CRYPTO

How To Recover From A Wallet Drainer

Plain-English how-to. ~60 minutes. Triage, secure remaining assets, revoke approvals, and recover what's recoverable.

A wallet drainer is malware — or, more often, a malicious smart contract — that empties a cryptocurrency wallet within seconds of being granted permission. The user typically signed something on a fake website, in a fake airdrop popup, or via a phishing Discord message: a transaction that looked like a routine swap or claim but was actually an unlimited-token approval that handed the entire wallet's contents to the attacker. The drain happens before the user can react. By the time they notice, the funds are gone and being laundered through a mixer.

The scale is enormous. Chainalysis reports billions of dollars stolen from individual crypto wallets every year, with wallet drainers and approval-phishing as the dominant single category. The pattern is well-documented: a Telegram channel offers an airdrop, a Discord bot pings about a new mint, a Twitter ad promotes a 'limited' opportunity. The destination is always a contract approval that, in a single signature, gives the attacker the keys to everything.

What makes recovery especially brutal in crypto is that there is no fraud reversal. Banks, credit-card companies, and brokers have chargeback mechanisms; crypto does not. Once the transaction confirms, it's done. The asset is in the attacker's wallet, often within seconds being routed through Tornado Cash or a similar mixer to obscure its trail. The on-chain visibility cuts both ways: you can watch your funds being stolen in real-time, but you can't stop it.

Recovery is therefore mostly damage limitation. The hour after a drain is critical: revoking active approvals on the compromised wallet, moving any remaining assets to a fresh hardware wallet, securing the seed phrase from any further exposure, and beginning the documentation that may help with law-enforcement reports, exchange recovery (if some funds passed through one), and possible tax-loss claims. The decisions you make in that first hour are the difference between losing what was stolen and losing everything in the wallet.

Most online 'recovered from wallet drainer' content is either a victim's anguished thread or a generic 'use cold storage!' post written by people who weren't drained. The practical, methodical playbook — exactly what to do, in what order, in the first hour, the first day, and the first week — is rarely written down. That's the gap this guide fills.

By the end of this guide you'll know exactly what to do in the first 60 minutes to contain the damage, how to revoke malicious approvals, when (and when not) to use recovery services that claim they can get your funds back (almost always a follow-up scam), how to document the incident for tax and law-enforcement purposes, and how to rebuild your crypto security posture so this can't happen again. The work is hard but the methodology is clear.

Quick snapshot

What you'll learn	Triage, containment, revocation, documentation, and rebuild after a wallet-drainer attack.
Skill level	Intermediate
Time required	60 minutes urgent + ongoing
What you'll need	Compromised wallet info, fresh device, new hardware wallet, time
Risk if you skip this	Loss of remaining assets, exposure to follow-up recovery scams
PDF kit	■ Download at the bottom of this page

Why this matters

Chainalysis reports billions stolen via wallet drainers and approval-phishing every year. It's the largest single category of crypto theft from individuals — larger than exchange hacks, larger than rug pulls, larger than ransomware revenue paid in crypto. The targeting is industrialized: Telegram channels coordinate, drainer-as-a-service platforms exist, and the laundering pipelines through mixers are well-rehearsed within minutes of a drain.

No fraud reversal exists in crypto. The hour after a drain determines whether you lose what's stolen or lose everything. Banks, brokers, and credit-card companies have chargeback mechanisms; crypto does not. Once a transaction confirms it's done. Recovery is therefore mostly damage limitation, not asset recovery — but the damage limitation step is what stops the drain from becoming total.

Follow-up 'recovery services' are almost always secondary scams targeting recent victims. The pattern is so reliable that some attackers run both the drain and the 'recovery' service. Victims who pay the recovery scam lose additional funds on top of the original drain. Real recovery, when it happens, comes through law enforcement and exchange cooperation — never through a DM.

