

PROTECT YOUR CRYPTO. CONTROL YOUR KEYS.

CRYPTO SECURITY & SELF-CUSTODY GUIDE

CHRIS SHEPLEY

IN PARTNERSHIP WITH



SHEPLEY CAPITAL

PRACTICAL STRATEGIES. REAL-WORLD EXAMPLES.

01 Why Security & Self-Custody Matters More Than Ever...

Cryptocurrency flips the traditional financial system on its head. Instead of banks, brokers, or institutions safeguarding your money, you become the bank. This is both liberating and dangerous. On one hand, no government, corporation, or middleman can freeze your account, deny your withdrawal, or take custody of your funds without your consent.

On the other, there is no safety net: if your wallet is compromised, if you fall for a scam, or if you simply mismanage your private keys, your assets are gone permanently. There's no "forgot password" button, no support ticket, no reversal. You are the first and last line of defence for your own finances.

In Traditional Finance	In Crypto
Banks protect deposits & insurers backstop losses	You are your own bank
Regulators enforce oversight	Your security decisions determine outcomes
Fraudulent charges can usually be refunded	Responsibility shifts entirely to the individual

This makes security and self-custody the most critical foundations of crypto participation. The best investment strategy means nothing if you can't keep your assets safe.

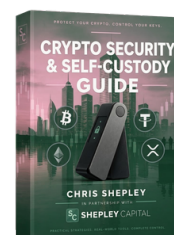
Why Security Matters More Than Ever

Innovation is typically accompanied by attention, attention brings emotion, and emotion brings rushed decisions. In 2024/2025 alone, roughly AUD \$16 billion was lost to scams and theft through exposed holdings and poor security practices.

- Billions lost to hacks and scams every year: Centralised exchanges breached, DeFi platforms exploited, individuals tricked into giving up seed phrases
- Rapid adoption means bigger targets: Bad actors constantly innovate to exploit newcomers and veterans alike through emails, fake SMS, and lookalike domains
- Losses are permanent: Sending crypto to the wrong network, exposing keys, or losing wallet access can mean losing everything, forever

Explore our full Cryptopedia here

CRYPTOPEDIA



02 Private Keys & Seed Phrases

At the core of cryptocurrency lies one simple truth:

"Control over your private keys equals control over your money."

The Significance of a Private Key & Seed Phrase

A private key is a long cryptographic string that acts as the master password to your crypto. Your entire portfolio sits behind a wall guarded by this string, which only you should ever know. As the holder, you control every movement of that capital: moving funds between wallets, depositing or withdrawing from third-party platforms, and authorising transactions.

When you create a new wallet, it generates a unique private key (usually around 50 characters) alongside a seed phrase, a human-readable backup made up of 12–24 words. These words are written in the exact order they're first shown, and act as your recovery method if the private key itself is lost. They're generated automatically at wallet creation and cannot be custom-chosen.

Seed Phrase

1. cat	5. rotate	9. flame
2. round	6. steel	10. capital
3. prosper	7. table	11. iconic
4. hound	8. park	12. white

Private Key

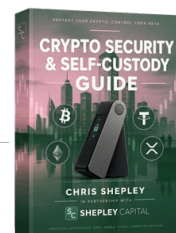
```
to7dnhdem57amech392111chrol
l05fd8954nukasds758bbcrevtsv
hrrbfgj4jfgmsdlsgsd
```

⚠ WARNING

If someone else gains access to your private key or seed phrase, they gain full access to your funds. There is no recovery process that can undo this.

It's important to clarify that there is a difference between a 'Private Key' and a 'Public Key'. Whilst all wallets have both a private key & a public key, like the name suggests; one is used as a private cryptographic string that acts as the master password to your crypto, the other being used as a cryptographic address used to receive crypto. A public key is safe to share with those who intend to send you cryptocurrency. Think of a public key just like an email address, or bank account number; you give this information out to receive correspondence or financial compensation, however you wouldn't give out your password to either one of these accounts.

