Web3 Anti-Fraud Handbook

Web3 Anti-Fraud Handbook

2024.10

Content

Introduction

Hello to all the friends reading this Web3 Anti-Fraud Handbook.

The Web3 industry has seen significant expansion in recent years. According to @CMC, as of late August 2024 when this handbook was written, the total cryptocurrency market capitalization had reached $2 trillion, which is roughly two-thirds of Nvidia's market cap or equivalent to half of the total market capitalization of Hong Kong stock market.

Total Market Cap of Cryptocurrency

Much of this rapid industry growth has occurred in relatively unregulated environments, inevitably attracting illicit activities. Therefore, whether you are a newcomer just beginning to learn about cryptocurrencies or a seasoned on-chain OG with extensive interaction experience, you have likely encountered varying degrees of negative criticism towards the crypto industry, both from within and outside the community. These criticisms often include remarks such as "cryptocurrencies are a tool for money laundering," "crypto wallets are insecure," or "scams involving worthless tokens are rampant."

Although such accusations are often exaggerated, the reality is that for the average crypto investor, this market is inherently less secure than traditional financial markets. A single mistake can lead to the loss of all your assets.

To address this, we have compiled this Web3 Anti-Fraud Handbook, aiming to provide a detailed breakdown of various scam tactics targeting users at different stages. Our goal is to equip readers with the knowledge to identify and avoid these threats. We believe this handbook will prove valuable not only for newcomers but also for seasoned participants in the crypto space.

Now, let's get started.

Unreliable Information Sources: You Might Have Been Misled from the Beginning

Many investors are first introduced to crypto-related concepts through social media, content platforms, or online communities. These environments often mix credible sources and misleading information, making it challenging for even experienced investors to sift through the noise and identify valuable insights. Inexperienced investors are particularly vulnerable to fraudulent details because of the difficulty of correctly identifying information.

Consequently, fraudsters exploit the existing information asymmetry to deceive users who lack the necessary background knowledge. Their tactics include distorting or fabricating facts, stealing private keys, and gaining unauthorized access to accounts. This manipulation not only leads to individual losses but also contributes significantly to the stigmatization of the industry.

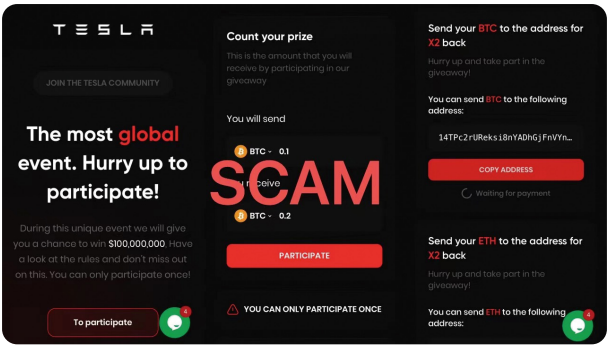
Video QR Code Scams

Scammers often induce victims to scan QR codes that redirect them to fraudulent third-party websites. In traditional scenarios, victims are typically prompted to submit personal information, install malicious software, or join deceptive online communities. With the rapid expansion of the crypto economy in recent years, this method has become more prevalent in the industry, targeting unsuspecting users.

A typical example involves scammers impersonating Elon Musk.

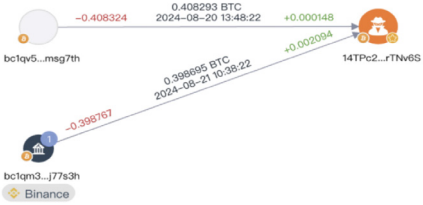
Due to his recent frequent mentions of blockchain-related concepts, Musk has generated significant interest in the crypto market. Taking advantage of this, malicious actors have used AI tools to create a deepfake video in which "Musk" claims that by scanning the QR code shown in the video, viewers can participate in a Bitcoin rebate campaign allegedly initiated by Tesla. The scammers distribute this fraudulent video by uploading it to YouTube or launching fake live streams.

Upon visiting the fraudulent website, “teslainc2x[.]org”(Don't be curious), users are instructed to transfer funds to a designated address with the promise that they have a one-time opportunity to receive double returns during the campaign period.



Scam Information

This is a classic investment scam. Using the BitracePro blockchain analytics platform, we can see that at least two victims have already sent Bitcoin to the fraudulent address without receiving any promised returns.(it' seems like Never)



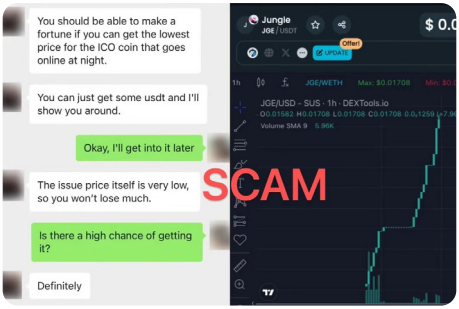
Analysis of the Video QR Code Scams

Social Media Scams

In addition to passively spreading fraudulent information and waiting for victims to take the bait, many investment scams are carried out through carefully orchestrated social engineering techniques. Scammers often lure victims with the promise of "helping you make money," step-by-step guiding them through creating a wallet, purchasing cryptocurrency, and investing in "profitable" schemes, ultimately stealing or deceiving victims out of their funds.

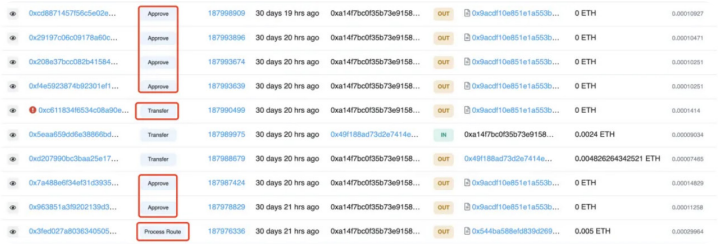
In the following example, I'll walk you through a typical scam tactic—

The victim encountered an introductory video about Bitcoin on TikTok (which was actually created and posted by the scammer) and left a comment. Shortly afterward, the victim received a private message from the video poster, who claimed to be able to teach him how to invest in Bitcoin. The victim readily agreed but, being a complete beginner, shared screenshots of every step with the scammer for guidance, unknowingly exposing his seed phrase in the process.



Chat Logs Between the Scammer and the Victim

The first project recommended by the scammer was a so-called ICO token named Jungle (JGE) (the official website itsjungle[.]me is now defunct, and its Twitter account has been deleted). The victim managed to gain a 50% profit from this transaction.

