

How To Stay Rekt-Free in WEB3



**Master the Web3 Security
layers protecting your
crypto assets**

KERBERUS



Your 3-Layer Defense System

1. Build Your Fortress

Securing wallets and private keys

2. Define Your Actions

Safe interactions with contracts and dApps

3. Set Your Shield

Mindset and habits against deception

Each layer builds on the next—master all three to stay protected

1st Layer: Build Your Web3 Fortress

Use Cold Storage

Hardware wallets keep keys offline—no transaction without physical approval

- Buy direct from established brands like Ledger, Trezor, CoolWallet, SafePal etc.
- Avoid unauthorized resellers or unverified 3rd parties to avoid supply chain attacks
- Malware can't press physical buttons to approve transactions





The \$5 Wrench Attack

2025 saw a resurgence of physical attacks targeting crypto holders —including the kidnapping of Ledger's co-founder

- ❏ **Critical Reality:** Even cold storage and multi-sig can't protect you if you expose a seed phrase by accident or under duress

Seed Phrase Hygiene

✗ Never Do This

- Take photos of your seed phrase
- Save to cloud storage
- Print digital copies

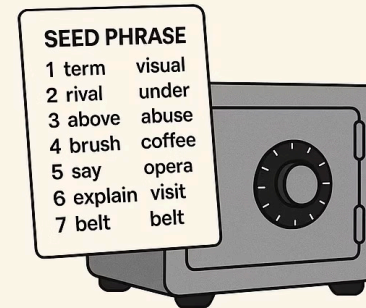
✓ Do This

- Write on paper or stamp into metal
- Store in physical safe
- Keep offline, always

Master Your Seed Phrase Hygiene



Write it down
and store it offline



Never create
a digital copy



One leaked photo such as "crypto_keys.jpg" = your entire portfolio gone

Hot vs. Cold Wallet Strategy



Cold Wallet = Your Vault

Hardware wallet should protect your longterm crypto holdings



Hot Wallet = Pocket Cash

Use a burner wallet for daily minting, trading, experimenting

If your hot wallet gets drained, you lose 0.1 ETH—not your entire bag

2nd Layer: Take the Right Actions



Read Before Signing

SetApprovalForAll = giving permanent access to all your assets



Use Transaction Simulators

Kerberos and Pocket Universe show what transactions do in plain English



Revoke Old Approvals

Use Revoke.cash to clean up permissions every few months

Transaction Simulator in Action

Without real-time Web3 security like Kerberus:

Click "Mint" → Sign blindly → Lose everything

With Kerberus:

See clear warning:

THIS TRANSACTION WILL:

- ✓ Send 0.1 ETH
- ✗ STEAL all Cool Cats NFTs

Reject immediately. Assets saved.



Layer 3: Strengthen Your Shield



Bookmark Official Links

opensea.xyz ≠ opensea.io—one letter steals everything. Only use bookmarks.



Use Burner Wallets for Mints

New wallet, exact mint amount only. Drainer gets 0.1 ETH—not your main bag.



Ignore fake airdrops: No Free Lunch in Web3

Random airdrops in your wallet are bait. Hide them. Never interact.



Disable or Ignore DMs

99% of unsolicited messages are scams. Turn off DMs on Discord and X.

The 2022 BAYC Instagram Hack

\$3M

Lost in minutes

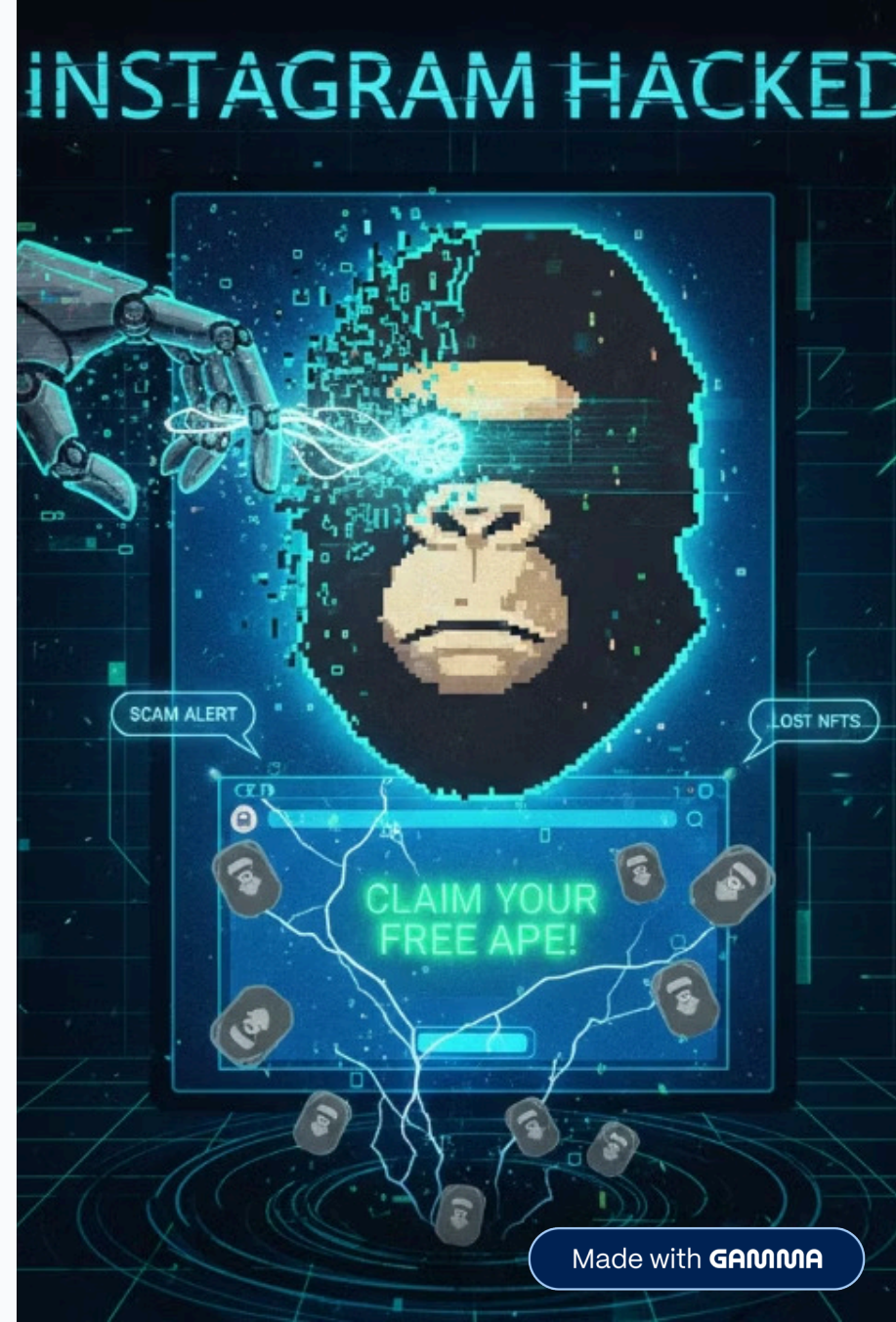
Phishing link on compromised
official account

100%

Preventable

With bookmarks and transaction
simulators

**Stay vigilant.
Stay rekt-free.**



Learn more at Kerberos.com

The world's leading Web3 security tool for real-time threat protection

**0 User Losses
Since 01/2023**

GET \$30,000 COVERAGE ON YOUR TRANSACTIONS

KERBERUS

