Phishing Awareness Training

Satvik Hatulkar
CodeAlpha, Cyber Security Intern

Phishing Awareness Training Introduction

01

Stay Vigilant

Always check sender email addresses for authenticity and legitimacy.

02

Verify Links

Hover over links before clicking to ensure they lead to expected destinations.

03

Report Suspicion

Immediately report any suspicious emails to your IT department for analysis.

04

Educate Regularly

Participate in regular training to stay updated on phishing tactics and trends.

Understanding Phishing: Definition and Impact

Know Types

Familiarize yourself with common phishing methods like emails, messages, and phone calls.

Verify Sources

Always check the sender's email address and phone number before responding or clicking links.

Report Suspicion

Report any suspicious communications to your IT department immediately for investigation.

Educate Regularly

Participate in regular training sessions on phishing awareness and security best practices.

Types of Phishing Attacks Explained

Email Phishing

Beware of unsolicited emails requesting sensitive information.

Spear Phishing

Verify identities before responding to targeted email requests.

Whaling

Be vigilant against fake emails from high-level executives.

Vishing

Never share personal information over the phone without verification.

Smishing

Ignore text messages requesting personal information or links.

Clone Phishing

Check links for legitimacy before clicking on cloned messages.

Recognizing Phishing Attempts: Key Indicators

Urgent Action

Messages that create a sense of urgency or threat are suspicious.

Unfamiliar Sender

Emails from unknown or unexpected sources should be treated cautiously.

Spelling Errors

Poor grammar or spelling mistakes are common signs of phishing.

Unexpected Attachments

Be wary of unsolicited attachments, as they may contain malware.

Links to Unknown Sites

Hover over links to check if URLs match the displayed text.

Request for Personal Info

Legitimate organizations will never request sensitive information via email.

Generic Greetings

Phishing emails often use vague salutations like 'Dear Customer'.

Best Practices to Avoid Phishing Scams

01

Verify Sources

Always confirm the identity of requests through separate channels.

02

Watch for Urgency

Be cautious of messages creating a false sense of urgency.

03

Use strong passwords.

Implement complex passwords and change them regularly for security.

04

Enable Two-Factor

Utilize two-factor authentication for an added layer of protection.

05

Report Suspicious Emails

Immediately report any suspicious emails to the IT department.

Mitigation Strategies for Phishing Threats

01

Regular Employee Training

- Conduct training sessions to identify phishing attempts.

02

Implement Email Filters

- Use advanced filters to block phishing emails.

03

Two-Factor Authentication

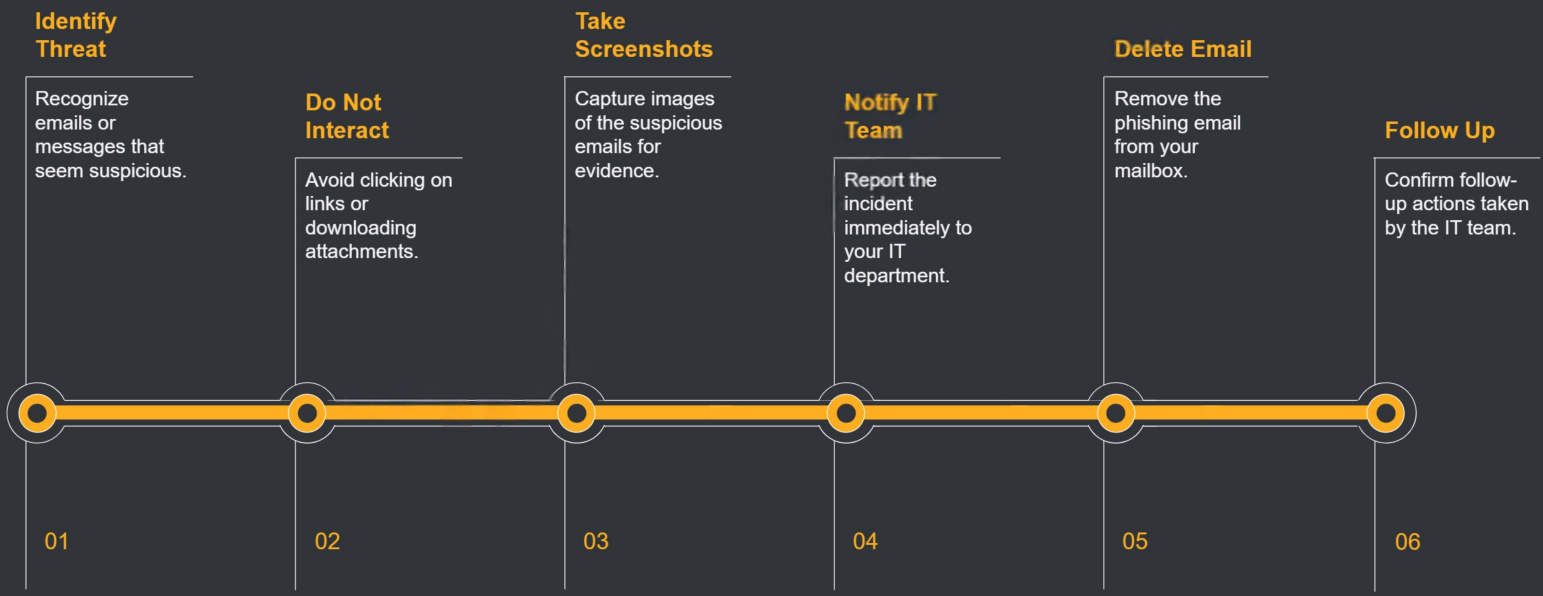
- Add an extra security layer to user accounts.

04

Report Suspicious Emails

- Encourage employees to report any suspicious messages.

Reporting Phishing Incidents: Protocols to Follow



Thank You

Recognize Phishing Attempts

Awareness of phishing techniques helps to identify suspicious communications.

Verify Email Sources

Always check the authenticity of emails before clicking on links.

Use Strong Passwords

Creating complex passwords can protect your accounts from unauthorized access.

Report Suspicious Activities

Promptly notifying IT about strange emails can prevent potential security breaches.