Before you start

Move to a clean device immediately — assume the compromised device may have malware. Use a phone or a separate computer. Continuing to operate the compromised wallet from the same device that allowed the drain risks losing whatever you move to the new wallet too.

Have ready: a new hardware wallet (Ledger / Trezor), the compromised wallet's address(es), transaction history, and time. The new hardware wallet must use a fresh seed phrase generated offline — never reuse the compromised seed.

Do not contact 'recovery services' or 'crypto investigators' that DM you. They are scams targeting drain victims. Anyone who proactively reaches out claiming they can recover your funds is lying. The only legitimate avenues are the FBI IC3, FTC, exchanges that may have processed the stolen funds, and known on-chain analytics firms that work with law enforcement.

Step 1 — Move remaining assets immediately

Set up a fresh hardware wallet (Ledger / Trezor) with a brand-new seed phrase generated offline. Do not import the compromised seed.

Transfer any remaining assets from the compromised wallet to the new one. Time is critical — additional approvals may still be active.

Step 2 — Revoke all active token approvals

Use Revoke.cash, Etherscan's Token Approvals page, or your wallet's built-in revoke. Connect the compromised wallet (from a clean device).

Revoke every approval on the compromised wallet, especially unlimited ones. This stops further drains via approvals you've forgotten about.

Step 3 — Identify the drain source

Check your transaction history. The drain transaction will show the unauthorized transfer. Look at the preceding transaction — that's typically the approval signature that enabled the drain.

Document the contract address, the approval transaction hash, and the drain transaction hash. You'll need these for reports.

Step 4 — Document everything

Screenshots of the drain transaction(s), the malicious contract address, the dApp or site you signed from, the timestamps.

Save your wallet's full transaction history (CSV export). This is needed for IRS reporting, possible insurance, and law enforcement.

Step 5 — Report the incident

FBI IC3: ic3.gov. FTC: reportfraud.ftc.gov. Chainabuse for the drainer contract.

If funds passed through a known exchange, contact that exchange's fraud/legal team immediately with the transaction hashes.

Step 6 — Ignore recovery-service DMs

You will receive DMs offering to 'recover your funds' on Telegram, Discord, X, and email. All of them are scams.

Real recovery comes from law enforcement, exchange cooperation, and on-chain analytics firms like Chainalysis — not from a DM.

Step 7 — Audit other wallets and accounts

If you used the same browser or device for other wallets, those are also at risk. Move assets to fresh wallets and revoke approvals on each.

Check email, exchange accounts, and any service that uses crypto wallets for authentication. The malware may have keylogged other credentials.

Step 8 — Rebuild with hardware-wallet-only signing

Going forward: hardware wallet for all assets above hot-wallet float. Hot wallet only for small amounts you can afford to lose.

Use a separate browser profile (or a dedicated machine) for crypto signing. Never sign airdrops or unfamiliar contracts.

Consider multisig (Safe, formerly Gnosis Safe) for larger holdings — requires two or more signatures from separate keys to move funds, making drainer attacks essentially impossible. The setup is more complex but the security model is fundamentally different from any single-wallet approach.

PRO TIP

Move Remaining Funds. Revoke Approvals. Ignore Recovery DMs.

First hour: fresh hardware wallet, move what's left, revoke all approvals.

Every 'recovery service' that DMs you is a scam. All of them.

Document everything for IRS / law enforcement / possible exchange cooperation.

Hardware-wallet-only signing going forward. Hot wallet small floats only.

If you want to go further: power-user upgrades

Power-user upgrade #1 — Multisig for large holdings

Safe / Gnosis Safe — requires multiple signers. Drainer can't move funds with a single signature.

Trade-off: setup complexity; small transaction fees per signer.

Power-user upgrade #2 — Hot wallet for everything risky

A separate hot wallet with negligible funds used for airdrop claims and new dApps. Hardware wallet untouched.

Trade-off: more wallets to manage.

