DON’T TAKE THE BAIT

PHISHING AWARENESS TRAINING

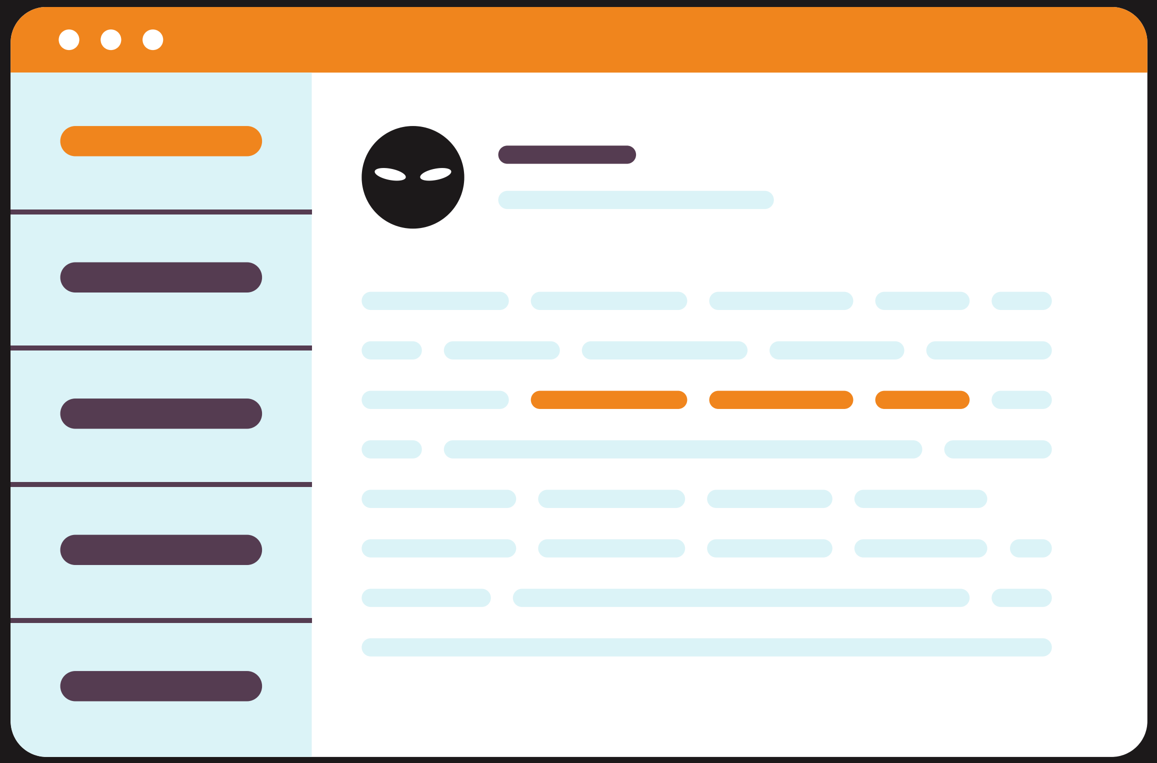
Understanding & Defending Against Phishing Attacks

INTRODUCTION

In today's digital landscape, phishing remains one of the most prevalent and effective cyber threats. It targets the human element, attempting to trick individuals into revealing sensitive information or compromising systems. This training will help you become the first line of defense.

WHAT IS PHISHING?

- Phishing is a type of cyberattack where attackers disguise themselves as a trustworthy entity (e.g., a legitimate company, colleague, or government agency) to trick individuals into giving up sensitive information, downloading malware, or performing actions that compromise security.
- The Attacker's Goal:
- Credential Theft: Stealing usernames, passwords, bank account details, credit card numbers.
- Malware Distribution: Tricking you into downloading viruses, ransomware, or spyware.
- Financial Fraud: Direct money transfers, fake invoices.
- Data Breach: Gaining access to sensitive corporate or personal data.
- Ransomware: Encrypting your files and demanding payment.
- How it Spreads: Primarily through email, but also via text messages, phone calls, and social media.



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

- Scammers send text messages with fake links orEmail Phishing (Broad): The most common type, sending mass emails to many recipients, hoping a few will fall for it.
- Spear Phishing: Highly targeted attacks against specific individuals or organizations. Attackers conduct research to make the email seem more legitimate and personalized.
- Whaling: A form of spear phishing specifically targeting senior executives or high-profile individuals ("the big fish") within an organization.
- Smishing (SMS Phishing): Phishing attempts conducted via text messages (SMS). Often contains malicious links or urges you to call a fraudulent number.
- Vishing (Voice Phishing): Phishing conducted over the phone. Attackers impersonate legitimate entities (e.g., bank, tech support, government) to extract information.
- Pharming: Redirecting users from a legitimate website to a fake one without their knowledge, often by poisoning DNS records.
- Clone Phishing: Creating an exact replica of a legitimate, previously sent email (including attachments and links) but replacing the links/attachments with malicious versions.

requests for 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:

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?

