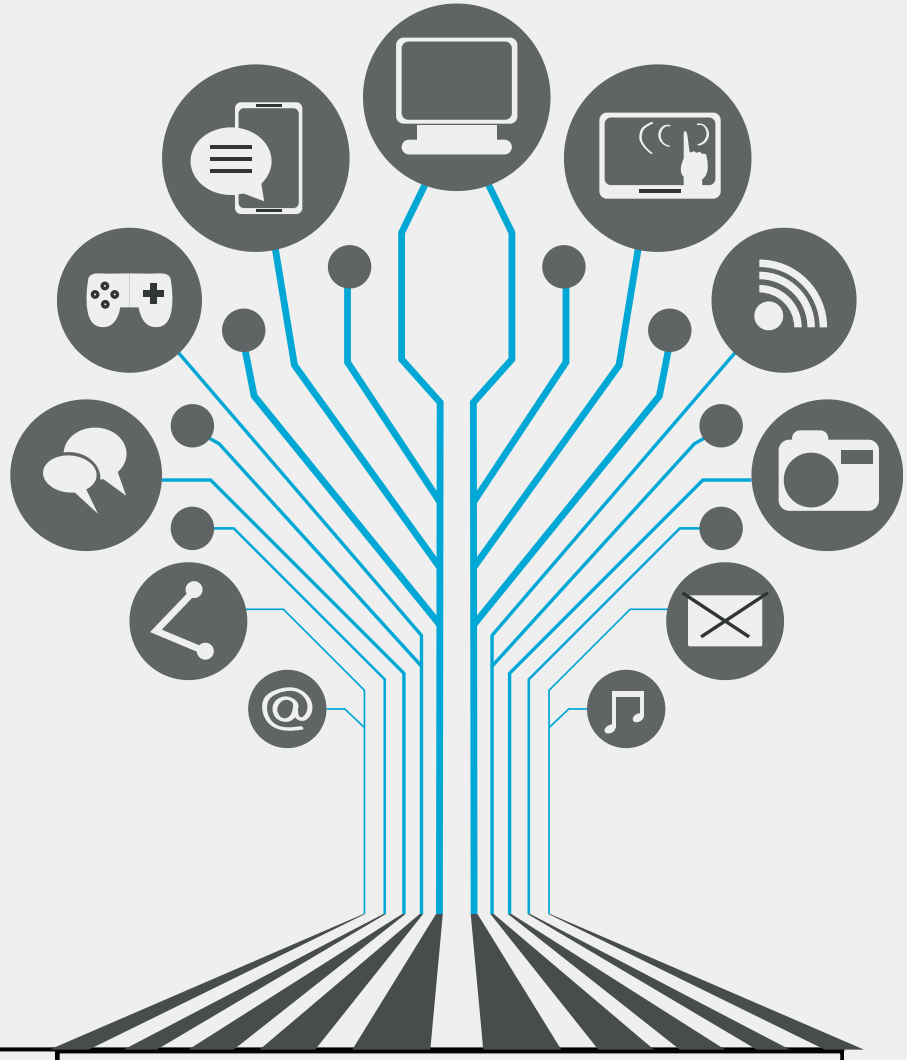
CYBER

THE SOCIAL ENGINEERING AWARENESS TOOLKIT

Think Like a Hacker



Your Quick-Start Guide to Building a Human Firewall Against Phishing, Vishing, and Impersonation

Prepared by: OxCyber Team

Date: November 2025

SECTION 1:
THE PSYCHOLOGY OF THE ATTACK
The Core Problem: The Human Element

No matter how advanced our firewalls are, the human element remains the easiest way in. Social engineering exploits trust, not code.

According to the UK Government's Cyber Security Breaches Survey 2025, **84% of organisations reported being targeted by phishing attempts in the past year,** confirming that most attacks begin by tricking an employee rather than breaching a system.

The Four Hacker Triggers

Hackers exploit emotion, not software. Their goal is to make you act before you think.

