unity
unifying...

Can you spot the Phish?

A one-page check for everyone in the team. Keep it by your desk and run through it before you click, reply, pay or call back.



Before you click, check for red flags

- [ ] **Was I expecting this?**
  Unexpected invoices, resets and deliveries are Phish's favourite bait.
- [ ] **Does the sender's address really match?**
  Look at the full address, not just the display name.
- [ ] **Where does the link really go?**
  Hover (or press and hold) to see the real web address before you tap.
- [ ] **Is it rushing or scaring me?**
  "Today only", "final warning" or "account locked" are pressure tactics.
- [ ] **Is it asking for money, a password or a code?**
  Genuine organisations won't ask for codes or passwords by email, text or phone.
- [ ] **Has someone changed their bank details?**
  Always confirm by phone, on a number you already have.
- [ ] **Is there an attachment I didn't ask for?**
  Don't open it until you've checked with the sender another way.
- [ ] **Is a QR code somewhere unexpected?**
  On a sticker, letter or email you weren't expecting? Don't scan it.



Check another way

If a message or call asks for money, codes or a click, confirm it using a phone number or contact you already trust, never the one in the message.