

The Usual Ways People Get Drained

Crypto Guidance, a trade name of Crypto Boutique LLC | Free guide | Education only. Nothing here is investment, tax, or legal advice.

Start here if you are scared

If you bought this because something already feels wrong, take a breath. Reading about scams cannot drain a wallet. Clicking a link usually cannot either. In almost every case, funds move only when someone types in a seed phrase, signs a transaction or approval, or sends coins themselves.

If you think your seed phrase has been exposed, the calm move is: set up a brand new wallet with a brand new seed, restore test it, and move what is left into it using the Moving Funds routine. Do not reuse the old words.

The rest of this guide walks through the five patterns behind most losses. Once you can name them, they get much less scary.

Pattern 1: Fake support

How it looks: you post a question in a public forum or social media, and within minutes someone friendly messages you. They say they are from the wallet company or exchange. They are patient and helpful. Eventually they send a link to a "support form" or "wallet repair" page.

What they want: your seed phrase, remote access to your computer, or for you to send coins to a "safe" address.

The calm rule:

- Real support does not DM you first.
- Real support never needs your seed phrase.
- Start every support conversation yourself, from the company's official website, typed by hand or from a bookmark you saved earlier.
- If someone has been kind for an hour and then asks for your words, the kindness was the setup.

Pattern 2: Lookalike sites

How it looks: a search ad, an email, or a social media post leads to a site that looks exactly like your wallet, exchange, or a popular app. The address bar has a small difference: an extra letter, a swapped character, a different ending.

What they want: your login, your seed phrase ("re-enter to verify"), or a wallet connection so you sign something.

The calm rule:

- Bookmark the real sites you use and only use the bookmarks.

- Be wary of search ads for crypto sites. Scroll past them.
- A wallet app or extension should never ask for your seed inside a web page. If it does, close the tab.

Pattern 3: Address poisoning

How it looks: you notice a tiny or zero value transfer in your history from an address that looks almost like one you use often. Same first few and last few characters. Later, when you copy "your usual address" from history, you copy theirs instead.

What they want: for you to send your next transfer to them by accident.

The calm rule:

- Never copy addresses from transaction history.
- Copy fresh from the receiver's deposit screen or your saved address book entry each time.
- Check characters in the middle, not just the start and end.
- Tiny unexplained incoming transfers are a warning sign, not a gift. You do not need to do anything with them. Ignore them.

Pattern 4: Token approvals

How it looks: you connect a wallet to a website to claim an airdrop, mint something, or swap. Your wallet asks you to approve or sign. It looks routine. Later, tokens leave your wallet without you sending them.

What happened: you gave a contract permission to spend certain tokens on your behalf. Some approvals are unlimited. A malicious contract can use that permission whenever it likes.

The calm rule:

- Read what your wallet says you are signing. Words like "approve," "set approval for all," "permit," or "increase allowance" grant spending permission.
- If you do not understand a signature request, reject it. Rejecting costs nothing.
- Use a separate "playground" wallet with little in it for trying new sites.
- Periodically review and revoke old approvals using a reputable approval checker or your wallet's built in tool, reached from a bookmarked official site.
- Free airdrops that require urgent action are a common lure.

Pattern 5: Seed phishing

This is the oldest one and still the most common. Everything above often ends here.

How it looks: a pop up, email, text, or support agent says your wallet needs to be "validated," "synced," "upgraded," or "unlocked," and asks for your 12 or 24 words. Sometimes it is a fake wallet app. Sometimes it is a printed card in a fake package.

What they want: the words. With them, they do not need anything else.

The calm rule, said plainly: there is no situation where typing your seed phrase into a website, form, chat, or email is part of a legitimate process. The only place it ever gets entered is on your own wallet device or official wallet app when you are restoring.

Crypto Guidance will never ask for it. Not by email, not by phone, not to "check" anything.

Quick self check

If you are unsure about something happening right now, ask yourself:

- ☐ Did I start this conversation, from a site I bookmarked?
- ☐ Is anyone asking for my seed words, PIN, or passphrase?
- ☐ Is there time pressure? ("Act in 10 minutes or lose access.")
- ☐ Am I being asked to sign something I do not understand?
- ☐ Did I copy this address fresh, not from history?

If any answer worries you, stop. Waiting a day is almost always free. Scammers depend on hurry.

If something already happened

- Exposed seed: new wallet, new seed, restore test, move remaining funds.
- Bad approval: revoke it from a trusted approval tool, then move remaining tokens to a fresh wallet if you are unsure.
- Sent to a poisoned address: transfers are usually final. Report to the exchange if one was involved, and save the transaction ID for records.
- Gave remote access: disconnect the computer from the internet and get help from someone you trust before using it for crypto again.
- Be careful of "recovery services" that contact you afterward. Many are a second scam.

Questions about this guide: john@cryptoguidance.org. We will never ask for your seed phrase.