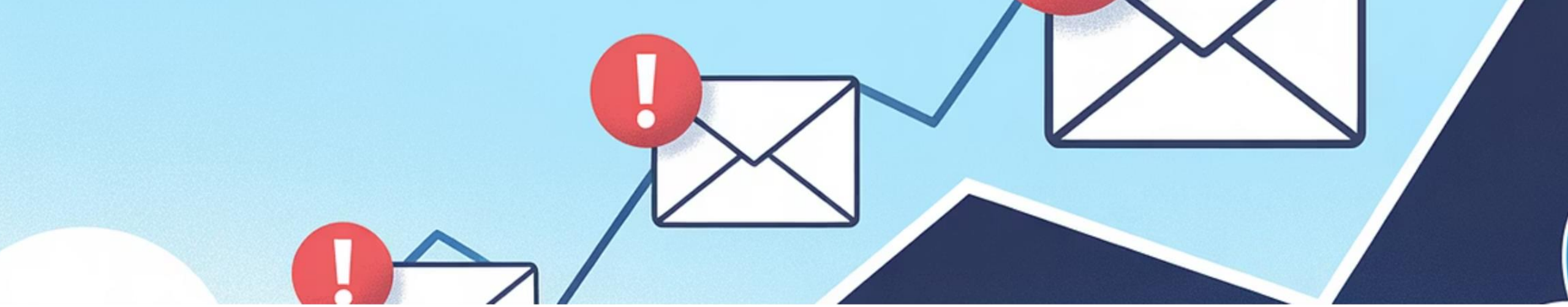
Phishing Awareness Training: Protecting Yourself and Your Organisation

Practical guidance and concise steps to recognise, report and stop phishing attacks — for every employee, on every device.



Why Phishing Matters: The Rising Threat

High volume

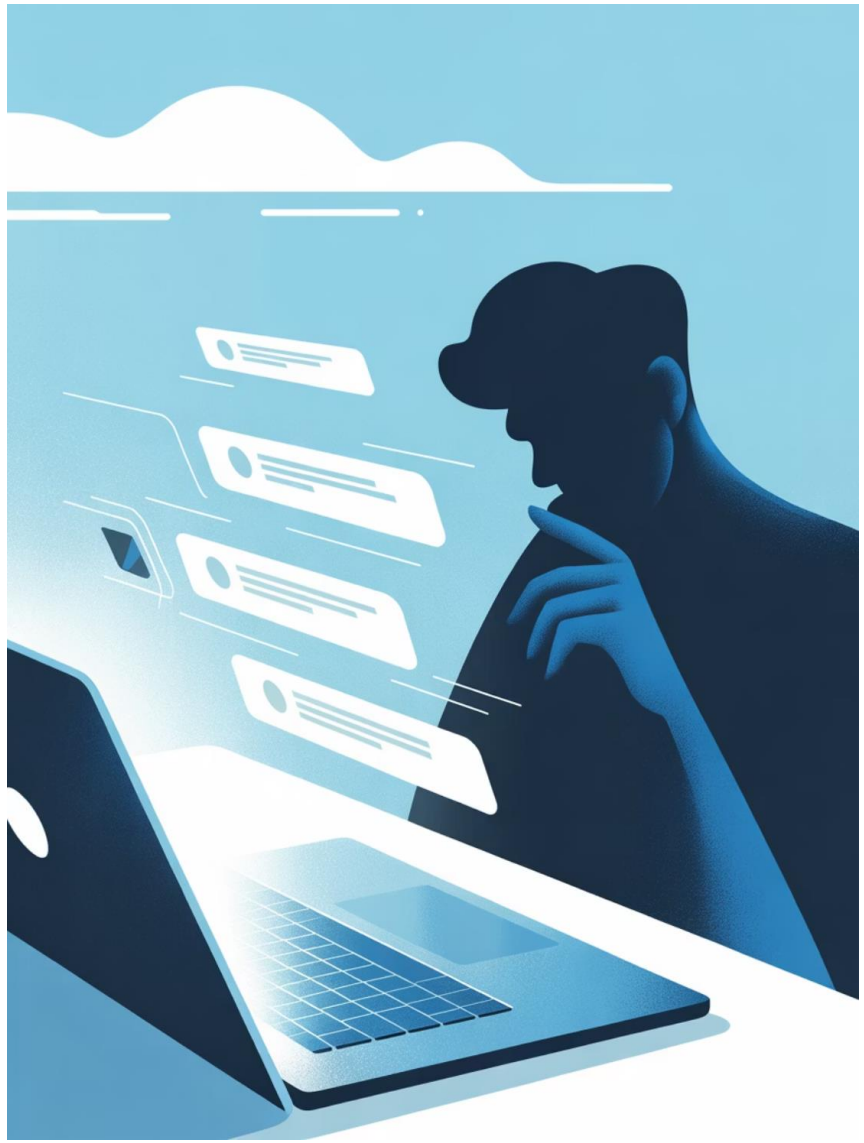
94% of malware is delivered via email (2025 data) — email remains the primary attack vector.

