Phishing Awareness Training

Stay Alert. Stay Secure.

Elevate your team's defense against evolving cyber threats.

Why Phishing Matters

Phishingposes acriticalthreat to organizations, leadingtofar-reaching consequences beyond initial compromise. Understanding these impacts is crucial for robust defense.

Financial Impact

Phishing leads to substantial monetary losses, covering direct theft, complex recovery operations, legal expenses, and heavy regulatory fines.

Data Breach Consequences

Compromised sensitive data erodes customer trust and can trigger severe penalties under strict global data protection laws like GDPR.

Reputational Damage

A successful phishing attack severely tarnishes an organization's brand, shattering customer and partner confidence, which is costly and difficult to restore.

Employee Vulnerability

Often the primary target, employees with insufficient awareness become entry points for attackers, compromising systems through human error and social engineering.

The Rising Threat of Phishing

Billions of Emails

Over 3.4 billion phishing emails are sent daily worldwide, creating a vast attack surface.

Massive Financial Losses

Phishing attacks led to an astounding **$50 billion** in losses globally just last year.

Widespread Success Rates

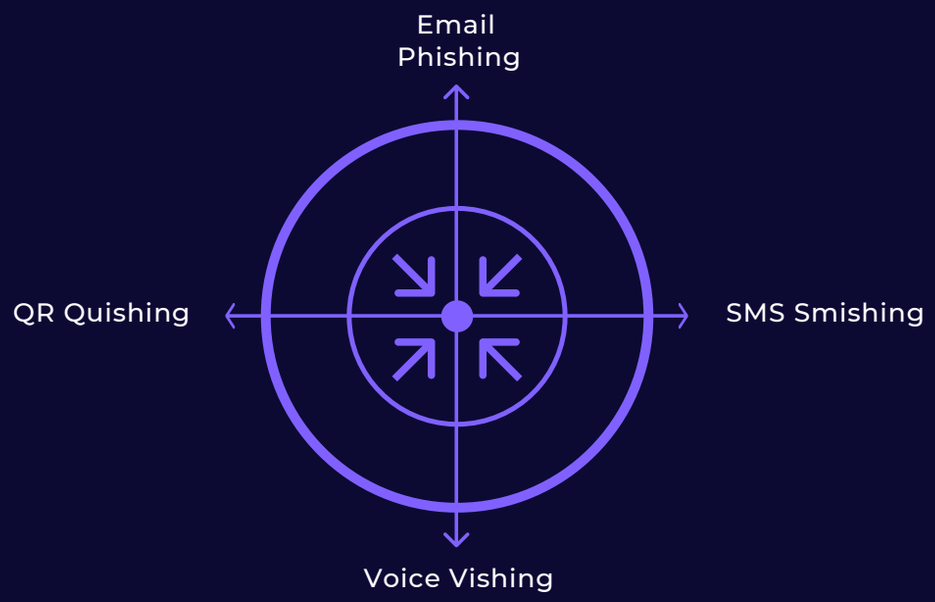
74% of organisations experienced successful phishing attacks in 2025.

Exploiting Current Events

Attackers cleverly exploit current events, like tax season or pandemics, to craft convincing scams.