HOW TO RECOGNIZE FAKE WEBSITES

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

CHECK THE URL (ADDRESS BAR) CAREFULLY:

- Mismatched Domain: Is it paypal.com or paypa1.com? Is it login.microsoft.com or microsoft.login.secure.com (where secure.com is the actual domain)? The legitimate domain should be right before the first single /.
- Typos: gooogle.com, appple.com.

HTTP vs. HTTPS: While HTTPS (with the padlock icon) indicates a secure connection, it does NOT mean the site is legitimate. Phishers can obtain SSL certificates for their fake sites. Always check the domain name.

EXAMINE WEBSITE DESIGN AND CONTENT:

- Poor Quality: Blurry images, inconsistent fonts, broken links, strange formatting.
- Missing Information: Legitimate sites usually have "About Us," "Contact," "Privacy Policy," and "Terms of Service" links. Fake sites might be missing these.

HOW TO RECOGNIZE FAKE WEBSITES

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

REQUESTS FOR EXCESSIVE INFORMATION:

- Is the site asking for more personal information than necessary (e.g., your mother's maiden name, SSN, bank PIN, or all credit card details just for a login)?

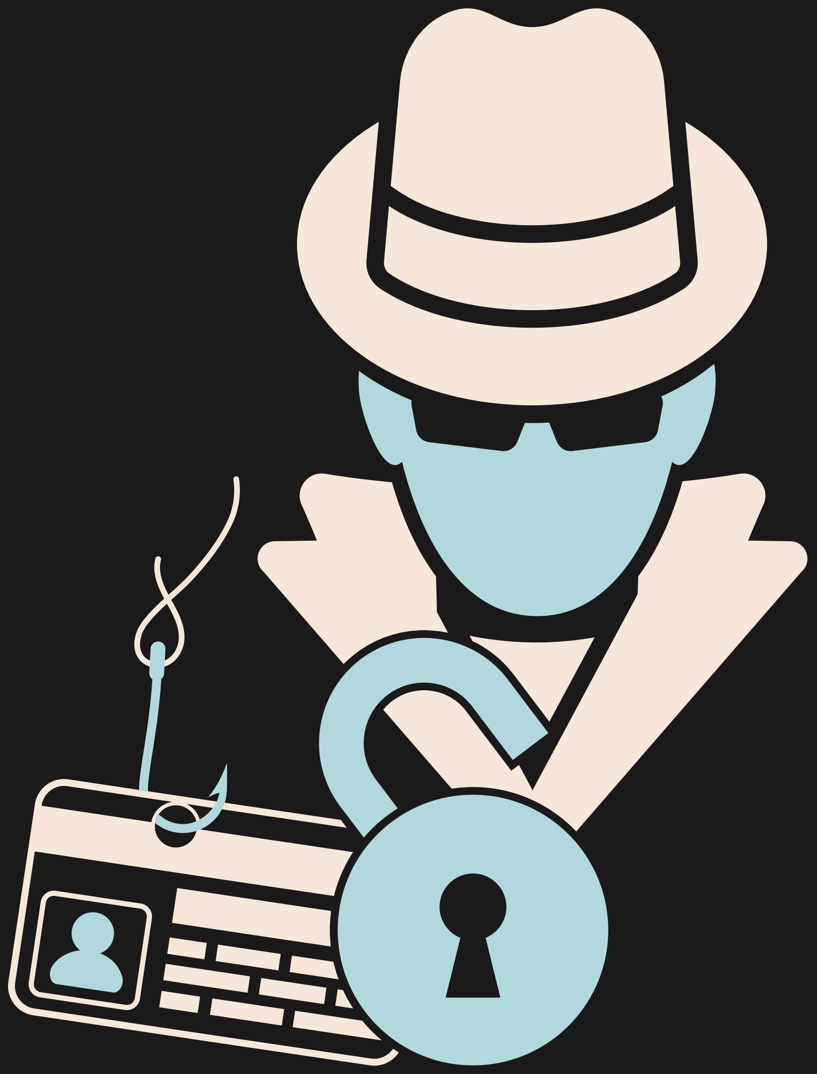
POP-UP WINDOWS:

- Be wary of login pop-ups that don't appear to be integrated with the main site.

