Phishing Awareness Training

By Manoj Kumar Chaudhary

Module 1: Introduction

What is Phishing?

- Phishing is a type of cybercrime where attackers attempt to trick you into giving up sensitive information.
- Think of it like digital "fishing." Attackers bait a hook (a fake email or message) and cast it out, hoping someone bites.
- **The "Catch":** They're after your usernames, passwords, credit card numbers, bank account details, or company data.

The Impact - Why Should You Care?

- **For You Personally:**
  - Identity Theft
  - Financial Loss
  - Unauthorized access to your personal accounts (email, social media)
- **For Our Organization:**
  - Major Data Breaches
  - Financial Loss (fraudulent wire transfers)
  - Ransomware attacks locking up our systems
  - Reputational Damage

Module 2: Anatomy of a Phishing Attack

Recognizing Phishing Emails - The Red Flags

❑ The Bait: How to Spot a Phishing Email

Checklist of Red Flags:

- **Mismatched Sender Address:** The display name says "Microsoft Support," but the email address is support@micros0ft.net or security.update@hotmail.com.
- **Urgent or Threatening Language:** "Your account will be suspended in 24 hours!" or "Suspicious activity detected!" They want you to panic, not think.
- **Generic Greetings:** "Dear Valued Customer" or "Hello User." Legitimate companies usually use your name.
- **Spelling & Grammar Mistakes:** Professional organizations proofread their emails. Multiple errors are a huge red flag.

- **Suspicious Links: (Critical Skill!)** Hover your mouse over a link *without clicking* it. The preview URL that pops up will often be different from the text and lead to a strange domain.
- **Unexpected Attachments:** Never open attachments you weren't expecting, especially .zip, .exe, or .html files. They can contain malware.
- **Unusual Requests:** Your CEO will not email you from a Gmail account asking you to buy gift cards. This is a common scam.

Recognizing Fake Websites - The Fake Landing Spot

❑The Trap: How to Spot a Fake Website

Checklist of Red Flags:

- **Check the URL:** Look for misspellings (paypa1.com instead of paypal.com) or strange subdomains (yourbank.security-alert.com).
- **No Padlock (No HTTPS):** Look for the padlock icon and https:// in the address bar. If it's missing or the browser warns you the site is "Not Secure," do not enter any information.
- **Poor Design or "Cloned" Look:** The logo might be low-resolution, the colors slightly off, or the fonts look wrong.
- **Pop-ups and Aggressive Forms:** The site immediately asks for your username and password through a pop-up, rather than a standard login page.

Module 3: The Psychology - Social Engineering

Mind Games - How Attackers Manipulate You

❑ The Psychology: Understanding Social Engineering

Attackers don't just hack computers; they hack people. Social engineering is the art of manipulating people into performing actions or divulging confidential information.

❑ Common Tactics:

- **Urgency:** Making you feel like you have to act NOW.
- **Authority:** Pretending to be someone in power (CEO, IT Admin, Law Enforcement).
- **Fear:** Convincing you that something bad will happen if you don't comply.
- **Curiosity & Greed:** Luring you with a "special offer," "prize," or a file named "Employee Salaries 2023."
- **Helpfulness:** Posing as a support technician who needs your password to "fix" a problem.

Module 4: Real-World Examples & Interactive Quiz

Example 1 - The "Package Delivery" Scam

You receive an email saying a package delivery failed. It asks you to click a link to reschedule or print a shipping label.

❑ Red Flags Breakdown:

- **From:** delivery-notice@fedex-express-intl.com (not the real fedex.com).
- **Urgency:** "You must reschedule within 48 hours or the package will be returned."
- **Link:** The hover-link shows a malicious URL like http://bit.ly/f3d3xTrack.
- **Attachment:** The "shipping label" is a .zip file containing malware.

Example 2 - The "CEO Fraud" / Gift Card Scam

An email from your "CEO" asks, "Are you at your desk? I need you to handle a quick task for me discreetly." If you reply, they ask you to purchase several hundred dollars in gift cards for a client and send them the codes.

- **Red Flags Breakdown:**
  - **Authority:** Uses the CEO's name to pressure you.
  - **Unusual Request:** Buying gift cards is not a standard business procedure.
  - **Urgency & Secrecy:** Asks you to do it "quickly" and "discreetly" to bypass normal verification channels.
  - **Sender Address:** Often sent from a personal email (ceo.name@gmail.com) with the excuse "I'm in a meeting and don't have my work phone."

