Phishing Awareness Training: Protecting Yourself Online

Phishingisthe starting pointfor 90% of cyberattacks worldwide. The global costof phishing attacks is estimated to exceed$12billion annually.In theUK alone, businesses lose on average £3,000 per phishing incident. Staying informed and vigilant is essential to protect sensitive data and assets.

What is Phishing?

Phishingis a deceptiveattempt to trick usersinto revealing sensitive information such as passwords and bank details. Attackers impersonate trusted entities like banks, government agencies, or IT support staff to gain trust. The ultimate goals include financial gain, data theft, and system compromise. In the UK, the National Cyber Security Centre blocks around 18 million phishing emails every month.

Spotting Phishing Emails: Red Flags (Part 1)

- **Sender Address:**Beware of suspiciousor mismatcheddomains like *micr0soft.com* insteadof *microsoft.com*.
- **Urgency or Threats:** Emails demanding immediate action, e.g., "Account suspended in 24 hours!" aim to provoke panic.
- **Generic Greetings:** Lack of personalised salutation such as "Dear Valued Customer" instead of your name.
- **Unexpected Requests:** Be cautious of unusual demands for personal data or urgent money transfers.

Spotting Phishing Emails: Red Flags (Part 2)

- **Hyperlinks:**Alwayshover overlinkstoverify theactual URL matches the displayed text.
- **Attachments:** Watch out for unexpected or suspicious file types like .exe, .zip, or .js.
- **Spelling & Grammar:** Poor language quality often indicates a phishing attempt.
- **Offers Too Good to Be True:** Unrealistic prizes or deals are common bait.

Helom/ɔre quility moodess.. |

Stapt is Aμliom cof/fer Phiggu siget.

Identifying Fake Websites & URLs

Always scrutinisewebsiteURLs; look for"https://"indicating encryption and ensure thedomain is correct, such as *amazon.co.uk*. The padlock icon showsSSL presencebut doesn9tguarantee legitimacy.Fakesites often feature low-quality images, outdated logos, or broken links. Excessive pop-ups demanding credentials are a warning sign. Use tools like WHOIS to check domain registration details for authenticity.

Social Engineering Tactics Used by Attackers

Pretexting

Fabricatingscenarios to gain trust, such as impersonating IT support to request passwords.

Baiting

Offeringenticing rewards like free software or gift cards in exchange for credentials.

Scareware

Usingfakevirus alerts or threats to frighten users into immediate action.

Quid Pro Quo

Demandinginformation as exchange for a supposed service, like password resets.

Real-World Phishing Examples

1. **HMRCTax Refund Scam (2023):** Fraudulent SMS andemails claiming refunds, leadingto fakesites,with over 1.2million reportsin theUK.
2. **Microsoft 365 Credential Theft:** Fake login pages targeting corporate users causing losses over £50M annually.
3. **CEO Fraud/Business Email Compromise (BEC):** Executive impersonations to authorise fraudulent payments, averaging £25,000 lost per UK incident.
4. **Bank of America Phishing:** Thousands of ongoing variations aimed at stealing banking credentials.

Best Practices: Don't Take The Bait!

Verify Sender

Confirmsenderidentityindependently via phone or official channels.

Think Before Clicking

Avoidclickingsuspiciouslinksordownloading unknown attachments.

Use Strong Passwords & MFA

Createuniquepasswordsorpassphrases and enable Multi-Factor Authentication.

Report Suspicious Emails

Forwardpotentialphishingemailsimmediately to your IT/security team, e.g., phishing@yourcompany.com.

Keep Software Updated

Regularlyupdateoperatingsystems,browsers, and antivirus tools for protection.

Quiz Time: Test Your Phishing IQ

Scenario 1: Youreceive anemail from<PayPal=urgingyou toreset your password via a link. Is this phishing? (Yes/No) Why?

Scenario 2: A callerclaimingto be<BankSupport=asksfor yourfull card number and PIN for identity verification. Is this social engineering? (Yes/No) Why?

Scenario 3: The website *www.amazon-support.co.uk* requests your login details. Is this site fake? (Yes/No) Why?

Conclusion: Your Role in Cybersecurity

Youare theorganisation9s crucial first lineof defenceagainstcyber threats. Vigilance and awareness in identifying phishingattemptshelp safeguard sensitive data. Promptly reporting suspicious activities reduces potential damage. Continuous training is proven to decrease successful phishing attacks by up to 90%, making your participation vital in maintaining robust cybersecurity.