My Crypto Guide

SECURITY CHECKLIST

Your quick-reference guide to protecting digital assets from common threats.
Follow these steps to safeguard your crypto, reduce risk of loss, and stay in control of your investments.

- □ Use a reputable hardware wallet like Ledger or Trezor
- □ Buy hardware wallets only from the official manufacturer
- □ Back up your seed phrase offline in multiple secure locations
- □ Never store your seed phrase on phone, computer, or cloud
- □ Enable 2FA using an authenticator app (not SMS)
- □ Keep wallet and firmware software updated
- □ Use a password manager for strong, unique passwords
- □ Do not reuse passwords across accounts
- □ Do not reuse passwords across accounts
- □ Check wallet addresses carefully before sending
- □ Be wary of phishing emails and fake websites
- □ Bookmark official crypto sites you use
- □ Double-check URLs for spelling or character changes
- □ Never share your seed phrase or private keys
- □ Use multi-signature wallets for large holdings
- □ Test seed phrase backups regularly
- □ Keep only small amounts in hot wallets
- □ Install and update antivirus/anti-malware software
- □ Avoid public Wi-Fi for crypto transactions
- □ Review security practices yearly

WWW.MYCRYPTOGUIDE.CO