Costly impact

Business Email Compromise (BEC) losses reached $2.4B globally in 2025 — direct financial and reputational damage.

Real consequences

Historic incidents (e.g., Colonial Pipeline) show how a single phishing entry point can disrupt critical services.



What is Phishing?

Phishing is social engineering where fraudsters impersonate trusted sources to trick people into revealing credentials, financial details or installing malware. It appears via email, SMS (smishing), phone calls (vishing) and counterfeit websites that mimic legitimate services.

- Targets: passwords, card details, personal and corporate data
- Channels: email, SMS, voice calls, fake login pages

Modern Phishing Techniques: Beyond the Classic Email

BEC (Business Email Compromise)

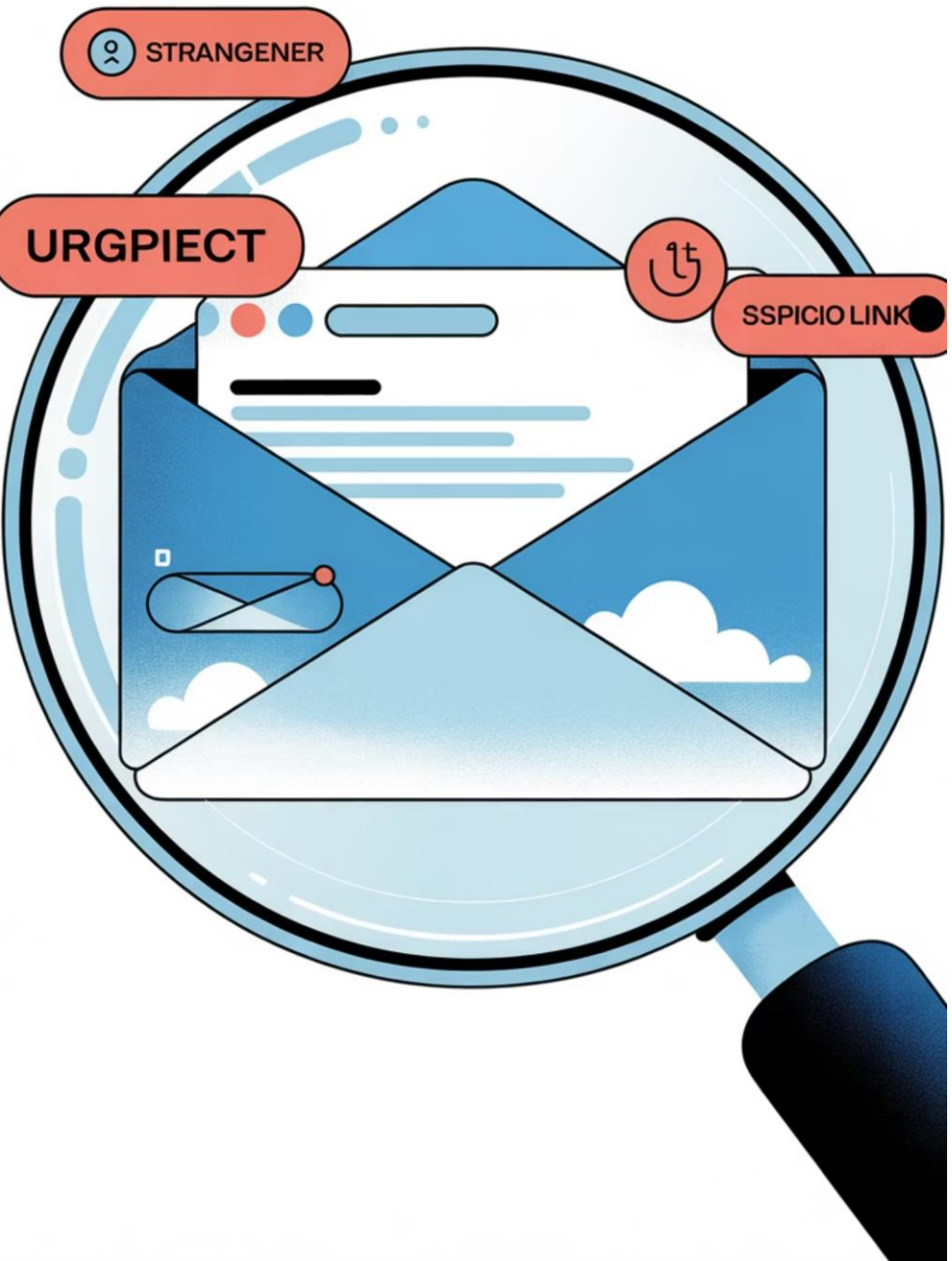
Attackers impersonate executives to request urgent transfers or confidential data — high high success when combined with authority authority pressure.

