

Small business IT | Easy | 2 min read

Phishing training for staff in 10 minutes

Most small business attacks begin with a message that tricks someone into clicking, paying or sharing a password. Ten minutes of regular, friendly training makes a real difference.

Minute 1 to 3: what phishing looks like

Phishing is a fake email, text, call or message designed to steal money, logins or data. Common disguises are the bank, HMRC, couriers, Microsoft, and, most dangerous of all, your boss or a supplier.

Minute 4 to 6: the warning signs

- It creates **urgency** or fear: "pay today", "account suspended".
- It asks for **passwords, codes or bank details**.
- A **change of bank details** for a supplier, or a request to buy gift cards.
- The sender's address is slightly wrong, or does not match the name.
- Links go somewhere unexpected. On a computer, hover over a link without clicking to see where it goes.
- Unexpected attachments, especially zip files and invoices.

Minute 7 to 9: what to do

1. **Stop and do not click.**
2. Check by another route, such as phoning a known number, not one in the message.
3. Report it to the person in charge, and use your email's Report phishing button.
4. If you did click or type a password, tell someone at once and change that password. Reporting quickly saves the day.

Minute 10: agree your rules

- Money and bank detail changes always need a second person to confirm by phone.
- Nobody gets in trouble for reporting a mistake.

Keep it going

Repeat a short refresher every few months, share real examples you receive, and consider the NCSC's free guidance for staff. Two-step sign-in means a stolen password alone is far less useful.

When to get more help

Ask for help if money has been sent to a scammer, if someone entered a password on a fake page, or if you would like a tailored session for your team.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.