Phishing Awareness Training

CODE ALPHA

Essential skills to recognise and avoid online threats in your daily work

Candidate Name : Mohammed Zuoriki

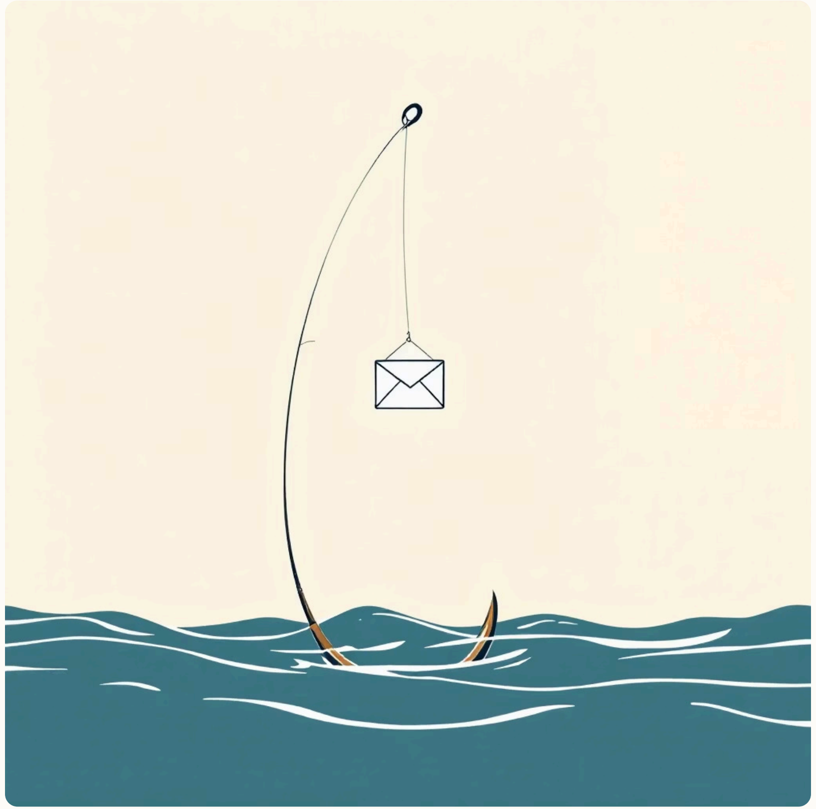
Candidate ID : CA/DF1/406

INTRODUCTION

What Is Phishing?

Phishing is a cyber attack where criminals disguise themselves as trustworthy sources to steal sensitive information such as passwords, credit card details, or personal data. These attacks typically arrive via email, text message, or fake websites.

Understanding phishing tactics is your first line of defence. In 2023, over 90% of successful data breaches began with a phishing email, making awareness absolutely critical for everyone.



Common Phishing Tactics

Email Spoofing

Attackers forge sender addresses to appear as colleagues, banks, or trusted companies.

Urgency & Fear

Messages create panic with threats of account closure, security breaches, or missed deadlines.

Too Good to Be True

Promises of prizes, refunds, or exclusive offers designed to bypass your critical thinking.

Malicious Links

Links directing to fake websites that harvest your login credentials or download malware.

Red Flags in Phishing Emails

□ **Generic greetings**

Legitimate companies use your name. Be wary of "Dear Customer" or "Valued User".

□ **Spelling and grammar errors**

Professional organisations proofread. Multiple mistakes indicate a scam.

□ **Suspicious sender addresses**

Check carefully : "support@amaz0n.com" isn't Amazon. Look for subtle misspellings.

□ **Unexpected attachments**

Never open attachments from unknown senders, especially .exe, .zip, or .scr files.

□ **Requests for sensitive information**

Banks and legitimate services never ask for passwords or PINs via email.

Recognising Fake Websites

URL Inspection

Always check the website address carefully. Phishing sites often use similar-looking domains with tiny variations.

- Look for HTTPS and the padlock icon
- Verify spelling exactly matches the official site
- Beware of extra characters or subdomains
- Check for certificate warnings in your browser

Example: "www.paypa1.com" uses the number "1" instead of the letter "l" a classic phishing trick.

SOCIAL ENGINEERING

Understanding Social Engineering Tactics

Social engineering exploits human psychology rather than technical vulnerabilities. Attackers manipulate emotions to bypass security measures.

Impersonation

Pretending to be IT support, executives, or trusted contacts to gain access to information.

Pretexting

Creating fabricated scenarios to build trust and extract sensitive data through seemingly legitimate requests.

Baiting

Offering something enticing free software, USB drives, or gift cards that contains malware or leads to compromise.

Real-World Phishing Examples

The CEO Fraud

An employee receives an urgent email appearing to be from the CEO, requesting an immediate wire transfer for a confidential acquisition. The email address was slightly altered, and the employee lost £50,000.

The Package Delivery Scam

A text message claims a package is waiting, with a link to track delivery. The link installs malware that steals banking credentials and personal information from the victim's phone.

The Microsoft Support Call

Attackers phone claiming to be from Microsoft, warning of a virus on your computer. They request remote access and then install ransomware or steal stored passwords.

Best Practices to Stay Protected

01

Verify before you click

Hover over links to preview the destination. When in doubt, navigate directly to the website rather than clicking email links.

02

Enable multi-factor authentication

Add an extra layer of security to your accounts. Even if credentials are stolen, MFA prevents unauthorised access.

03

Keep software updated

Install security patches promptly. Updated systems close vulnerabilities that attackers exploit.

04

Use strong, unique passwords

Employ a password manager to create and store complex passwords for each account.

05

Report suspicious activity

Forward phishing emails to your IT department immediately. Quick reporting helps protect colleagues.

06

Trust your instincts

If something feels wrong, it probably is. Take a moment to verify rather than rushing to respond.

Interactive Knowledge Check

Scenario Quiz

Scenario 1: You receive an email from "HR Department" asking you to verify your salary details by clicking a link and entering your employee ID and password.

Question: Is this legitimate?

> **Answer:** No. HR would never ask for passwords via email. This is a phishing attempt designed to steal credentials.

Scenario 2: A colleague sends you an email with an unexpected attachment labelled "Urgent_Invoice.zip". The message is brief and slightly unusual in tone.

What should you do?

> **Answer:** Don't open it. Contact your colleague through another channel (phone, instant message) to verify they sent it before opening any attachment.

Key Takeaways

1

Stay vigilant

Phishing attacks are constantly evolving. Maintain a healthy scepticism towards unexpected requests.

2

Verify everything

When in doubt, use alternative channels to confirm authenticity before taking action.

3

Report immediately

Quick reporting protects the entire organisation. Your IT team depends on your awareness.

Remember: You are the strongest defence against phishing attacks. By staying informed and cautious, you protect not only yourself but your entire organisation from cyber threats.