PROTECT YOUR CRYPTO!

Keep yourself as safe as possible!

SCAMS, ATTACKS & TRADING-ASSOCIATED RISKS

SCAMS - A deceptive scheme designed to trick you into giving money, data, or access. Someone intentionally lies or manipulates you.

Example: You click a DM link, land on a fake exchange, and send crypto to ‘unlock’ a bonus.

ATTACKS - An intentionally-designed and executed malicious technical action that breaches, damages, or steals from a system.

Example: Malware hijacks your clipboard and swaps your wallet address. Your crypto is sent to the attacker’s address.

TRADING RISKS - An uncertainty that can cause loss even if no one is trying to hurt you.

Example: You set a stop loss that doesn’t get triggered.

COMMON SCAMS

- **Phishing**: Message sent that leads you to a fake exchange, wallet, or DeFi login pages designed to steal passwords, seed phrases, or session access.
- **Impersonation scams:** Fake support agents, founders, influencers, exchange staff, or ‘account recovery’ specialists reaching out by DM, email, or phone.
- **Giveaway scams:** Promises that sending crypto first will unlock a bigger return later.
- **Investment scams:** Fake funds, fake managed accounts, or ‘too-good-to-miss’ opportunities with guaranteed returns.
- **Pig butchering**: Long-con social engineering where the scammer builds trust, then pushes you into a fake platform or bad transfer.
- **Ponzi and pyramid schemes:** Early payouts are funded by new victims, with pressure to recruit others.



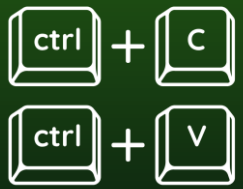



COMMON SCAMS

- **Pump-and-dump schemes:** Coordinated hype around coins, followed by insiders selling into the run-up.
- **Fake token sales:** ICOs, or presales. Non-existent or junk projects that vanish after collecting funds.
- **Rug pulls**: Creators drain liquidity or abandon the project after attracting buyers.
- **Airdrop scams**: Fake claim pages or malicious wallet-connect prompts that drain assets.
- **Recovery scams**: Fraudsters claim they can recover stolen crypto for a fee, then steal the remaining.
- **Sextortion/extortion scams**: Threats to expose private content unless paid in crypto.
- **Fake mining/cloud-mining scams**: Claims that you can earn passive crypto yield from hardware or hosted mining.
- **Job or freelance scams**: Fake hiring offers that involve ‘training deposits’ in crypto.
- **Payment spoofing scams**: Fake invoices, fake deposit confirmations, or altered wallet addresses.

ATTACK METHODS

- ☹ **Malware:** Keyloggers, remote-access trojans, browser hijackers, or wallet-stealing software.
- ☹ **Clipboard hijacking:** Malware swaps copied wallet addresses with the attacker's address.
- ☹ **Wallet drainers**: Malicious smart contracts that empty a wallet after a bad approval or signature.
- ☹ **Malicious approvals**: You sign a transaction that grants hidden transfer permissions.
- ☹ **Seed phrase theft:** Tricking you into entering your recovery phrase into a fake site, form, or support chat.
- ☹ **SIM swapping:** Attackers hijack your phone number to intercept 2FA codes and password resets (works on SMS 2FA only)



ATTACK METHODS

- **Session Cookie Theft**: Attackers steal browser cookies from your logged-in session using malware. Since you're already authenticated, they can access your account without needing 2FA.
- **Fake login pages:** Steal your password, then prompt for the 2FA code. You enter both, and the attacker uses them in real-time on the real site (man in the middle attack).
- **MFA fatigue**: You keep receiving 2FA requests. You eventually approve one out of frustration.
- **Account takeover:** Stolen passwords, session cookies, or email access used to lock you out of exchanges and wallets.
- **Deepfake or AI impersonation:** Synthetic voice or video used to fake executives, support staff, or urgent trading instructions.

TRADING RISKS

- ☹ **Fake exchange websites:** Cloned platforms that look real but are built to steal deposits or credentials.
- ☹ **Fake trading bots or signal groups:** Promises of easy profits that usually lead to deposits, referral schemes, or malicious links.
- ☹ **Fake margin/borrow offers:** Scams that lure traders with high leverage, bonus funds.
- ☹ **Front-running and MEV traps:** Especially in DeFi, where bad transaction design or slippage settings can be exploited.
- ☹ **Smart-contract exploits:** Vulnerable DeFi protocols, bridges, or staking contracts that get drained.
- ☹ **Bridge attacks:** Cross-chain transfer systems are a frequent target because they're complex and high value.
- ☹ **Stop Loss:** Stop losses not set, or if set they can be hunted or not trigger.
- ☹ **(alleged) Market manipulation**: Coins don't do what the indicators are indicating.
- ☹ **Education:** Not being educated at all, or listening to 'YouTube' educators that teach conflicting indicators.
- ☹ **Hype:** Social media and news hype that doesn't amount to anything.
- ☹ **Emotional trading**: Greed and fear sets in, instead of calm analysis.
- ☹ Not using what works for you.

MISCONCEPTION: HARDWARE WALLETS PROTECT EVERYTHING

*Hardware wallets do not fully protect against smart contract exploitation. They protect your private keys from malware, but if you sign a malicious transaction, the contract can still drain assets from that wallet.

