

PHISHING & SCAM SPOTTER

Before you click, reply or pay — stop and check the clues.

THE RANGER RULE

STOP • CHECK • ASK

Never let urgency make the decision for you.

1 URGENCY

“Do it now!” “Last chance!” “Your account will close!”

Scammers want you to react before you think.

2 STRANGE SENDER

The name looks familiar, but the address or username is odd.

Check the real address — not just the display name.

3 SUSPICIOUS LINK

The link is shortened, misspelled or goes somewhere unexpected.

Don't use it. Open the real app or website yourself.

4 SECRET OR PAYMENT

You're asked for a password, code, gift card, money or private info.

Passwords and verification codes are not for sharing.

5 TOO GOOD TO BE TRUE

A prize, free item or amazing offer appears out of nowhere.

Unexpected rewards are a common scam hook.

IF SOMETHING FEELS WRONG:

1. Don't click or reply.
2. Check using a trusted route.
3. Ask a trusted adult if you're unsure.
4. Report or delete the message.