Crypto Security Checklist: Essential Steps to Protect Your Cryptocurrency

Wallet Security

- Use a Cold Wallet for storing large amounts or long-term holdings.
- Set up a Hardware Wallet and store the seed phrase securely offline.
- Enable Multi-Signature Authentication if available for enhanced security.

Two-Factor Authentication (2FA)

- Enable 2FA for all crypto exchanges and wallet accounts.
- Use an App-Based 2FA (e.g., Google Authenticator, Authy) instead of SMS-based 2FA.

Password and Login Security

- Use Strong, Unique Passwords for each account, ideally stored in a password manager.
- Regularly Update Passwords and avoid reusing them across accounts.
- Set up Biometric Authentication on mobile wallets for added security.

Avoid Phishing and Scams

- Double-Check URLs of crypto exchanges or wallets before logging in.
- Do Not Click on Suspicious Links in emails or messages.
- Verify Sender Identity if contacted by support or representatives from exchanges.

Network Security

- Avoid Public Wi-Fi when accessing crypto accounts.
- Use a VPN for an additional layer of security when accessing your wallet or exchange.

Backup and Recovery

- Write Down and Secure Your Seed Phrase offline, not on a digital device.
- Create Multiple Backups of wallet recovery information and store in secure locations.

Regular Security Checkups

- Review Your Account Settings on exchanges and wallets for any unauthorized changes.
- Stay Informed on the latest crypto security best practices.
- Perform Routine Device Scans for malware or potential threats.

How to Use the Checklist

Print or save this checklist for quick reference.

Review each step regularly to ensure ongoing security.