Bulletproof Crypto

How to Outwit Hackers, Outsmart Scammers, and Outsurvive Exchange Collapses

Stephen Bradshaw

BULLETPROOF CRYPTO.

How To Outwit Hackers, Outsmart Scammers, And OutSurvive Exchange Collapses

By Stephen Bradshaw

www.CryptoKnowledge.digital

Start Here: Your Shortcut To Protection

Welcome and what this Book will do for you.

Well done and welcome.

By opening this guide you've already done something that most people never do: you chose to protect your crypto before you try to chase profits.

That simple decision separates casual dabblers from people who keep their money.

This book is practical, plain-English, and written for people who want to get things done — not for people who want to learn blockchain theory.

If you finish this guide and do the exercises, you'll be able to:

- Recognise the biggest security mistakes beginners make (and avoid them).
- Lock down your accounts so you're not an easy target.
- Spot and dismiss scams and social engineering instantly.
- Move coins off an exchange into a hardware wallet safely.
- Use a practical, repeatable 5-step security checklist every time you touch crypto.

This is a working manual — not a manifesto.

Read, act, repeat. Start small. Build confidence.

The small actions you take now will protect you from large losses later.

CHAPTER 1

THE BIG LIE – WHY EXCHANGES AREN'T BANKS

The False Comfort

When you first use a big exchange (Coinbase, Kraken, Binance), it feels like a bank.

You sign up, verify your identity, link a card or bank account, and you see balances on a neat dashboard.

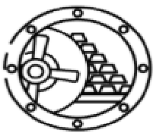
That user experience is deliberate: convenience builds trust.

But exchanges are not banks. They are businesses running software on servers.

They may be regulated in some places, but they do not provide blanket deposit insurance like banks do.

If an exchange is hacked, mismanaged, or collapses, customer funds can be frozen or lost.

No friendly ombudsman will magically restore everything.



Why beginners fall into this trap

You can buy crypto in five minutes and then leave it sitting on an exchange.

That's what most people do. It's easy, and it feels fine — until it isn't.

Two common reasons people leave funds on exchanges:

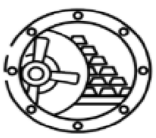
1) Convenience: "I'll trade more later."

2) Fear of making a mistake with wallets: "Hardware wallets look terrifying."

   Both are avoidable.

The one principle you must remember

Not your keys, not your coins.



If you don't control the private keys, you don't control the funds. Exchange's control keys for you. That's fine for trading, but dangerous for long-term holding.

Practical first steps (for beginners)

1. Think of exchanges as **transit hubs**, not safes. Buy and withdraw — don't "store" your lifetime savings there.

2. Open a non-custodial wallet app on your phone (Trust Wallet, Exodus) and practice transferring a tiny amount (e.g., £5).

Getting hands-on is the fastest way to learn. We will run through some step-by-step examples in Chapter 4.

3. When you're ready, plan a migration path: short-term holdings on exchange; day-to-day funds in hot wallet; long-term funds in a hardware wallet.

Chapter 2

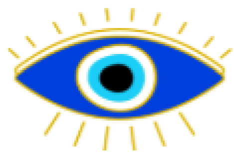
OUTWIT HACKERS: - STRONG ACCESS SECURITY

Hackers vs. human error

Most account breaches are not blockbuster, headlinemaking hacks.

They are thefts of credentials, SIM swap takeovers, or successful phishing attacks.

Hackers will try the easiest path: your password, your phone, your email.



The layered security mindset

Create layers (like locks): password manager → unique password → 2FA → email hardening → device hygiene.

Each layer makes you a harder target. Hackers prefer soft targets.

Step-by-step: Build your “Access Shield”

Step A — Password hygiene (the foundation)

Install a trusted password manager: Bitwarden or 1Password are great choices.

Generate a unique, long password for: email, exchange accounts, wallets, and anything crypto-related.

Never reuse passwords.

Enable the password manager’s secure notes for storing recovery codes (encrypted).

How to use a password manager (practical):

Install Bitwarden (desktop + mobile).

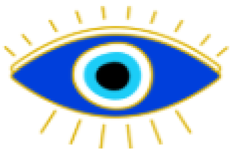
Create a strong master password — something you can remember but long enough to be secure.

