Scam-Proof Your Phone

The free 2-page checklist · UK · version 1

Flag It First
Spot UK scams early.
Know exactly what to do.

Tick each box as you go. Most take under two minutes. Menus can change with updates: if a path looks different on your phone, search for the setting's name in Settings. Small numbers point to the official source on page 2.

1 · Scam texts

- ☐ **Don't tap links in surprise delivery texts.** Royal Mail says it would not ask for payment by text or email for underpaid postage. It leaves a grey *Fee To Pay* card instead. The exception is customs fees, where it may text or email a link to its Fee to Pay site.[1]
- ☐ **Check for yourself.** Type `royalmail.com` into your browser and enter the reference from the card. Never use the link in the message.[1]
- ☐ **Evri** will never ask you to reschedule a delivery or pay to do so, and only ever sends a tracking link.[2]
- ☐ **Forward scam texts to 7726** (it's free). iPhone: press and hold the message → More → arrow. Android: press and hold → three dots → Forward.[3]
- ☐ **Android spam filter:** `Messages settings › Protection and safety › Spam protection` (available on some phones; on by default where it is).[4]
- ☐ **iPhone unknown senders:** `Settings › Apps › Messages › Unknown Senders` → turn on Screen Unknown Senders. It sorts unknown senders into a separate list; it doesn't block them.[5]
- ☐ **Browser warnings:** in Chrome, set Safe Browsing to **Enhanced protection** (real-time checks).[6] On iPhone: `Settings › Apps › Safari` → Fraudulent Website Warning on.[7] Warnings cover sites already identified as dangerous, so a brand-new scam site may not be flagged yet.[6]

2 · Scam calls

- ☐ **If "your bank" calls, hang up and call 159.** 159 cannot be spoofed or impersonated and covers more than 99% of UK current accounts.[8]
- ☐ **iPhone:** `Settings › Apps › Phone › Screen Unknown Callers` → choose *Ask Reason for Calling* or *Silence* (Silence sends calls to voicemail).[9]
- ☐ **Android (Google Phone app):** `Settings › Caller ID and spam` → turn on filtering of spam calls. Filtered calls still show in your call history.[10]

3 · Your accounts

- ☐ **Start with your email.** A criminal in your email could reset all your other account passwords. 2-Step Verification on email stops them even if they know your password.[12]
- ☐ **Use passkeys wherever they're available**; otherwise use strong, unique passwords and turn on 2-Step Verification.[11] Google passkey: `myaccount.google.com/signinoptions/passkeys`.[13] Google 2-Step: `myaccount.google.com › Security & sign-in › 2-Step Verification`.[14]
- ☐ **Never reuse a password.** With a reused password, criminals only need one to get into all your accounts.[12]
- ☐ **WhatsApp:** `Settings › Account › Two-step verification` → set it up and add an email address so you can reset it.[15]
- ☐ **Check your saved passwords.** Android/Google: `passwords.google.com` → Password Checkup. iPhone: Passwords app → Security. Change any compromised password as soon as you can.[16, 17]
- ☐ **Social media:** check your privacy settings so posts are seen only by people you intend. Fraudsters use details like birthdays, locations and family names.[11]

4 · Your phone

- [ ] **iPhone Stolen Device Protection** (iOS 17.3 or later): `Settings › Face ID & Passcode` → turn it on **before** you ever need it.[18]
- [ ] **Android Theft protection** (Android 10+; some features need 15+): `Settings › Google › All services › Theft protection`.[19]
- [ ] **SIM PIN:** after a restart or if the SIM is moved to another phone, a code is needed before calls or mobile data work. Use the default PIN from your network provider. **Don't guess**: wrong guesses can lock the SIM permanently.[20]
- [ ] **Automatic updates on.** iPhone: `Settings › General › Software Update › Automatic Updates`. Android: `Settings › System › Software updates`.[21, 22, 23]

5 · If it goes wrong

- [ ] **Tapped the link but entered nothing?** The NCSC says it's unlikely you need to take further action. Stay alert to unusual emails and notifications.[24]
- [ ] **Typed in a password?** Change it, and change it everywhere else you used the same one.[24]
- [ ] **Entered card details?** Contact your bank straight away. Call **159**, and cancel the card in your online banking.[8, 24]
- [ ] **Report it** (including hacked email or social accounts): **reportfraud.police.uk** or **0300 123 2040**. In Scotland: Police Scotland on **101**.[11, 25, 26]

Family rule: if "your bank" calls, hang up and call 159. If a message has a link, don't tap it: go to the official website yourself.

Sources (checked 15–24 Oct 2026)

1. Royal Mail — Scam protection: https://www.royalmail.com/help/scam-protection
2. Evri — Cyber security: https://www.evri.com/cyber-security
3. NCSC — Report a scam text message: https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-text-message
4. Google Messages Help — spam protection: https://support.google.com/messages/answer/9327903?hl=en-GB
5. Apple Support — filter unknown senders: https://support.apple.com/en-gb/125068
6. Google Chrome Help — Safe Browsing: https://support.google.com/chrome/answer/9890866?hl=en-GB
7. Apple iPhone User Guide — Safari privacy and security: https://support.apple.com/en-gb/guide/iphone/iphb01fc3c85/ios
8. Stop Scams UK — 159: https://stopscamsuk.org.uk/159
9. Apple Support — Screen Unknown Callers: https://support.apple.com/en-gb/111106
10. Phone app Help — caller ID and spam: https://support.google.com/phoneapp/answer/3459196?hl=en-GB
11. Report Fraud press release, 5 Oct 2026 (as republished by wired-gov.net): https://www.wired-gov.net/wg/news.nsf/articles/Switch+to+passkeys+Report+Fraud+warning+as+email+and+social+media+account+hacking+sums+stolen+rise+by+more+than+400+per+cent+05102026161500?open=
12. NCSC — Use a strong and separate password for email: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/use-a-strong-and-separate-password-for-email
13. Google Account Help — passkeys: https://support.google.com/accounts/answer/13548313?hl=en-GB
14. Google Account Help — 2-Step Verification: https://support.google.com/accounts/answer/185839?hl=en-GB
15. WhatsApp Help Centre — two-step verification: https://faq.whatsapp.com/580707210518585
16. Google Account Help — Password Checkup: https://support.google.com/accounts/answer/9457609
17. Apple iPhone User Guide — weak or compromised passwords: https://support.apple.com/guide/iphone/change-weak-or-compromised-passwords-iphd5d8daf4f/ios
18. Apple Support — Stolen Device Protection: https://support.apple.com/en-gb/120340
19. Android Help — Theft protection: https://support.google.com/android/answer/15146908?hl=en-GB
20. Apple Support — SIM PIN: https://support.apple.com/en-gb/118228
21. NCSC — Install the latest software and app updates: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates
22. Apple Support — Update your iPhone: https://support.apple.com/en-gb/HT204204
23. Android Help — Check and update your Android version: https://support.google.com/android/answer/7680439?hl=en-GB
24. NCSC — Phishing: what to do if you've responded: https://www.ncsc.gov.uk/section/respond-recover/phishing
25. GOV.UK — Report Fraud: new service from City of London Police: https://www.gov.uk/government/news/report-fraud-new-service-from-city-of-london-police
26. Report Fraud: https://www.reportfraud.police.uk/

Flag It First is an independent channel. It isn't linked to any bank, police force or company named here. This is general safety information, not legal or financial advice. Every step is checked against the official sources above. Version 1, 29 Oct 2026. Newer versions: doflagitfirst.com/checklist