Phishing Awareness Training

HACHEMI RYM

TABLE OF CONTENTS

TABLE OF CONTENTS

01 Introduction

Introduction: Understanding Phishing

Phishing is a cyberattack technique where attackers impersonate legitimate entities to trick individuals into providing sensitive information such as usernames, passwords, or financial data.

02 Types of Phishing Attacks

Phishing Email

- Most common form of phishing.
- Attackers send fraudulent emails pretending to be from a trusted source (e.g., banks, social media, IT support).
- Often contains malicious links, attachments, or fake login pages.

Phishing Websites

- Fake websites designed to steal login credentials or spread malware.
- Often mimics real websites with minor differences (e.g., www.paypa1.com instead of www.paypal.com).
- Typically linked within phishing emails or fraudulent ads.

SMS Phishing (Smishing)

- Attackers send phishing messages via SMS or messaging apps.
- Common tactics include:
- Fake package delivery notifications.
- Urgent security alerts from banks.
- Phony contest winnings.

Phone Call Phishing (Vishing)

- Attackers use phone calls to impersonate officials (e.g., tech support, government agencies, or financial institutions).
- Can involve:
- Requesting passwords, PINs, or bank details.
- Persuading victims to install remote access software.
- Urging urgent action to "prevent account suspension."

03 Recognizing a Phishing Email

Recognizing a Phishing Email

Phishing emails often look convincing but have subtle red flags:

Grammar and Spelling Errors

Professional organizations rarely send emails with poor grammar or typos.

Suspicious Email Addresses

Attackers may use email addresses that look similar to legitimate ones.

Hover Over Links to Check the Actual URL

Fake emails often contain links that redirect to malicious sites.

Hover your mouse over a link (without clicking) to see the actual destination.

Example:

Visible: https://www.apple.com

Real URL: https://apple-support-reset-login.com (fake site)

Urgent or Threatening Messages

Attackers create a sense of urgency to provoke immediate action.

Common phrases:

"Your account will be suspended in 24 hours!"

"Unusual login detected! Verify your identity now."

"You have won a prize! Claim it within 5 minutes!"

04 Spotting a Phishing Website

Spotting a Phishing Website

Check for Security Indicators

Ensure the URL starts with https:// (not just http://).

Look for a lock icon 🔒 in the browser address bar.

Note: Some phishing websites use https:// but still trick users with fake forms!

Look Out for Cloned Websites

Attackers may copy a real website's design to deceive users.

Small differences in domain names:

Real: www.amazon.com

Fake: www.amaz0n-secure.com

Check for Unusual Pop-ups or Login Requests

Be wary if a site suddenly asks for sensitive information like passwords or payment details.

Example: Fake PayPal login page that asks for credit card information.

Verify the Domain Before Entering Credentials

If unsure, manually type the official website's URL instead of clicking on email links.

05 Understanding Social Engineering Tactics

Understanding Social Engineering Tactics

1. What is Social Engineering?

Social engineering is a psychological manipulation tactic used by attackers to trick people into revealing confidential information.

2. Common Social Engineering Scenarios

Calls or Messages Pretending to be from Authorities

Example: A fraudster calls pretending to be from your bank or government.

They claim your account has been compromised and ask for:

Your password.

Your One-Time Password (OTP) or verification code.

"Too Good to Be True" Offers

Fake lottery winnings: "Congratulations! You've won $1,000,000! Click here to claim your prize."

Free vacation scams.

Fake giveaways (e.g., "Win a free iPhone!").

Fake Customer Support Scams

Attackers pretend to be tech support from Microsoft, Apple, or Amazon.

They may ask you to install software that gives them access to your device.

Always verify with the official support number on the company's website.

06 Prevention Measures

Prevention Measures

Avoid Clicking Suspicious Links

Use Strong and Unique Passwords

Report Suspicious Emails or Activities

Enable Mul
ti-Factor Authentication (MFA)

07 Conclusion

Conclusion

Phishing attacks are a major cybersecurity threat, exploiting human trust to steal sensitive information. By learning to recognize phishing emails, fake websites, and social engineering tactics, individuals can significantly reduce their risk of falling victim. Key takeaways include:

- Think before you click – Always verify links and sender details.
- Never share sensitive information via email, SMS, or phone calls.
- Use strong security measures like multi-factor authentication (MFA) and unique passwords.
- Report suspicious activity to protect yourself and others.