PORTFOLIO SECURITY GUIDE

SHEPLEY CAPITAL

Portfolio Security Guide

How to protect every dollar of your crypto portfolio

In the world of crypto, you are your own bank. That statement carries more weight than most investors initially appreciate. The decisions you make about custody, access management, platform selection, and seed phrase storage are the difference between a portfolio that compounds over years and one that is lost in a single avoidable event. This guide covers every dimension of portfolio security for Australian crypto investors.

Access Cryptopedia

- ✓ 750+ Educational Resources
- ✓ 10 Topic Categories
- ✓ 100% Free Access, Forever

1. Exchange Risk

Centralised exchanges represent the single largest source of preventable capital loss for retail crypto investors. Events such as the FTX collapse (November 2022), Celsius Network freeze (July 2022), Mt. Gox hack (2014), and the most recent forced regulatory closures of many exchanges, collectively resulted in billions of dollars in permanent user losses. Whilst the intended purpose of exchanges are unquestionably safe by design, extended reliance on 3rd party security architecture is where the risks begin to unfold.

◆ Key Exchange Risks

Risk Type	Description	Protection
Insolvency	Exchange cannot meet withdrawal obligations due to mismanagement or fraud	Never hold more than 30-40% of portfolio on any single exchange
Hacks	Exchange hot wallets breached; user funds drained	Move non-trading capital to self-custody immediately after purchase
Regulatory freeze	Government or regulator orders exchange to freeze withdrawals	Diversify across multiple licensed, regulated exchanges
Account lockout	Account suspended due to KYC, regional restrictions, or security flags	Maintain verified accounts on multiple platforms; keep records of all activity
Insecure access	Weak password or absent 2FA allows account takeover	Strong unique password + authenticator app 2FA on every account

◆ Exchange Exposure Framework

> THE 30% RULE
>
> No single exchange should hold more than 30% of your total crypto portfolio at any time. Anything above this threshold represents concentrated counterparty risk. Funds not actively required for trading or investment activity belong in self-custody.

2. Custody: Hot, Warm & Cold Wallets

Custody refers to who holds the private keys that control your cryptocurrency. The custody model you choose determines your level of security, convenience, and personal responsibility. There is no single right answer for how you choose to setup your portfolio storage as everybody's situation is different; the appropriate choice depends on portfolio size, activity level, and technical confidence.

Wallet Type	Network Access	Key Holder	Best For	Risk Level
Hot Wallet (Exchange/App)	Always online	Exchange / third party	Active trading; small balances under $10,000	HIGH — no key ownership; exchange counterparty risk
Warm Wallet (MetaMask etc)	Online when open	You	DeFi access; regular use; medium balances $10k–$50k	MEDIUM — key ownership; internet exposure when active
Cold Wallet (Hardware)	Offline by default	You	Long-term holding; large balances over $25,000	LOW — fully offline; physical device security required

◆ Recommended Custody Thresholds

Portfolio Value	Recommended Custody Model
Under $5,000	Hot wallet acceptable for active traders. Self-custody warm wallet preferred for investors.
$5,000–$25,000	Warm wallet (self-custody) for active funds. Consider hardware wallet for holdings above $10,000.
$25,000–$100,000	Hardware wallet (cold storage) for the majority. Warm wallet only for active trading allocation.
$100,000+	Primary cold storage essential. Consider multi-signature setup. Warm wallet for active trading slice only.

For detailed guides on choosing a wallet, setting up hardware devices, and safe custody practices, check out any of these extended resources:

Choosing a Wallet | Setting up Hardware Wallet | Safe Custody Practises

3. Seed Phrase & Private Key Safety

Your seed phrase; typically 12 / 24 words generated at wallet creation, is the master key to your entire crypto portfolio. Anyone who obtains your seed phrase gains complete and irreversible control over all assets in that wallet. There are no exceptions, no recovery options, and no appeals process. This makes seed phrase management the single highest-stakes security decision in crypto.

