THE CYBER RESILIENCE CENTRE FOR LONDON

Training your Staff

Cyber criminals target staff to gain access to your organisation's resources and data.

Train staff to spot fraud and understand cyber security best practices so they can avoid falling victim. Document expectations of staff behaviour when using work equipment in policies. Staff can be your strongest asset for resilience and positively contribute to the organisation's success if they are trained appropriately and provided with the tools needed to comply with organisation procedures.

Train Staff about Social Engineering (Fraud)

Social engineering (known as fraud) manipulates a victim into actioning a request, including but not limited to clicking a link, opening an attachment, providing login credentials and paying an invoice. Should staff action the request this can lead to malware infection (such as ransomware), disruption to business, data loss, monetary loss, reputational damage, account takeover and much more. Train staff to spot common signs of fraud to avoid these repercussions - there are lots of free training resources available when you sign up as a **Community Member.**

Training Staff on Cyber Security Best Practices

- Updating software and Operating Systems to fix known vulnerabilities.
- Strong passwords so it takes longer for criminals to guess and "brute force" their way into online accounts.
- 2-Step Verification to prevent unauthorised access to online accounts when passwords are compromised.
- Running Antivirus to scan and remove malware.
- Reporting fraud internally to prevent others from falling victim.
- Social Media Etiquette to avoid accidental and intentional leaks of confidential business information and strategy.

Look out for:

- **Phishing** - fake emails
- **Smishing** - fake text messages
- **Vishing** - fake phone calls
- **Whaling** - social engineering targeting and pretending to be senior management

Offer Positive Reporting

Encourage your staff to report a cyber incident internally to their line manager, even when they receive fraudulent messages. Communicating threats prevents others from falling victim and action can be taken to avoid further damage to the organisation. The line manager can follow up by reporting the incident to appropriate reporting bodies such as **Action Fraud.**