Spot the Phish

The 5-second email checklist

01

Check the sender, not just the name.

Look for altered, missing, or extra characters in the full email address.

02

Pause when the message creates pressure.

Threats, deadlines, secrecy, and “act now” language are meant to rush you.

03

Inspect links before you use them.

A link can display familiar words while leading somewhere else. Open the official app or site yourself.

04

Treat unexpected attachments as dangerous.

Do not open a file you did not request—especially when the message pushes urgency.

05

Question unusual requests.

Passwords, sign-in codes, payments, gift cards, and sensitive details should never be handed over on demand.

WHAT TO DO INSTEAD

Stop. Leave the message. Verify through a channel you trust.

Open the official app, type the known site address yourself, or call a number you already know is real. Do not use the suspicious message’s links, phone number, or reply address to verify it.

Sources: CISA, “Avoiding Social Engineering and Phishing Attacks”; FTC, “How To Recognize and Avoid Phishing Scams.”

Free to share · Educational use

Keep the checklist. Get the warnings.

This checklist stays free — print it, share it, keep it by the keyboard.
But a checklist is a snapshot. The threats keep moving.

Get the Field Briefing — free, plain-English breach alerts
the day they land:

https://buttondown.com/redflagcyber

No spam, no selling your data, unsubscribe anytime.