Phishing Awareness Training

Protect Yourself from Online Scams

Understanding the Threat: What is Phishing?

Phishing is a deceptive attempt to trick you into revealing sensitive information, such as usernames, passwords, and credit card details, often for malicious purposes. These attacks typically disguise themselves as a trustworthy entity in electronic communication.

Globally, phishing remains one of the most prevalent and damaging cybersecurity threats. Its sophisticated nature means it can bypass many traditional security measures, making human vigilance our most critical defence.

Spotting the Red Flags: Email Deception

Phishing emails often contain tell-tale signs. Learning to recognise these can prevent you from falling victim to a scam.

Suspicious Sender

Check the sender's email address carefully. Does it match the alleged organisation? Look for subtle misspellings or unusual domains.

Grammar and Spelling Errors

Professional organisations typically proofread their communications. Numerous errors are a strong indicator of a phishing attempt.

Urgent or Threatening Language

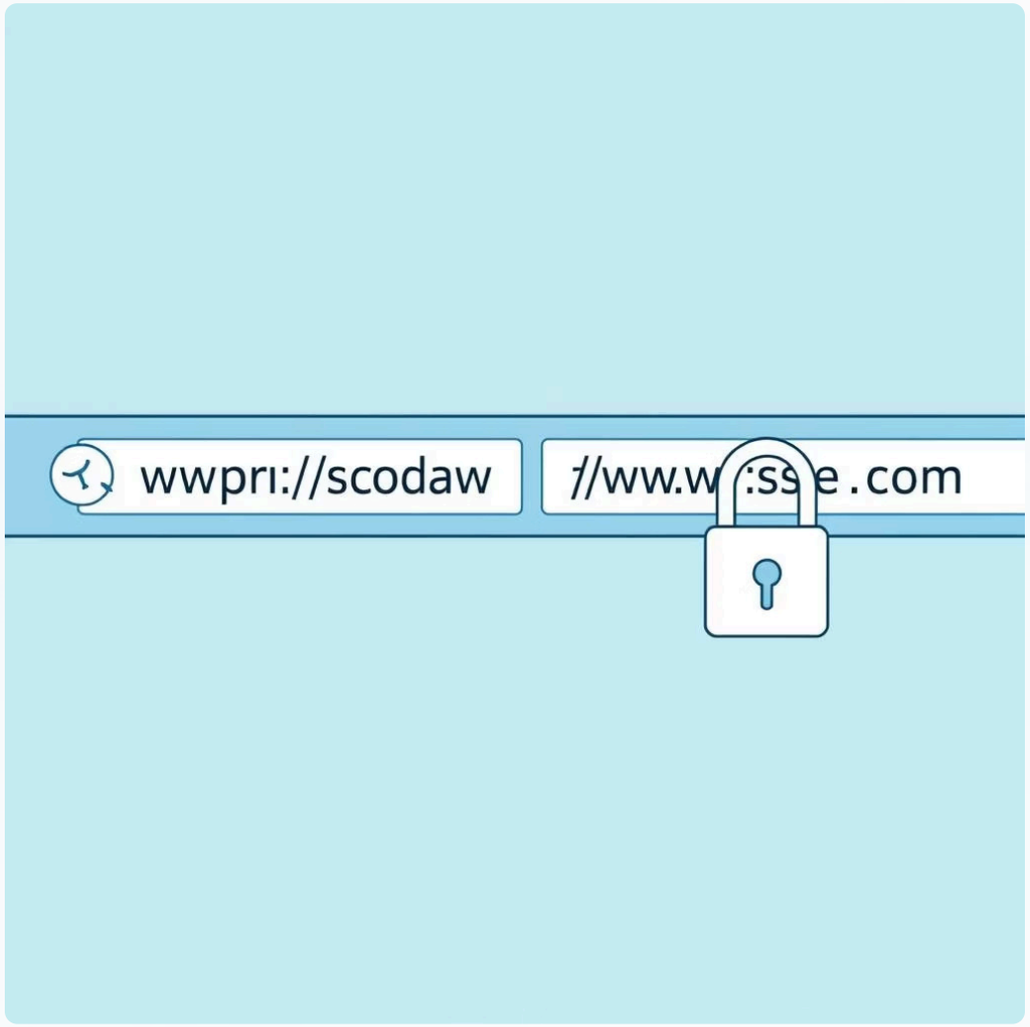
Attackers often create a sense of panic or urgency to prompt immediate action, such as threats of account closure or legal action.

Fake or Malicious Links

Hover over links without clicking to see the true destination URL. If it looks suspicious or doesn't match the expected site, do not click.

Navigating the Web: Identifying Fake Websites

Beyond emails, phishing attempts often lead to deceptive websites designed to steal your credentials.