Phishing-as-a-Service

Pre-built kits on underground markets make attacks accessible to novice criminals, increasing frequency and variety.

AI-crafted messages

AI can generate highly convincing, grammatically flawless emails tailored to targets — making detection harder.



Spotting a Phishing Attempt: Key Key Red Flags

Urgency & pressure

Look for language demanding immediate action or threatening consequences — a classic classic manipulation tactic. tactic.

Suspicious sender

Check the full sender address (not just the display display name). Small domain changes or extra extra characters are giveaways.

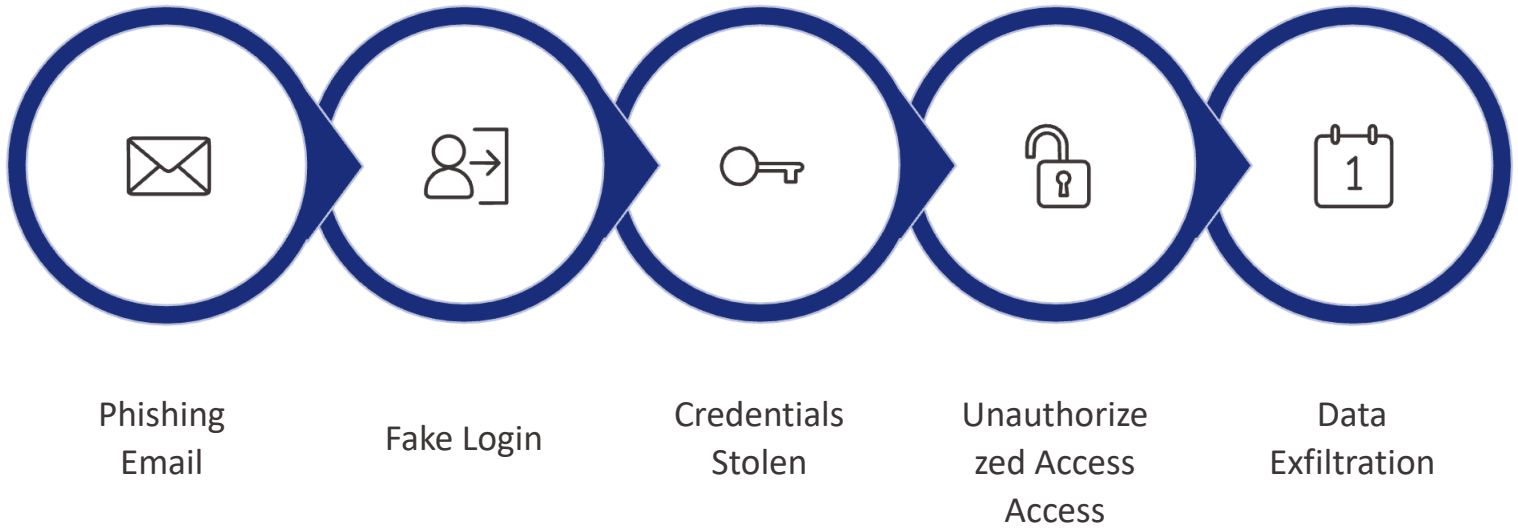
Formatting errors

Poor spelling, odd punctuation or inconsistent branding can can signal a fraudulent message.

Verify links

Hover over links (desktop) to reveal the destination URL; on mobile, press-and-hold and-hold links to preview. Never assume a link matches its visible text.

