Phishing Awareness Training: Protect Yourself and Your Organisation

In an increasingly connected world, understanding and defending against phishing attacks is crucial for both personal and organisational security. This training will equip you with the knowledge to recognise and respond to these pervasive threats.

What is Phishing?

Deceptive Tactics

Cybercriminals employ fraudulent emails, websites, or phone calls to trick individuals into revealing sensitive information, often by impersonating trusted entities.

Criminal Objectives

The primary goals are to steal credentials such as passwords, financial data, or to secretly install malicious software (malware) onto your device.

Leading Cyber Threat

Phishing remains the number one cyber threat globally, responsible for delivering over **94%** of all malware via email. It's the most common entry point for cyberattacks.

The Human Factor: Social Engineering

Phishing attacks leverage **social engineering**, a manipulation technique that exploits human psychology rather than technical vulnerabilities.

Exploiting Personal Information

Attackers gather your personal details from social media platforms—like your name, workplace, and hobbies—to craft highly convincing and personalised messages.

Building False Trust

They design believable scenarios to manipulate you into trusting their deceptive communications, often preying on urgency, fear, or curiosity.

Common Impersonations

You might receive a fake email that appears to be from your bank, a colleague, or even a senior executive like your company's CEO, making it difficult to distinguish from genuine communication.

Understanding the Threat Landscape

Types of Phishing Attacks

Phishing comes in many forms, each designed to deceive you differently. Knowing the various types helps in recognising potential threats.

1

Spear Phishing

Highly targeted attacks using personalised information, accounting for **91%** of all phishing attempts.

2

Clone Phishing

Replicates legitimate emails but replaces genuine links with malicious ones to install malware.

3

Vishing

Voice phishing through phone calls, where attackers impersonate trusted sources to extract sensitive details.

4

Smishing

Phishing via SMS text messages, often containing urgent calls to action or deceptive links.

5

Whaling

Elite phishing attacks exclusively targeting high-profile individuals like senior executives with highly tailored messages.

Spotting a Phish: Key Warning Signs

Unexpected Urgency

Emails that are unsolicited, unexpected, or demand immediate action should raise your suspicion. Criminals often create a sense of panic.

Suspicious Links

Always hover your mouse cursor over links without clicking to reveal the true URL. Look for mismatched or misspelled domain names.

Poor Language Quality

Emails with grammatical errors, spelling mistakes, or awkward phrasing are strong indicators of a phishing attempt.

Mass Mailings

Check the recipient fields. Hidden or blanked-out fields often mean it's a mass email, not a personal communication.

Learning from Experience

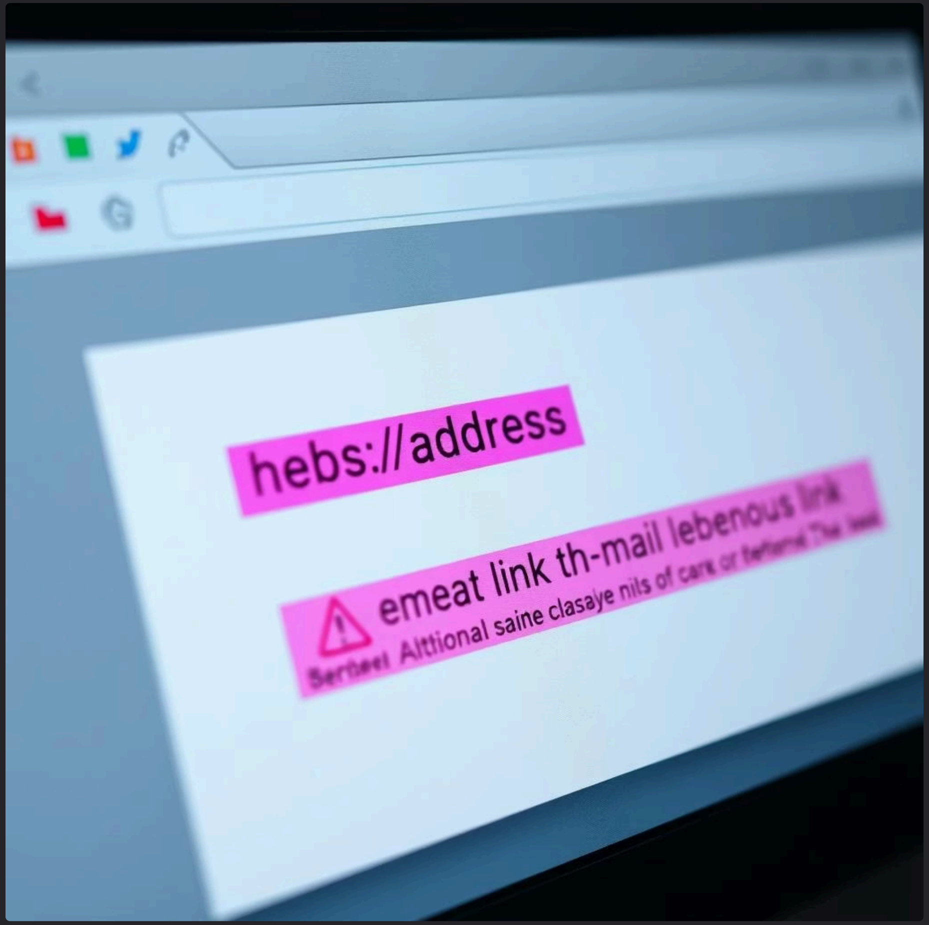
Real-World Example: Spear Phishing Attack