Explore our full educational resources on Private Keys and Seed Phrases with the buttons below:

[PRIVATE KEYS](#)
[SEED PHRASE](#)


03 Non-Custodial vs. Self-Custody

 **Non-Custodial** = Convenience, but you trust someone else to protect your funds.

 **Self-custody** = Freedom & Security, but greater personal responsibility.

A **Non-custodial** crypto service is one where a third party holds your private keys on your behalf. When you hold Bitcoin on CoinSpot, Swyftx, Binance, or any other centralised exchange, you do not actually hold Bitcoin. You hold a claim on Bitcoin that the exchange has recorded in its internal ledger. The exchange holds the actual private keys that control the on-chain assets. You are trusting the exchange to honour your claim when you want to withdraw.

Self-custody is the practice of personally holding and managing your own private keys with full responsibility for their security, backup, and recovery. It is a practice and a philosophy as much as a technical state. True self-custody means you have generated your own seed phrase, recorded it correctly, stored it securely in a location only you control, understand how to use it to recover your wallet if your device is lost or damaged, and have taken responsibility for every aspect of your crypto security.

NON-CUSTODIAL

BENEFITS:

- ✓ Easy to access Funds.
- ✓ User-friendly Exchange Interface.
- ✓ Dedicated support team.
- ✓ Broad Range of Asset Offerings.

RISKS:

- ✗ Exchange Data/Funds hacks.
- ✗ Exchange Insolvency.
- ✗ Frozen withdrawals.
- ✗ Government seizures.

SELF-CUSTODY

BENEFITS:

- ✓ Total sovereignty over your funds.
- ✓ Zero reliance on external parties.
- ✓ Instant 24/7 Access to 100% funds.
- ✓ Freedom to Transfer when desired.

RISKS:

- ✗ 100% responsible for security.
- ✗ Loss of keys, loss of crypto funds.
- ✗ No support team to help you.
- ✗ Physical Device must be kept safe.

Explore our full educational resources on Non-Custodial vs. Self-Custody with the button below:

[Non-Custodial vs. Self-Custody](#)



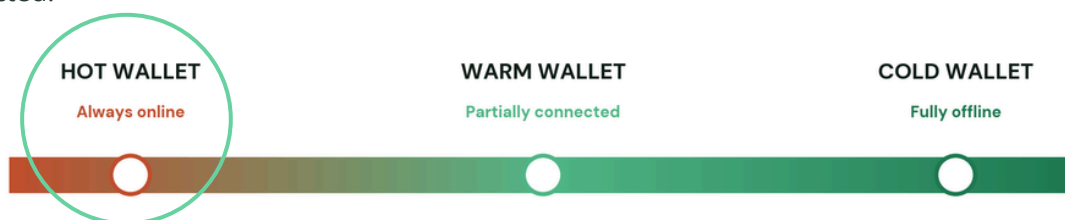
RULE OF THUMB

We recommend self-custody for all amounts above AUD \$10,000. Anything below that can still be self-custodied, especially for long-term holding.



04 Hot Wallets

Hot Wallets are the most popular form of Non-custodial wallet, especially for newer investors. A hot wallet is a custodial wallet that is permanently connected to the internet, typically associated with exchanges. This constant connectivity makes it fast and convenient for everyday investors to make trades on the go, with the choice to access your funds via mobile phones, desktop applications, or web browsers. However hot wallets also rely on the security & storage of the chosen exchange to protect your funds, whilst avoiding being exposed to cyberattacks and human error if not properly protected.