Add all your crypto-related logins and let the manager generate unique passwords.

Save the emergency recovery key for your password manager in a safe place (paper + second location).

Step B — Two-Factor Authentication (2FA)

Use an authenticator app (Authy, Google Authenticator, or a built-in manager like 1Password).



Do not use SMS 2FA for crypto accounts — SIM swap attacks can defeat SMS.

Save backup codes for each site and store them offline (not on your phone).

How to set up 2FA (practical):

Log into your exchange. Go to Security settings → Two-factor authentication.

Choose "Authenticator app." Scan the QR with Authy/GA.

Enter the 6-digit code the app generates.

Save or print the backup codes and store them physically (***not*** in an unencrypted note).

Optional: Hardware 2FA (YubiKey)

For high-value holdings, hardware U2F keys (YubiKey) add powerful protection. They require you to **physically possess** the key to log in.

Step C — Lock your email (the key to everything)

- Use a separate email for crypto accounts (create a dedicated "crypto" email).
- Secure that email with the password manager + app 2FA (or hardware key).
- Make recovery details tough: don't use obvious security questions or reuse emails.

Step D — Phone & carrier security

- Add a PIN/passcode on your mobile with biometric information where available.

- Contact your phone carrier and set a SIM PIN or a porting/passcode so attackers cannot port your number with a social engineering call.

- Each carrier offers different options — ask support for a port-out PIN.

Step E — Device hygiene

- Keep your OS and apps up to date.

- Avoid unknown browser extensions, and don’t sideload apps.

- Use antivirus on PCs if you’re using Windows, and keep Mac security tight.

Quick checklist (do this now)

- Install password manager & save master key offline.

- Update all crypto-related passwords to unique ones.

- Turn on app-based 2FA for email and exchanges.

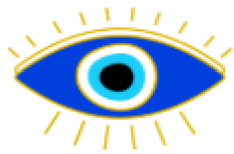
- Create a dedicated crypto email and secure it well.

Chapter 3

OUTSMART SCAMMERS: SPOTTING SOCIAL TRICKS

Scammers rely on emotion, not tech

Scammers will use FOMO (**F**ear **O**f **M**issing **O**ut) (get-rich-fast) and urgency (act now!) to push you into mistakes. They want you to click before you think.



Common scam types you'll see

Fake giveaways: "Send 0.1 ETH and get 1 ETH back." (Never.)

Phishing websites: Sites that look identical to official exchanges but have slightly different URLs.

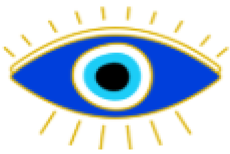
Fake support: Imposters posing as exchange support asking for login details.

Common scam types you'll see

- Fake giveaways: "Send 0.1 ETH and get 1 ETH back." (Never.)
- Phishing websites: Sites that look identical to official exchanges but have slightly different URLs.
- Fake support: Imposters posing as exchange support asking for login details.
- Impersonation on social media: Accounts pretending to be influencers or brands.

The three-check filter (a simple mental routine)

1. **Pause**. If a message forces you to act immediately, breathe. Real organizations don't bully you into instant action.
2. **Verify the source**. Type the official site URL yourself or use your bookmark. Confirm social accounts are verified.



3. **Never reveal keys or codes**. If asked for private keys, recovery phrases, or sign messages, that's a scam.

Real-life scripts you can use

- If someone DMs: "Please send your recovery phrase." → **Reply**: "No thanks — I don't share that. If you're in official support, show me a ticket number and I'll contact support from the official website."

- If a "friend" shares a hot tip: pause and check the contract address on CoinGecko and Etherscan. If it's a scam, the token will often have suspicious tokenomics.

Deeper checks (practical verification)

- Check contract addresses against CoinGecko/official website. Don't trust token names alone.

- For NFTs and token airdrops: be careful about signing transactions. Many dApps ask for spending approval; check exactly what you're approving before you sign.

Training your scam radar

- Spend 15–30 minutes each week scrolling through crypto groups. Identify common scam patterns. After you recognize a few, the rest become obvious.