The Deception

Attackers sent a fake "email upgrade" notice, spoofing a legitimate university address. The email looked authentic, mimicking official branding and tone, designed to lure unsuspecting students and staff.

The Threat

The embedded link in the email led recipients to a malicious website designed to steal their login credentials or silently install malware. This compromise could lead to data breaches or system control.


hebs://address
emeat link th-mail lebenous link
Alltional saine clasaye nils of cark or

⚠ Key Lesson:

Always verify the sender's email address and question any unexpected requests for your credentials or personal information, even if they appear to be from a known source.

Protecting Yourself: Best Practices

Your active participation is key to a robust defence against phishing. Implement these practices into your daily digital routine.

Never Share Sensitive Data

Under no circumstances should you share passwords, bank details, or other sensitive personal information via email or phone calls.

Enable Two-Factor Authentication (2FA)

Utilise 2FA wherever possible. It adds an extra layer of security, making it much harder for attackers to gain access, even with a stolen password.

Keep Software Updated

Regularly update your operating system, applications, and antivirus software. Updates often include critical security patches that block new threats.

Verify Directly

If you receive a suspicious request, contact the purported sender directly using an **independently verified** phone number or email, never through links or contact details provided in the suspicious message itself.

Immediate Response Protocol

What to Do If You Suspect a Phish

01

Do NOT Engage

Do not click on any links or download any attachments from the suspicious email. Interacting with the content can compromise your device.

02

Report Immediately

Forward the suspicious email to your organisation's IT or security team. They have dedicated systems to analyse and mitigate potential threats.

03

Delete Message

Once reported, delete the suspicious message from your inbox and trash folder to prevent accidental interaction in the future.