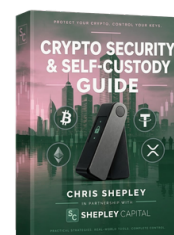


Pros	Cons
Instant access for quick trading/payments	High hacking risk if not secured properly
User-friendly, clean interfaces	Device dependency
Required for DeFi, NFTs, & Staking protocols	Centralisation risk, you don't own the keys
Free to download and start using within minutes	Not suitable for large or long-term storage

Benefits & Use Cases

Hot wallets possess a number of benefits & use cases that are tailored towards the everyday investor, making the overall cryptocurrency experience much smoother than other wallet variants. These are some of the environments where a hot wallet is best suited for an investor:

-  **Convenience:** Simplistic Crypto investing process.
-  **Liquidity:** Quickly buying, selling, or swapping coins.
-  **DeFi Access:** Yield farming, lending, NFT marketplaces, token launches.
-  **Active Trading:** Perfect for frequent traders who need speed.
-  **Mobile Access:** Manage assets anytime, anywhere from your phone or laptop.



Risks & Vulnerabilities

With any benefit comes a risk aspect, and Hot wallets are no different. Whilst some may seem less obvious than others, all risk profiles have their own unique rankings to the individual investor.

- 🐟 Phishing attacks: Fake websites and apps trick users into entering their seed phrase.
- 🦟 Malware/Spyware: Malicious software that reads your clipboard, replacing wallet addresses.
- 💥 Exchange hacks: Centralised platforms holding millions of hot wallets are prime hacker targets.
- 👤 Human error: Sending funds to the wrong chain or address.
- ⌚ Custody Risks: Keeping large balances in hot wallets increases exposure over time.
- 🔑 No Keys, No Crypto: You don't own the keys or seed phrase... the exchange does. If something was to happen to the exchange, you'll be the first affected.

Is a Hot Wallet Right for You?

Whilst hot wallets are among the easiest to manage, they might not be the ideal option for everyone. Here are the For & Against of selecting a hot wallet:

Who Should Use a Hot Wallet?	Who Shouldn't Use a Hot Wallet?
Active Traders	Long Term Holders
Experimenters / Learners	Life Savings
Daily Spenders	Low-Security Users

Best Practices for Hot Wallet Safety

These are our best practise tips for those of you that decide that a hot wallet is right for you:

- 1 Only keep small balances (think "wallet cash," not savings).
- 2 Always enable two-factor authentication on exchange wallets.
- 3 Double-check URLs and apps before logging in.
- 4 Never store seed phrases digitally (screenshots, cloud storage, notes). Write them down on paper.
- 5 Use hot wallets as transactional tools, not as financial vaults.

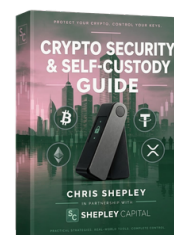


BEST PRACTICE

Keep only small, "wallet cash" balances. Enable 2FA, double-check URLs before logging in, and never store seed phrases digitally, write them down on paper.

Visit the full Hot Wallet Guide here

HOT WALLET GUIDE



05 Warm Wallets

A warm wallet sits between a hot wallet (always online) and a cold wallet (completely offline). It provides a balanced solution between investors who are looking for a more secure setup than a hot wallet, but still easier to access than cold storage. Unlike a hot wallet, you personally control your own private keys that give you exclusive access over your crypto holdings. In line with such, warm wallets are the favourite for those who want broad access to the market that an exchange provides, yet desire the sole-custody ownership of their assets that owning your own keys provides.

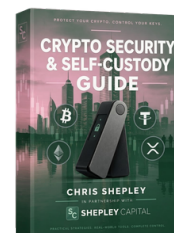
With this in mind, a greater level of self-reliance emerges where investors must be able to confidently navigate the DeFi space of cryptocurrency in a safe & secure manner. Failure to do so could lead to serious risks & financial exposure.