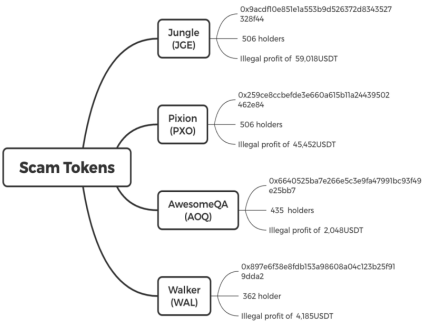


0xcd8871457f56c5e02e...	Approve	187998909	30 days 19 hrs ago	0xa14f7bc0f35b73e9158...	OUT	0x9acdf10e851e1a553b...	0 ETH	0.00010927
0x29197c06c09178a60c...	Approve	187993896	30 days 20 hrs ago	0xa14f7bc0f35b73e9158...	OUT	0x9acdf10e851e1a553b...	0 ETH	0.00010471
0x208e37bcc082b41584...	Approve	187993674	30 days 20 hrs ago	0xa14f7bc0f35b73e9158...	OUT	0x9acdf10e851e1a553b...	0 ETH	0.00010251
0x4e5923874b92301ef1...	Approve	187993639	30 days 20 hrs ago	0xa14f7bc0f35b73e9158...	OUT	0x9acdf10e851e1a553b...	0 ETH	0.00010251
0xc611834f6534c08a90e...	Transfer	187990499	30 days 20 hrs ago	0xa14f7bc0f35b73e9158...	OUT	0x9acdf10e851e1a553b...	0 ETH	0.0001414
0x5eaa659dd6e38866bd...	Transfer	187989975	30 days 20 hrs ago	0x49f188ad73d2e7414e...	IN	0xa14f7bc0f35b73e9158...	0.0024 ETH	0.00009034
0xd207990bc3baa25e17...	Transfer	187988679	30 days 20 hrs ago	0xa14f7bc0f35b73e9158...	OUT	0x49f188ad73d2e7414e...	0.004826264342521 ETH	0.00007465
0x7a488e6f34ef31d3935...	Approve	187987424	30 days 20 hrs ago	0xa14f7bc0f35b73e9158...	OUT	0x9acdf10e851e1a553b...	0 ETH	0.00014829
0x963851a3f9202139d3...	Approve	187978829	30 days 21 hrs ago	0xa14f7bc0f35b73e9158...	OUT	0x9acdf10e851e1a553b...	0 ETH	0.00011258
0x3fed027a803634050 5...	Process Route	187976336	30 days 21 hrs ago	0xa14f7bc0f35b73e9158...	OUT	0x544ba588efd839d269...	0.005 ETH	0.00029964

On-chain Transaction Records of Multiple Victims

However, the reality on-chain was that this was a classic “honeypot” token. Other unsuspecting victims who had purchased the token were desperately trying to grant permissions on various DEX platforms in an attempt to sell off their tokens, only to find themselves blocked. The victim’s “profit” was merely an illusion created by the scammer, who had whitelisted his address in the contract, allowing only him to sell. This token pool was specifically designed to make the victim feel successful and encourage further investment.

As expected, the next day, the scammer invited the victim to participate in another token sale. After the victim deposited 2.39 ETH, the scammer used the previously obtained seed phrase to steal all the assets from the victim’s wallet.



Scam Tokens Issued by the Fraud Ring

A subsequent investigation by Bitrace into the JGE token's issuance address revealed that the group had launched at least four fraudulent tokens and profited over $130K. If we include assets stolen through other illegal means, the total value of the damages would be even greater.

Romance Scams: A Hybrid of Investment and Romantic Fraud

Romance scams combine elements of investment fraud and relationship scams, primarily targeting high-net-worth individuals outside the crypto community who lack technical knowledge of the industry. Scammers carry out extensive background research on their victims, fabricating identities that cater to the victim's preferences and initiating online romantic relationships to lure them into participating in non-existent investment projects.

At the start of these "investment" activities, victims typically see their supposed returns grow rapidly. However, when they attempt to withdraw their profits, the fraudulent platform invents a variety of excuses, such as "tax payments," "late fees," "transaction fees," or "lock-up periods," to delay withdrawals and demand even more funds. Throughout this process, victims are squeezed dry of their assets and may even be pressured to take out loans until they have no remaining capital left to exploit.

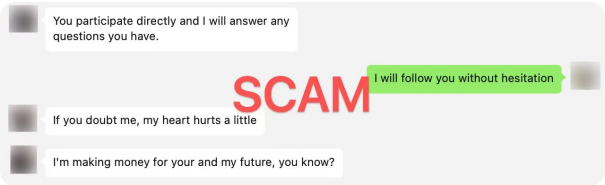
These malicious actors have no sympathy for their victims. They refer to the latter as "pigs," while the fabricated identities and deceptive scripts they use are considered "pig feed." The process of building a fake relationship is described as "fattening the pig," and the final stage, when all funds are drained, is known as " butchering the pig." Hence, this type of scam is commonly referred to as a "pig butchering scam," where victims suffer both financial and emotional losses.

Case Study: The "Gao Rui Business Academy" Pig Butchering Scam

The victim in this case was a young woman with some personal assets. In February 2023, she met a wealthy young man online through a social media platform. The scammer claimed to be traveling across the country for investment opportunities and would send her photos of himself at various sites. These images occasionally included selfies of him driving luxury cars or wearing designer watches. Coupled with daily affectionate messages, he gradually won her trust and affection.

During their online relationship, the scammer frequently mentioned an entity called the “Gao Rui Business Academy” and claimed it was a blockchain investment project. Participants were required to purchase Tether (USDT) to buy investment shares, with promises of high returns upon maturity.

The scammer insisted that he had personally invested in multiple rounds and had already earned substantial profits. To persuade the victim to participate, he even employed psychological manipulation techniques (commonly known as PUA).



Chat Logs Between the Scammer and the Victim

The victim, completely convinced, exhausted her own assets and borrowed heavily from family and friends, ultimately investing over 200,000 USDT into this so-called project. Predictably, her online "boyfriend" vanished without a trace, leaving her with no way to recover her losses.

Mismanagement of Assets: A Major Pitfall at the Start of the Crypto Journey

Unlike the centralized account login and verification systems commonly seen in traditional Web2 platforms, Web3 infrastructures such as crypto wallets do not store user identity information or account permissions. They also lack the typical account-related functionalities of conventional internet platforms, such as account deletion, re-binding, or identity recovery. This means that Web3 users must personally manage and safeguard their private keys—once lost, users permanently lose control over their on-chain identities, or if leaked, risk having their digital assets stolen.

To better grasp crypto wallet management, it is essential to first understand what private keys and seed phrases are.

A private key is a string of alphanumeric characters used to decrypt data or sign transactions. By importing the private key, users can "log in" to their crypto address on any wallet program and gain full account control. Using specific cryptographic methods, a private key can be converted into another unique string of characters, known as the public key, which serves as the counterparty address for sending and receiving funds. In practice, the public key is akin to a publicly shared home address, while the private key functions as the house key held exclusively by the owner.

A seed phrase, on the other hand, is an alternative representation of the private key. It consists of 12, 24, or another specified number of words derived from a particular dictionary, making it more readable and easier to remember. By using a seed phrase, a wallet can derive and manage one or more pairs of public and private keys according to specific standards. Popular wallets like imToken and TokenPocket allow users to create multiple blockchain addresses under the same seed phrase, including multiple addresses within the same blockchain and across different blockchains. By importing the seed phrase into any compatible wallet, users can restore access to their on-chain assets.

In addition to private keys, some wallet software also supports exporting keys in a QR code format. While designed for convenience, these keys are just as critical as plaintext private keys or seed phrases.