Interactive Quiz - Test Your Skills!

- **(Quiz Question 1)**
  You receive an email from IT-Support@company.net with the subject "URGENT: Your password expires in 1 hour." It tells you to click a link to reset it immediately. What is the **safest** first step?
  a) Click the link and reset your password. It's from IT.
  b) Reply to the email and ask if it's real.
  c) Hover your mouse over the link to inspect the URL without clicking.
  d) Forward the email to your manager.
- **(Quiz Question 2)**
  Which of these website URLs is most likely to be **safe** for logging into your bank, "MyNationalBank"?
  a) http://login.mynationalbank.com
  b) https://www.mynationalbank.security.com
  c) https://www.mynationalbank.com
  d) https://www.my-national-bank.net
- **(Quiz Question 3)**
  You receive an unexpected email with a Microsoft Word attachment named Invoice.docx. The email says, "Please see attached invoice for payment." What should you do?
  a) Open it to see if it's a bill you need to pay.
  b) Delete the email immediately without opening the attachment.
  c) Forward it to the accounting department.
  d) Open the attachment, but don't enable macros if it asks.

Quiz Answers & Explanations

- **Q1 Answer: (c)** Hovering over the link is the best first step. It allows you to verify the link's destination without risk. Replying could confirm your email is active, and clicking is dangerous.
- **Q2 Answer: (c)** This URL uses https:// (secure) and has the correct primary domain (mynationalbank.com). The others use http (insecure), have suspicious subdomains, or incorrect top-level domains (.net).
- **Q3 Answer: (b)** The safest action for an *unexpected* invoice attachment is to delete it. If you think it might be legitimate, contact the sender through a known, separate channel (like calling them or starting a new email) to verify. Never open unsolicited attachments.

Module 5: Your Defense Shield - Best Practices

Best Practices - The THINK Acronym

- **Your Defense: Best Practices to Stay Safe**
- **Mnemonic:** Before you click, **THINK!**
  - **T - Think Before You Click:** Be suspicious of every unexpected email and link. A few seconds of caution can save you hours of trouble.
  - **H - Hover to Discover:** Always hover over links to see the real destination URL before you click.
  - **I - Inspect the Sender:** Don't just trust the display name. Check the full email address for anything unusual.
  - **N - Never Give Up Personal Info:** Legitimate organizations will never ask for your password or full credit card number via email.
  - **K - Keep it to Yourself (and Report it!):** Don't forward phishing emails. Report them using your company's "Report Phishing" button or by forwarding them to the IT/Security department.

More Key Defenses

❑ Strengthen Your Shield

- **Use Multi-Factor Authentication (MFA):** This is your single best defense. Even if an attacker steals your password, they can't log in without the second factor (like a code from your phone).
- **Use Strong, Unique Passwords:** Don't reuse passwords across different sites. Use a password manager to help.
- **Verify, Verify, Verify:** If a request seems odd (like a wire transfer or gift card purchase), pick up the phone and call the person to confirm.
- **Keep Software Updated:** Keep your browser, operating system, and antivirus software up to date to protect against the latest threats.

Module 6: Conclusion - What to Do If You Fall Victim

You Clicked! Now What?

❑I Clicked a Phishing Link! What Do I Do?

Don't panic and don't be embarrassed. Acting quickly is key.

- **Disconnect:** Immediately disconnect your computer from the internet to prevent malware from spreading.
- **Change Your Password:** If you entered your credentials on a fake site, go to the *real* website and change your password immediately. Change it on any other site where you use the same password.
- **Report It: This is the most important step.** Contact the IT Help Desk or Security Team immediately. They need to know what happened to protect you and the company. They are here to help, not to blame.
- **Scan Your Computer:** Run a full antivirus scan on your device.

Key Takeaways & Final Message)

❑ You Are the Human Firewall

Summary:

- **Be Skeptical:** Treat all unsolicited communication with caution.
- **Verify:** When in doubt, verify through a separate, trusted channel.
- **Report:** Reporting suspicious emails protects everyone.

Final Message: Technology can block many threats, but a savvy, well-trained user is the best defense against phishing. You are our first and most important line of defense. Thank you

Thank You