Real-World Example: Microsoft 365 Phishing Phishing Campaign



Attackers sent convincing login prompts prompts to thousands of users, harvesting credentials and gaining unauthorised access. Consequences Consequences included data exposure exposure and account misuse. The incident underscores the importance of importance of multi-factor authentication (MFA) and rapid reporting.

Enable MFA and report suspicious login prompts immediately — this stops stolen credentials from granting access.

Protecting Yourself and Your Organisation

Think before you click

Pause on unexpected messages. Verify via a separate channel (phone call, official app) before app) before acting on requests.

Verify & confirm

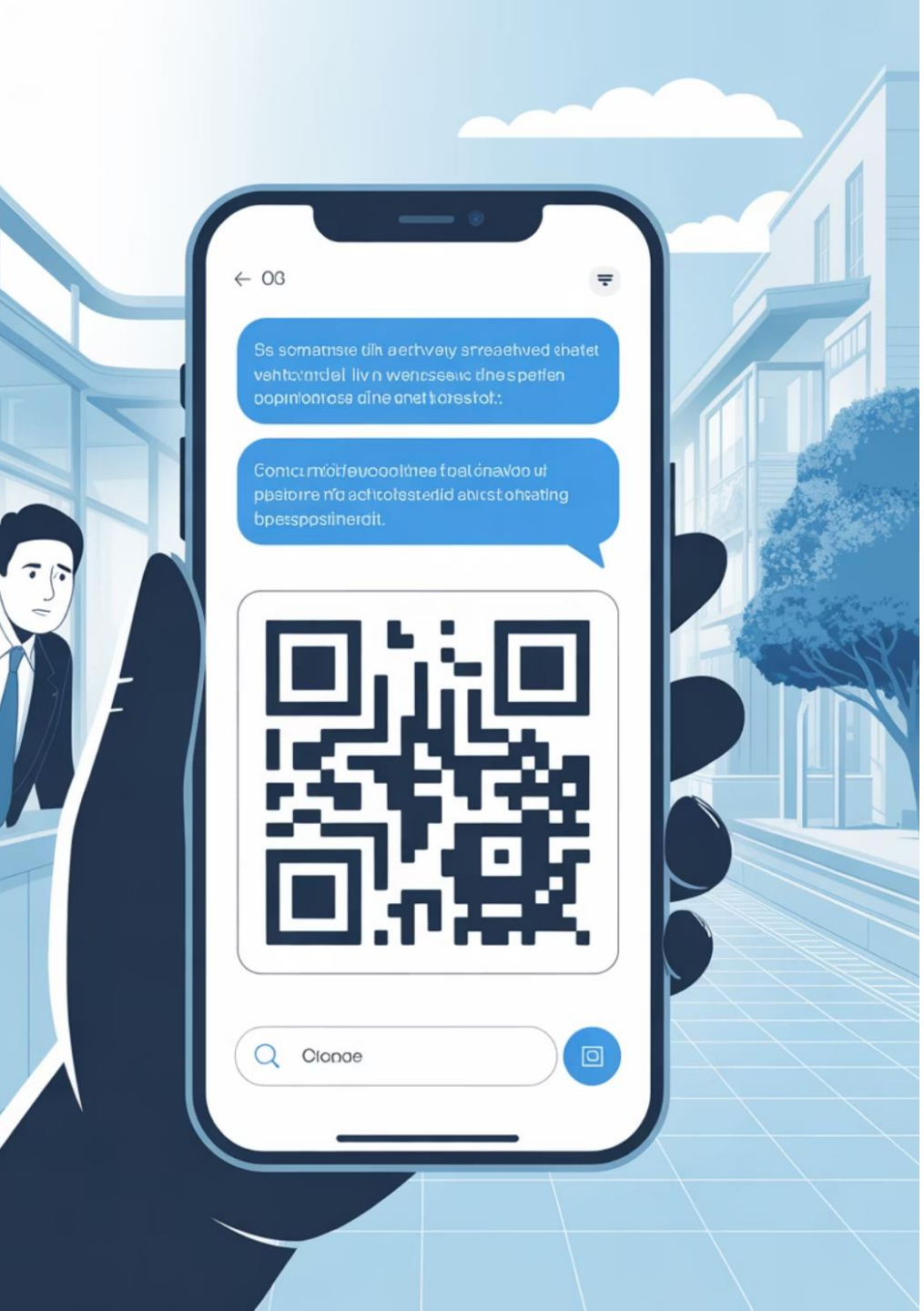
Contact the sender using known contact details rather than reply or using info in the in the suspicious message.