Some malicious actors take advantage of investors' lack of knowledge regarding blockchain wallets and employ various tactics to deceive users into revealing their seed phrases, private keys, or granting access permissions. This, in turn, allows them to gain unauthorized access and steal the victims' assets.

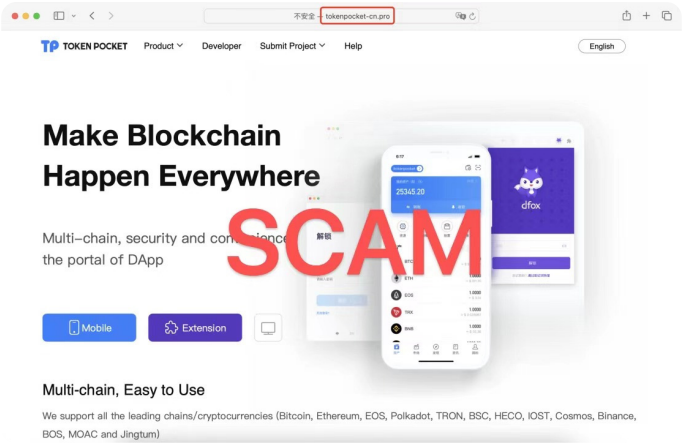
Fake Wallet Apps: A Trap for Asset Theft

Fake apps are a common type of malicious software that replicate the logos, names, and interface elements of legitimate applications to deceive users into downloading and using them. These apps are designed to compromise network security, steal user information, and enable unauthorized use of paid services.

In the cryptocurrency industry, wallet apps are particularly targeted by such high-quality replicas. A common tactic used by attackers is to inject malicious code into the source files of legitimate wallet apps. Once a victim installs this malicious software and imports their seed phrase or private key, the scammers behind the fake app can immediately gain access to these credentials and proceed to transfer the victim's assets without authorization.

Currently, the most prevalent methods for distributing fake wallet apps include using search engines, fake wallet websites, and fake social media accounts—

Search Engine Channels: Scammers produce crypto-themed articles or short videos embedded with malicious download links and promote them using Search Engine Optimization (SEO) or Search Engine Marketing (SEM) techniques. When potential victims search for related keywords—especially brand-specific wallet names—these fraudulent links may appear at the top of the search results, sometimes even as the very first entry. Victims unable to distinguish between genuine and fake results are at high risk of losing their assets.



Fake Website

Fake Wallet Websites: Fake wallet websites are typically paired with fake wallet apps. By creating high-quality replica websites and deploying them on look-alike domains, these fake sites are often more deceptive than typical SEO techniques. For example, the fake TokenPocket wallet site **tokenpocket-cn[.]com** is a counterfeit version of the legitimate domain **tokenpocket.pro**. The intent is to mislead investors into downloading fake wallet apps, resulting in the loss of their assets.

Fake X(Twitter) Account

Fake Social Media Accounts: Fake social media accounts are also rampant, especially on platforms frequently used by crypto investors, such as X (formerly Twitter). These accounts often pose as "imToken 中文客服 / 官方 " (imToken Chinese Customer Service/Official) or "imToken SupportTeam," aiming to pollute platform information channels and promote malicious wallet apps to unsuspecting users.

Multisig Case: A New Breed of Crypto Theft

Multisignature (multisig) wallets are a crucial asset security solution. Unlike standard wallets, a multisig wallet requires multiple private keys to authorize a transaction. For example, the most common setup is a 2-of-3 multisig wallet, which requires signatures from at least two of the three private key holders to initiate a transaction. The strength of this model lies in its redundancy—at least two private keys must be compromised before the assets in the wallet are at risk.

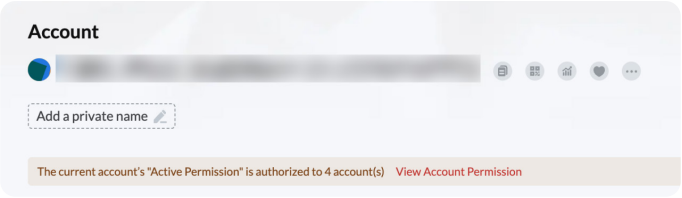
However, this very solution has been exploited by hacking groups, giving rise to a new variant known as multisig theft.

In traditional fake wallet scams, hackers obtain access to a wallet's private key through a fake wallet's backend, thereby gaining shared control over the address with the user. Under such schemes, both the hacker and the user can independently transfer funds out of the compromised wallet. Scammers typically have two strategies:

Immediate Theft: They may drain the wallet's assets immediately. Once the user sees that the balance is zero, they are unlikely to use the wallet again.

"Fish Farming" Tactic: Alternatively, the hacker might take the risk of not stealing the funds immediately, choosing to leave the assets untouched and wait for the user to accumulate more over time. This approach is referred to as "fish farming" by malicious actors.

In these scenarios, fraudsters often act impatiently and quickly siphon off the funds, regardless of the amount.



Victim Accounts with Altered Permissions in Multi-Signature Scams

In multisig scams, the situation is more covert because the user actually loses control of their account permissions. During this time, the address remains in a "funds only moving in, never moving out" state. Theoretically, as long as the user does not attempt to withdraw funds, they may never realize that they are on the verge of losing all their assets.

For the scammer, this tactic requires less effort and involves simply waiting for the unsuspecting victim to keep depositing assets into the compromised wallet.

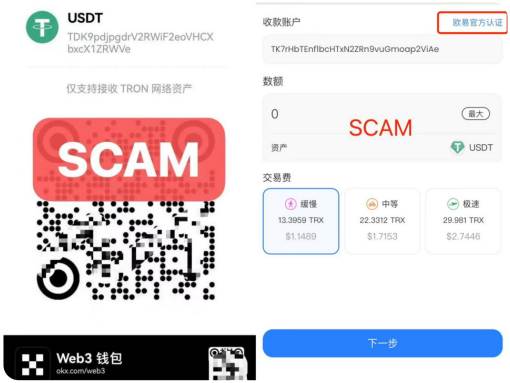
Clearly, multisig scams are much more subtle, with a higher success rate and greater overall threat potential. They allow scammers to accumulate larger amounts of stolen assets without raising immediate suspicion, making this method a particularly dangerous evolution of traditional crypto theft.

Payment Authorization Scams: A Growing Threat to Wallet Security

In addition to the risks of losing wallet control through compromised multi-signature setups, another increasingly common method of crypto theft targets the authorization of specific digital assets. The fundamental principle is that blockchain networks allow users to delegate the operational authority of a certain number of tokens in their address to another address through smart contracts. This process requires the user to initiate an on-chain transaction.

For example, suppose Alice has 1,000 USDT in her address. By calling a smart contract, she initiates an on-chain transaction that grants Bob's address permission to operate up to 100 USDT from her address. Once the authorization is complete, Bob can initiate transactions from his own address to transfer up to 100 USDT from Alice's wallet—without needing any further approval from Alice.

Scammers exploit this feature by disguising authorization links as QR codes and claiming that they are merely "payment" QR codes. When victims scan the code and approve the transaction, they unknowingly delegate the entire token authorization limit to the scammer's address.