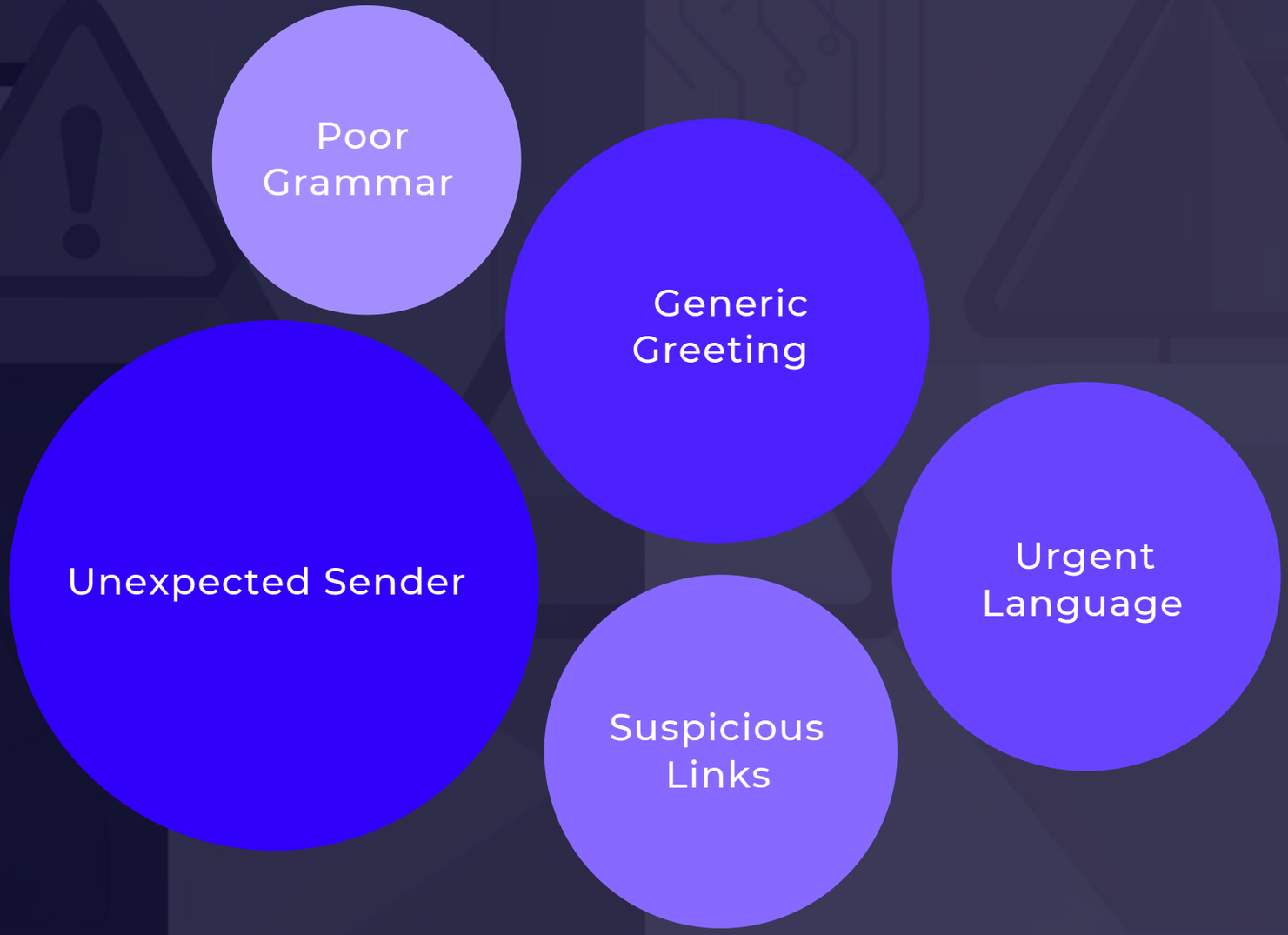
What Is Phishing?

Phishing involves fraudulent communicationsdesignedto trick individuals into divulging sensitive information or installing malicious software.

