Phishing Awareness Training Module

Objective

Equip users with the knowledge and practical skills to recognize and avoid phishing attacks, understand social engineering tactics, and implement safe online behaviors.

Section 1: Introduction to Phishing

What is Phishing?

Phishing is a cyberattack technique used by attackers to deceive users into providing sensitive information such as passwords, credit card numbers, or personal details by pretending to be a trustworthy entity.

Common Types of Phishing:

- Email Phishing: Mass emails pretending to be from reputable sources.
- Spear Phishing: Targeted emails using personal information.
- Smishing: Phishing via SMS/text messages.
- Vishing: Voice-based phishing (fraudulent calls).
- Clone Phishing: Legitimate email cloned and modified with malicious links.

Section 2: Recognizing Phishing Emails and Fake Websites

Signs of a Phishing Email:

- Generic greeting ("Dear user")
- Poor grammar or spelling errors
- Sense of urgency or threats ("Act Now!", "Account Suspended")
- Unusual sender email addresses
- Unexpected attachments or links

Identifying Fake Websites:

- Slight variations in URL (e.g., `micr0soft.com`)
- No HTTPS or expired certificates
- Visual inconsistencies and typos
- Unusual requests for sensitive data

Section 3: Social Engineering Tactics

Attackers often exploit psychological principles to manipulate users:

- Authority: Impersonating figures of authority

- Urgency: Creating panic to elicit quick action
- Scarcity: Limited-time offers or threats of losing access
- Sympathy/Help: Playing on empathy or asking for help

Case Example:

In 2016, attackers used spear-phishing to gain access to the Democratic National Committee's network via a fake Gmail login page.

Section 4: Prevention Tips and Best Practices

Do's:

- Verify the sender before clicking links
- Use multi-factor authentication (MFA)
- Regularly update your devices and software
- Use strong, unique passwords (consider a password manager)
- Report suspicious emails to your IT/security team

Don'ts:

- Don't click on unknown links or open suspicious attachments
- Don't share passwords or OTPs
- Don't ignore security warnings

Section 5: Real-World Examples

Example 1: PayPal Scam Email

- Subject: "Unusual login activity"
- Red Flag: Urgent call to click a login link that leads to a fake site

Example 2: COVID-19 Relief Scam

- Pretending to offer government aid with a link that steals banking info

Example 3: Fake Google Docs Invitation

- Fake collaboration request prompting users to log in via a phishing page

Section 6: Interactive Quiz (Sample Questions)

1. What should you do if you receive an email from your "bank" asking you to urgently verify your account?

✅ **Correct Action:**

- **Do not click** on any links or download attachments.
- **Check the sender's email address** carefully. Fraudulent emails often come from addresses that look similar to legitimate ones (e.g., support@secure-banklogin.com instead of support@yourbank.com).
- **Contact the bank directly** using official contact methods (their website, phone number).
- **Report the email** to your internal security team or the bank's phishing report system.

❌ **Wrong Action:**

- Clicking the link and entering your credentials.
- Replying to the email with your personal information.

---

2. Which of the following URLs is suspicious?

A. https://accounts.google.com
B. https://secure.paypal.com
C. https://secure-paypal.login.com ✅
D. https://www.microsoft.com

🎯 **Explanation:**

- The third URL (secure-paypal.login.com) is **suspicious** because it's trying to mimic a trusted domain. Attackers use subdomains to make URLs look legitimate.
- Always look for the **main domain** (e.g., paypal.com, not login.com).

---

3. What is a tell-tale sign of a phishing website?

✅ **Signs to Watch For:**

- **Misspelled URLs** or odd domain names.
- **No HTTPS encryption** (look for the padlock in the address bar).
- **Urgent warnings** or pop-ups demanding immediate action.
- **Unprofessional design** or broken links.
- **Requests for sensitive information** like passwords, SSNs, or bank details.

---

4. How can you confirm the legitimacy of a login request?

🔍 **Verification Steps:**

- Hover over the link (without clicking) to inspect the URL.
- Cross-check the link with the official website's login page.
- Do not log in through links in emails — instead, **open a new browser tab** and type the official site URL manually.
- Look for **HTTPS** and valid SSL certificates.
- Check for **typos or unusual language** in the email prompting the login.

---

5. True or False: Multi-factor authentication can help reduce phishing risks.

✅ **True**

🛡 **Explanation:**

- MFA adds an **extra layer of security** even if your password is stolen.
- It usually requires a **code sent to your mobile**, a **biometric scan**, or a **security token**.
- Phishers will have a harder time accessing your account without the second factor.

Section 7: Conclusion & Action Items

Summary:

- Be skeptical of unexpected messages
- Double-check URLs and sender info
- Avoid sharing sensitive info via email or SMS
- Stay informed and alert

Call to Action:

- Bookmark official websites you use frequently
- Participate in regular security training
- Report phishing to your organization's security team

Section 8: Reporting Phishing Incidents

Why Reporting Matters:

Reporting phishing attempts helps protect your coworkers and the organization by enabling IT/security teams to block further attacks.

How to Report:

- Forward the email to security@yourorganization.com (replace with your actual address).
- Do not delete the suspicious email until IT confirms.
- If using Outlook or Gmail, use the "Report Phishing" button if available.
- Provide screenshots and full email headers if requested.

📌 Note: If you clicked on a link or entered credentials, report it immediately and change your passwords.

Phishing on Mobile Devices

- Smishing (SMS-based phishing) is increasingly common — be wary of links in text messages.
- Quishing (QR code phishing): Attackers embed malicious links in QR codes, especially in posters or event invites.
- Shortened URLs (like bit.ly) are often used — never click unless verified.
- Some mobile apps mimic official ones — download only from official app stores.
- Always preview links if your device allows it before clicking.

Appendix: How to Spot a Phish – Quick Checklist ☑

✔ Check This	🚩 Watch Out For
Is the sender address correct?	Generic greetings like "Dear Customer"
Is the message expected?	Spelling/grammar mistakes
Hover over links — legit domain?	URLs that don't match the claimed brand
Look for HTTPS in URLs	Urgent action like "Verify Now" or "Your account is suspended"
Contact sender via official means	Attachments you weren't expecting

🧠 When in doubt: Don't click. Don't reply. Report it.

Resources:

- Google Phishing Quiz: https://phishingquiz.withgoogle.com/
- Stay Safe Online – Phishing: https://staysafeonline.org/stay-safe-online/online-safety-basics/spam-and-phishing/