Phishing Red Flags

Most cyber attacks start with a message designed to make you act before you think. If you spot one of these signs, stop, check, and report it.

The sender

- Display name doesn't match the email address.
- Look-alike domains, such as micros0ft.com or yourcompany-support.com.
- A known contact writing from a personal or unusual address.

The pressure

- Urgency: “today”, “within 1 hour”, “final notice”.
- Threats: account closure, fines, legal action.
- Secrecy: “don't tell anyone”, “I'm in a meeting”.

The request

- Change of bank details or an urgent payment.
- Gift cards, crypto or wire transfers.
- Passwords, MFA codes or personal details.

The links

- Hover first: the real address doesn't match the text.
- Shortened links or long, random-looking URLs.
- A login page reached from an email link.

The attachments

- Unexpected invoices, delivery notes or voicemails.
- Files asking you to “enable content” or macros.
- Zip, HTML, ISO or password-protected files.

The details

- Generic greetings like “Dear customer”.
- Branding, spelling or tone that feels slightly off.
- A reply to a thread that seems out of place.

It's not just email

Texts and messaging apps (smishing). Fake delivery notices, bank alerts and “Hi Mum, I've got a new number” messages.

Phone calls (vishing). Callers posing as IT support, your bank or a senior colleague. Never share MFA codes on a call.

QR codes (quishing). Codes in emails, posters or parking meters that lead to fake login or payment pages.

AI voice and video. Deepfakes can imitate a colleague or executive. Verify unusual requests even if they look or sound real.

What to do

If you...	Do this
Spot a suspicious message	Don't click, reply or forward it to colleagues. Use your **Report Phishing** button or send it to your IT or security team.
Get an unusual request	Verify it through a channel you already trust: call a known number or speak in person. Never use contact details from the message itself.
Already clicked or entered details	Tell IT or security **immediately**. Change the password if asked. Reporting quickly is what matters, and nobody should be blamed for it.
Made a payment	Contact your bank and finance team straight away. Speed improves the chance of recovering funds.

Stop. Check. Report. When in doubt, report it. A false alarm costs nothing, and a missed attack can cost a lot.

Print this page and keep it near your desk. For phishing simulations and awareness training, contact Scarlet Dragonfly at scarlet-dragonfly.com.

© 2026 Scarlet Dragonfly · scarlet-dragonfly.com · Free to use and share with attribution