WalletLegacy

Security Check-up

Prepared for Jordan Reid

Your crypto security, worked out from your own answers. This pack contains no recovery phrases, passwords or keys. Keep it with your records and check again once a year.

Security score	Scam exposure	Checked
52/100 · D	Elevated	1 Oct 2026

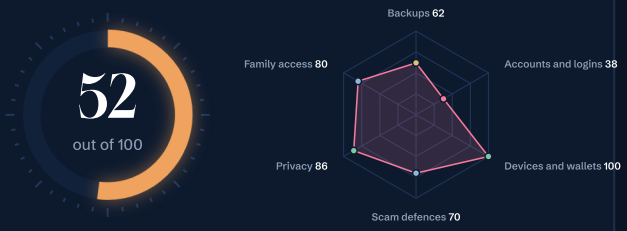
Security Check-up · Jordan Reid

Checked 1 October 2026 · 28 of 28 questions answered · worked out on this device

Read-only | No phrases or keys

Security score	Scam exposure	Open routes to your crypto	Within a thief's reach	Urgent fixes	Score after fixes
52 /100	Elevated	5 /8	£30,000	2	100 /100
Grade D	Index 65 of 100	3 blocked	100% of your crypto	0 critical, 2 high	+48 points

Overall security



Scam exposure



Elevated

Most exposed to: sim swap

SIM swap	73
Account ta...	60
Fake websi...	51
Address p...	48
Theft and t...	43
Wallet drai...	33
Fake supp...	28
Investment...	8

Routes to your crypto

OPEN	A SIM swap intercepts your codes	OPEN	A fake website captures your login
OPEN	A wallet drainer takes your tokens	OPEN	Someone finds your recovery phrase
OPEN	You send to a lookalike address	OPEN	A broken or lost device takes your crypto with it
OPEN	Your family can't find or claim it	BLOCKED	A leaked password opens your exchange
BLOCKED	Your email is taken over and used to reset everything	BLOCKED	Fake support talks you into giving access

Priority grid

	Inconvenient	Costly	Could lose everything
Likely		3 Passwords used on more than one site	FIX FIRST
Possible	10 No backup codes for two-step sign-in 11 Your details were in a data breach	2 Only one backup, in one place 4 Finding exchanges through search 5 Old token approvals left open 6 Checking only part of an address 7 Your family only roughly knows	1 Text message codes on exchange accounts
Unlikely	14 Crypto not mentioned in your will 15 Old exchange accounts you no longer use 16 Friends and colleagues know you hold crypto	12 No extra protection on your phone number 13 No withdrawal allow-list or lock on exchanges	8 Recovery phrase kept loose at home 9 Backup never tested

Your results in brief

Your security score is **52 out of 100** (grade D), and your scam exposure is **elevated**. We found 16 gaps: 0 critical, 2 high, 12 medium and 2 low.

5 of 8 routes criminals use are open for you, putting roughly **£30,000** (100% of your crypto) within reach. The most exposed: a SIM swap intercepts your codes; a fake website captures your login; a wallet drainer takes your tokens.

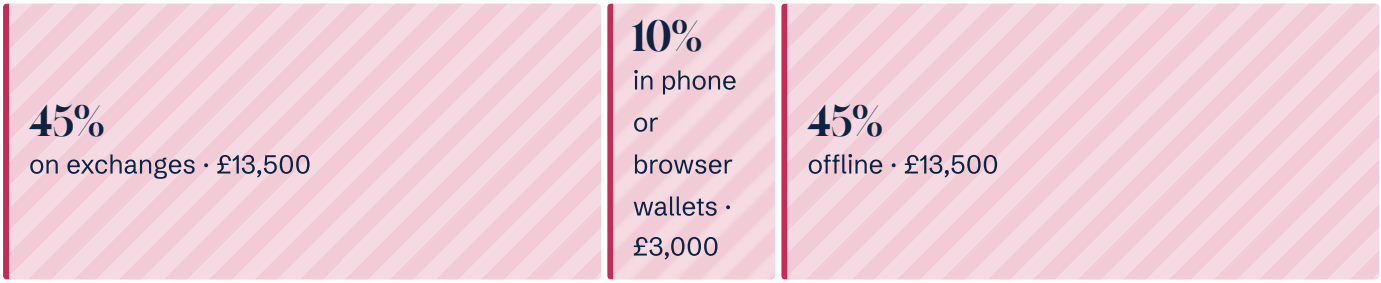
Separately, about £16,500 (55%) could be lost for good if a device breaks, because your backup has never been tested.

