CLOUDSWITCHED

FREE RESOURCE — TRAINING GUIDE

# Phishing Awareness Training

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 | 4 | 8 |
|---|---|---|---|
| ATTACKS START WITH EMAIL | PHISHING EMAILS SENT DAILY | TRAINING SECTIONS | RED FLAGS TO SPOT |

EMAIL SECURITY · SOCIAL ENGINEERING · SIMULATIONS · CULTURE


| PREPARED FOR | PREPARED BY | VERSION | FORMAT |
|---|---|---|---|
| Cloudswitched Knowledge Library | Cloudswitched Ltd. | 2026 Edition | Read-only PDF |

# 01

# Understanding phishing

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. The technical defences (filters, EDR, MFA) catch most of it; the rest depends on people knowing what to look for.

**91%**
OF CYBER ATTACKS BEGIN WITH EMAIL

**3.4bn**
PHISHING EMAILS SENT EVERY DAY

**Report**
DON'T DELETE — REPORT IT TO IT

## The six phishing variants your team will meet

| TYPE | METHOD | TARGET | TYPICAL LURE |
|---|---|---|---|
| **Mass phishing** | Generic emails to thousands | Anyone | *"Your account has been suspended — click here to verify."* |
| **Spear phishing** | Targeted email to a 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 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."* |

### WHY YOUR TEAM IS THE TARGET

Modern email gateways and endpoint protection stop the vast majority of malicious traffic. Attackers know this, so they target the one part of the stack that is hardest to patch — people. Phishing remains profitable because it only has to work once, and one click can be enough.

# 02

# How to spot a phishing email

Train your team to recognise these eight red flags. Most phishing emails carry more than one — the more you see together, the more confident the call.

**Check the sender address.** Hover over the sender name. Does the email address match the claimed sender? Look for subtle misspellings such as `@micr0soft.com` or `@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 instant action.

**Generic greetings.** “Dear Customer”, “Dear User”, “Dear Sir/Madam” instead of your actual name — a sign the sender does not know who they are emailing.

**Suspicious links.** Hover over any link (do not click) to see the real destination URL. Does it go to the expected domain? Watch for lookalike domains like `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 carry malicious macros.

**Requests for sensitive information.** No legitimate organisation will ask for passwords, PINs, or full bank details by email — ever.

**Grammar and spelling.** While improving, many phishing emails still contain unusual phrasing, grammar errors, or inconsistent formatting that does not match the brand.

**Too good to be true.** Unexpected refunds, prizes, inheritance, or unbelievable offers are almost certainly scams. If you weren’t expecting it, treat it as suspicious.

### 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 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.

# 03

# Running phishing simulations

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 sessions. Classroom training alone does not change behaviour — testing does.

**Tools.** KnowBe4, Proofpoint Security Awareness, and Microsoft Attack Simulator (included in M365 E5 / Defender for Office P2) are the most widely used UK SME platforms.

**Frequency.** Run simulations at least quarterly. Vary the difficulty, the lure style, and the target groups each time so the campaign cannot be predicted.

**Progression.** Start with obvious phishing emails to set a baseline, then increase sophistication over time — brand impersonation, internal impersonation, then targeted spear phishing.

**Metrics to track.** Click rate, report rate, and 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, focused training — not punishment. Education changes behaviour; blame just makes people hide their mistakes.

## Sample simulation programme

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

**EDUCATION, NOT BLAME**

The aim of a simulation is to find out where the gaps are, not to punish individuals. Pair every click with a short, targeted micro-lesson on the specific tactic that caught the user. Repeat clickers get more practice; everyone else gets a quick refresher.

# 04

# Building a security culture

Tools and policies on their own do not stop phishing. A team that knows what to look for, feels safe reporting, and gets a steady drip of reminders is the difference between a near-miss and a 72-hour ICO notification. These five habits are the foundation of a healthy security culture.

**Make reporting easy.** Install the *Report Phishing* button in Outlook. Publish the helpdesk email address everywhere. Thank people who report — a quick reply matters more than a poster on the wall.

**Celebrate reporters.** Publicly acknowledge staff who report phishing (without naming those who clicked). Reporting culture is built by recognition, not lectures.

**Regular reminders.** Short monthly tips via email or Teams. Rotate topics — phishing, passwords, social engineering, physical security — so awareness stays current.

**New starter training.** Include phishing awareness in the onboarding process on day one, before the new joiner has a live mailbox to make mistakes with.

**Board reporting.** Report phishing simulation results to senior management quarterly. This demonstrates due diligence and supports the case for security investment at budget time.

### UK-SPECIFIC LURES TO HIGHLIGHT

Remind staff about the lures attackers know UK targets respond to: **HMRC tax refunds**, **NHS appointment messages**, **Royal Mail delivery notifications**, **TV Licensing threats**, and **energy company billing scams**. These hit hardest because they feel relevant and timely — use real examples in every session.

CLOUDSWITCHED

CYBERSECURITY & AWARENESS TRAINING

**info@cloudswitched.com**

New London House, 6 London St
London EC3R 7LP · United Kingdom