Payment Authorization Scams

A recent example of this scam type is the "fake transaction approval" theft scheme. Take note of the interface on the right side of the image above—not an authentic OKX Web3 wallet system transaction page, but rather a well-crafted replica by the scammer. The legitimate OKX Web3 wallet transaction interface would look significantly different and would never display labels such as "OKX official certification."

The real objective of these scams is to deceive victims into visiting phishing sites through their wallet browsers. Using highly realistic imitation pages, the scammer misleads victims into believing that they are executing a regular transaction. However, the actual content of the transaction is a token authorization request.

If the wallet does not perform a proper validation and alert the user, it is almost impossible for the victim to realize they have been tricked until it's too late. By the time they notice, the scammer would already have full authorization to drain their wallet's assets.

This method of authorization scam poses a significant threat, as it leverages both the complexity of smart contract interactions and the victim's unfamiliarity with technical transaction details, making it a highly effective tool for fraudsters to exploit.

Fake Telegram Scams: Targeting Crypto Investors with Counterfeit Apps

Telegram is a popular social platform among the crypto investment community and is especially favored by OTC traders due to its high level of anonymity. As a result, scammers have specifically developed counterfeit Telegram apps to target this group.

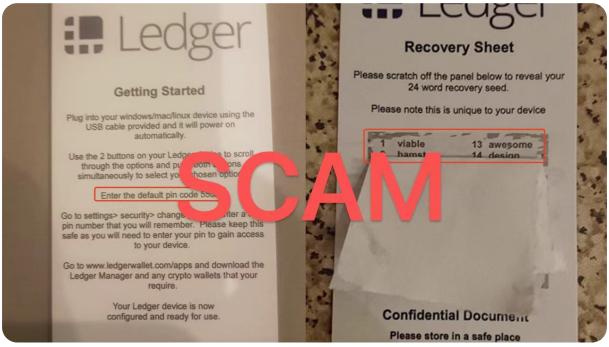
The tactics used in fake Telegram scams are similar to those employed in the fake wallet scams mentioned earlier. The core strategy involves injecting malicious code into the legitimate Telegram app's codebase, and it serves two primary purposes:

Harvesting Victims' Chat History: Some users store or share their seed phrases, private keys, or other sensitive information through Telegram's chat history. By using these compromised apps, scammers can gain direct access to this information and subsequently steal the associated assets.

Manipulating Outgoing Messages: Another malicious function involves altering the content of the victim's messages. The counterfeit app is designed to automatically recognize specific patterns, such as strings beginning with "0x" (which are typical for Ethereum addresses). It then replaces these values with a scammer-controlled address. For the sender, everything appears normal in their local client, but the recipient receives a modified message with the altered address.

Hardware Wallet Fraud: A Social Engineering Scheme

Hardware wallets are widely regarded as one of the safest methods for storing digital assets. By isolating seed phrases and private keys from the internet, they theoretically protect investors from key exposure. However, there are still specific social engineering tactics that scammers can exploit to steal funds. Here, I will outline one such method.



Fake Hardware Wallet Manuals Created by Fraudulent Teams

A victim purchases a hardware wallet from a third-party online marketplace. After receiving the wallet, the victim follows the instructions provided in the "manual" to set up the device. The manual includes a "pre-set PIN code" to unlock the hardware wallet and a "seed phrase" that the victim is instructed to back up. After depositing a significant amount of funds into the wallet address, the victim eventually discovers that their assets have been stolen.

In this case, the theft did not occur due to a hardware vulnerability. Instead, the scammer had pre-activated the wallet and obtained the associated seed phrase. They then forged a fake manual, repackaged the device, and sold the already-compromised wallet through unofficial channels to the victim. This highlights the critical importance of purchasing hardware wallets only through official retailers—just as important as verifying official websites.

By manipulating the trust users place in hardware wallets and preying on the assumption that these devices are inherently secure, scammers are able to steal assets through this elaborate yet effective social engineering tactic.

When You Begin Trading Crypto

Up to this point, you've successfully navigated through the initial learning phase(Congratulations!). You are now able to identify and avoid false information channels and have an understanding of unsafe asset storage methods. But now comes the real challenge—putting your hard-earned capital into the market and engaging in actual transactions.

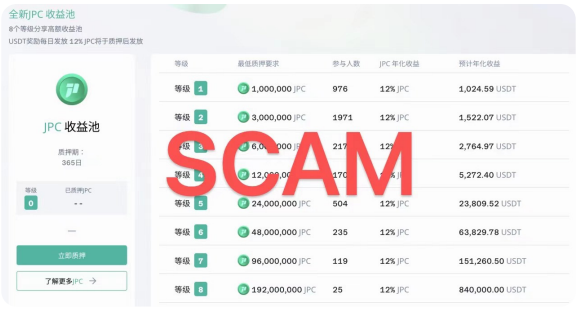
Do you believe that there are sustainable investment products in the crypto market offering annual returns of over 50%? Do you think that staking your idle stablecoins in a certain "mining pool" will generate stable profits? Or that participating in a "staking event" promoted by an "official exchange" will easily yield gains?

If your answer to any of these questions is "yes," then you might be treading on dangerous ground.

High-Yield Exchange Investment Scams

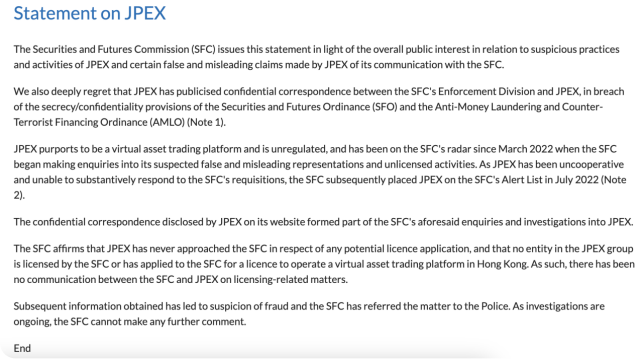
Purchasing cryptocurrencies through centralized exchanges is one of the most common investment methods. To attract and retain more user funds, some centralized exchanges offer crypto investment products, such as staking tokens to earn additional tokens of the same or different type. Typically, these investment products offer relatively low returns and are subject to certain investment limits. Legitimate exchanges rarely make these products their core offering.

However, fraudulent platforms often lure unsuspecting investors by advertising fake investment products with exceptionally high yields. These platforms encourage users to lock up their funds for extended staking periods, effectively restricting their ability to withdraw. By the end of the staking period, the investment product might either default on payouts, payout with severely devalued tokens, or the platform might vanish entirely (commonly known as a "rug pull"), causing significant financial losses for investors.



JPEX's High-Yield Exchange Investment Scams

The JPEX exchange, which collapsed in September 2023, is a typical case. JPEX adopted an aggressive business strategy, using balance-based referral rewards instead of transaction fee rebates to incentivize users to deposit large amounts of crypto and invite friends and family to join. JPEX also issued a token called JPC, claiming that it was the platform's governance token. Token holders were promised participation in so-called "node staking" with a guaranteed annual return of at least 12%. By increasing the amount invested or extending the lock-up period, this yield was marketed as potentially rising even higher.