The single biggest improvement is to fix **text message codes on exchange accounts**, which takes your score to 58. The 7 free quick wins in your fix plan take about an hour in total and lift your score to 74. Fixing everything takes about 6 hours and gets you to 100.

If something happened to you, your family would only have a rough idea where to look. Of all the routes above, this one doesn't need a criminal.

Routes to your crypto

The ways criminals actually get to people's crypto, step by step, checked against your answers. A route is open when nothing you do stops it. One blocked step is enough to close it.



Based on £30,000, the middle of the band you chose, and a typical split for where you said most of your crypto is held. Shaded parts can be reached through at least one open route. This shows what's exposed, not what will be lost.

OPEN A SIM swap intercepts your codes

- A criminal finds your number and enough details to pose as you
- Your mobile network moves your number to their SIM
- Your sign-in or reset codes go to their phone
- They withdraw your crypto

Reaches your crypto on exchanges. Close it by blocking any one step.

OPEN A fake website captures your login

- You reach a copy of your exchange from a link or search advert
- You type your password and code into it
- Your code works for them too

Reaches your crypto on exchanges. Close it by blocking any one step.

OPEN A wallet drainer takes your tokens

- You connect your wallet to a website
- You approve a request without reading what it allows
- It moves your tokens

Reaches your crypto in phone or browser wallets, offline. Close it by blocking any one step.

OPEN Someone finds your recovery phrase

- Someone gets into your home, cloud or password manager
- Your phrase is there to be found
- They restore your wallet on their own device

Reaches your crypto in phone or browser wallets, offline. Close it by blocking any one step.

OPEN You send to a lookalike address

- A scammer plants a lookalike address in your history
- You copy it without checking all of it

Reaches your crypto on exchanges, in phone or browser wallets, offline. Close it by blocking any one step.

OPEN A broken or lost device takes your crypto with it

- Your phone or hardware wallet is lost, broken or reset
- There's no working backup to restore from

OPEN Your family can't find or claim it

- Something happens to you
- Nobody has a written list of what you hold and where

BLOCKED A leaked password opens your exchange

- A password of yours leaks in another site's data breach
- It's tried on your exchange
- ~~Nothing else is needed to sign in~~
  Blocked: Your exchange asks for a second step.
- Crypto is sent straight to their address

BLOCKED

Your email is taken over and used to reset everything

- → Your email password is guessed or leaked
- ✓ ~~Nothing else is needed to get into your email~~
  Blocked: Your email has two-step sign-in.
- → Exchange passwords are reset from your inbox

BLOCKED

Fake support talks you into giving access

- → A stranger posing as support or a "recovery expert" contacts you
- ✓ ~~You reply, share your screen or install an app~~
  Blocked: You've never engaged with or let them in.
- → They get your login, phrase or screen

Area by area

What you're already doing well, and what to fix, in each part of your security.

Backups 62/100

TO FIX

- **Only one backup, in one place.** Keep a second copy in a different secure place, such as with your solicitor or in a safe deposit box.
- **Recovery phrase kept loose at home.** Keep it in a locked, fire-resistant place such as a home safe, or a sealed envelope with your solicitor or in a safe deposit box.
- **Backup never tested.** Use your wallet's "check recovery phrase" feature, or restore it on a spare or reset device, to prove the written copy works. Never type it into a website.

Accounts and logins 38/100

DOING WELL

- ✓ Your email, the key to every reset, has strong two-step sign-in.

TO FIX

- **Text message codes on exchange accounts.** Switch each exchange to an authenticator app or a passkey, then remove your phone number as a sign-in method if the exchange allows it.
- **Passwords used on more than one site.** Use a password manager to give every account its own long password, starting with your email and exchanges.
- **No backup codes for two-step sign-in.** Download the backup codes for each exchange and your email, print them and keep them with your plan.
- **No extra protection on your phone number.** Ask your mobile network to add a PIN or password to your account and to block number transfers without it.
- **No withdrawal allow-list or lock on exchanges.** Turn on the exchange's address allow-list (or "address book lock") so crypto can only go to addresses you've approved, with a waiting period for new ones.
- **Old exchange accounts you no longer use.** List every exchange you've ever used. Close the ones you don't need after withdrawing any balance, and add strong sign-in to the rest.

Devices and wallets 100/100

DOING WELL

- ✓ Part of your crypto is offline on a hardware wallet.
- ✓ Your hardware wallet came straight from the maker.
- ✓ Your browser is kept lean, with only extensions you know.
- ✓ Your devices update themselves.
- ✓ Your phone has a strong lock.

NOTHING TO FIX HERE.

Scam defences 70/100

DOING WELL

- ✓ You read what you're approving before you sign.
- ✓ You've never let a stranger control your screen.
- ✓ You ignore strangers who contact you about crypto.
- ✓ You turned down an online investment pitch.

