CRYPTO 101

CRYPTO SAFETY GUIDE

INTRODUCTION

Cryptocurrency offers freedom, privacy, and innovation, but with that freedom comes responsibility. Unlike banks, there's no "forgot password" or chargeback if you lose funds. This guide teaches you how to stay safe, secure your crypto, and spot red flags before it's too late.

🔐 1. Protect Your Wallet

Custodial vs. Non-Custodial

- Custodial wallets: Managed by an exchange (like Binance, Coinbase, etc.). Easier to use but you don't fully control your keys.
- Non-custodial wallets: You hold your own keys (like MetaMask, Phantom, Ledger). Safer long-term, but you're fully responsible.

Your Private Key / Seed Phrase

- Your seed phrase (12–24 words) = access to all your funds.
- Never share it. Never store it online.
- Write it on paper (or metal backup) and keep it offline, in multiple safe locations.
- If anyone asks for your seed phrase or private key, it's a scam.

Use Hardware Wallets

- For serious holdings, use Ledger, Trezor, or Keystone.
- Hardware wallets keep your private keys offline, making it much harder for hackers to access.

CRYPTO 101

CRYPTO SAFETY GUIDE

2. Stay Alert Against Scams

🚫 Common Crypto Scams

Phishing
Fake websites or emails asking for login info
Always check the URL and enable 2FA

Giveaway scams
“Send 1 ETH and get 2 back!”
Never send crypto expecting returns

Fake support
Imposters pretending to be exchange or wallet support
Real support never asks for keys

Pump-and-dump
“Guaranteed profits!” tokens hyped on social media
Research before investing

Airdrop scams
“Claim your free tokens” links that steal your wallet
Avoid connecting your wallet to random sites

CRYPTO 101

CRYPTO SAFETY GUIDE

3. Secure Your Accounts

- Enable 2-Factor Authentication (2FA) (preferably with Authy or Google Authenticator, not SMS).
- Use unique, strong passwords for every crypto account.
- Store passwords in a reputable password manager (Bitwarden, 1Password, etc.).
- Regularly review your device security – update OS, use antivirus, and avoid public Wi-Fi for transactions.

4. Keep Your Investments Safe

- **Don’t keep all funds on exchanges. Withdraw to your own wallet.**
- **Verify before you send. One wrong address = lost funds forever.**
- **Double-check networks (ERC20 vs. BEP20, etc.).**
- **Start small. Test with a small amount when sending to new wallets.**
- **Be skeptical of “too good to be true” returns or “guaranteed profits.”**

CRYPTO 101

CRYPTO SAFETY GUIDE

5. Learn Before You Invest

- Research every project before buying – check whitepapers, teams, tokenomics, and audits.
- Follow trusted sources (CoinGecko, CoinMarketCap, Decrypt, etc.) instead of random YouTubers or influencers.
- Understand basic blockchain concepts – gas fees, smart contracts, and consensus mechanisms.

6. Backup and Recovery Plan

- Store offline copies of wallet backups, exchange recovery codes, and seed phrases.
- Plan what happens if you're unavailable – trusted family or executor with instructions in a will.
- Periodically test your backups (e.g., restore a test wallet).

CRYPTO 101

CRYPTO SAFETY GUIDE

7. Mental Checklist Before Any Transaction

✅ Am I on the correct website/app?
✅ Is this the real recipient address?
✅ Do I trust this project/person?
✅ Have I checked for scams or phishing?
✅ Am I comfortable losing this money if it goes wrong?

💬 Final Advice

Crypto is empowering, but only if you protect yourself.

Stay skeptical, stay secure, and remember:
“Not your keys, not your coins.”