Pros	Cons
Stronger security than hot wallets	Still compromisable, not fully offline
Moderate convenience for moving funds	More complex to use
Scalable protection (2FA, multi-sig)	Slower transactions from extra security layers
Better suited to medium-term holding	Zero built-in support, fully self-reliant

Benefits & Use Cases

Warm wallets shine in situations where speed & accessibility are equally as desired as self-custody & security. For investors who seek the ability to hold securely for the long-term, or actively trade the markets at will, these are the highlight benefits that a warm wallet provide:



- ⚡ Convenience: Easier access than cold wallets for regular transactions.
- 🛡️ Enhanced Security: More protected than hot wallets, often using hardware or multi-sig features.
- 🔗 Flexible Use: Can interact with exchanges or DeFi while keeping larger balances relatively safe.
- 🔑 Key Ownership: You retain control of your private keys, unlike hot wallets.
- 💳 Regular Payments: Manage recurring crypto transactions or medium-term holdings with better security.
- 👛 Integration: Can connect safely to multiple platforms, apps, or dApps with reduced risk.

Risks & Vulnerabilities

Whilst warm wallets provide greater security measures than hot wallets, they can also hold more risk if the individual investor lacks the knowledge to correctly use the wallet.

- 👤 Targeted cyberattacks: Hackers often go after warm custody services and institutional platforms.
- 🏢 Insider risks: Because warm wallets are often multi-user, bad actors within a company can exploit access.
- 🌐 Not Disconnecting: Forgetting to disconnect your warm wallet from 3rd party websites (DeFi Applications) can keep your funds open to be exploited.
- 😬 Overconfidence: Some users treat warm wallets as “just as safe as cold,” which they are not.
- 🧑 Human error: Sending funds to the wrong chain or address increases risk.

Is a Warm Wallet Right for You?

Whilst a warm wallet seems from the outside to offer the best of both worlds, there are a few trade-offs that should be considered. Here are the For & Against of selecting a warm wallet:

Who Should Use a Warm Wallet?	Who Shouldn't Use a Warm Wallet?
An active or mid-term trader moving funds every few days/weeks	A complete beginner (added complexity, easy mistakes)
An institution needing controlled access & audit trails	Storing large, long-term holdings
Security-conscious without wanting a hardware wallet daily	Sharing a device with multiple users

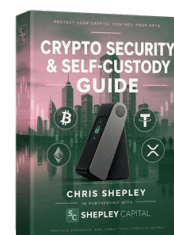


BEST PRACTICE

Use 2FA and/or multi-sig where available, add withdrawal alerts, and keep an offline paper backup of your keys in case the software fails.

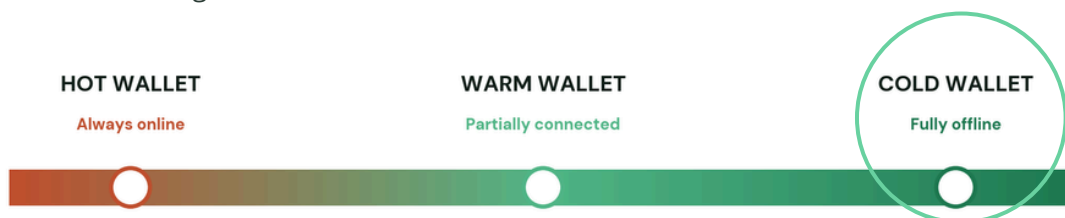
Visit the full Warm Wallet Guide here

WARM WALLET GUIDE



06 Cold Wallets

Cold wallets (also known as a hardware storage device) are the gold standard for securing large sums of crypto, both for long-term holders (HODLers) and institutions managing internal funds. Designed as a 2FA device that functions completely offline, cold wallets are considered by far the safest form of crypto storage method, removing the risk exposure when it comes to hacks, phishing attacks, malware, and other online threats. As the preferred choice for long-term wealth holding, cold wallets generate their own unique private keys & recovery phrase inside the physical device, never touching an internet connection.