◆ The Non-Negotiable Rules

- NEVER store your seed phrase digitally: No photos, no cloud documents, no notes apps, no email drafts, no password managers.
- NEVER type your seed phrase into any website, application, or form: Legitimate wallets never ask for it after setup.
- NEVER share your seed phrase with anyone: No support team, advisor, or platform representative has a legitimate reason to request it.
- ALWAYS write your seed phrase on paper at the moment of wallet creation, in the exact order shown.

- ALWAYS store written seed phrases in at least two physically separate, secure locations (e.g., home safe and bank safety deposit box).
- ALWAYS verify your seed phrase backup by testing wallet recovery on a secondary device before storing significant funds.

◆ Seed Phrase Storage Options

Storage Method	Security Level	Recommended?	Notes
Paper (handwritten)	Medium	YES — baseline minimum	Water and fire risk; use quality paper; store in sealed bag
Metal backup plate	High	YES — recommended	Fire and waterproof; products like Cryptosteel, Bilodl; best option for long-term
Password manager	Low-Medium	NO	Digital storage creates online exposure; not acceptable for seed phrases
Cloud storage (Drive/iCloud)	Very Low	NEVER	Any cloud breach exposes seed phrase immediately and permanently
Photo on phone	Very Low	NEVER	Phone theft, backup sync, or cloud upload creates critical exposure
Bank safety deposit box	High	YES — as second copy	Excellent secondary location; verify access rules for estate planning

4. Account Protection

Exchange account security is the first line of defence for funds held on centralised platforms. The following practices are non-negotiable for anyone holding meaningful capital in crypto.

Security Practice	Priority	How to Implement
Two-Factor Authentication (2FA)	CRITICAL	Use an authenticator app (Google Authenticator, Authy). SMS-based 2FA is vulnerable to SIM-swap attacks — do not use it.
Unique strong passwords	CRITICAL	Use a different password for every exchange. Password manager recommended. Minimum 16 characters, random.
Withdrawal address whitelisting	HIGH	Set up a whitelist of approved withdrawal addresses on major exchanges. New addresses require a time-delay or email confirmation.
Anti-phishing codes	HIGH	Many exchanges allow you to set a custom phrase that appears in all legitimate emails. If missing from an email, it is a phishing attempt.
Email security	HIGH	The email tied to your exchange is as valuable as your account. Secure it with a strong password and 2FA. Use a dedicated email for crypto.
Device security	MEDIUM	Only access exchanges from trusted devices. Keep operating systems updated. Use antivirus software. Avoid public Wi-Fi without a VPN.

5. Portfolio Diversification as Security

Diversification in the security context is not just about spreading market risk, but also about ensuring that no single failure point can wipe out your entire portfolio. Apply this thinking across exchanges, custody methods, and asset types.

Diversification Layer	Rule
Across exchanges	Maximum 30–40% of total crypto on any single exchange. Use at least two regulated platforms.
Across custody types	Never hold 100% of assets on exchanges. Maintain self-custody for the majority of holdings above $10,000.
Across asset types	Core large-caps (BTC/ETH) should anchor the portfolio. Reduce exposure to unaudited or anonymous projects.
Across locations	Seed phrase backups and hardware wallets stored in multiple physically separate locations.

Further Reading — Cryptopedia

Topic	Cryptopedia Resource
Wallet types and selection	Access Resource
Self-custody security practises	Access Resource
Exchange selection and due diligence	Access Resource
Scam awareness and avoidance	Access Resource
Crypto security awareness guide	Access Resource

GENERAL ADVICE DISCLAIMER

This document is produced by Shepley Capital (shepleycapital.com) for general educational and informational purposes only. It does not constitute financial product advice, investment advice, or any other form of regulated advice.

Security information provided reflects general best practices as of the date of publication. Threats evolve rapidly — readers should regularly verify that their security practices remain current. No security measure is guaranteed to prevent all loss.