Gladstone

**Quick Guide: Training Your People for Cyber Resilience**

**Why It Matters**

Even the strongest systems can fail if staff aren't prepared. Phishing, SIM swapping, and social engineering aren't IT problems - they're human ones. Here's how to keep your people ready.

**Top Tips for Frontline Teams**

**1. Stay Alert to Phishing**

- **Don't trust unexpected messages**: Be suspicious of requests for passwords, codes, or personal details - even if they appear to come from management.
- **Check the sender**: Look at the actual email address or phone number. Does it match official channels?
- **Don't click on suspicious links**: Hover to preview URLs before clicking.

**2. Understand Social Engineering**

- **Know the tactics**: Attackers might pretend to be a supplier, a colleague, or IT support. They use urgency, charm, or fear to push you into action.
- **Pause and check**: If something feels off, verify through a separate channel - don't reply to the same email or number.

**3. SIM Swapping Awareness**

- **Protect mobile numbers**: Avoid using personal phone numbers for two-factor authentication. Use work-issued numbers where possible.
- **Look for service issues**: If your phone suddenly loses service, contact your provider immediately - it could signal SIM swap fraud.

**4. Report Early, Report Often**

- **Create a clear reporting line**: Know who to contact if something suspicious happens. Don't delay.
- **No blame culture**: Encourage openness. Mistakes can happen, but early reporting can prevent bigger breaches.

### 5. Control Access

- **Limit permissions**: Staff should only have access to the systems and data they need.
- **Regular reviews**: Disable access for former staff and review permissions regularly.

### Cyber Resilience Checklist

✅ I know how to spot phishing messages and suspicious requests.
✅ I verify any unusual requests through a separate channel.
✅ I use secure, dedicated phone numbers for system authentication.
✅ I understand the risks of SIM swapping and mobile fraud.
✅ I report anything suspicious immediately and without fear.
✅ I only have access to the systems I need, and unused accounts are disabled.
✅ I attend regular training or refreshers on cyber security.