- **AI / Deepfake Impersonation Scams**
  Scammers are using AI-generated videos & voices to impersonate known crypto figures, exchange CEOs, or influencer endorsements. They run fake live streams or Zoom calls promising giveaways, "investment opportunities," or token sales. People believe them because they look and sound so real, then lose money

- **Rug Pulls (especially with Memecoins & DeFi Projects)**
  New tokens are launched, hype builds up via social media, then the developers quickly withdraw liquidity ("pull the rug"), making the token worthless. Losses are often huge. This has been more common in 2025, especially for memecoins.

- **Pig-Butchering / Long Con Investment Scams**
  These are social engineering scams where fraudsters build a relationship over time, promise big returns, gradually involve victims in false investment platforms, then eventually take large sums. These are more psychologically complex and damaging.

- **Fake Giveaways, Airdrops, & Free Token Offers**
  People are being lured by seemingly generous "free tokens" or "airdrops" where you have to send a small amount first or

connect your wallet. Often they lead to phishing links, wallet draining, or giving someone access to your seed phrase.

- **Fake Bots / Trading Bots & Arbitrage Bots**
  Platforms or people selling “auto-profit” bots or arbitrage tools. The catch is the contract or code is rigged so once you provide access or pay, they drain your funds or never deliver.

Always verify the identity of people or platforms via multiple channels (official website, known Twitter/X handle, etc.).

Never trust unsolicited offers (“giveaway”, “double your coins if you send X amount”, etc.). If it requires sending crypto first or giving up your seed phrase, it’s almost always a scam.

Be extra careful clicking links, especially in DMs, social media or via email. Always check domain names carefully.

Keep only small amounts in hot wallets or exchanges. Store main holdings in wallets you control (hardware or well-secured software wallets).

Use tools to limit permissions (for smart contracts, wallet approvals, etc.), and revoke old / unused permissions.

Test the process with a small amount first before moving larger amounts.

Chapter 4

OUTSURVIVE EXCHANGE COLLAPSES: SELF-CUSTODY BASICS (UPDATED FOR LEDGER FLEX + EXODUS)

This is the heart of the book.

Self-custody is where beginners stop trusting other people to “look after” their coins and take real ownership of their digital wealth.

It sounds bigger than it is — and once you do it once, you’ll wonder why you waited.

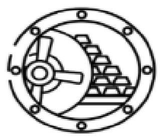
Below I’ll first explain the simple idea again, then walk you through two practical, hands-on transfers you can follow step-by-step:

1. Move Bitcoin from Kraken to a Ledger Flex (hardware — cold storage; best for long-term holdings).

2. Move Bitcoin from Kraken to an Exodus (hot wallet – mobile/desktop; good for everyday use or practice).

Do a small test transfer first (a tiny amount) until you are comfortable. That single habit — testing before sending big sums — prevents almost every horror story.

Why self-custody matters (short recap)



- Exchanges can freeze withdrawals, suffer hacks, or become insolvent. When that happens, funds held on the exchange are at risk.

- When you hold the private keys (seed phrase) yourself, you control the funds. But that control comes with responsibility: back up the seed and keep it offline.

- Self-custody = ownership. A little practice turns fear into confidence.

Wallet types (the short practical view)

- Hot wallets (Exodus, Trust Wallet, MetaMask) — connected to the internet, convenient for spending and small amounts. Great learning step.

- Cold wallets (Ledger Flex, Ledger Nano family, Trezor) — hardware devices keeping keys offline. Best for long-term savings.

Rule of thumb: keep only “spending” money on exchanges and hot wallets; the majority of savings should go into cold storage.

Part A — Transfer Bitcoin from Kraken → Ledger Flex (very detailed)

Quick note: Ledger Flex is a hardware wallet (a portable, offline device).

The steps below follow the safest practices: initialize device in private, never store seed digitally, always verify the receive address on the device screen, and always test with a small amount first.

What you'll need (prep before you start)
Your Ledger Flex device, cable, and packaging. (New device recommended.)

A desktop or laptop you control (avoid public/shared machines). Use Ledger Live desktop app from the official Ledger website.

Your Kraken account with BTC balance and 2FA enabled.

