Coincub

Premium content

First-Hour Incident Checklist

Purpose: Stop further loss without panic.

Coincub

Premium content

Contain

- Close tabs (exit any suspicious website)
- Cancel prompts (wallet popups or confirmations)
- End DMs / calls (stop all chat-based “support”)
- Stop using suspect device (switch if anything feels off)

Revoke

- Open approvals checker from clean device (device you trust)
- Revoke suspicious or unknown approvals (permissions you didn’t intend to grant)
- Prioritize high-value tokens

Move Funds

- Send remaining assets to safe vault address (wallet you fully control)
- Test small amount first
- Then sweep (move the rest)

Rotate

- Email password + passkeys / 2FA (email controls resets)
- Password manager
- Exchanges and API keys (disable or rotate keys)
- Review active sessions and inbox rules (logins and auto-forwards)

Document

Capture:

- Lure (post, DM, email) (what led you there)
- URLs
- Tx hashes (transaction IDs)
- Revoke hashes (transactions that removed approvals)
- Timestamps (UTC) (use one timezone)

Notify (Calm, Factual)

Internal message template:

"Suspected wallet exposure at [time UTC].
Actions taken: funds moved, approvals revoked, credentials rotated.
Evidence stored in [location].
Next update at [time]."

Do NOT

- Argue with attackers
- Test send funds
- Sign to "verify ownership" (signatures requested in chats or calls)
- Chase recovery in the first hour

Order matters. Calm beats speed.