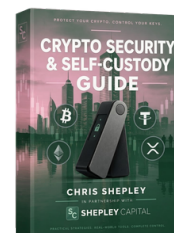


Pros	Cons
Highest security level, virtually immune to online attacks	Less convenient to access
Ideal for long-term storage	Physical risks — loss, theft, fire, damage
Full ownership sovereignty	Initial cost, typically AUD \$75–\$375 per device

Benefits & Use Cases

Cold wallets are setting the standard for long-term digital wealth storage. Closely comparable to a traditional banking system, cold wallets act as a vault for your funds that remain locked away from the cyber world. Only in this case, that bank is located right in the palm of your hand. For most people, the idea that you could access any amount of your funds without having to go through the hassle of explaining yourself to the teller is enough of a reason to choose a cold wallet. Here are just a few of the core benefits that a cold wallet provide:

- 🛡️ Long-term investors storing life savings in BTC, ETH, or other major assets.
- 🏛️ Institutional holdings requiring maximum security (custody firms often split keys across locations).
- 👤 High-net-worth individuals protecting crypto from theft or hacks.
- 🔒 Offline backup for hot or warm wallets: Moving funds in & out of cold storage for extra protection.
- 💳 Sole custody of assets at the highest level of security available (on par with banks)
- 👵 Wealth Succession Planning: Properly stored seed phrase, private keys, & hardware wallet creates a clear inheritance plan for family without relying on centralised exchanges.



Risks & Vulnerabilities

Whilst from a security of usability perspective cold wallets could be deemed seamless, there are a few tangible risks & vulnerabilities that could arise if not responsibly used:

-  Seed phrase loss/misplacement: Without it, your funds are lost forever.
-  Physical theft or destruction: Hardware wallets or paper backups can be stolen or damaged.
-  Improper setup: Using an unverified device or compromised firmware can introduce vulnerabilities.
-  Human error: Mismanaging multiple wallets, copying keys incorrectly, or sending funds to the wrong chain or address increases risk.
-  Excessive 3rd party DeFi connections: Ignoring the nature of a cold wallet by treating it as if it was a warm wallet.

Is a Cold Wallet Right for You?

Whilst a cold wallet for most investors is typically the right move, there are some caviars that may persuade alternative wallet choices. Here are the For & Against of selecting a cold wallet:

Who Should Use a Cold Wallet?	Who Shouldn't Use a Cold Wallet?
Long Term Investors / HODLers (<i>\$10K+ Holdings</i>)	Active day traders needing instant access.
Institutions managing internal funds.	Newer investors seeking a simplistic approach to crypto (<i>Less than \$10K Holdings</i>)
Investors seeking self-custodial & high level security systems.	Investors who aren't able to safely store their hardware wallet

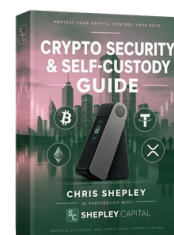


KEY TAKEAWAY

For long-term holders and anyone with significant wealth (AUD \$10,000+), a cold wallet paired with a metal seed-phrase backup is the recommended approach.

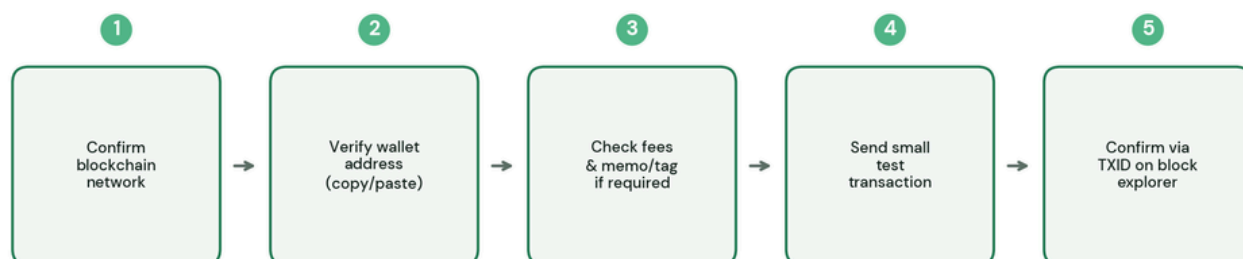
Visit the full Cold Wallet Guide here

COLD WALLET GUIDE



07 Safe Transfers, Deposits & Withdrawals

When most people think about security in crypto, they imagine hackers breaking into wallets or exchanges. But in practice, one of the riskiest parts of the entire process is something much more ordinary: moving your funds. Transfers, deposits, and withdrawals are the moments where the majority of costly mistakes occur. The blockchain does not forgive human error, so understanding how to execute these steps with precision is essential.