Pen and the recovery card that comes with the Ledger box (or steel backup if you have one).

A quiet, private space. No photos of seed words.

Step-by-step: Initialize Ledger Flex & set it up

(Time: ~10–20 minutes)

1. Unbox and inspect

2. Open the box.

3. Confirm packaging seal is intact and the device looks new.
4. Ledger devices are supplied to customers sealed; if anything looks tampered, return it and contact Ledger.

5. Install Ledger Live

6. On your desktop/laptop, go to the official Ledger website (type the URL yourself) and download Ledger Live for your OS. Install the app.

7. Connect the Ledger Flex

8. Attach the Ledger Flex to your computer via the supplied cable (USB). If using Bluetooth later, **we still recommend** an initial wired connection for setup.

9. Open Ledger Live → Get started → Set up as new device

10. Follow the prompts. When the device asks, choose Set up as a new device.

11. Create a PIN

12. On the Ledger Flex, pick a 4–8 digit PIN code you'll remember. Do not use obvious codes (e.g., 1234, birthdates).

13. Confirm the PIN on the device.

14. Write down your recovery phrase (24 words)

15. The device will display the 24 words, one at a time. Write them down in order on the recovery sheet included with the Ledger box.

16. **DO NOT** take photos. **DO NOT** type them into a computer or phone. These words are your backup —
if you lose them, your crypto is gone.

17. Confirm the recovery phrase on the device

18. Ledger will test you by asking you to confirm several words from the list. This ensures you wrote them down correctly.

19. Finish initial configuration

20. Ledger Live and the device will confirm setup is complete.

21. **Security tip**: Keep one written copy somewhere safe (e.g., a fireproof safe) and consider a second copy stored in a different secure location (bank safe deposit box, trusted family member) — never store both copies together.

Step-by-step: Install the Bitcoin app and add a BTC account in Ledger Live

(Time: ~5–10 minutes)

1. Open Ledger Live → Manager

2. Connect the Ledger Flex and unlock it with your PIN. Ledger Live will ask for permission to access the device; approve on the device.

3. Install Bitcoin app

4. In the Manager, find Bitcoin and click Install. The app on the device will appear (icon). This installs the Bitcoin manager on the Ledger Flex (it doesn’t transfer funds yet).

5. Add a Bitcoin account

6. In Ledger Live, go to Accounts → Add account → Bitcoin. Follow prompts while the Bitcoin app is open on the device. Ledger Live will create a Bitcoin account and display it.

Step-by-step: Generate & verify a Bitcoin receive address (<u>critical verification</u>)

(Time: ~2–5 minutes)

1. In Ledger Live, open the Bitcoin account and click Receive.

2. Ledger Live will show an address on your computer — but the most important step is to verify the address on the Ledger Flex screen: the device will display the same full address.

3. Confirm the address on the device by pressing buttons; only then copy it from Ledger Live.

    a. Why : malware can tamper with clipboard addresses. The physical device screen verification is the only secure confirmation.

4. Label the address in Ledger Live (e.g., "Ledger Flex — BTC Savings") so you know where it's going later.

Step-by-step: Add the Ledger receive address to Kraken for withdrawal

(Time: ~5–10 minutes)

1. Log into Kraken securely (use your dedicated crypto email and 2FA).

2. Go to Funding → Withdraw (or Funding → Withdraw Crypto).

3. Search/select Bitcoin (XBT) for withdrawals. Kraken may list BTC as XBT internally — that's standard.

4. Click Add Address (New Address) and paste the address you copied from Ledger Live.

5. Label the withdrawal address (e.g., “Ledger Flex Cold Storage”).

6. Select network: Bitcoin (BTC). If the address starts with bc1 (bech32), ensure Kraken supports bech32 (most exchanges do). If Kraken warns network mismatch, stop and check.

7. Kraken will prompt for confirmation via email and 2FA; complete those steps. Kraken may have a waiting or security hold — follow their instructions.

Step-by-step: Withdraw a small test amount from Kraken to Ledger Flex

(Time: ~5–30 minutes depending on network)

1. Choose a small test amount — something you’re comfortable risking, e.g., 0.0005–0.001 BTC (or equivalent). Test transfers prevent big mistakes.