What hardware wallets *do* protect against

Protection	How it works
Private key theft	Keys never leave the device; malware can't steal them
Remote hacking	Device is offline (cold storage), so attackers can't reach keys
Clipboard hijacking	You verify the recipient address on the device screen
Phishing pages	Transaction details shown on hardware, not just browser

What hardware wallets *don't* protect against

Threat	Why hardware wallets fail here
Malicious smart contracts	If you sign a bad approval, the contract can drain your wallet
Permission abuse	You grant unlimited token approval. The contract steals all of that token.
Wallet drainers	You sign a transaction that gives transfer rights. The funds are gone.
EVM complexity	Hardware firmware can't validate all Ethereum/BSC/Tron contract code.
User error	You approve the wrong thing. The device shows it, but you still sign.

Hardware wallets are essential for key security, but they're not a magic shield against smart contract exploits. The real protection is wallet separation + approval hygiene + transaction verification.
Make sure you purchase from a verified store!

RED FLAGS

- Guaranteed profits or “risk-free” returns.
- Urgency, secrecy, or pressure to act now.
- Requests for seed phrases, remote access, or extra deposits to ‘unlock’ funds.
- Unsolicited DMs offering help, recovery, alpha, or special access.
- URLs that are slightly wrong, shortened, or hidden behind QR codes.
- Any transaction you do not fully understand before signing.
- Computer is running slower than usual
- Incorrect spelling in correspondence
- Log-in sessions are not recognised by you
- Coin has strange pattern, and/or very low liquidity
- **If a deal sounds too good to be true…it normally is**

SO, WHAT CAN YOU DO? THE BEST DEFENCES ARE…

- *Use a hardware wallet for meaningful holdings.
- Never share a seed phrase or private key.
- Verify URLs manually and bookmark official sites.
- Treat every approval seriously.
- Use separate wallets for trading, DeFi experimentation, and long-term storage.
- Keep 2FA on an authenticator app, not SMS, and on a separate device. Even better, use Passkey or a hardware security key.
- Assume ‘support’ and ‘recovery’ DM offers are hostile until proven otherwise.
- Revoke approvals regularly (MetaMask maximum token limit, etc)
- Use burner wallets for new/untested/untrusted projects.
- Check slippage on low liquidity coins and set tight limits.
- Never sign transactions blindly; read what is actually being asked of you.
- Avoid pirated software.
- Install a reliable anti-virus software program.
- Keep your devices OS and Anti-virus/malware programs updated.
- Limit installing browser extensions.
- Use a VPN on public wi-fi.
- Ensure the site is HTTPS (not just HTTP).
- Clear your cookies regularly.
- Log out of sensitive accounts.
- Disconnect wallets from sites when you are finished using them.
- Manage active sessions regularly.
- Look at liquidity closely.
- Trade in the style that suits the coin.
- DYOR

SAFETY CHECKLIST

BEFORE YOU TRADE

- □ Verify the exchange/wallet URL manually (bookmark official sites)
- □ Check for phishing indicators: misspelled URLs, unusual domains, unsolicited links
- □ Ensure 2FA is on an authenticator app (not SMS)
- □ Use a hardware wallet for significant holdings
- □ Keep seed phrase secure, never shared (not your keys, not your crypto)

BEFORE CONNECTING WALLET OR SIGNING

- □ Review every transaction detail (amount, recipient, network)
- □ Treat approvals as granting transfer power; don't sign blindly
- □ Use a separate ‘burner wallet’ for DeFi experimentation
- □ Check slippage settings to avoid MEV/front-running traps
- □ Verify the smart contract address on official source

DURING TRADING

- □ Never share seed phrase, private key, or remote access with anyone
- □ Assume all DMs offering ‘support’ or ‘recovery’, are scams until you verify them
- □ Double-check clipboard content (clipboard hijacking swaps addresses)
- □ Verify deposit confirmations’ fake screenshots are common
- □ Don't trust guaranteed profits or risk-free return promises
- □ Use the correct amount to trade for the liquidity
- □ Watch the pattern of the coin (be careful of newly launched coins)

SAFETY CHECKLIST

IF YOU'RE TARGETED

- □ Stop all communication with the scammer immediately
- □ Do NOT send more crypto to unlock or recover funds
- □ Report to the exchange/platform and relevant authorities
- □ Check wallet approvals and revoke malicious permissions
- □ Move remaining assets to a fresh wallet with new seed phrase

CORE RULES

- » Never share your seed phrase; legitimate support will never ask
- » Verify everything twice (URLs, addresses, contracts)
- » Use separate wallets for different purposes
- » Assume unsolicited contact is hostile until proven otherwise
- » Trade in the style that the coin can take
- » If it feels wrong, it IS wrong; step away
- » DYOR

SIMPLE CONVERSATION OR MORE NEFARIOUS?

5 of the most common personal data points that make up passwords:

- **Pet names**
- **Family member names**
- **Birthdays and anniversaries**
- **Favourite sports or teams**
- **Car brands and models**

BY THE WAY…DID YOU CLICK THE LINK?

https://bit.ly/bltcointaf

Stay safe.
Trade smart.