



CRYPTO HONEYPOTS

How to Detect and Avoid These Scams

2026 Web3 Security Guide • Kerberos Learn





Billions at Risk

\$4B

Lost Annually

Crypto scam victims

87%

Irreversible

Funds never recovered

24/7

Active Now

New honeypots daily

What Is a Crypto Honeytrap?

Malicious Smart Contracts

Allows buying but **blocks selling**

Hidden logic traps your funds permanently

Only deployer can withdraw liquidity

Contrast

Web2 honeypots defend systems •

Crypto honeypots steal funds

Contract Exploitation

Hidden logic prevents withdrawals

Liquidity Drain

Deployer siphons funds

Irreversible Loss

No technical recovery option



The Rise of Meme Coin Honeypots



Rapid Deployment

Tokens created in minutes



Low Fees, Fast Chains

Fuel scam volume



FOMO Overrides Caution

Traders rush in to FOMO buy

Honeypot Lifecycle

01

Deployment

Malicious contract with hidden sell restrictions

02

Hype & Promotion

Liquidity seeded, social media campaigns launch

03

Sales Blocked

Buyers trapped by code, nothing appears wrong

04

Exit Strategy

Liquidity drained or deployer accumulates funds



Honeypot Variants (2026)



Smart Contract Honeypots

Code-based sell restrictions



High Sell-Tax Honeypots

Excessive fees prevent withdrawals



Liquidity Honeypots

Deployer removes liquidity only



Wallet Sweeper Honeypots

Steals approval credentials



Honeypot-as-a-Service

Deploy ready-made scams



Hardware Wallet Attacks

Compromised device supply chains

Real Honeytrap Cases

1

Squid Game Token

Multi-million dollar collapse after rapid rise

2

Dechat Contract Incident

Hidden logic prevented all sales from launch

3

Serial Campaigns

Recurring operations across multiple chains

Key Takeaway

Hype and celebrity endorsements override red flags



KERBERUS



Honeypot Detection Checklist

- 1 Inspect Smart Contract**
Review permissions and restrictions
- 2 Use Checker Tools**
Verify with multiple honeypot detectors
- 3 Analyze Patterns**
Check trading volume and holder distribution
- 4 Test Sell**
Try selling small amount first
- 5 Verify Liquidity Lock**
Check if liquidity is truly locked
- 6 Research Team**
Verify credibility and track record



Honeypot vs Rug Pull

Honeypot

- Sell blocked via code
- Trap exists from launch
- Contract prevents trading

Rug Pull

- Liquidity removed later
- Price collapses instantly
- Market-based attack

📌 Many scams combine both tactics for maximum deception



KERBERUS

What To Do If Trapped

1

Revoke Token Approvals

Immediately revoke contract permissions

2

Report the Contract

Submit to blockchain security trackers

3

Community Warning

Alert others and mark as malicious

4

Move Assets

Transfer funds to new wallet address

5

Avoid Interaction

Never engage with suspicious contracts

Keep Your Crypto Safe with



Real-Time Threat Protection

- Transaction simulation before signing
 - Smart contract risk analysis
 - Real-time threat detection
 - Active protection vs passive scanners
- Stay skeptical. Verify every transaction.



Visit Kerberus.com/Learn



 Twitter

Kerberus

We protect you from drainers on all EVM and SOL – 0 user losses since 01/2023 – \$30,000 Coverage On Your Txns You make the profits, we kee...



Guide created by [Werner Vermaak](#) for Kerberus