

Phishing: five red flags

Nearly every attack on a small business starts with one email that looked normal enough to click.

1 It is rushing you

Your account closes in 24 hours. Pay today to avoid a fee. Genuine suppliers are rarely that dramatic.

2 The sender is not who it says

A display name is easy to fake. Hold your finger on it, or hover on a computer, to see the real address behind it.

3 It wants to change how you pay

New bank details, a redirected payment, confirm your account. Ring the supplier on a number you already have.

4 You were not expecting it

An invoice, a delivery, a shared document out of nowhere. Check with the person before you open anything.

5 It just feels off

Odd phrasing, a greeting a colleague would not use, a logo that looks stretched. Trust that feeling.

If something looks wrong

- Stop. Do not click, do not reply, do not pay.
- Check with the sender on a number or address you already have, never one from the email.
- Report it, even if you are not sure. Nobody is ever in trouble for asking.

Report it to: _____