CROSS-REFERENCE:

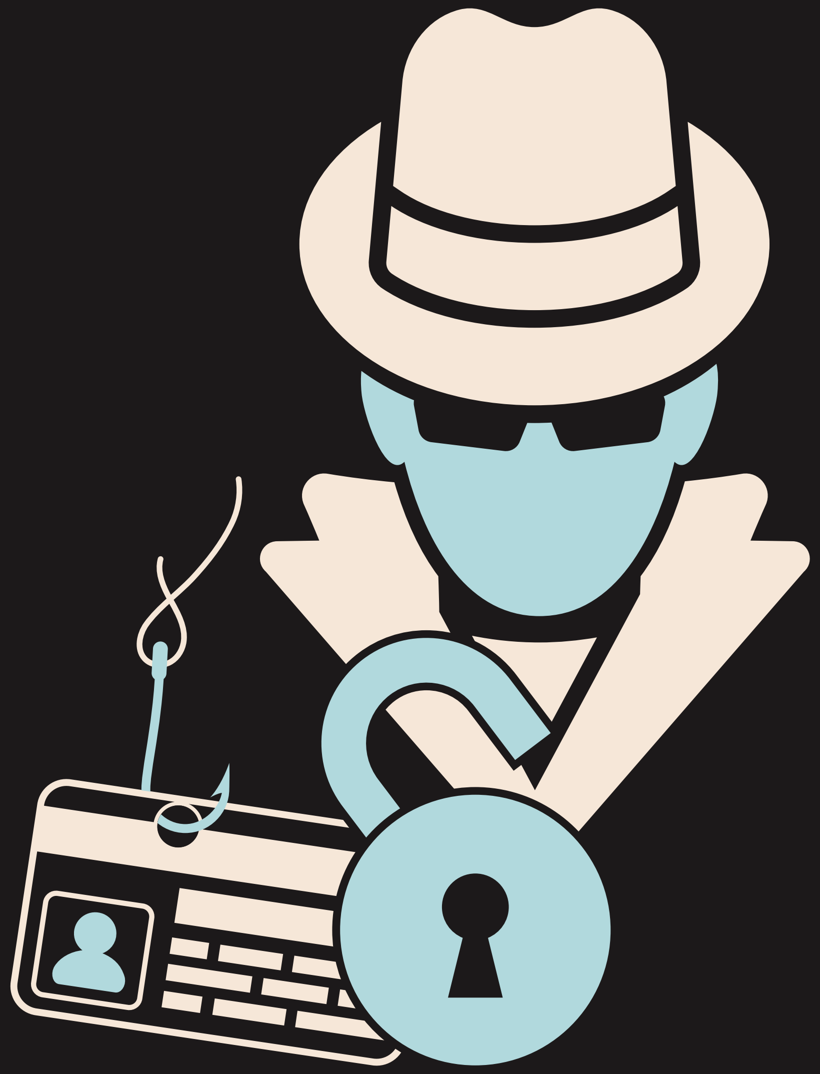
If you suspect a website, type the known legitimate URL directly into your browser or use a search engine to find the official site.

SOCIAL ENGINEERING TACTICS USED BY ATTACKERS



Phishing often relies on social engineering – manipulating people into performing actions or divulging confidential information.

1. Pretexting: Creating a fabricated scenario (a "pretext") to engage a target and extract information.
- Example: An attacker calls pretending to be IT support needing your password to "fix a critical issue."
2. Baiting: Offering something enticing to lure victims.
- Example: "Free movie downloads!" (but you click a malicious link) or "Congratulations! You've won a gift card!" (but it requires your bank details).
3. Quid Pro Quo: A "something for something" exchange.
- Example: An attacker promises a service (e.g., a fix for a supposed computer problem) in exchange for information (e.g., your login credentials).
4. Authority: Impersonating someone in a position of power or trust.
- Example: An email from a fake "CEO" demanding an urgent wire transfer, or a "police officer" calling to demand payment for a fake fine.
5. Intimidation/Fear: Creating a sense of urgency or threat to bypass critical thinking.
- Example: "Your account will be shut down immediately if you don't respond!" or "Legal action will be taken!"
6. Urgency/Scarcity: Implying a limited-time offer or immediate threat to create panic.
- Example: "Last chance to claim your prize!" or "Your login expires in 5 minutes!"



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!

RESOURCES