phishing attacks have increased by 400% since the COVID-19 pandemic began.

EXAMPLE 1: The Target Breach (2013)

Attackers used phishing emails to gain access to Target's network.

Outcome: 40 million credit card numbers were stolen.

EXAMPLE 2: The Google Docs Scam (2017)

Phishing emails impersonated Google Docs to steal user credentials.

Outcome: Thousands of accounts compromised.

EXAMPLE 3: The Netflix Phishing Scam (2020)

Emails pretending to be from Netflix asked users to update their billing information.

Outcome: Many users' personal information was compromised.

CODE ALPHA

THINK CRITICALLY

Best Practices to Avoid Phishing..

Be skeptical of emails, messages, or posts that seem too good to be true or too urgent. Remember, if it sounds too good to be true, it probably is!

- Educate yourself and others.

Think before clicking on any links, sharing personal information online, or opening any suspicious attachments. Ask yourself if it seems legitimate and if you were expecting it.

- Install an Anti-Phishing Toolbar

Verify the authenticity of the sender and the information provided before taking any action.Trust your instincts and be cautious when sharing information online.

- Use Firewall

REPORT PHISHING ATTEMPTS

If you suspect a phishing attempt, report it to a trusted adult, teacher, or the school's IT department. Please don't forward the phishing email or message to another user. You can show them on your device. Forwarding phishing emails could lead to others being phished.

What to do if you suspect Phishing?
➞Change Your Passwords
➞Run a Security Scan
➞Monitor Accounts

THINK TWICE BEFORE YOU CLICK!

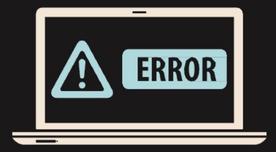
Don't share your personal information online!

Stay Vigilant: Always approach unsolicited communications with caution and verify their authenticity before taking any action.

Implement Best Practices: Follow established security practices and continuously educate yourself and your team to stay ahead of evolving threats.

Report Suspicious Activity: Prompt reporting can prevent potential damage and help in addressing security breaches effectively.

Thank you for participating in this phishing awareness training. Stay safe and secure online!


ERROR


ADMIN
****
LOGI


PRIVATE


PRIVATE
ERROR


****
1 2 3
4 5 6
7 8 9