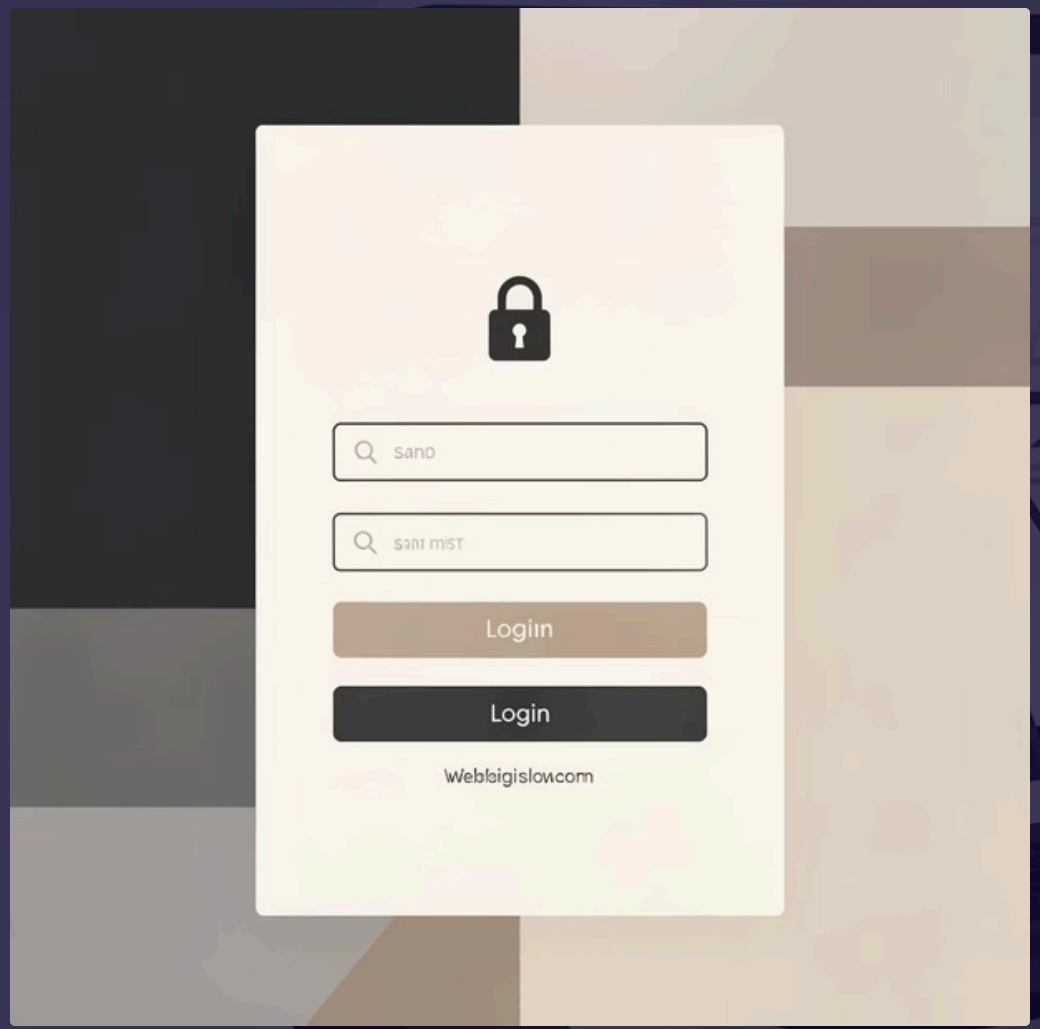


- Commonly targets login credentials, financial data, and confidential company secrets.
- Example: A fake invoice email demanding urgent payment, containing a link to a malicious site.

Recognising Phishing Emails: Key Red Flags



Spotting Fake Websites



- **Check the URL Carefully** Look for subtle misspellings, extra characters, or unusual subdomains in the website address.
- **HTTPS and Padlock Icon** Legitimate sites use HTTPS (secure connection) and display a padlock. However, attackers can sometimes obtain fake certificates, so this isn't a foolproof sign.
- **Poor Design or Quality** Shoddy design, low-resolution images, or inconsistent branding can be red flags.
- **Unexpected Redirection** If you are redirected to a login page unexpectedly, do not enter your credentials. Close the tab immediately.
- **Example: Fake Bank Login** A fake bank login page might perfectly mimic your bank's site but have a URL like "mybank-login.com" instead of "mybank.com".

Types of Phishing Attacks

Phishing isn'ta single threat;it'sadiversearrayoftactics.Understandingthese variants helps in recognizing and defending against specific attack vectors.

SpearPhishing

Highly personalized attacks leveraging specific information about an individual to gain trust.

Clone Phishing

Replicates legitimate, previously sent emails to swap links or attachments with malicious versions.

Whaling

A sophisticated spear phishing attack specifically targeting senior executives for high-value data or funds.

BEC (Business Email Compromise)

Impersonates executives or vendors to trick employees into fraudulent wire transfers or data disclosures.

Vishing

Voice phishing, where criminals use phone calls to manipulate victims into revealing sensitive information.