Statement on JPEX

The Securities and Futures Commission (SFC) issues this statement in light of the overall public interest in relation to suspicious practices and activities of JPEX and certain false and misleading claims made by JPEX of its communication with the SFC.

We also deeply regret that JPEX has publicised confidential correspondence between the SFC's Enforcement Division and JPEX, in breach of the secrecy/confidentiality provisions of the Securities and Futures Ordinance (SFO) and the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) (Note 1).

JPEX purports to be a virtual asset trading platform and is unregulated, and has been on the SFC's radar since March 2022 when the SFC began making enquiries into its suspected false and misleading representations and unlicensed activities. As JPEX has been uncooperative and unable to substantively respond to the SFC's requisitions, the SFC subsequently placed JPEX on the SFC's Alert List in July 2022 (Note 2).

The confidential correspondence disclosed by JPEX on its website formed part of the SFC's aforesaid enquiries and investigations into JPEX.

The SFC affirms that JPEX has never approached the SFC in respect of any potential licence application, and that no entity in the JPEX group is licensed by the SFC or has applied to the SFC for a licence to operate a virtual asset trading platform in Hong Kong. As such, there has been no communication between the SFC and JPEX on licensing-related matters.

Subsequent information obtained has led to suspicion of fraud and the SFC has referred the matter to the Police. As investigations are ongoing, the SFC cannot make any further comment.

End

Statement from the Hong Kong Securities and Futures Commission (SFC) regarding JPEX

This deceptive model successfully attracted significant funds from inexperienced investors across Hong Kong, Taiwan, Mainland China, Singapore, and other regions, until the platform maliciously executed a rug pull, leaving investors with severe financial losses. According to the Hong Kong police, more than 2,000 victims reported the crime after the incident, involving a sum of up to HK$1.3 billion.

Such high-yield investment scams are highly dangerous because they exploit the allure of seemingly safe, lucrative returns and the credibility of established exchange platforms to target non-professional investors.

Honeypot Token Scams: The "Buy-Only, No-Sell" Trap

The "buy-only, no-sell" scam not only occurs on centralized platforms but can also happen on decentralized exchanges (DEXs). However, the issue does not lie with the DEX itself, but rather with the malicious design of the token by its issuer.

When developers issue a token on the blockchain according to a specific standard, they can set basic parameters, such as the token's name, symbol, and supply cap. Additionally, they have the ability to restrict certain addresses from accessing specific functions of the token, such as transferring or selling it. When these restrictions are applied to almost every address except a select few controlled by the issuer, the token is referred to as a “Honeypot Token.”

As the name suggests, addresses that are not included in the whitelist can buy or receive these tokens, but they cannot sell them through regular means in DEX trading pairs. This results in a situation where holders watch helplessly as the token value fluctuates, without the ability to cash out. There are several variants of this scam:

Simple Sell-Restriction Scam: The most straightforward version of the scam involves setting up sell restrictions. The scammer issues a honeypot token and creates a liquidity pool on a DEX. They then promote the token through social platforms, community broadcasts, and airdrops to known addresses, using various methods to attract attention. At the same time, they use multiple addresses to trade back and forth, artificially inflating the token price.

Unsuspecting investors who buy into the hype soon find that the value of their position increases rapidly, but they are unable to sell to realize these profits. Once there are enough victims holding the token, the scammer withdraws all liquidity from the pool, effectively draining all the funds and leaving victims with worthless tokens.

A Whitelist Manipulation Honeypot Token that incorporates "Pig Butchering" scam tactics. A more sophisticated variation combines honeypot restrictions with the techniques of a pig butchering scam. After issuing a honeypot token, scammers employ social engineering to lure novice investors into buying. In the early stages, they whitelist target addresses, allowing these investors to sell and make profits, thereby building trust. However, once the victim increases their investment, the scammer removes their address from the whitelist, preventing them from selling and ultimately completing the scam.

This approach is highly deceptive, as victims believe they are engaging in a legitimate investment due to their initial successful transactions.

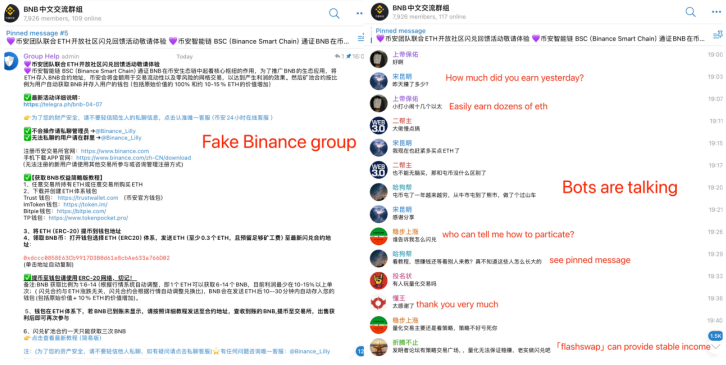
Exploiting "Smart Money" Follower Behavior: Another advanced strategy targets so-called "Smart Money" followers. "Smart Money" refers to on-chain addresses with a high success rate in investments. Due to the transparency of the blockchain, anyone can monitor the activity of any address. Consequently, some traders and intelligence firms closely follow these high-performance addresses. When a Smart Money address buys a particular token, other traders often follow suit.

Scammers exploit this behavior by issuing a honeypot token and establishing a liquidity pool. Using a specially crafted smart contract, they send a portion of the token to the Smart Money address, making it appear as if the address has actively bought the token. Some automated trading bots may misinterpret this transaction as a legitimate purchase by the Smart Money address, triggering a wave of follower activity.

This results in a series of follow-up buys from traders who are unaware that the token is a honeypot. The scammers then wait for a sufficient number of victims to buy in before withdrawing the liquidity, leaving the followers trapped with unsellable tokens.

Fake Binance Mining Pool Scam: A Sophisticated Deception Targeting Crypto Users

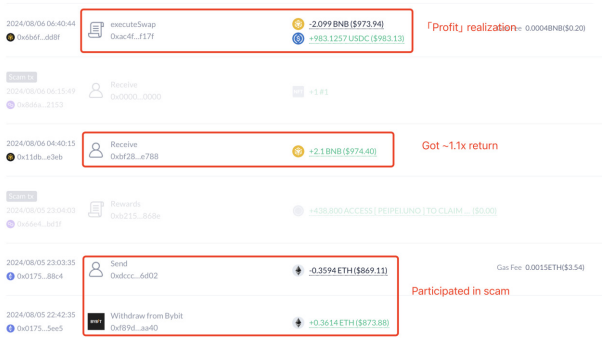
Earlier, we discussed the "Double Returns" scam impersonating Musk, which mainly targets outsiders unfamiliar with blockchain technology. Now, I will introduce a more deceptive scam aimed at experienced users within the crypto community: the Fake Binance Mining Pool Scam.



Fake Binance Group Chat Logs

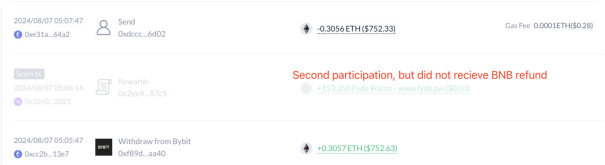
This type of fraud has been around for a long time. Scammers typically create Telegram groups with names like “Binance Exchange Community” or “Binance Reward Program Group” and populate them with thousands or even tens of thousands of bot accounts to create the illusion of an official Binance community. In reality, the only human in the group is the targeted victim.

