PIN THIS UP · SHARE IT AROUND

Spotting a phishing email

Most attacks on a business start with one email and one person having a busy day. You are not expected to be technical — just to recognise a few patterns and know what to do.

EIGHT THINGS TO LOOK FOR

01 **It wants you to hurry**

"Within the hour", "final notice", "your account will be closed". Urgency is the oldest trick there is, because rushing stops people checking. Genuine requests can wait ten minutes.

02 **It asks you to change bank details**

A supplier emails new account details for an invoice. This is the single most expensive scam affecting UK businesses. **Always ring them on a number you already had** — never one from the email.

03 **The address is nearly right**

One letter changed, a word added, or a different ending — **.co** instead of **.co.uk**. Click or tap the sender name to see the real address, not just the display name.

04 **It asks you to sign in**

An unexpected link to a Microsoft, banking or delivery login page. Never sign in from an email link. Open the app or type the address yourself — it takes seconds and defeats the whole attack.

05 **It is your boss, but not quite**

A short message from a director asking for a payment, a gift card, or a favour — often "I'm in meetings, just email me back". Check by phone or in person, however awkward that feels.

06 **An attachment you were not expecting**

Especially an invoice, a delivery note, a CV or anything asking you to "enable content". If you did not ask for it, do not open it — check first.

07 **Something is just off**

Wrong signature, a colleague writing unusually formally, a reply to a thread that never existed. Note that **good spelling no longer means an email is genuine** — attackers now write flawlessly. Your instinct is a legitimate reason to stop and check.

08 **An unexpected QR code**

In an email, or on a printed letter or invoice. Scanning one takes you to a page you cannot inspect first, and it can be a fake sign-in exactly like a bad link. Treat an unexpected code as you would an unexpected link — and remember your phone may have less protection than your work laptop.

What to do

IF YOU ARE UNSURE

Stop and ask

Do not click, reply or open the attachment. Ask a colleague or forward it to whoever handles IT. Nobody will mind. Checking is always cheaper than not checking.

IF YOU ALREADY CLICKED

Say so immediately

Right away, even if you feel foolish. Minutes matter enormously. Nobody is in trouble for reporting quickly — the damage comes from the hours nobody knew.

IF YOU ENTERED A PASSWORD

1. Change that password now, from a different device if you can.
2. Tell whoever handles your IT, immediately.
3. Change it anywhere else you have used the same password.
4. Approve no sign-in prompts you did not start yourself.

THREE HABITS THAT STOP MOST OF THIS

Verify by phone

Any request involving money or bank details, on a number you already had.

Never sign in from a link

Open the app or type the address. This alone defeats most attacks.

Approve only what you started

An unexpected prompt means someone already has your password. If you did not start the sign-in, deny the request and report it immediately.

FILL THIS IN BEFORE PINNING IT UP

REPORT ANYTHING SUSPICIOUS TO _____

OUT OF HOURS, CONTACT _____