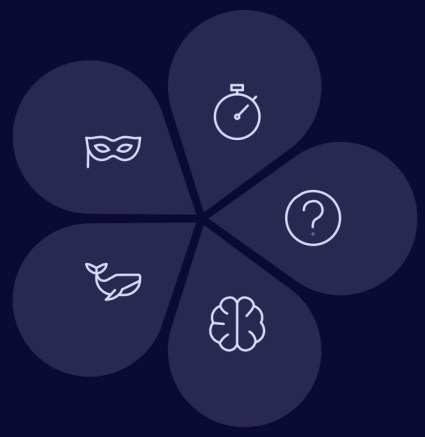
Social Engineering Tactics Attackers Use

Impersonation

Attackers pretendto be trusted individuals like your boss, colleagues, or vendors to gain your trust.

Urgency & Fear

They create a sense of panic or immediate threat ("Your account will be locked!") to bypass rational thinking.



Curiosity & Greed

Exploiting human nature with fake prize notifications or tempting offers to lure you into clicking.

Whaling Attacks

These are highly targeted phishing attacks aimed at senior executives, often involving urgent financial requests.

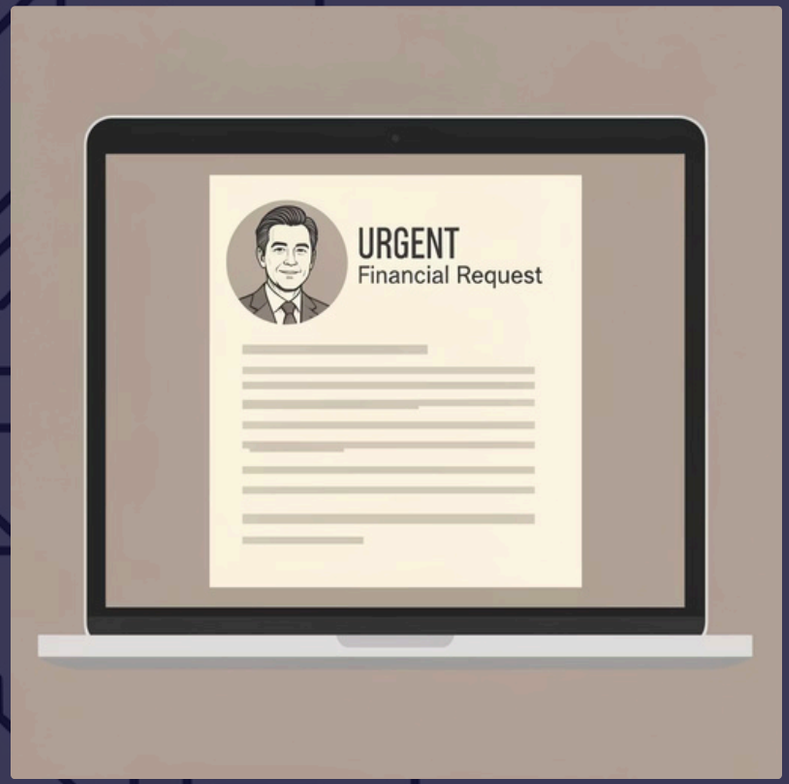
AI-Enhanced Scams

Sophisticated AI tools are now used to craft highly convincing, personalised, and grammatically flawless messages.

Real-World Example: The CEO Fraud Scam

TheCFO received an email, seemingly from the CEO, requestingan urgent wire transfer to an unfamiliar account. The email meticulously mimicked the CEO's writing style and language, showing no obvious signs of fraud.

- The attacker had likely researched the CEO's communication patterns.
- The email contained subtle cues to rush the transaction, preventing the CFO from thorough verification.
- Result: **£1.2 million** was transferred to the attacker's account before the scam was discovered, leading to significant financial loss and reputational damage.



Lesson Learned:

Always verify unusual or urgent financial requests through an alternative, trusted communication channel, such as a direct phone call or in-person conversation.

Best Practices to Avoid Phishing

1 **Verify Before Clicking**

Neverclickonlinksoropenattachments from unknown or unexpected senders.

2 **Separate Verification**

Alwaysverifyrequestsforsensitive information or payments using a separate communication channel (e.g., phone call).

