KRYPTOTECK
YOUR CRYPTO HUB

Crypto Security Toolkit

This Crypto Security Toolkit is designed to help you lock down your digital assets. Use these steps and tools to reduce the risk of hacks, phishing, or user error.

Top Password Managers

- 1Password – Simple interface and strong encryption.
- Bitwarden – Open-source and affordable with excellent browser integration.
- LastPass – Popular and feature-rich (free and premium versions).

2FA Setup Steps

- Use an authenticator app like Google Authenticator or Authy (avoid SMS-based 2FA).
- Scan the QR code provided by your exchange or wallet.
- Save your backup codes securely – not on your phone.
- Enable 2FA on exchanges, wallets, and email accounts connected to crypto.

Recommended Hardware Wallets

- Ledger Nano S Plus – Widely trusted, supports many cryptocurrencies.
- Ledger Nano X – Bluetooth-enabled, ideal for mobile use.
- Trezor Model One – Great for beginners, open-source software.
- Trezor Model T – Touchscreen interface, supports more advanced users.

Phishing Examples & Warning Signs

- Emails or messages asking for your private keys or seed phrase.
- Fake websites mimicking real crypto platforms – always check the URL.
- Urgent 'account suspension' warnings demanding immediate login.
- Never click suspicious links from Telegram, Twitter, or Discord DMs.

Secure Browser Tips

- Use privacy-focused browsers like Brave or Firefox.
- Install extensions like uBlock Origin and HTTPS Everywhere.
- Clear cookies regularly and avoid saving passwords in your browser.
- Never access your wallet on public Wi-Fi without a VPN.