DON'T TAKE THE BAIT: THE ULTIMATE "SPOT THE PHISH" CHECKLIST

A single click can compromise our entire network. Before you click any link or download an attachment, run through this 60-second security check.

1. CHECK THE "FROM" ADDRESS

Does it match? Hover over the sender's name. If the name says "Microsoft" but the email is support@xyz-123.com, it's a trap.
Lookalikes: Watch for subtle misspellings like unite-gr0up.co.uk instead of @theunitegroup.co.uk.

2. READ THE SALUTATION

Generic Greeting: Real partners usually know your name. "Dear Valued Customer" or "Dear Employee" is a major red flag.

3. INSPECT THE LINKS

The Hover Test: Hover your mouse over any button or link without clicking. Look at the bottom corner of your screen, if the URL looks suspicious or completely unrelated, do not click.

4. ANALYSE THE TONE

Artificial Urgency: Does the email demand "Immediate Action" or threaten to "Deactivate your account"? Hackers use fear to make you act before you think.

5. VERIFY THE CONTENT

- **Unexpected Attachments:** Were you expecting this invoice or file? If an "Invoice" arrives as a .zip or .html file, it likely contains malware.
- **Poor Grammar:** While hackers are getting smarter, many phishing emails still contain awkward phrasing or spelling errors.

6. THE GOLDEN RULE

When in doubt, shout. If something feels "off," do not reply. Call the sender on a trusted number or contact our IT support desk immediately.

Whether you're facing a security nightmare or just need a plan, we're on hand to guide you through every step without the jargon.

Call Us: 0191 466 1050
Email: sales@theunitegroup.co.uk

BECAUSE TECHNOLOGY MATTERS