Scam Tactics and Execution: The scammer then acts as a “Binance Customer Support” representative and posts messages in the fake group, claiming that Binance has partnered with the Ethereum Foundation to conduct a user reward campaign. According to the scammer, users are allowed to exchange ETH for BNB at a rate higher than the market price, enabling them to profit from the price difference. The group is flooded with bots mimicking genuine users, enthusiastically claiming that they have made significant gains through this "flashswap" opportunity.



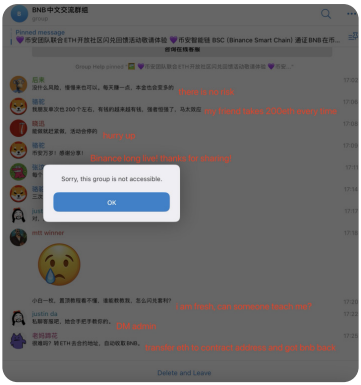
Fraudulent Bait

Following the scammer's instructions, the victim is first asked to transfer a certain amount of ETH to a designated smart contract address on the Ethereum network. Shortly after, the victim receives BNB on the Binance Smart Chain (BSC) network, valued at roughly 1.1 times the original amount of ETH sent. The difference above the market rate is presented as the victim's "profit."



On-chain Transaction Records of the Victim

How the Scam Unfolds: After experiencing this initial success, the victim, lured by the apparent profitability, is likely to reinvest a larger amount. However, on the second transaction, no BNB is returned. If the victim attempts to voice their concern or express suspicion within the Telegram group, they are immediately banned by the fake group administrator, and the entire group is promptly disbanded. At this point, the scam has been successfully executed.



Fake Binance Group chat logs

Fake OKX Public Chain Scam: "Hold USDT to Earn OKT"

Liquidity mining is a popular concept in the DeFi era of the crypto industry. Users can participate in various decentralized applications (dApps) by depositing a certain number of tokens into specific smart contract addresses, enabling them to engage in activities such as governance, obtaining voting rights, lending, and providing security for on-chain protocols. In return, participants typically receive certain rewards.

Scammers have taken advantage of the growing popularity of liquidity mining by creating numerous fraudulent schemes under this guise. One such scheme, which targets inexperienced users, is the Fake OKX Public Chain "Hold USDT to Earn OKT" scam.

Scam Information

How the Scam Works: This scam claims that users simply need to hold USDT in their wallets to continuously earn OKT tokens at an exceptionally high annualized rate. The scam further advertises that there are no lock-up periods for the deposited tokens, and users are free to transfer the funds from their addresses at any time.

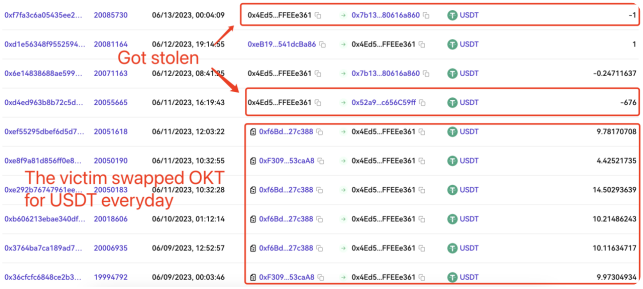
Scam Information

According to the rules promoted by the scam, even the lowest tier supposedly offers an annualized return of 475%. Many new investors, unfamiliar with the mechanics of blockchain and lured by the promise of high returns, are easily deceived by such seemingly lucrative offers.

Txn hash	Method	Block	Date time	From	To	Amount	Txn fee
0x72eeef0aec...	approve	19946834	06/06/2023, 21:25:51	0x4Ed5...BF0FFEEe361	0x382b...5C6C65C50	0 OKT	0.00000642 OKT
0xf9f44ac34c...	0x9871efa4	19940919	06/06/2023, 15:11:10	0x4Ed5...BF0FFEEe361	0xf6Aa...42593385c	-0.16399231 OKT	0.00001759 OKT
0x3c6972245...	increaseAllo...	19933776	06/06/2023, 07:38:42	0x4Ed5...BF0FFEEe361	0x382b...5C6C65C50	0 OKT	0.0000768 OKT
0x08855d17a...	0x	19933745	06/06/2023, 07:36:45	0x4C45...BabEcaDd620	0x4Ed5...BF0FFEEe361	0.001 OKT	0.00000318 OKT

Malicious authorization

Initial Interaction with the Fraudulent Contract: Victims are asked to interact with a smart contract advertised as a "mining contract" to start earning OKT. In reality, this contract is a malicious smart contract that grants the scammer's address unlimited approval to transfer USDT from the victim's wallet.



On-chain Transaction Records of the Victim

Small Initial Returns to Build Trust: Over the first few days, the victim receives a small, regular amount of OKT, reinforcing the scam's credibility. This tactic gives the impression that the system is functioning as advertised, thereby encouraging the victim to increase their investment.

The Exit Scam: Once the victim either increases their holdings significantly or shows no additional activity for an extended period, the scammer activates the transferFrom function, draining all of the USDT from the victim's wallet. At this point, the victim's funds are gone, and the scam is complete.

Liquidity Withdrawal Scams: Exploiting AMM Mechanisms for Profit

Automated Market Makers (AMMs) are the most prevalent form of decentralized exchange (DEX) platforms. Instead of using a traditional order book for matching buyers and sellers, AMMs operate by quoting prices to users automatically through smart contracts, thereby eliminating the need for peer-to-peer order matching. To facilitate this, liquidity providers (LPs) deposit a proportional amount of two different tokens into a smart contract based on a specified exchange rate. Every trade that occurs affects the ratio of these two tokens in the pool, and consequently, their price. For instance, if a liquidity pool holds tokens A and B, and a user swaps their A tokens for B tokens, the quantity of A in the pool increases while the quantity of B decreases, causing the price of token B (relative to token A) to rise.

How the Liquidity Withdrawal Scam Works: Scammers have leveraged this feature to design a type of scam known as the Liquidity Withdrawal Scam. Here's how it typically unfolds:

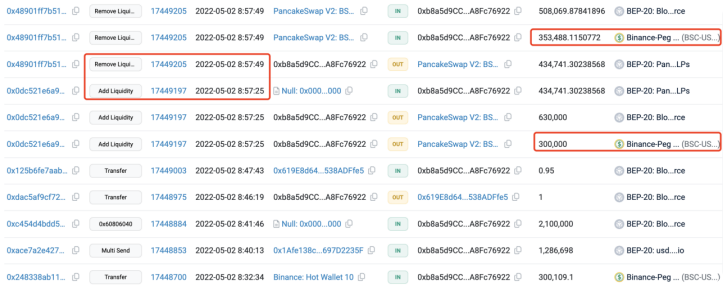
Token Creation: The scammer first creates a new token on the blockchain, which usually costs no more than $100. They then provide liquidity for this token on a major DEX, pairing it with a widely-used token like WETH (Wrapped Ether) or USDT.

