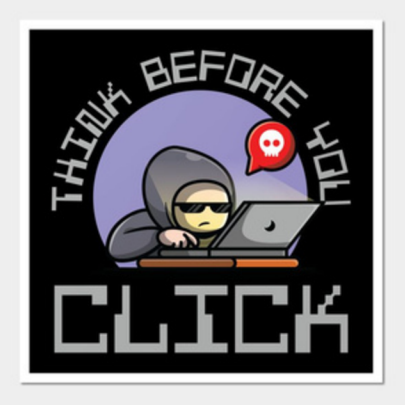
THINK BEFORE YOU CLICK: SPOTTING THE PHISH IN THE NET



INTRODUCTION

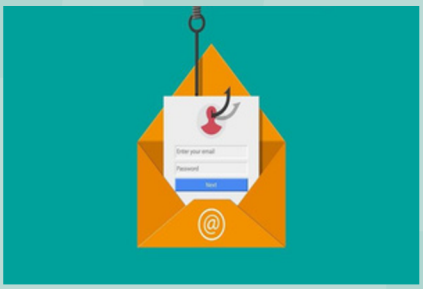
“Spotting the Phish in the Net”

Welcome to the “Think Before You Click” phishing awareness training. In today’s digital world, phishing is one of the most common and dangerous cyber threats individuals and organizations face. Understanding how to recognize and respond to these threats is critical—especially when over 90% of data breaches begin with a phishing email. By the end of this session, you'll be better equipped to protect yourself and your organization from falling victim to these attacks. Remember: one careless click is all it takes — so always think before you click.

WHAT IS PHISING ?

Phishing is a type of cyberattack in which attackers impersonate legitimate individuals, organizations, or services — usually through emails, messages, or fake websites — to trick people into revealing sensitive information such as usernames, passwords, credit card numbers, or personal data. Phishing relies on social engineering techniques to create a sense of urgency or trust, causing victims to act quickly without verifying the authenticity of the request.

ANATOMY OF A PHISING EMAIL



Suspicious Sender or Email Address

The sender's email may look similar to a legitimate one but contain small typos or strange domains

Urgent or Threatening Language

The message often pressures you to act quickly — like "Your account will be locked" or "Immediate action required" — to trigger panic.

Malicious Links or Attachments

The email includes clickable links or files designed to steal your credentials or install malware on your device.

SOCIAL ENGINEERING TACTICS

Phishing attacks often rely on social engineering tactics, which are psychological manipulation techniques used to trick individuals into taking unsafe actions. One common tactic is impersonation, where attackers pose as a trusted coworker, IT support personnel, or even senior management to gain your confidence. Another method is authority pressure, where messages claim to come from high-ranking officials—like the CEO—demanding urgent action, such as sharing confidential data or transferring funds. Lastly, pretexting involves crafting a believable scenario or backstory—such as a security alert or service request—to make the interaction seem legitimate. Understanding these techniques is crucial to recognizing and resisting social engineering attempts.

SPOTTING FAKE WEBSITES :

Identifying a fake website requires close attention to detail

Identifying a fake website requires close attention to detail, as many phishing sites are designed to closely mimic legitimate ones. One of the first steps is to carefully inspect the URL—attackers often use visually similar characters or subtle misspellings to trick users (for example, www.bankofamerica.com versus www.bankofarncrica.com). It's also important to remember that HTTPS does not always mean a site is safe; while HTTPS indicates encrypted communication, even malicious websites can obtain valid security certificates.

REAL WORLD PHISHING EXAMPLE

Phishing attacks often use current events and popular services to make their messages appear legitimate. A common example is the fake PayPal email, which falsely claims that the user's account has been suspended and prompts them to click a link to "verify" their credentials —ultimately leading to credential theft. During the height of the pandemic, attackers also circulated COVID-19 alert emails, pretending to be from trusted organizations like the WHO or government agencies, luring recipients into clicking malicious links under the guise of health alerts or policy updates.

HOW TO PROTECT YOURSELF FROM PHISHING ATTACKS

- pause and evaluate before opening links or attachments.
- Avoid downloading attachments from unknown or untrusted sources.
- Verify suspicious emails by contacting the sender through official channels.
- Use strong, unique passwords and enable Multi-Factor Authentication (MFA) for added security.
- Report phishing attempts immediately to your IT or security team.

INNOVATIVE QUIZ

Scenario 1:
You receive an email from “admin@yourbank-alerts.com” saying:

“Your account has been compromised. Click here to secure it now!”

What’s your next move?
A) Click the link immediately to protect your account
B) Reply asking for more information
C) Hover over the link and verify the sender’s domain ✅
D) Delete the email without reading

INNOVATIVE QUIZ

Scenario 2:
Your manager sends a file named Salary_Updates_2025.xls via email—but it looks slightly different from their usual address.

What should you do?
A) Open the file since it's from your manager
B) Forward it to your team
C) Call or message your manager to confirm they sent it ✅
D) Report it as spam

SUMMARY AND KEY TAKEAWAYS

To stay safe online, always remember to pause and think before you click. Phishing attacks rely on urgency and deception, so it's important to stay alert for red flags like suspicious links, fake websites, and unusual requests. Social engineering works by tricking you into making quick decisions—don't let it succeed. If something feels off, trust your instincts and report it to your IT or security team. Staying informed is your best defense. For more practice and learning, explore tools like the Google Phishing Quiz or visit StaySafeOnline.org.

Thank You ...!