Online security reflexes

5 daily reflexes + 3 questions before you click, to avoid the most common scams.

THE 5 REFLEXES

1 — Read the address before entering anything
A single different character = a fake site. The padlock doesn't prove legitimacy: it only means the connection is encrypted.

2 — Never through the link you received
Unexpected message? Open a new tab and type the official address yourself. UK/US: forward scam texts to 7726.

3 — One unique password per account
Password manager (e.g. Bitwarden, free). 12 characters minimum; a long phrase beats a complicated word.

4 — Automatic updates turned on
On all your devices and apps. Every postponed update is a flaw left open.

5 — Two-factor authentication (2FA) wherever possible
Email first, then banking and social media. Prefer an authenticator app over SMS.

When in doubt — the 3 questions before you click

1. Was I expecting this message?
2. Am I being pushed to act fast (urgency, threat, limited offer)?
3. Can I verify through another safe channel (official app, number on the back of my card)?

One worrying answer → don't click, verify first.

Victim or attempted scam?

Bank details shared: call your bank immediately · Fake-site password: change it everywhere.
UK: report@phishing.gov.uk · texts 7726 — US: ic3.gov (FBI) · reportfraud.ftc.gov (FTC)
EU help: FR cybermalveillance.gouv.fr · ES 017 (INCIBE) · BG cybercrime.bg