DOC LDK-20261127-81FFB6
FOR Sample household
UTC 2026-11-27T23:03:39Z

Your everyday accounts, in plain English

READ THIS FIRST

The biggest risk to you this week is impersonation, not mathematics.

Criminals use headlines like this one to rush people into moving money, reading out codes or installing software. Your bank, tax authority, or wallet provider will never ask you to move money to a 'holding account', read back a one-time code, or 'upgrade encryption' by phone, text, or email. If anyone does, hang up, wait, and call the number printed on your card or statement.

PREPARED FOR

Sample household

DATE 27 November 2026
SERVICES 6 selected
STATES 1 documented · 1 mixed · 1 action · 3 no statement

Scenario shown: RSA factoring is assumed practical; elliptic-curve and symmetric encryption are not assumed broken. Most everyday banking and messaging connections already use methods other than RSA for the parts that matter most.

01 Your selected services — what the public record says and what to do today

SERVICE	PUBLIC RECORD	WHAT TO DO TODAY	SOURCE · REVIEWED
Monzo Banks & Fintech (UK & US)	No public statement found Public guidance is not detailed enough to judge Monzo's protection in either scenario.	Check call status in the Monzo app and report unexpected requests through in-app support.	Monzo: Keep your money protected from fraudsters 2026-11-27
Gmail Messaging & Email	No public statement found Gmail encryption varies by message, recipient and account settings.	Check the message security details before sending sensitive information and use your saved Google sign-in address for alerts.	Gmail Help: Check your email security 2026-11-27
Signal Messaging & Email	Mixed — review account settings Signal adds protection against future decryption, but identity checks still depend on older cryptography.	Update Signal on every linked device and compare safety numbers with important contacts through another trusted channel.	Signal: The PQXDH Key Agreement Protocol 2026-11-27
1Password Password Managers & 2FA	Provider has published action / RSA noted 1Password encrypts vault contents with AES, but its documented vault-key wrapping uses RSA.	Update 1Password, keep your Secret Key and recovery information private, and follow official advice before changing shared vaults.	1Password Security Design, sections 5.2 and 8.1 2026-11-27
Bitcoin Crypto & Wallets	Publicly documented non-RSA protection An RSA-only break does not break Bitcoin's signatures; an elliptic-curve break would.	Do not move coins because of RSA-only claims or unsolicited migration offers; if ECC is affected, follow verified Bitcoin and wallet guidance.	Bitcoin Core: libsecp256k1 2026-11-27
Apple iCloud (Advanced Data Protection) Consumer Devices & Cloud	No public statement found Advanced Data Protection covers more iCloud content, but it is not a blanket guarantee against either scenario.	Check whether Advanced Data Protection is available for your account and region, review backup settings and keep a working recovery method.	Apple: iCloud data security overview 2026-11-27

No public statement found as of 27 November 2026 does not mean this service is affected. Statuses summarise each provider's own public documentation on the date shown; they are not a judgement about the provider or a measurement of your account.

CUT OUT · STICK ON THE FRIDGE · SHARE WITH FAMILY

Nobody genuine will ever ask you to do these things

Banks · HMRC and the IRS · wallet and crypto providers · password managers

- [X] Ask you to move money to a 'holding' or 'protected' account.
- [X] Ask you to read back a one-time passcode or app approval code.
- [X] Ask for your recovery phrase, Secret Key, master password or full card PIN.
- [X] Ask you to install remote-access software or a new 'secure' app from a link.
- [X] Threaten arrest, account closure or loss of funds unless you act within minutes.
- [X] Tell you to keep the call secret from family or your bank's own staff.

THE THREE-STEP VERIFICATION RULE

1. Stop. Genuine organisations do not mind if you take ten minutes.
2. Hang up or close the message. Do not use any number or link they gave you.
3. Call back on the number printed on your card, statement or the provider's official app, or ask a trusted family member first.

If you have already shared a code or moved money, contact your bank now using the number on your card. Acting quickly matters more than feeling embarrassed.

DOC LDK-20261127-81FFB6
FOR Sample household
UTC 2026-11-27T23:03:39Z

Lock down what matters, without lockouts

02 Password manager hygiene

A password manager is still the right tool. Do not delete it or export everything to a spreadsheet because of a headline.

- [ ] Update the app on every device before changing anything else.
- [ ] Make one encrypted backup or emergency kit export and store it offline (a printed copy in a sealed envelope counts).
- [ ] Change the master password only if you suspect someone else knows it. Rotating everything at once causes lockouts, not security.
- [ ] Turn on the strongest second step your manager supports: a hardware key or passkey first, then an authenticator app. Avoid SMS where you have a choice.
- [ ] Review 'authorised devices' or 'sessions' and remove anything you do not recognise.
- [ ] Follow your provider's own published guidance for any change to how shared vaults or recovery keys are protected.

03 Account recovery checklist

Most account takeovers go through recovery, not through encryption. Check these for each email, bank and cloud account you picked.

- [ ] Recovery email and phone number are yours and current.
- [ ] Recovery codes are printed or stored offline, not in your inbox.
- [ ] Unused 'legacy' sign-in methods, app passwords and old devices are removed.
- [ ] Login alerts are turned on and go to a channel you actually read.
- [ ] Your email account has the strongest protection of all, because it resets everything else.

04 Crypto security rules — factual, no wallet recommendations

Facts only. This kit does not recommend any wallet, exchange or coin, and contains no referral links. Bitcoin and Ethereum sign transactions with secp256k1 elliptic-curve keys; Solana uses Ed25519. None of these use RSA for transaction signing.

1. Never move funds because of a message, call, advert or 'migration tool'. Legitimate protocol changes are announced on the project's own documentation site and take time.
2. No provider, support agent or 'validator' ever needs your seed phrase or private key. Anyone asking is a thief.
3. Verify announcements by typing the provider's official address yourself, or opening its app, never through a link you were sent.
4. Hardware wallets and exchanges have their own sign-in and recovery paths; check each provider's official statement separately from the coin itself.
5. RSA-only claims are not a reason to move coins. Treat 'RSA is broken, move your Bitcoin now' as a scam signal.

Crypto services you selected: Bitcoin. Their provider statements and primary documentation links are in the table on page 1.

05 Sole trader & small business quick check

Sole traders and small teams: five checks that take under an hour, using tools you already have.

Email domain	Confirm SPF, DKIM and DMARC records are published for your sending domain; your email or DNS provider's help pages show how. Ask them whether DKIM can use Ed25519 (RFC 8463) alongside RSA.
Domain registrar	Turn on registrar lock and two-step sign-in at your domain registrar; a stolen domain redirects your customers' payments and email.
Banking and payments	Enable multi-factor sign-in on business banking, card acquirers and invoicing tools, and set payee-change approvals to require a second person or a callback.
Staff script	Agree with staff that no payment detail change is actioned from an email or call alone. Verify through a known number.
Your company website	Run the free 10-second business check at postrsa.com to see what certificates and sign-in keys your customers can already observe.

PROVENANCE AND SCOPE

This kit summarises public documentation reviewed on 27 November 2026. It is not a security audit, not legal or financial advice, and not a statement about whether any provider has had an incident. 'No public statement found' means exactly that: no claim is made that the service is affected. Follow each provider's own verified guidance over anything in this document. Prepared by Degaus Ltd (England and Wales).

SNAPSHOT consumer-v2026.11.27-662203f3
DATASET SHA-256 662203f3e2a1a71405859e6419bc260e86fce0728a0fd9ccc53545844a74d43c
GENERATED 2026-11-27T23:03:39Z · LDK-20261127-81FFB6