Phishing Awareness Training Guide

Identify and report phishing emails, recognise red flags, and run simulation exercises. Build a human firewall with practical phishing awareness training for your team.

91%	3.4bn	Report	Free
ATTACKS START WITH EMAIL	PHISHING EMAILS SENT DAILY	DON'T DELETE REPORT IT	TRAINING GUIDE

1 Understanding Phishing

What phishing is, why it works, and why your team is the primary target.

Phishing is a social engineering attack that uses fraudulent emails, messages, or websites to trick people into revealing credentials, installing malware, or transferring money. It works because it exploits human psychology — urgency, authority, fear, and curiosity.

PHISHING TYPE	METHOD	TARGET	EXAMPLE
Mass phishing	Generic emails to thousands	Anyone	'Your account has been suspended, click here to verify'
Spear phishing	Targeted email to specific person	Named individual	'Hi Sarah, please review the attached invoice from our meeting'
Whaling	Targeting senior executives	CEO, CFO, Directors	'Urgent: board papers attached for tomorrow's meeting'
Smishing	SMS text message	Mobile phone users	'HMRC: You are owed a tax refund. Claim here: [link]'
Vishing	Voice phone call	Anyone	'This is your bank's fraud team, we need to verify your identity'
BEC	Impersonating a colleague	Finance, HR, PA	'Can you process this payment urgently? I'm in a meeting'

2 How to Spot a Phishing Email

Train your team to recognise these common red flags in suspicious emails.

- **Check the sender address:** Hover over the sender name. Does the email address match the claimed sender? Look for subtle misspellings (e.g., @micr0soft.com, @amaz0n.co.uk).
- **Urgency and pressure:** 'Your account will be closed in 24 hours', 'Immediate action required', 'Failure to respond will result in...' Legitimate organisations rarely demand immediate action.
- **Generic greetings:** 'Dear Customer', 'Dear User', 'Dear Sir/Madam' instead of using your actual name.
- **Suspicious links:** Hover over any link (do not click) to see the real destination URL. Does it go to the expected domain? Look for lookalike domains (e.g., paypa1.com instead of paypal.com).
- **Unexpected attachments:** Were you expecting this file? Is the file type suspicious (.exe, .zip, .js, .scr)? Even Office documents can contain malicious macros.
- **Requests for sensitive information:** No legitimate organisation will ask for passwords, PINs, or full bank details by email.
- **Grammar and spelling:** While improving, many phishing emails still contain unusual phrasing, grammar errors, or inconsistent formatting.
- **Too good to be true:** Unexpected refunds, prizes, inheritance, or unbelievable offers are almost certainly scams.

When in Doubt, Do Not Click

If you are even slightly unsure about an email, do not click any links or open any attachments. Report it to your IT team using the report phishing button or by forwarding to your IT helpdesk. It is always better to report a legitimate email than to click a malicious one.

3 Running Phishing Simulations

Test your team's resilience with simulated phishing campaigns.

Phishing simulations are a critical component of security awareness. They measure your organisation's susceptibility, identify users who need additional training, and reinforce the lessons from classroom training.

- **Tools:** KnowBe4, Proofpoint Security Awareness, Microsoft Attack Simulator (included in M365 E5/Defender P2)
- **Frequency:** Run simulations at least quarterly. Vary the difficulty and style each time.
- **Progression:** Start with obvious phishing emails, then increase sophistication to targeted spear phishing.
- **Metrics to track:** Click rate, report rate, credential submission rate. The goal is to reduce click rate below 5% and increase report rate above 70%.
- **Follow-up:** Users who click should receive immediate training (not punishment). Focus on education, not blame.

SIMULATION TYPE	DIFFICULTY	EXAMPLE LURE	EXPECTED CLICK RATE (TRAINED STAFF)
Generic phishing	Easy	Account suspension notice	< 5%
Brand impersonation	Medium	Microsoft password expiry	< 10%
Internal impersonation	Hard	IT department security update	< 15%
Spear phishing (personalised)	Very hard	CEO requesting urgent help	< 20%

4 Building a Security Culture

- **Make reporting easy:** Install the 'Report Phishing' button in Outlook. Make the helpdesk email address visible. Thank people who report.
- **Celebrate reporters:** Publicly acknowledge staff who report phishing (without naming those who clicked).
- **Regular reminders:** Short monthly tips via email or Teams. Rotate topics: phishing, passwords, social engineering, physical security.
- **New starter training:** Include phishing awareness in the onboarding process on day one.
- **Board reporting:** Report phishing simulation results to senior management quarterly. This demonstrates due diligence and supports the case for security investment.

UK-Specific Threats to Highlight

Remind staff about UK-specific phishing lures: HMRC tax refund scams, NHS appointment messages, Royal Mail delivery notifications, TV Licensing threats, and energy company billing scams. These are used because they are relevant and timely.

Notes

Need Security Awareness Training?

We deliver engaging security awareness training and run phishing simulations to build your organisation's human firewall.

info@cloudswitched.com

New London House, 6 London St, London EC3R

© 2026 CloudSwitched Limited. All rights reserved. This resource is provided for informational purposes and does not constitute professional IT advice.