04

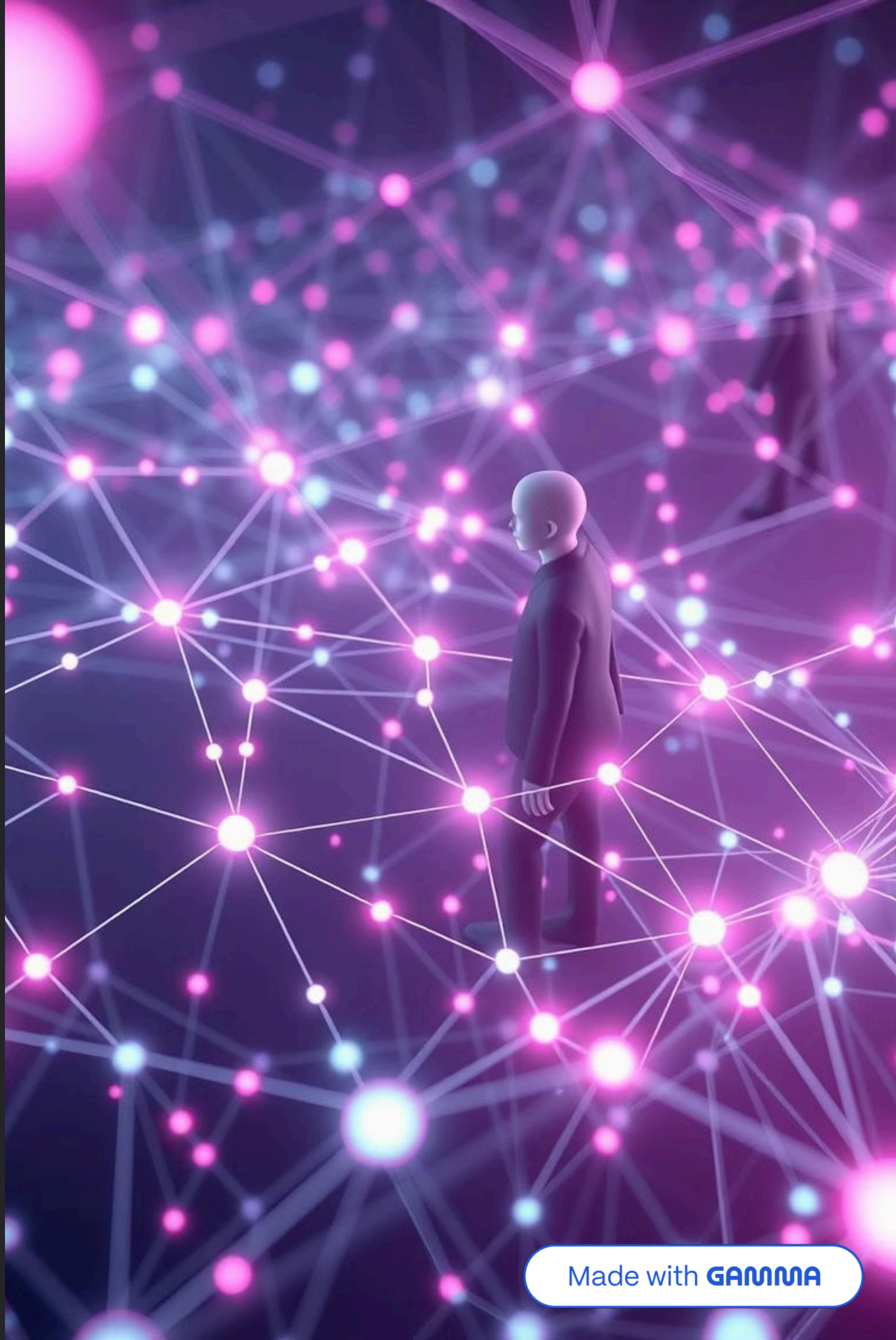
Change Passwords

If you suspect you may have inadvertently clicked a link or entered your credentials, change all relevant passwords immediately, especially for email and critical accounts.

Organisational Defence: Training & Technology

Beyond individual vigilance, robust organisational measures are crucial for a comprehensive defence against phishing attacks.

- **Regular Phishing Simulations:** Conduct periodic simulated phishing campaigns to test employee awareness and reinforce training.
- **Advanced Email Filtering:** Implement strong email filtering and anti-phishing software layers to block malicious emails before they reach inboxes.
- **Clear Verification Protocols:** Establish and communicate clear procedures for verifying payment requests or sensitive data transfers.
- **Continuous Awareness Updates:** Keep employees informed about the latest phishing tactics and evolving cyber threats through ongoing education.



Final Thought: Stay Vigilant, Stay Safe

1

Evolving Threats

Phishing attacks are constantly evolving. Your awareness and proactive actions are the most effective defence against new and emerging threats.

2

Collective Security

By remaining vigilant, you contribute significantly to protecting not just your own data and finances, but also the entire organisation's reputation and security.

3

Verify Before You Click

Remember this simple rule: **When in doubt, verify before you click.** A moment of caution can prevent a major incident.