Artificial Hype and Promotion: Using various deceptive strategies—such as fake social media announcements, fabricated endorsements, or fraudulent partnerships, as discussed in previous examples—the scammer makes it appear as if this token has the potential for significant appreciation, thus luring unsuspecting investors into buying the token.

Rising Price Through Victim Purchases: As more victims buy into the token, the demand pushes up the token's price. This makes it appear as though the value of the newly minted token is genuinely increasing, encouraging more purchases and further inflating the price.

Liquidity Withdrawal (Rug Pull): At this point, the scammer performs a "rug pull" by withdrawing all of the liquidity from the pool. Due to the increased trading activity, the liquidity pool now holds a large amount of WETH or USDT, which the scammer extracts. The scammer's initial investment in liquidity was minimal, yet they walk(walked) away with a substantial profit.

BFF Token Scam Case: On February 20, 2024, the High-Tech Industry Development Zone People's Court in Nanyang, Henan Province, ruled on a crypto fraud case. The defendant was found guilty of fraud for issuing a fake cryptocurrency, misleading victims to deposit 50,000 USDT, and quickly "withdrawing the funds," resulting in financial losses for the victims.



0x48901ff7b51...	Remove Liqui...	17449205	2022-05-02 8:57:49	PancakeSwap V2: BS...	IN	0xb8a5d9CC...A8Fc76922	508,069.87841896	BEP-20: Blo...rce
0x48901ff7b51...	Remove Liqui...	17449205	2022-05-02 8:57:49	PancakeSwap V2: BS...	IN	0xb8a5d9CC...A8Fc76922	353,488.1150772	Binance-Peg ... (BSC-US...)
0x48901ff7b51...	Remove Liqui...	17449205	2022-05-02 8:57:49	0xb8a5d9CC...A8Fc76922	OUT	PancakeSwap V2: BS...	434,741.30238568	BEP-20: Pan...LPs
0x0dc521e6a9...	Add Liquidity	17449197	2022-05-02 8:57:25	Null: 0x000...000	IN	0xb8a5d9CC...A8Fc76922	434,741.30238568	BEP-20: Pan...LPs
0x0dc521e6a9...	Add Liquidity	17449197	2022-05-02 8:57:25	0xb8a5d9CC...A8Fc76922	OUT	PancakeSwap V2: BS...	630,000	BEP-20: Blo...rce
0x0dc521e6a9...	Add Liquidity	17449197	2022-05-02 8:57:25	0xb8a5d9CC...A8Fc76922	OUT	PancakeSwap V2: BS...	300,000	Binance-Peg ... (BSC-US...)
0x125b6fe7aab...	Transfer	17449003	2022-05-02 8:47:43	0x619E8d64...538ADFfe5	IN	0xb8a5d9CC...A8Fc76922	0.95	BEP-20: Blo...rce
0xdac5af9cf72...	Transfer	17448975	2022-05-02 8:46:19	0xb8a5d9CC...A8Fc76922	OUT	0x619E8d64...538ADFfe5	1	BEP-20: Blo...rce
0xc454d4bdd5...	0x60806040	17448884	2022-05-02 8:41:46	Null: 0x000...000	IN	0xb8a5d9CC...A8Fc76922	2,100,000	BEP-20: Blo...rce
0xace7a2e427...	Multi Send	17448853	2022-05-02 8:40:13	0x1Afe138c...697D2235F	IN	0xb8a5d9CC...A8Fc76922	1,286,698	BEP-20: usd...io
0x248338ab11...	Transfer	17448700	2022-05-02 8:32:34	Binance: Hot Wallet 10	IN	0xb8a5d9CC...A8Fc76922	300,109.1	Binance-Peg ... (BSC-US...)

Scammer's On-chain Actions

According to blockchain explorer records, on May 2, 2022, at 08:41:46 UTC, the scammer issued a token named BFF and created a BFF-USDT trading pair on a DEX at 08:57:25. The initial liquidity provided was 300,000 USDT and 630,000 BFF tokens. However, only 24 seconds later, the scammer withdrew all the liquidity. During this brief period, a significant number of victims had already purchased BFF tokens, altering the pool's exchange rate. As a result, the scammer's liquidity withdrawal yielded over 50,000 USDT in illicit gains—all within just 25 minutes.

Similar scams are occurring continuously on the blockchain, and in most cases, it is almost impossible to recover lost funds. The BFF case was fortunate in that the scammer was prosecuted and the funds (were) partially tracked. However, most victims are not so lucky, as liquidity withdrawal scams operate with relative ease and minimal regulatory oversight.

Phishing: The Viral Growth of Deceptive Tactics

Phishing is a form of social engineering attack where deceptive emails, messages, phone calls, or websites are used to trick users into revealing sensitive information or performing malicious actions. In the traditional internet era, phishing (is) typically aimed at stealing cash or virtual assets. However, with the rapid development of the crypto economy, scammers have increasingly set their sights on Crypto.

We'll introduce three common phishing tactics targeting crypto users.

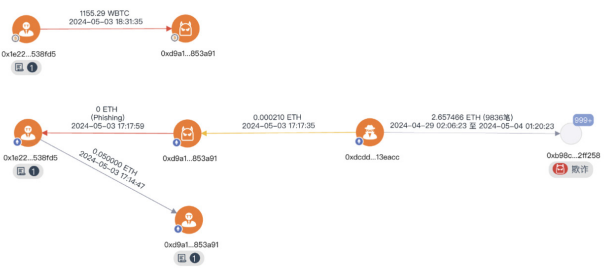
Address Poisoning

If you have a frequently used blockchain address, you may have noticed small, unsolicited transactions appearing in your transaction history. These transactions do not affect your wallet's functionality and simply sit passively in your records.

This phenomenon is known as address poisoning—a prevalent form of phishing in which scammers send minuscule amounts of ETH, USDT, TRX, or other tokens to a target address, thereby "polluting" the transaction history. If the victim has poor wallet management habits, they might accidentally copy the poisoned address from the transaction history when making a future transfer, thereby mistakenly sending funds to the scammer.

A deeper look into the addresses initiating these transactions reveals a distinctive pattern: the tail end of the scammer's address often matches that of the legitimate counterparty frequently interacted with by the victim. This similarity is the key trick of this scam—these "phishing addresses" are crafted to resemble the victim's usual counterpart by using similar trailing characters.

Implementation of the Scam: Scammers use software to generate large batches of blockchain public-private key pairs and filter for addresses with specific characteristics, such as a string of repeated numbers like "666" or "888," which are considered "vanity addresses" due to their appealing patterns. In the case of address poisoning, the generated addresses mimic the target's addresses, creating a look-alike for deception.