Choosing the Right Blockchain

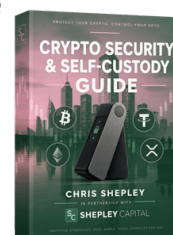
The first layer of risk comes from sending assets across the wrong blockchain. Many cryptocurrencies exist in multiple formats: USDT alone can be issued on Ethereum (ERC-20), Tron (TRC-20), Binance Smart Chain (BEP-20), and others. If you attempt to withdraw to a wallet that doesn't support the network you selected, those funds may be permanently lost. Before every transfer, confirm that both the sending and receiving platforms support the same network. If you are unsure, always default to the most widely supported version of the token (for example, ERC-20 for Ethereum-based assets) or consult the official documentation of your wallet or exchange.

Double-Checking Transaction Details

It's not just addresses that matter. Transaction fees, token amounts, and even memo tags can determine whether your funds arrive safely. Some cryptocurrencies such as XRP, XLM, or ATOM require a destination tag or memo in addition to the address. Forgetting this step can result in your funds being stuck or delayed indefinitely. Exchanges typically display reminders for these assets, but never rely solely on prompts. Make it a habit to review every field carefully before clicking confirm.

Transaction Hashes and Confirmations

Every transaction on the blockchain generates a unique transaction hash (TXID), which serves as its permanent receipt. Once you initiate a transfer, save the TXID and use it to track progress on a block explorer. This step confirms that your transaction is not only sent, but also verified by the network. Block explorers show the number of confirmations, which provides assurance that the transfer has been permanently settled and cannot be reversed by a chain reorganization. If you ever need to troubleshoot with an exchange, the TXID is the first piece of information support will request.



Timing and Network Congestion

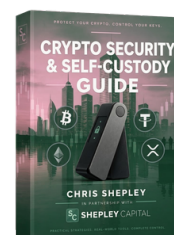
During periods of high network congestion, transaction fees can spike, and confirmation times may slow dramatically. If you attempt to move funds without adjusting for this, your transaction could be delayed for hours or even days. As an optional step, check current network fees using tools like Etherscan's gas tracker or similar dashboards before sending, and consider adjusting your fee level if you need faster settlement.

Deposits and Withdrawals on Exchanges

When depositing funds into an exchange, always verify that the exchange supports the token and network you are using. Sending unsupported tokens to an exchange wallet is one of the fastest ways to lose funds permanently. Likewise, when withdrawing from an exchange to self-custody, check whether the withdrawal network aligns with your receiving wallet. Many traders default to cheaper chains (like TRC-20 for USDT), but saving a few dollars in fees is meaningless if it introduces compatibility issues later.

Final Layer of Safety

The golden rule with all transfers, deposits, and withdrawals is this: slow down. Most losses occur because people are in a rush; rushing to buy a dip, rushing to move funds before a trade, or rushing under pressure from FOMO. Instead, take a breath and verify everything two or three times before hitting confirm. Precision is the only safety net in crypto.



08 Avoiding Scams & Trading Risks

The fastest way to lose your cryptocurrency is not through a bad trade, but through deception. Hackers and scammers don't usually break blockchains themselves — instead, they exploit human error. In a system where transactions are irreversible, once your funds leave your wallet, there is no customer service line to call, no bank dispute to file, and no “undo” button. This makes scam awareness and risk management just as important as investment strategy.

Here's how to spot and avoid the biggest threats & trading risks:

Trading Risks Worth Managing

Check out our *“How to Avoid Crypto Scams”* lesson in our Cryptopedia for a more detailed resource guide.