2. On Kraken Withdraw → Bitcoin, choose the saved Ledger address, paste if needed, and enter the amount. Kraken will show estimated network fees. Confirm.

3. Confirm via Kraken’s email/2FA when prompted. Submit withdrawal.

4. Kraken will display a TXID (transaction ID) or show it in withdrawal history. Copy the TXID.

5. Use a block explorer (e.g., blockstream.info, mempool.space) and paste the TXID to see confirmations.

6. In Ledger Live, your Bitcoin account will show a pending transaction and, after confirmations, a completed balance.

7. Wait — only treat funds as fully secure after the required confirmations (Ledger Live shows status). For high values, wait for more confirmations (Ledger Live gives guidance).

After the transfer: Final checks & best practices

- Verify the received address shown in Ledger Live matches the confirmed on-device address before you send the second, larger transfer.

- Store recovery phrase in two separate secure places (not the same location). Consider steel backups for fire/flood protection.

- Label accounts in Ledger Live for bookkeeping.

- Practice a restore on another device using your written seed (optional, advanced): buy a spare hardware device, test restoring the seed with a tiny amount — only if you're confident.

- Never enter your recovery phrase into a phone/computer; only use the device itself to recover.

Troubleshooting & common pitfalls (Ledger Flex)

Address mismatch: If address on Ledger Live doesn't match device screen, disconnect, re-open Bitcoin app on device, and retry — do NOT proceed until matched.

Wrong network: Only send BTC over Bitcoin network. Sending tokens over wrong chains (BEP-20, ERC-20, etc.) can result in complicated recovery.

Withdrawal holds: Kraken can place holds on new withdrawal addresses — read Kraken's emails.

TX not showing: If Kraken says "complete" but no TXID appears, contact Kraken with screenshots; sometimes withdrawals are queued or need manual processing.

Part B — Transfer Bitcoin from Kraken → Exodus (Hot Wallet) (very detailed)

- A hot wallet like Exodus is a great practical step: it's easy, quick, and a good way to practice withdrawals.

- Exodus is user-friendly and great for beginners. Treat a hot wallet as your day-to-day wallet — not your long-term safe.

- **What you'll need (prep)**
- Exodus app installed on your mobile or desktop (download only from Exodus website or official app stores).

- Kraken account with BTC.

- A safe place to write down Exodus seed phrases (12–24 words depending on version).

- A small test amount to transfer.

Step-by-step: Install Exodus & create a wallet

(Time: ~5–10 minutes)

1. Download Exodus from the official site (type the URL yourself) or the official app store to your phone/desktop.

2. Open Exodus and create a new wallet. Choose a strong password for the app (this protects the app on that device).

3. Exodus will generate a backup/seed phrase for your wallet. Write it down on paper and store it securely. Exodus often also offers a recovery kit PDF — use it if you prefer.

4. Important: Exodus sometimes shows a 12-word seed and optionally a 24-word. **Follow its instructions exactly**. Backup is essential.

5. Confirm the backup words when prompted by Exodus to ensure you wrote them down correctly.

Security note: If you plan to use Exodus for real money, consider later pairing it with a hardware wallet (Exodus supports some hardware devices) for higher security.

Step-by-step: Get your Bitcoin receive address in Exodus

(Time: 1–2 minutes)

1. In Exodus, from the main wallet screen, choose Bitcoin (BTC).

2. Click Receive. Exodus will display a BTC receive address (a long string).

3. Copy the address or use the QR code (for mobile). Exodus displays the address in the app — verify the length and the first/last few characters if you want to be extra sure. Exodus **does not** have a physical device to verify on, so be careful to copy-paste correctly.

Step-by-step: Add Exodus address to Kraken & withdraw

(Time: ~5–15 minutes)

1. On Kraken: Funding → Withdraw → Bitcoin (XBT).

2. Add the Exodus address as a withdrawal address. Label it e.g., "Exodus — Mobile Wallet."

3. Confirm via Kraken's email/2FA flows. Kraken may require a waiting period if it's a new address.

4. Submit a small test withdrawal (e.g., 0.0001–0.001 BTC). Confirm transaction details and fees.

5. Copy the TXID from Kraken when available and paste into a block explorer to monitor confirmations.

6. In Exodus, check the Bitcoin wallet for incoming pending transaction; after confirmations it will display in your balance.