TO FIX

- **Finding exchanges through search.** Bookmark the real sites once and always use the bookmark or official app.
- **Old token approvals left open.** Review and remove approvals you no longer need with a token approval checker such as your wallet's built-in tool, Revoke.cash or Etherscan's token approvals page.
- **Checking only part of an address.** Check the whole address against a saved contact, and send a small test amount first for anything large.

Privacy 86/100

DOING WELL

- ✓ Your number and address aren't easy to find online.

TO FIX

- **Your details were in a data breach.** Treat any contact about your crypto as fake until you've checked it in the official app, and never act on a letter asking you to "verify" your wallet.
- **Friends and colleagues know you hold crypto.** Keep amounts private and be wary of anyone who later raises crypto out of the blue.

Family access 80/100

TO FIX

- **Your family only roughly knows.** Write it down in a plan your executor can follow, and keep it with your will.
- **Crypto not mentioned in your will.** Ask your solicitor to add wording about digital assets, and keep the details in a separate private letter of wishes.

Every risk, and how to fix it

#	Level	Risk	How to fix it
1	High	**Text message codes on exchange accounts** Criminals can move your phone number to their own SIM and receive your codes. This is one of the most common ways crypto accounts are emptied.	Switch each exchange to an authenticator app or a passkey, then remove your phone number as a sign-in method if the exchange allows it.
2	High	**Only one backup, in one place** One fire, flood or house move can destroy the only copy.	Keep a second copy in a different secure place, such as with your solicitor or in a safe deposit box.
3	Medium	**Passwords used on more than one site** When any site you use is hacked, criminals try the same email and password on exchanges and email providers.	Use a password manager to give every account its own long password, starting with your email and exchanges.
4	Medium	**Finding exchanges through search** Scammers pay for search adverts that lead to fake copies of real exchange and wallet sites.	Bookmark the real sites once and always use the bookmark or official app.
5	Medium	**Old token approvals left open** Approvals you gave to apps months ago may still let them move your tokens. If one of those apps is hacked, so are you.	Review and remove approvals you no longer need with a token approval checker such as your wallet's built-in tool, Revoke.cash or Etherscan's token approvals page.

#	Level	Risk	How to fix it
6	Medium	**Checking only part of an address** Scammers send tiny amounts from look-alike addresses so the fake one appears in your history with the same start and end.	Check the whole address against a saved contact, and send a small test amount first for anything large.
7	Medium	**Your family only roughly knows** Knowing that crypto exists isn't enough: they need to know which accounts, which devices and where the backups are.	Write it down in a plan your executor can follow, and keep it with your will.
8	Medium	**Recovery phrase kept loose at home** A phrase in a drawer can be lost in a move, damaged by fire or water, or found by a visitor or burglar.	Keep it in a locked, fire-resistant place such as a home safe, or a sealed envelope with your solicitor or in a safe deposit box.
9	Medium	**Backup never tested** A word written down wrongly, or in the wrong order, only shows up when you need it, and by then the wallet may be gone.	Use your wallet's "check recovery phrase" feature, or restore it on a spare or reset device, to prove the written copy works. Never type it into a website.
10	Medium	**No backup codes for two-step sign-in** If you lose your phone you could be locked out of your own accounts for weeks, and your family would struggle even more.	Download the backup codes for each exchange and your email, print them and keep them with your plan.

#	Level	Risk	How to fix it
11	Medium	**Your details were in a data breach** Scammers use leaked names, addresses and phone numbers to send convincing fake letters, emails and calls.	Treat any contact about your crypto as fake until you've checked it in the official app, and never act on a letter asking you to "verify" your wallet.
12	Medium	**No extra protection on your phone number** Without a PIN or port-out protection, it's easier for someone to move your number to their SIM.	Ask your mobile network to add a PIN or password to your account and to block number transfers without it.
13	Medium	**No withdrawal allow-list or lock on exchanges** If someone gets into your exchange account, nothing slows them down before they send your crypto to their own address.	Turn on the exchange's address allow-list (or "address book lock") so crypto can only go to addresses you've approved, with a waiting period for new ones.
14	Medium	**Crypto not mentioned in your will** Without it, executors may not know to look, and there may be arguments about who gets what.	Ask your solicitor to add wording about digital assets, and keep the details in a separate private letter of wishes.
15	Low	**Old exchange accounts you no longer use** Forgotten accounts often still have old passwords and weak sign-in, and your family won't know to claim anything left in them.	List every exchange you've ever used. Close the ones you don't need after withdrawing any balance, and add strong sign-in to the rest.