Power-user upgrade #3 — Tally / Wallet Guard / Pocket Universe

Browser extensions that simulate transactions before you sign, flagging unlimited approvals.

Trade-off: occasional false positives.

Power-user upgrade #4 — Subscribe to drainer alerts

ScamSniffer and SlowMist publish drainer indicators and known malicious contracts.

Trade-off: occasional email.

Power-user upgrade #5 — Dedicated crypto-only device

Old laptop or Chromebook used only for crypto. Reduces compromise risk.

Trade-off: extra hardware.

Power-user upgrade #6 — Tax-loss documentation

Drained funds may be deductible. Work with a crypto-aware CPA.

Trade-off: tax-prep cost.

Common mistakes & pitfalls

Mistake — Mistake

Fix — Importing the compromised seed phrase into a new wallet. The seed is compromised; do not reuse.

Mistake — Mistake

Fix — Paying a 'recovery service.' They're scams. Real recovery doesn't work that way.

Mistake — Mistake

Fix — Skipping approval revocation. Future drains can happen via leftover approvals.

Mistake — Mistake

Fix — Continuing to sign new transactions from the compromised device. Likely malware-infected.

Mistake — Mistake

Fix — Not reporting to law enforcement. Helps build the case against drainer operations.

Mistake — Mistake

Fix — Not documenting for taxes. Drained funds may be deductible.

Pro tips

Pro tip 1. Hardware wallet plus a clean device — the only safe combo.

Pro tip 2. Revoke approvals quarterly even if you haven't been drained — leftover approvals are a long-tail risk.

Pro tip 3. Suspicious DMs after a public drain are nearly always follow-up scams.

Pro tip 4. If using an exchange, ask them to flag the destination address — slows laundering.

Pro tip 5. Don't sign blind. Use Wallet Guard / Pocket Universe to simulate every transaction.

Frequently asked questions

Can the funds really not be recovered?

Usually no. Once the transaction confirms, it's done. Rare cases (passed through a centralized exchange, caught early, frozen) allow some recovery.

Should I pay the 'recovery service' DMing me?

No. 100% of unsolicited recovery-service offers are scams targeting recent victims.

Will the FBI actually do anything?

Reports help build case files. Recovery for individuals is rare, but operations occasionally get dismantled.

How do I know which approvals to revoke?

Revoke.cash shows all active approvals. Revoke any you don't currently need; especially unlimited approvals.

What's the difference between a drainer and a hack?

Drainer: you signed something malicious. Hack: attacker stole your seed phrase or private key. Both end with empty wallet; defenses differ.

Is this tax-deductible?

May be. The IRS rules on theft losses in crypto are evolving. Work with a crypto-aware CPA.

Should I publicly disclose the drain?

Many do, to warn others. Brings follow-up scammers; have your defenses up before posting.

Quick recap — do these in order

DO THIS RIGHT NOW

The 8-step recap.

Move remaining assets to a fresh hardware wallet immediately.

Revoke all active token approvals on the compromised wallet.

Document the drain — transactions, contracts, dApp source.

Report to FBI IC3, FTC, and Chainabuse.

Ignore every recovery-service DM. They're scams.

Audit other wallets and accounts; assume malware spread.

Rebuild with hardware-wallet-only signing going forward.

Work with a crypto-aware CPA on tax-loss documentation.

Mini glossary

Wallet drainer: Malware or malicious contract that empties a crypto wallet via approval phishing or seed theft.

Token approval: Permission granted to a contract to spend tokens from your wallet.

Unlimited approval: Approval with no spending cap — gives the contract full access to that token.

Hardware wallet: Physical device that signs transactions offline. Ledger, Trezor.

Hot wallet: Software wallet on a connected device — convenient but more exposed.

Mixer: Service that obscures the on-chain trail of stolen funds. Used to launder drained crypto.

Approval phishing: Tricking a user into signing a malicious approval that grants the attacker access to tokens.