3 **Multi-Factor Authentication (MFA)**

EnableMFAwhereverpossibletoaddanextralayer of security to your accounts.

4 **Keep Software Updated**

Ensureallyoursoftware,operatingsystems, and security tools are consistently updated.

5 **Report Suspicious Activity**

Immediatelyreportanysuspiciousemails or activities to your IT or security team.

6 **Regular Training**

Activelyparticipateinphishing simulations and ongoing awareness training.

What to Do If You Fall for a Phishing Attack

It can happen to anyone. If you suspect you've been compromised, taking these immediate steps can significantly mitigate the damage. Act quickly and don't hesitate to seek help.

01

Act Immediately

Change passwords for any compromised accounts. Enable Multi-Factor Authentication (MFA) everywhere possible.

02

Report the Incident

Notify your IT or security team immediately. Provide all relevant details about the phishing attempt.

03

Monitor Accounts

Scrutinize bank statements, credit reports, and other sensitive accounts for any suspicious or unauthorized activity.

04

Seek Support

Follow the guidance provided by your IT team. Remember, early reporting and action are crucial for effective recovery.

Interactive Quiz: Spot the Phish!

Quiz Question:

Whichof these emailtraits is a **phishing red flag**?

a) Personalised greeting

b) Urgent request for password reset

c) Email from known colleague's address

d) Proper company branding

Answer: b) Urgent request for password reset. Attackers use urgency to bypass your critical thinking.

Tools and Resources for Protection

Equipyourself withthe right toolsandknowledge tobuildarobustdefenseagainstphishingandothercyber threats. These resources are designed to help you stay secure online.

Email Security Software

These tools filter out malicious emails, spam, and phishing attempts before they reach your inbox.

Password Managers

Securely store unique, strong passwords for all your accounts, reducing the risk of credential theft.

Multi-Factor Authentication (MFA) Apps

Add an essential layer of security by requiring a second verification step, like a code from your phone.

