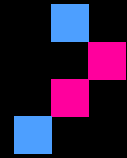


Phishing

Awareness Toolkit



Initial
TECH

Overview

This toolkit helps organisations teach staff to spot, report, and avoid phishing attacks. It includes quick wins, checklists, reporting steps, and training ideas.

How to use this toolkit

- 1) Share the Spot-the-Phish tips with staff.
- 2) Run monthly phishing simulations.
- 3) Use the reporting steps if someone clicks.
- 4) Track progress in the Action Plan.

Quick Wins

- Stop. Check. Protect. before clicking links or opening attachments.
- Turn on MFA for email and key accounts.
- Keep software updated.
- Use a password manager.
- Report suspicious messages to IT.

Spot-the-Phish: What to look for

- Check sender address carefully.
- Hover over links before clicking.
- Beware urgency or scare tactics.
- Unexpected attachments or requests for sensitive info.
- Payment changes – always verify out-of-band.

If you clicked a suspicious link

- 1) Disconnect from the network.
- 2) Change passwords and enable MFA.
- 3) Run antivirus scan.
- 4) Report to IT and provide details.

How to report

- Forward suspicious emails to IT/security team.
- Report scams to Scamwatch and incidents to ReportCyber.

Action Plan

Action	Owner	Due Date	Status