

SECURITY ESSENTIALS CHECKLIST



#DocDren

Digital Sovereignty & Security: Your Essentials Checklist

PROTECTING YOUR ASSETS AND IDENTITY IN THE DIGITAL AGE

You don't own it unless you control it. In the digital world, control means security. This checklist ensures you're taking the fundamental steps to protect your digital assets and identity, safeguarding your financial future and legacy.

HOT VS COLD WALLETS & SELF-CUSTODY

Understand the Difference

Know when to use hot (convenient) vs cold (secure) wallets.

Self-Custody Principle

If you don't control the private keys, you don't truly own the asset.

Action Item

Store the majority of significant holdings in a cold wallet.

PRIVATE KEYS & SEED PHRASES

Never Share:

Your private key or 12/24-word seed phrase should *never* be shared with anyone.

Secure Storage:

Write down your seed phrase and store it in multiple secure physical locations (e.g., fireproof safe, safety deposit box).

Digital Storage Risks:

Avoid storing seed phrases digitally (on computers, phones, cloud) unless encrypted.

Action Item:

Back up your seed phrase today and verify you can restore your wallet from it.

AVOIDING SCAMS, FAKE AIRDROPS & PHISHING

Red Flags: Unsolicited messages, promises of guaranteed returns, requests for private keys, misspelled URLs.

Verification: Always double-check URLs and official social media handles before interacting.

Airdrop Caution: Legitimate airdrops rarely require you to send funds or private information.

Phishing Awareness: Be skeptical of urgent requests or fake alerts.

Action Item: Bookmark official websites and use official apps only.

MULTI-SIG & ADVANCED SECURITY TOOLS

What is Multi-Sig? Requires multiple signatures (private keys) to authorize a transaction, adding a significant security layer.

When to Use: For significant holdings or shared accounts.

Tools: Hardware wallets often support multi-sig. Services like Gnosis Safe (for Ethereum) are popular.

Action Item: Research multi-sig options for your major assets.

DIGITAL ESTATE PLANNING

Why it Matters:

Ensuring your digital assets aren't lost forever when you're gone.

Planning Steps:

- Document your holdings and wallet locations.
- Safely store access information for your beneficiaries (e.g., in a sealed envelope with a trusted advisor/lawyer).
- Consider legal structures (trusts) for complex holdings.

Action Item:

Start documenting your digital asset inventory and discuss plans with your family/trusted advisor.

THE CHECKLIST

- ☐ I understand the difference between hot and cold wallets.
- ☐ I have backed up my seed phrase and stored it securely offline.
- ☐ I never share my private keys or seed phrase with anyone.
- ☐ I verify URLs and official handles before interacting with any service.
- ☐ I am cautious of unsolicited offers, airdrops, and "urgent" requests.
- ☐ I know how to restore my wallet from my seed phrase.
- ☐ I use strong passwords and enable 2FA where possible.
- ☐ I have researched multi-sig options for significant holdings.
- ☐ I have started documenting my digital assets for estate planning.
- ☐ I have discussed digital asset access with my family/trusted advisor.

CONCLUSION & CTA

Security is not an option; it's a necessity. This checklist is your first line of defense. Regularly review and update your security practices.

Call to Action:

- [Download Our Full Security Guide](#): Deep dive into advanced security strategies.
- [Join Our Community](#): Share tips and stay updated on new security threats.
- [Explore Wallet Options](#): Find the right secure wallet for your needs.