Use MFA & strong passwords

Enable multi-factor authentication everywhere and use a password manager for unique, complex credentials.

Report quickly

Report suspected phishing to IT/security immediately — rapid response limits damage and damage and accelerates containment.

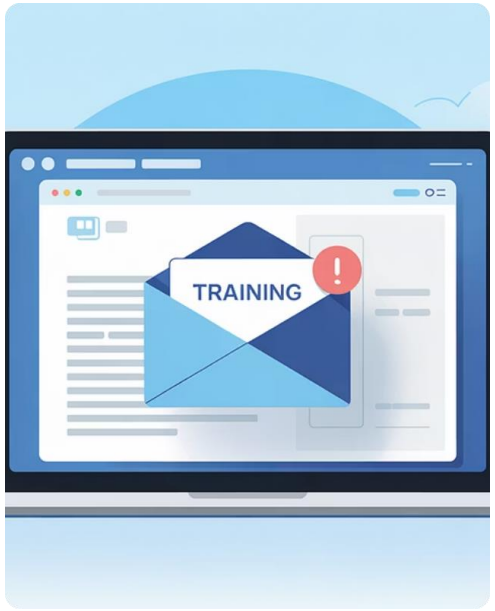


Phishing on Mobile Devices: Hidden Dangers

Small screens and truncated URLs make phishing harder to spot. SMS phishing (smishing), malicious QR codes (quishing) and deceptive app prompts are on the rise. Treat unexpected mobile messages with the same suspicion as email.

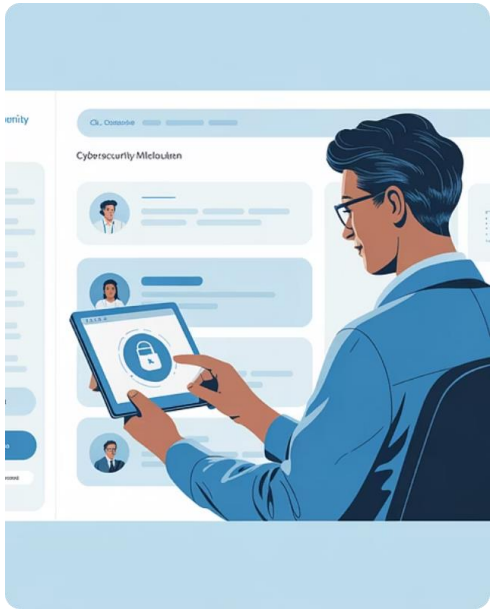
- Preview links carefully — avoid tapping unknown QR codes
- Check app store permissions and authenticity before installing
- Use device security features (screen lock, app vetting)

Training and Awareness: Your Best Defence



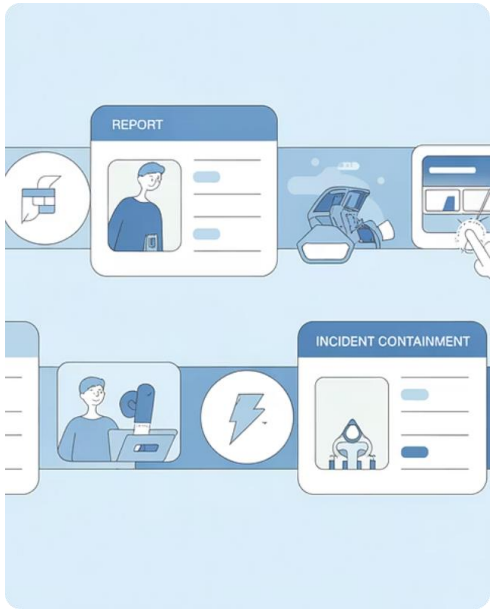
Simulated campaigns

Realistic phishing simulations train staff to recognise threats and measure readiness.



Regular microtraining

Short, frequent lessons keep skills fresh and awareness high — proven to reduce click rates substantially.



Clear reporting

Simple, well-advertised reporting procedures empower employees act quickly and reduce exposure.

Take Action Today:
Stay Vigilant, Stay Secure

Think before you click — pause and verify every unexpected message. message. Keep systems updated, enable MFA, and report suspicious suspicious activity. Build a culture where security is everyone’s responsibility. Together, we can stop phishing before it starts.

PROTECT

REPORT

RESPOND