After the transfer: Practical follow-ups
Check transaction history in Exodus and the block explorer to verify full confirmations.

Secure your seed — that's the key to restoring your Exodus wallet if the device is lost. Consider a second backup copy in a different secure place.

Practice spending/receiving small amounts to become comfortable with the UI. Sending a small amount out of Exodus later (back to exchange or friend) is a good learning step.

Troubleshooting & common pitfalls (Exodus)

Clipboard malware risk: On desktop, malware can alter clipboard contents and swap your address with an attacker's. Always double-check the **first/last** characters of the pasting address before confirming.

Wrong address type: Be sure Exodus address is Bitcoin native (bech32 bc1) or legacy (starts with 1) depending on what Kraken supports. Kraken will warn of a network mismatch.

Seed phrase backup: If you lose the seed and your device fails, your funds are gone — Exodus cannot recover the backup for you. Keep it safe.

Quick comparison: Ledger Flex vs Exodus (when to use each)
Ledger Flex (cold) — best for long-term savings and high value: offline keys, highest security.

Exodus (hot) — best for everyday usage, small trades, practice, and DeFi experiments on supported chains (with caution).

Practice plan: Use Exodus for small, everyday amounts and learning. Move core savings to Ledger Flex.

Final Transfer Checklist (copy/paste printable)

Before any transfer

- Use a private, secure computer or phone.
- Confirm official software/URLs by typing them manually.
- Ensure 2FA is enabled on your exchange and email.
- Decide on a small test amount to send first.

For Ledger Flex (cold)

- Initialize Ledger Flex: PIN + write 24-word seed offline.
- Install Ledger Live + Bitcoin app.
- Generate receive address → verify on device.
- Add address in Kraken, complete email + 2FA confirmations.

- Withdraw a small test amount, track TXID on block explorer.
- After confirmation, send remaining funds if the test is OK.

For Exodus (hot)

- Install Exodus, set a strong app password.
- Write down and confirm the seed phrase.
- Get BTC receive address from Exodus (copy carefully).
- Add to Kraken, confirm email + 2FA.
- Withdraw a small test amount, monitor with TXID.
- Verify receipt in Exodus; then transfer remaining funds if all OK.

Troubleshooting summary (if things go wrong)

No TXID or pending forever: check Kraken withdrawal page; contact Kraken support with screenshots.

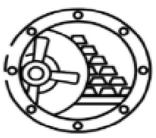
- Sent to the wrong network: contact the receiving platform immediately — sometimes recoverable, often complex.

- Address mismatch: do not proceed — re-generate address and verify on device or app.

- Hardware failure during setup: stop and contact Ledger support; do not use a compromised device.

You're Ready: Now Let’s Go

Final words for Chapter 4



Self-custody is the single most important skill you’ll learn in crypto.

The first time you move funds out of an exchange, your confidence will grow.

You'll know you control your money.

Do it carefully, do a test transfer, keep backups, and you'll be in the small group of crypto owners who have both upside and protection.

Final Notes & Disclaimers (Short)

This guide is educational — not financial or legal advice. For large holdings or complicated setups, consult a security professional.

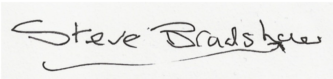
Always use official downloads and official support channels. Do not trust links sent in DMs.

The "Exclusive Invite"

You've just taken the first real steps toward bulletproofing your crypto journey.
Most people stop here.
But you don't have to.
To celebrate you finishing this book, I want to give you something special: **70% off my full step-by-step crypto mastery course**.
It's where I go deeper into the "how" — live demos, detailed strategies, and advanced techniques to actually make serious money.
Techniques that simply wouldn't fit here.
This discount is for readers only. Think of it as your fast-track ticket to true confidence in crypto.

Claim it now before it expires. Special Discount Code Applied Below:
(CLICK HERE)

To Your Success



https://www.cryptoknowledge.digital/