#	Level	Risk	How to fix it
16	Low	**Friends and colleagues know you hold crypto** News travels. The fewer people who know, the fewer targeted scams you'll see.	Keep amounts private and be wary of anyone who later raises crypto out of the blue.

Your fix plan

Do these in order. Each one raises your score, and the first few make the biggest difference. Times are rough guides.

> **Quick wins:** 7 free fixes that take 15 minutes or less each, about an hour in total. They're marked below. Everything on the list takes about 6 hours, and 11 of 16 fixes cost nothing.

1 **Text message codes on exchange accounts** QUICK WIN — This week ☐

Switch each exchange to an authenticator app or a passkey, then remove your phone number as a sign-in method if the exchange allows it.

About 15 minutes · Free · +6 points, to 58

---

2 **Only one backup, in one place** — This week ☐

Keep a second copy in a different secure place, such as with your solicitor or in a safe deposit box.

About 30 minutes · Free · +5 points, to 63

---

3 **Passwords used on more than one site** — This month ☐

Use a password manager to give every account its own long password, starting with your email and exchanges.

About an hour · Free, or a few pounds a month for a password manager · +3 points, to 66

---

4 **Finding exchanges through search** QUICK WIN — This month ☐

Bookmark the real sites once and always use the bookmark or official app.

About 5 minutes · Free · +3 points, to 69

---

5 **Old token approvals left open** — This month ☐

Review and remove approvals you no longer need with a token approval checker such as your wallet's built-in tool, Revoke.cash or Etherscan's token approvals page.

About 15 minutes · A small network fee per approval · +3 points, to 72

---

6 **Checking only part of an address** QUICK WIN — This month ☐

Check the whole address against a saved contact, and send a small test amount first for anything large.

About 5 minutes · Free · +3 points, to 75

7 **Your family only roughly knows** This month ☐

Write it down in a plan your executor can follow, and keep it with your will.

About 30 minutes · Free with the WalletLegacy planner · +3 points, to 78

8 **Recovery phrase kept loose at home** This month ☐

Keep it in a locked, fire-resistant place such as a home safe, or a sealed envelope with your solicitor or in a safe deposit box.

About 30 minutes · Free, or about £30 for a small safe · +3 points, to 81

9 **Backup never tested** This month ☐

Use your wallet's "check recovery phrase" feature, or restore it on a spare or reset device, to prove the written copy works. Never type it into a website.

About 20 minutes · Free · +3 points, to 84

10 **No backup codes for two-step sign-in** QUICK WIN This month ☐

Download the backup codes for each exchange and your email, print them and keep them with your plan.

About 10 minutes · Free · +3 points, to 87

11 **No extra protection on your phone number** QUICK WIN This month ☐

Ask your mobile network to add a PIN or password to your account and to block number transfers without it.

About 10 minutes · Free · +3 points, to 90

12 **Your details were in a data breach** This month ☐

Treat any contact about your crypto as fake until you've checked it in the official app, and never act on a letter asking you to "verify" your wallet.

About 20 minutes · Free · +2 points, to 92

13 **No withdrawal allow-list or lock on exchanges** QUICK WIN This month ☐

Turn on the exchange's address allow-list (or "address book lock") so crypto can only go to addresses you've approved, with a waiting period for new ones.

About 10 minutes · Free · +3 points, to 95

14 **Crypto not mentioned in your will** This month ☐

Ask your solicitor to add wording about digital assets, and keep the details in a separate private letter of wishes.

About an hour · Usually £150 to £600 with a solicitor · +3 points, to 98

15 **Old exchange accounts you no longer use** When you can ☐

List every exchange you've ever used. Close the ones you don't need after withdrawing any balance, and add strong sign-in to the rest.

About 45 minutes · Free · +1 points, to 99

16 **Friends and colleagues know you hold crypto** QUICK WIN When you can ☐

Keep amounts private and be wary of anyone who later raises crypto out of the blue.

About 5 minutes · Free · +1 points, to 100

Scam field guide

The scams aimed at UK crypto owners, with how exposed your answers make you to each one, and the latest published figures.

8%
of UK adults hold crypto, about 5 million people
FCA, 2025

158,000
personal wallets were broken into worldwide in 2025, with $713 million taken
Chainalysis, 2026

£221.5m
lost to investment scams in the UK in 2025, a record
UK Finance, 2026

+1,055%
rise in UK SIM swap fraud in 2024
Cifas, 2025

SIM swap

Your exposure 73/100

Your phone number is moved to a criminal's SIM, so they receive your text message codes and reset your accounts.

Warning signs: Your phone suddenly loses signal, texts from your network about a SIM change.