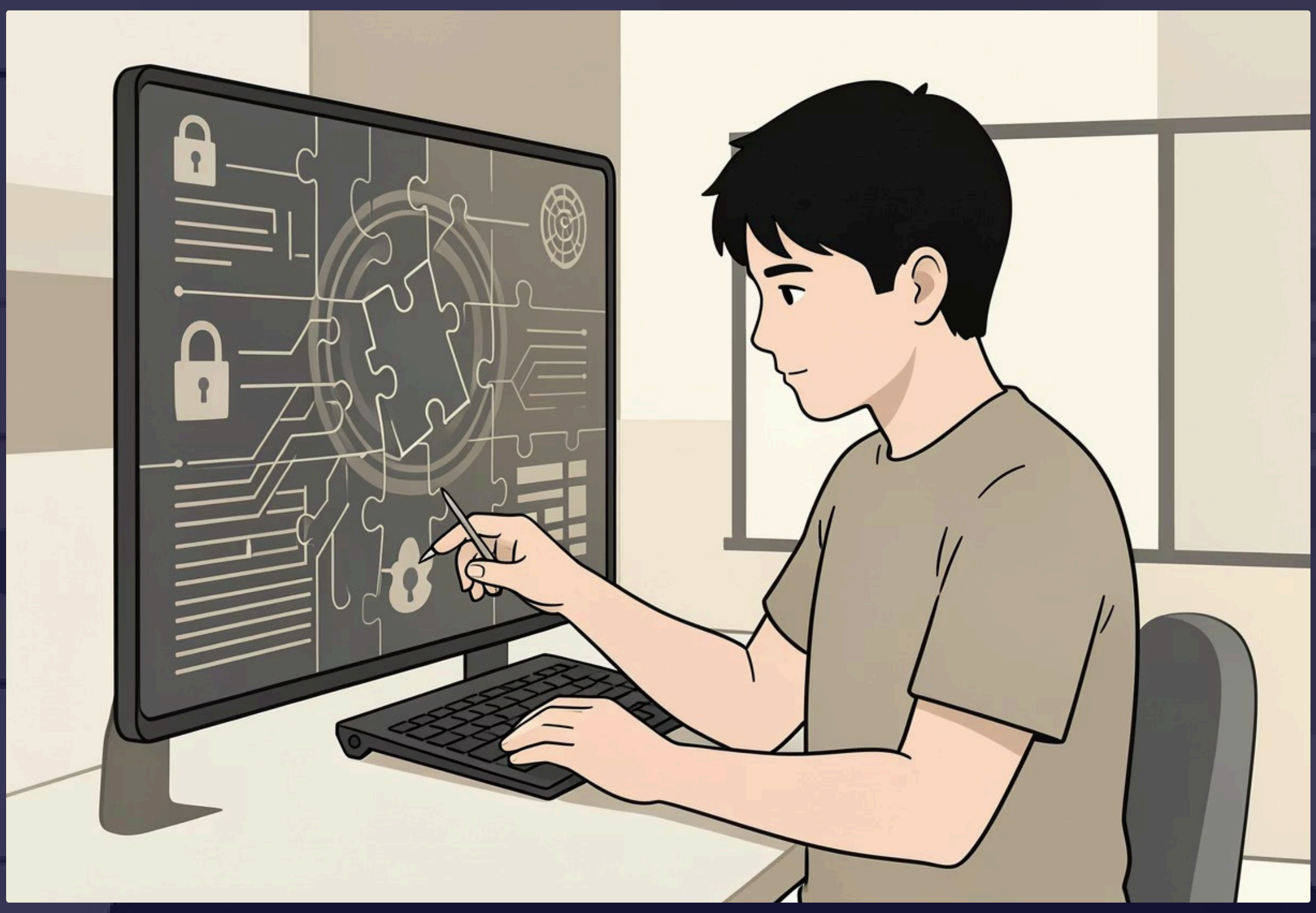
Security Awareness Training

Platforms offering interactive courses and simulations to help you recognize and respond to cyber threats.

Reporting Tools

Know how and where to report suspicious emails or incidents to your IT/security team immediately.

Interactive Quiz: Boost Your Phishing IQ!



Question 1: Identifying Phishing Emails

Whichof these is the strongest indicator that an email might be a phishing attempt?

- **a)** It includes your full name in the greeting.
- **b)** It contains a link to reset your password for an account you don't recognise.
- **c)** It comes from a well-known company you have an account with.
- **d)** The email has a professionally designed signature.

Answer: b) It contains a link to reset your password for an account you don't recognise. Unexpected requests, especially for credentials, are a major red flag.

Question 2: Spotting Fake Websites

You receive an email asking you to verify your bank account by clicking a link. Which URL is most suspicious?

- **a)** `https://www.yourbank.com`
- **b)** `https://secure.yourbank.com/login`
- **c)** `http://yourbank-verify.net`
- **d)** `https://customer.yourbank.co.uk`

Answer: c) `http://yourbank-verify.net` The lack of HTTPS and an unusual domain name are critical warning signs.

Question 3: Social Engineering Tactics

YourCEO sends anurgent email requesting a wire transfer to a new vendor. This is a common tactic known as:

- **a)** Baiting
- **b)** Whaling
- **c)** Quid Pro Quo
- **d)** Smishing

Answer: b) Whaling. This is a highly targeted phishing attack aimed at senior executives to manipulate them into actions like urgent financial transactions.

Question 4: Best Security Practices

Ifyou receive a suspicious email,what is the best immediate action to take?

- **a)** Click on any links to see where they lead.
- **b)** Reply to the sender asking for more information.
- **c)** Report it to your IT security team and delete it.
- **d)** Forward it to a colleague for their opinion.

Answer: c) Report it to your IT security team and delete it. Never interact with suspicious emails; always involve your security team.

Your Role in Cyber Defence

- Phishing remains the number one cyber threat, but it can be effectively mitigated through vigilance and awareness.
- Stay vigilant, always question unexpected messages, and promptly report any suspicious activity.
- Together, we can build a strong "human firewall" to protect our organisation from cyber threats.

Thank You!

Questions? Please feel free to ask.

Resources & Further Training

Thank You

For your commitment to cybersecurity awareness and building a stronger, safer digital environment together.

represented by : Poorna Sri A