URL Verification

Always manually type important URLs or use trusted bookmarks. Check for HTTPS in the address bar and a padlock icon, indicating an SSL certificate.

Lookalike Domains

Be wary of domains that are almost identical to legitimate ones (e.g., "Amaz0n.com" instead of "Amazon.com").

Fake Login Pages

Attackers replicate legitimate login pages to capture your credentials. Always ensure you are on the official site before entering any information.

The Human Element: Social Engineering

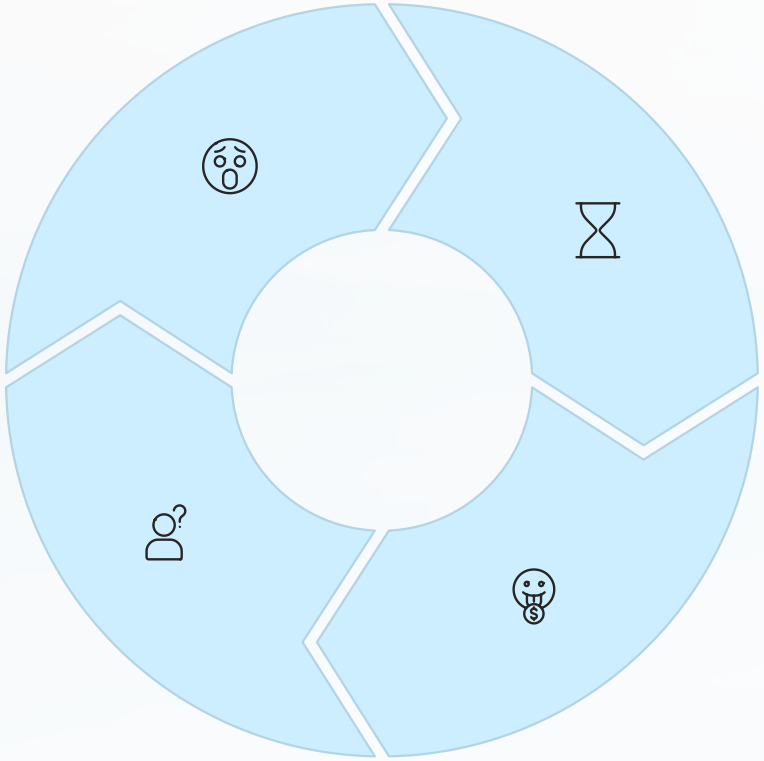
Phishing isn't just about technical tricks; it leverages psychological manipulation to bypass your critical thinking.

Fear & Intimidation

Threats of legal action, account suspension, or data loss push victims into hasty, irrational decisions.

Curiosity

Messages promising exclusive content, scandalous news, or unexpected information can entice clicks.



Urgency & Scarcity

Time-sensitive offers or warnings create pressure, preventing careful consideration of the message's legitimacy.

Greed & Opportunity

Appealing to financial gain (e.g., lottery winnings, investment opportunities) can lead individuals to overlook warning signs.

Your Shield: Best Practices for Digital Safety

Adopting these simple habits can significantly reduce your risk of falling victim to phishing attacks.

1

Verify Before You Click

Always confirm the sender's identity through an alternative, trusted method before engaging with suspicious emails or links.

2

Hover Over Links

Before clicking, hover your mouse over any hyperlink to reveal the actual destination URL. If it looks suspicious, don't click.

3

Avoid Unknown Attachments

Never open attachments from unknown or suspicious senders, as they often contain malware.

4

Enable Multi-Factor Authentication (MFA)

MFA adds an extra layer of security, making it significantly harder for attackers to access your accounts even if they steal your password.

Test Your Knowledge: Spot the Phish!

Let's put your newfound skills to the test. Can you identify the phishing attempts?

Scenario 1: Urgent Account Update

You receive an email from "service@paypall.com" stating your account will be suspended if you don't click a link to verify details immediately. What's wrong?

- Incorrect domain spelling.
- Sense of urgency and threat.

Scenario 2: Unexpected Package Delivery

An email from "DHL Express" (but the sender's address is a random Gmail account) informs you of a package delivery issue and asks you to download an attachment to resolve it. What's wrong?

- Mismatch between sender name and email address.
- Request to download an unexpected attachment.

Remember: Think Before You Click!

Phishing attacks are constantly evolving, but your awareness is the best defence.

Stay Alert:

Always be suspicious of unexpected communications, especially those requesting personal information.

Verify:

Confirm sender identities and website legitimacy through independent means.

Report:

If you suspect a phishing attempt, report it to your IT department immediately.

Your Vigilance Is Our Strongest Defence

Questions & Discussion

Thank you for your attention. We are now open for any questions you may have regarding phishing awareness and cybersecurity best practices.

Contact Support

Learn More