> Unauthorised SIM swaps in the UK rose 1,055% in 2024 to almost 3,000 cases, then by a further 38% in 2025.
> Cifas, Fraudscape 2025 and 2026

Account takeover

Your exposure 60/100

Criminals log in to your email or exchange with a leaked or guessed password and withdraw your crypto.

Warning signs: Sign-in alerts you don't recognise, password reset emails you didn't request.

> More than 78,000 account takeover cases were reported to the UK's National Fraud Database in 2025.
> Cifas, Fraudscape 2026

Fake websites and emails

Your exposure 51/100

Emails, texts and search adverts that copy your exchange or wallet, leading to a fake site that takes your login or phrase.

Warning signs: Urgent warnings about your account, links you didn't ask for, slightly wrong web addresses.

> In 2025, bribed support contractors stole Coinbase customers' names, addresses, ID images and balances: exactly what convincing fake emails and calls are built from.
> Coinbase filing to the SEC, May 2025

Address poisoning

Your exposure 48/100

Scammers send tiny amounts from an address that looks like one you use, hoping you'll copy it from your history.

Warning signs: Tiny or zero-value transfers you don't recognise in your history.

> A single address-poisoning campaign seeded 82,031 lookalike addresses in 66 days. Chainalysis, 2024

Theft and threats in person

Your exposure 43/100

Theft of devices or written phrases, or threats against people known to hold crypto.

Warning signs: People asking about your crypto, visitors near where you keep backups.

> Value taken in violent "wrench attacks" on crypto holders hit a record $58 million in 2025. Chainalysis, 2026

Wallet drainers and approvals

Your exposure 33/100

A fake site asks your wallet to approve or sign something that lets it take your tokens.

Warning signs: Free mints and airdrops, "claim" buttons, requests to approve unlimited spending.

> Wallet-drainer phishing took $83.85 million from 106,106 victims in 2025. Scam Sniffer, 2025 report

Fake support and impersonation

Your exposure 28/100

Strangers posing as exchange staff, wallet makers or "recovery experts" who offer help, then ask for remote access, your phrase or a payment.

Warning signs: Anyone who contacts you first, help offered on social media, requests to install an app or share your screen.

> Ledger's 2020 data leak exposed the names, home addresses and phone numbers of about 272,000 customers, who were then targeted by fake support letters and calls. Ledger, 2020

Investment and romance scams

Your exposure 8/100

Fake trading platforms and online "friends" or partners who share tips, show growing profits, then block withdrawals until you pay more.

Warning signs: Guaranteed or very high returns, a new contact steering you to a platform, fees to withdraw.

> UK victims lost a record £221.5 million to investment scams in 2025, up 40%, and £39.2 million to romance scams. UK Finance, Annual Fraud Report 2026

If something goes wrong

1 **Stop and don't send anything more** — First minutes

Don't pay any "fee", "tax" or "release charge" to get money back. That's always part of the scam.

2 **Move what's left** — First hour

If a wallet's recovery phrase may have been seen, set up a new wallet with a new phrase on a device you trust, and move everything left into it. If an exchange login was taken, contact the exchange through its app and change your email password first.

3 **Tell your bank** — Same day

If you paid by card or bank transfer, call the number on the back of your card. Banks can sometimes stop or recover payments.

4 **Report it** — Same day

Report it to the police through the UK's national fraud reporting service, or Police Scotland on 101. Keep screenshots, addresses and transaction IDs.

5 **Beware of "recovery" offers** — Afterwards

People who lose crypto are targeted again by fake recovery firms and fake police. Nobody can reverse a blockchain payment for a fee.

Your yearly security check

Security slips over time. Tick these off through the year, then take the check-up again.

Every three months

- [ ] Check each exchange's sign-in history and connected devices
- [ ] Review and remove old token approvals
- [ ] Make sure your devices have updated

Every six months

- [ ] Check your recovery phrase backups are where you left them, sealed and readable
- [ ] Look for new data breaches involving your email at a breach checking site
- [ ] Remove apps, extensions and wallets you no longer use

Once a year

- [ ] Retake this check-up and compare your score
- [ ] Update your crypto plan for your family, and tell your executor where it is
- [ ] Check your mobile network PIN or transfer block is still on
- [ ] Close exchange accounts you no longer need

Whenever something changes

- [ ] New phone: move your authenticator app before you wipe the old one
- [ ] New wallet or exchange: add it to your plan the same day
- [ ] Lost device: move crypto from any wallet on it, then change passwords

General information only, not financial, legal or security advice for your situation.
WalletLegacy never asks for recovery phrases, private keys or passwords.