Phishing Attacks

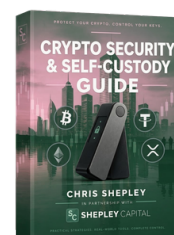
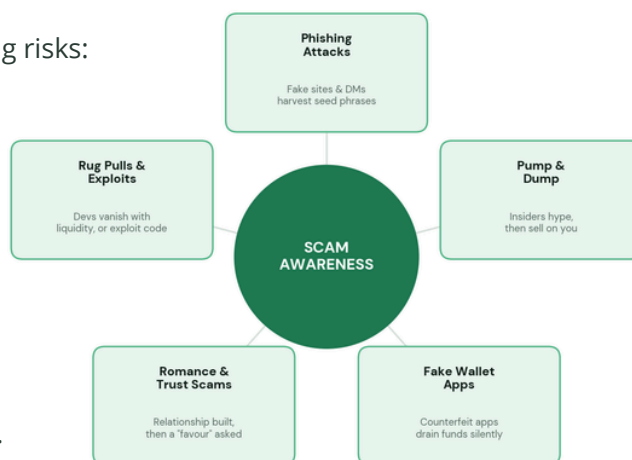
These scams mimic the websites of exchanges, wallets, or decentralized applications, tricking people into entering sensitive information such as private keys or seed phrases. Often, they arrive via emails, fake Google ads, or direct messages on platforms like Telegram and Twitter. Once you type in your details, the scammer has complete access to your wallet.

The defence is simple but non-negotiable: never click unknown links, always use bookmarked URLs, and remember that no legitimate crypto platform will ever ask you for your seed phrase.

Pump-and-dump schemes

This is where a group of insiders hypes up a new or obscure token, often spreading promises of “guaranteed moonshots” in online communities. By the time unsuspecting buyers rush in, the insiders are already selling at inflated prices, leaving newcomers holding worthless bags.

The solution here lies in discipline and skepticism. Before buying into any asset, check its trading volume, liquidity, and whether the project has real fundamentals. If the only selling point is “we’re going to the moon,” it’s already too late. Keep in mind that this has essentially described the entire Memecoin market.



Fake Wallet Apps or Extensions

Fake wallet apps and browser extensions present yet another risk. Criminals often publish counterfeit versions of well-known wallets in app stores or as downloadable software. Once installed, these apps silently drain your funds or capture your seed phrase.

Protecting yourself comes down to diligence: only download wallets from official websites, and double-check that the app developer matches the legitimate team.

Romance & Trust-Based Scams

Fake wallet apps and browser extensions present yet another risk. Criminals often publish counterfeit versions of well-known wallets in app stores or as downloadable software. Once installed, these apps silently drain your funds or capture your seed phrase.

Protecting yourself comes down to diligence: only download wallets from official websites, and double-check that the app developer matches the legitimate team.

Rug Pulls & Exploits

These occur when developers launch a token or decentralised finance project, attract liquidity, and then vanish overnight with investor funds. In some cases, the exploit comes from within the project code itself, malicious backdoors written into smart contracts that allow developers to drain liquidity pools at will.

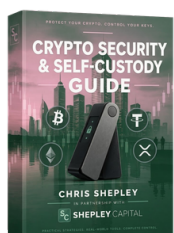
To avoid these traps, research is critical. Look into whether the development team is anonymous or publicly recognised, whether smart contracts have undergone security audits, and whether the project has long-term credibility beyond social media hype. Never invest in projects you have no knowledge about.

Trading Risks Worth Managing

Check out our *"How to Manage Trading Risks"* lesson in our Cryptopedia for a more detailed resource guide.

Incorrect Blockchain / Address

Even outside of scams, trading itself carries risks that beginners often underestimate. A simple mistake such as sending funds on the wrong blockchain can result in permanent loss. Likewise, mistyping a wallet address or copying the wrong string is enough to lose funds forever. The best practice is to always copy and paste addresses, never type them manually, and send a small test transaction before moving large sums.



