PHISHING AWARENESS TRAINING

Think Before You Click!

- OM BARVALIYA

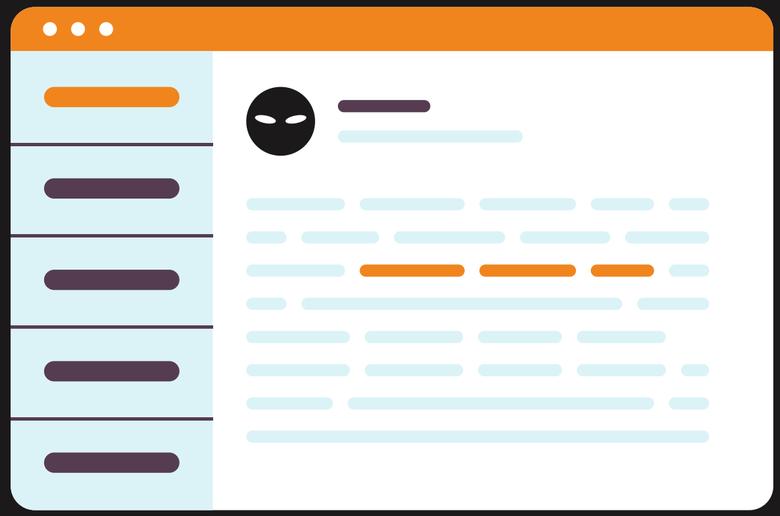
OBJECTIVES

By the end of this lesson, students 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 a fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity.
- Attackers often use email, phone, or text messages.
- Data targeted: passwords, credit card numbers, social security numbers, login credentials.



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

SPEAR PHISHING

Tailored to a specific target with personal information.

WHALINGING

Targets high-profile executives with custom attacks.

TYPES OF PHISHING

Phishing attacks come in different forms

SMISHING

Phishing via SMS (e.g., fake delivery messages)

VISHING

Voice phishing, often pretending to be tech support or banks.

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.

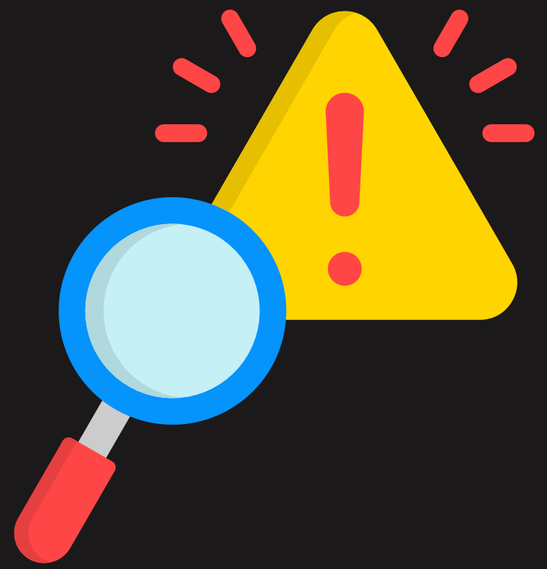
07 TOO GOOD TO BE TRUE

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?

RECOGNIZING PHISHING WEBSITES

1. Check for HTTPS and lock icon.
2. Look for misspelled URLs or fake subdomains.
3. Be wary of websites that ask for excessive information.
4. Use bookmarked or official URLs, not links from unknown emails.



CONSIDER THESE RED FLAGS

Read the examples and then identify which form of phishing it is and what red flags make it a phishing attempt.

EXAMPLE 1

You come across a pop-up window while browsing a website that asks you for your credit card information to claim a prize or discount within the next 10 minutes. The website looks legitimate, but you only have 10 minutes to submit your personal information.

EXAMPLE 2

You receive a message on social media from someone claiming to be a friend or family member, asking for your address and phone number. You've never met this person and don't see photos of them with your family or friends.

PREVENTIVE MEASURES

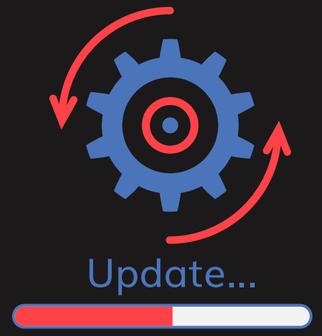
Be skeptical of emails, messages, or posts that seem too good to be true or too urgent. Remember, if it sounds too good to be true, it probably is!

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.

PREVENTIVE MEASURES

Use updated antivirus software with real-time protection and configure firewalls to monitor inbound and outbound traffic. Enable advanced email filters and spam detection systems to identify and block phishing links and spoofed domains.



Regularly install operating system and application patches to fix security vulnerabilities. Enable automatic updates and monitor for critical security advisories from trusted vendors.

TOOLS & RESOURCES

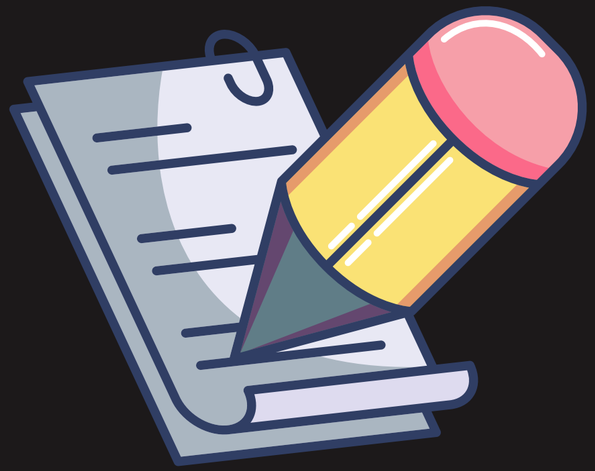
Google Safe Browsing:
Check if a website is safe.

Have I Been Pwned:
See if your email/data has been leaked.

Stay Safe Online:
Cybersecurity resources.

SUMMARY & KEY TAKEAWAYS

1. Always verify communications.
2. Never trust unsolicited emails or links.
3. Be cautious and report suspicious activity.
4. Keep learning - phishing tactics evolve.



THINK BEFORE YOU CLICK!

PROTECT YOURSELF FROM PHISHING

Don't share your personal information online!