CODE ALPHA CYBER SECURITY INTERNSHIP

PHISHING AWARENESS TRAINING

Think Before You Click!

Prepared by: Zakaria Ouahi

OBJECTIVES

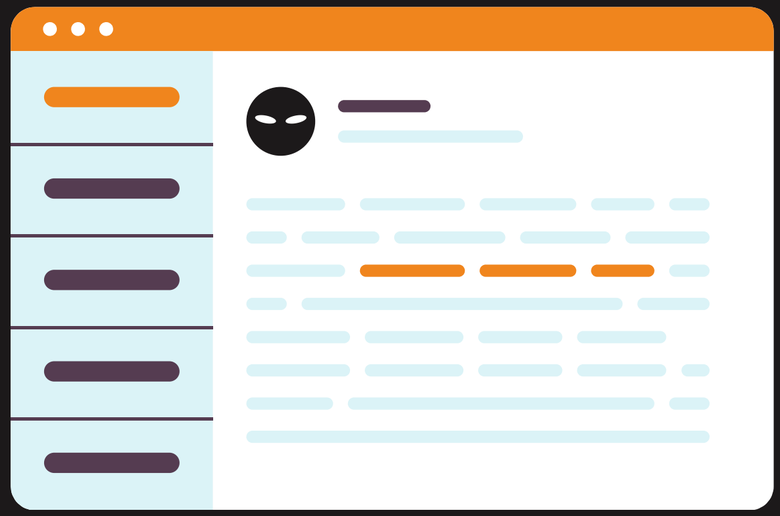
By the end of this training, you will be able to:

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.



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

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 informaion

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.

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

EXAMPLES OF REAL LIFE INCIDENTS

EXAMPLE 1

Credential Theft - Yahoo (2014):
Incident:
Yahoo suffered a massive data breach when attackers used a combination of spear-phishing and credential theft to gain unauthorized access to user accounts.
Consequences:
The breach exposed the personal information of 500 million users. This event severely damaged Yahoo's reputation, resulting in legal consequences and a decrease in user trust.

EXAMPLE 2

Ransomware Attack - WannaCry (2017):
Incident: While not a traditional phishing attack, the WannaCry ransomware spread via phishing emails. It exploited a Windows vulnerability to encrypt files and demanded a ransom for their release. **Consequences:** The attack impacted over 200,000 computers in 150 countries, affecting critical infrastructure, healthcare systems, and businesses. The financial and operational consequences were significant.

PROTECTING YOURSELF AGAINST PHISHING

BEST PRACTICES

- Keep software and systems up to date
- Use strong, unique passwords
- Enable multi-factor authentication
- Educate yourself and others about phishing threats.

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.

Reporting phishing attempts helps protect others from falling victim to the scam.

THINK CRITICALLY

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!

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.

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

THINK BEFORE YOU CLICK!

PROTECT YOURSELF FROM PHISHING

Don't share your personal information online!