- **Urgency or Fear:** Threats of account suspension or job loss that pressure you to act fast.
- **Authority:** Messages pretending to come from a CEO, IT administrator, or regulator demanding immediate action.
- **Curiosity or Greed:** "You've won a reward" or "See attached confidential document."
- **Familiarity or Liking:** Emails that appear to come from trusted contacts, partners, or known brands to lower your guard.

Understanding these triggers is your first defence against manipulation.

SECTION 2:
PRINTABLE PHISHING RED FLAGS

CYBER

Category	Red Flag Indicators	Action to Take
Source & Address	❌ Sender email is slightly misspelled or from a free domain (e.g., @gmal.com).	Do not reply.
	❌ Link text does not match the actual destination URL (hover to check).	Do not click.
Content & Tone	❌ Subject lines like “FINAL WARNING” or “IMMEDIATE ACTION.”	Pause and verify.
	❌ Requests for passwords, payments, or personal data.	Never comply.
	❌ Poor grammar, spelling errors, or distorted logos.	Report it.
Attachments	❌ Unexpected ZIP, ISO, or macro-enabled files (e.g., .docm).	Do not open.
Your Instincts	❌ “Too good to be true” offers or prizes.	Trust your gut.
	❌ Messages that feel odd or out of character for the sender.	Call to confirm.

Print this checklist and share it across your organisation or classroom. It takes seconds to scan but can prevent serious damage.

SECTION 3:
SELF-TEST: ARE YOU VULNERABLE?

Answer honestly. Give yourself 1 point for every "Yes."

#	Question	Yes	No
1	**Do you ever click a link without checking where it leads?**	☐	☐
2	**Do you reuse passwords for personal and work accounts?**	☐	☐
3	**Would you act on an urgent email from your "CEO" without confirming verbally?**	☐	☐
4	**Have you ever entered credentials after a random pop-up warning?**	☐	☐
5	**Do you share project details or team information on social media?**	☐	☐
6	**Do you ignore software update reminders?**	☐	☐

Your Human Firewall Score:

- *0–1 Points: Vigilant – strong instincts, keep them sharp.*
- *2–3 Points: Moderate Risk – review the red flags and slow down before you click.*
- *4+ Points: High Risk – your habits make you a target. Start applying the action plan today.*

SECTION 4:
BUILDING YOUR HUMAN FIREWALL (ACTION PLAN)

This is not about paranoia. It is about preparation.

CYBER

1. MASTER THE 3-SECOND VERIFICATION RULE

STOP before clicking or replying to urgent messages.
LOOK at the sender's real address, not just the display name.
HOVER over links to confirm they lead to legitimate sites. If unsure, delete or report.

2. VERIFY OUT-OF-BAND (THE GOLDEN RULE)

If a request involves money, data, or credentials, never reply to the same email thread.
Call the person directly using a verified number or start a new chat to confirm authenticity.

3. ENABLE MFA EVERYWHERE

Multi-Factor Authentication (MFA) blocks over 99% of automated attacks, according to Microsoft research. Enable it on all professional and personal accounts.

4. REPORT, DON'T DELETE

If something looks suspicious, report it immediately. Security teams can analyse and block threats for everyone else.

5. SECURE YOUR DIGITAL FOOTPRINT

Avoid sharing details like "My boss is away this week" or "Our project launches Monday."
Hackers use small details to create convincing, targeted messages.

FINAL NOTE

Cybersecurity is a team sport. Awareness turns individuals into defenders. By training your instinct and learning to pause before you act, you are already one step ahead of the attacker.

Let's make social engineering harder, one smart click at a time.

CYBER

www.oxcyber.org

hello@oxcyber.org

+44 7443 449 811

JOIN THE MOVEMENT

Not everything that is valuable comes free, but our membership does.
Be part of a growing community of cybersecurity professionals across the Thames Valley.
Share insights, access resources, and help strengthen our region's cyber resilience.

🔗 Do not let this opportunity pass you by. Join OxCyber today.

JOIN NOW ›