**Phishing Awareness Training Module**

**Introduction**

Phishing is a type of cyber attack where attackers attempt to deceive individuals into providing sensitive information such as passwords, financial details, or personal data. Understanding phishing attacks and how to recognize them is crucial in safeguarding yourself and your organization.

**Objectives**

By the end of this training, you will:

* Understand what phishing is and its different types.
* Be able to identify phishing attempts in emails, websites, and social engineering tactics.
* Learn practical steps to protect yourself from phishing attacks.

**What is Phishing?**

Phishing attacks are deceptive techniques designed to trick you into:

* Sharing personal or financial information.
* Clicking malicious links or downloading harmful attachments.
* Logging into fake websites that steal your credentials.

**Types of Phishing Attacks**

1. **Email Phishing**:
   * Fraudulent emails that appear to come from legitimate sources (e.g., banks, companies).
   * Contain urgent requests like "Update your account information now."
2. **Spear Phishing**:
   * Targeted attacks aimed at specific individuals or organizations.
   * Often highly personalized to increase trust.
3. **Smishing**:
   * Phishing attempts via SMS or text messages.
   * Contain suspicious links or requests for personal information.
4. **Vishing**:
   * Voice phishing through phone calls to extract information.
5. **Pharming**:
   * Redirecting users to fake websites without their knowledge.

**Recognizing Phishing Attempts**

**Common Signs of Phishing Emails**

* **Urgency or Threats**: Phrases like "Act now!" or "Your account will be locked!"
* **Generic Greetings**: "Dear Customer" instead of your name.
* **Suspicious Links**: Hover over links to verify the URL (e.g., "[www.bank-secure-login.com](http://www.bank-secure-login.com/)" may not be legitimate).
* **Unexpected Attachments**: Avoid opening attachments from unknown sources.
* **Grammar and Spelling Errors**: Professional organizations rarely send emails with errors.

**Phishing Websites**

* Check for secure connections (look for https:// and a padlock icon).
* Verify the website’s URL and avoid clicking links in unsolicited emails.
* Look for inconsistencies in branding or design.

**Social Engineering Tactics**

* **Impersonation**: Attackers pretend to be someone you trust (e.g., IT support, a manager).
* **Pretexting**: Creating a false scenario to obtain information.
* **Baiting**: Luring victims with promises of rewards (e.g., free software).

**How to Avoid Phishing Attacks**

**Best Practices**

1. **Verify the Source**:
   * Contact the sender directly through official channels if you are unsure.
2. **Think Before You Click**:
   * Hover over links to check their destination.
3. **Use Security Software**:
   * Enable firewalls, anti-virus software, and spam filters.
4. **Enable Multi-Factor Authentication (MFA)**:
   * Add an extra layer of security to your accounts.
5. **Educate Yourself**:
   * Stay informed about new phishing techniques and scams.

**What to Do If You Suspect Phishing**

1. Do not respond, click any links, or download attachments.
2. Report the email or message to your IT department or email provider.
3. Delete the suspicious message from your inbox.
4. If you accidentally provided sensitive information, change your passwords immediately and monitor your accounts for unusual activity.

**Interactive Exercise**

**Scenario-Based Activity**

You receive the following email:

* Subject: "Urgent! Verify Your Account Now"
* Message: "We noticed unusual activity on your account. Please click here to verify your details within 24 hours."
* Link: http://secure-login-bank-example.com

**Question**: What should you do?

1. Click the link and verify your account.
2. Ignore the email.
3. Hover over the link, verify its destination, and report the email.

**Answer**: Option 3 - Hover over the link, verify its destination, and report the email.

**Conclusion**

Phishing attacks are a prevalent threat, but with awareness and vigilance, you can protect yourself and your organization. Remember:

* Always verify sources before sharing information.
* Think before you click.
* Stay informed about the latest phishing techniques.

Together, we can build a safer online environment.

**Resources**

* [Anti-Phishing Working Group](https://apwg.org/)
* [StaySafeOnline](https://staysafeonline.org/)
* [Report Phishing Emails](https://www.us-cert.cisa.gov/report-phishing)