Lack of 2FA on Exchanges & Wallets

Many people still fail to secure their exchange accounts with Two-Factor Authentication (2FA), leaving themselves vulnerable to hackers who only need a password leak to get in. Even worse, some rely on SMS-based 2FA, which can be bypassed with SIM swap attacks. Adopting the simple practise of using an authenticator app such as Google Authenticator can strengthen protection greatly.

Trading on Unsecured Wi-Fi

Trading on unsecured public Wi-Fi networks opens the door to man-in-the-middle attacks, where attackers intercept your data in transit. The rule of thumb is to only trade on trusted networks and, when possible, use a VPN for an added layer of protection.

Overexposure & Leverage

One of the greatest trading risks of all isn't scams or hacks... it's your own trading psychology.

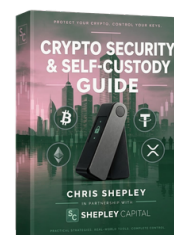
Over-leveraging, going all-in on a single trade, or risking more than you can afford to lose is a guaranteed way to get liquidated. Many traders who survive the technical threats still destroy their portfolios through greed and lack of discipline. Risk management is a security practice in itself. A strong rule, such as never risking more than 5-10% of your portfolio on a single trade, is as essential as any hardware wallet. This percentage can vary depending on investor experience.

Golden Rules to Stay Safe

The golden principles of safety in crypto boil down to discipline and paranoia.

- ✓ Treat your seed phrase like the keys to your vault; never store them digitally, never share them, and never trust anyone who asks for them.
- ✓ Double-check every transaction detail; address, blockchain, and amount before confirming. If a situation feels rushed, don't act. Scammers thrive on urgency and FOMO.

And above all, remember that every stranger in this space could be trying to take your crypto. Keeping that mindset may sound harsh, but it's the one thing that could save you from catastrophic loss.



09 FAQ

What is self-custody in crypto?

Personally holding the private keys to your cryptocurrency, rather than leaving them with an exchange or third party. Only you control access, which removes counterparty risk but places full security responsibility on you.

Why is self-custody considered safer than an exchange?

Exchanges can be hacked, go bankrupt, or freeze withdrawals, as seen with FTX. With a hardware wallet, your funds remain accessible regardless of what happens to any exchange.

What are the biggest risks of self-custody?

Losing your seed phrase, storing it insecurely, falling for phishing attacks, and using malware-infected devices during setup or transactions.

What is a seed phrase and why does it matter?

A 12–24 word recovery phrase generated at wallet setup. It's the master key to all funds in that wallet, and must be written on paper and stored securely offline, never digitally.

What's the best type of wallet for self-custody?

A hardware wallet is generally the gold standard. For large holdings, pairing it with a metal seed-phrase backup is the recommended approach.

Can I recover my crypto if I lose my hardware wallet?

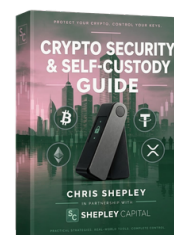
Yes, as long as you still have your seed phrase. Import it into a new hardware or compatible software wallet to regain full access.

How should I store my seed phrase safely?

Write your seed phrase on paper or stamp it into a metal plate, and store it in a physically secure location such as a safe. Never store it digitally, in email, cloud storage, or photos. Consider keeping a second copy in a separate secure location in case of fire or flood. Never share it with anyone.

What common mistakes do beginners make with self-custody?

Common beginner mistakes include taking a photo of the seed phrase, storing it in a notes app, never testing wallet recovery before depositing large amounts, buying hardware wallets from unofficial resellers, and entering seed phrases on fake wallet websites. Always buy direct from the manufacturer and verify device authenticity before use.



Stay safe out there.

This playbook is part of Shepley Capital's Premium library.
For the full lesson series, visit shepleycapital.com/cryptopedia

— Chris Shepley, Founder, Shepley Capital

This document is for general information and education only. Nothing in this playbook constitutes financial advice. Always do your own research before making any investment decisions.