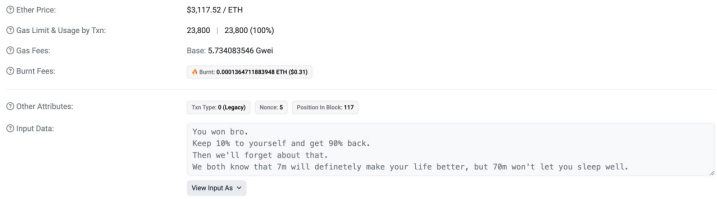
Analysis of the Address Poisoning Case

The Largest Address Poisoning Incident to Date: On May 3, 2024, the largest address poisoning incident on record occurred, where the victim mistakenly transferred 1,155 BTC (worth $68 million at the time) to a poisoned address. A review of the incident revealed that the victim, 0x1e22, transferred 0.05 ETH to their new address, 0xd9a1b0b1e1ae382dbdc898ea68012ffcb2853a91, for purchasing DAI. This action was immediately detected by the phishing group, who, three minutes later, used a look-alike address, 0xd9a1c3788d81257612e2581a6ea0ada244853a91, to send a 0 ETH transaction to the victim. Seventy-five minutes later, the victim accidentally copied the wrong address and sent 1,155 BTC to the scammer.

Tracking the transaction fees for these phishing addresses shows that the upstream address had conducted 9,836 similar scams, indicating that this incident is just the tip of the iceberg.

Advertising Tokens

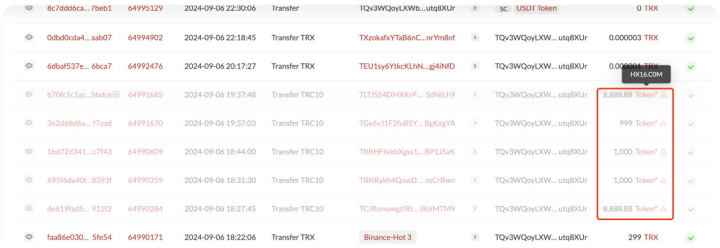
On-chain transactions can carry additional information unrelated to the actual transfer. For example, Ethereum's official blockchain explorer supports displaying user messages alongside transactions. Since this metadata is publicly visible, anyone can read its content.



Phishing Victim Leaves a Message for the Scammer via On-chain Transaction

In the aforementioned 1,155 BTC phishing incident, the victim initially used this feature to send messages to the phishing address, offering to settle by returning 90% of the stolen funds and not pursuing legal action. Both parties subsequently established contact and eventually reached an agreement for partial restitution—all while maintaining complete anonymity.

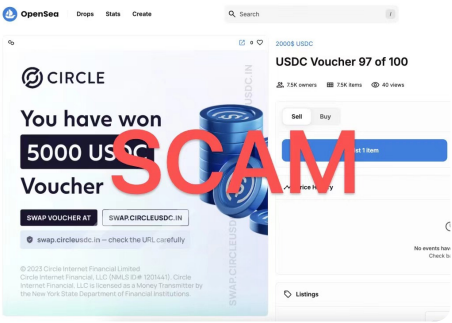
However, this form of message-based communication, while useful, is not sufficiently direct for advertisers. Thus, they began embedding ads into the token name or symbol itself.



Advertising Token

Tron Network's Advertising Tokens: On major blockchains like the Tron Network, many transactions involve tokens with names formatted as domain addresses, advertising gambling sites, adult content, energy rental services, and more, including numerous scam links. If recipients of these tokens are curious and interact with the associated websites, they may risk financial loss.

As the NFT market has surged, this advertising technique has expanded to include non-fungible tokens (NFTs). NFT users often find themselves airdropped with unsolicited tokens. Many of these are well-designed scams, featuring promotional posters that claim the recipient has won thousands of dollars in rewards and direct them to phishing websites. Some scammers even manipulate the floor price of these NFTs to make them appear genuinely valuable.

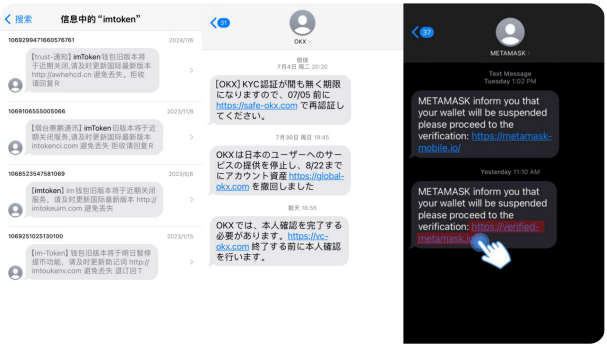


Phishing NFT

Phishing NFT "2000$USDC": In the example above, an NFT named “2000$USDC” claims that the recipient is eligible to receive a 5,000 USDC reward and is one of only 100 lucky winners. In reality, the scammer airdropped this NFT to over 7,500 addresses, clearly indicating a fraudulent scheme. Visiting the website shown on the NFT poster would only result in the recipient losing their funds.

Fake Exchange Clearance SMS

Impersonating law enforcement or industry regulators to distribute phishing links is one of the most common forms of crypto-related scams.



Scam Text Messages

When personal information is leaked, victims receive a flood of fraudulent SMS messages or emails. The primary tactic is to claim that an “outdated version of software needs updating” and prompt the victim to visit a phishing site. If the phishing message targets wallet users, they are usually directed to download a fake wallet app. If the message targets exchange users, the phishing attempt often leads to a pig butchering scam.

Fake Wallet APP Theft

Fake Exchange Clearance SMS: Bitrace investigated one such case in November 2023, when Binance co-founder Changpeng Zhao was reportedly arrested. Scammers capitalized on this news by spreading messages that storing funds on centralized exchanges was no longer safe. Out of fear, a victim transferred their funds out of OKX, only to have their private keys stolen in the process, resulting in a loss of 166.7 ETH.

The core strategy of this scam is to exploit investors' lack of understanding about industry policies and create fear through appeals to authority. By impersonating authoritative figures or institutions, scammers are able to scare victims into divulging their seed phrases or private keys.

The End of Industrial Specialization: The Rise of Crypto Drainers

According to David Ricardo's theory of comparative advantage, in a market economy, each sector naturally specializes to increase production efficiency. Surprisingly, this economic principle also applies to the world of crypto fraud.

The hallmark of this phenomenon is that the technical development departments at the forefront of the crypto fraud supply chain are no longer directly involved in distributing or promoting malicious software. Instead, they offer their software as a service (SaaS) to brokers and affiliates, taking a cut of the stolen assets as a share of the proceeds. This division of labor significantly lowers the entry barrier for initiating fraud schemes—scammers can now focus solely on marketing the software, while the technical aspects are handled by specialized providers.

These SaaS providers are known as Crypto Drainers.

The Stolen Wallets Affiliate Model

The fake wallet apps mentioned earlier are powered by the rapidly expanding ecosystem of Crypto Drainers. These entities specialize in reverse-engineering popular crypto wallet software and modifying specific code elements to steal target seed phrases. To support affiliates in managing the influx of stolen seed phrases, some Drainers develop dedicated management dashboards, enabling affiliates to automate the transfer of victims' funds or control multisig wallet addresses.

Just like traditional SaaS providers in the conventional internet space, fake wallet Crypto Drainers typically offer a variety of affiliate models:

Direct Distribution of Crypto Drainer Trojan Links: This is the simplest model with no backend management required. Affiliates only need to drive traffic to malicious wallet download links through social media platforms, search engines, and content networks. The Drainer itself handles the theft, and revenue is shared with the affiliate according to a predefined split.

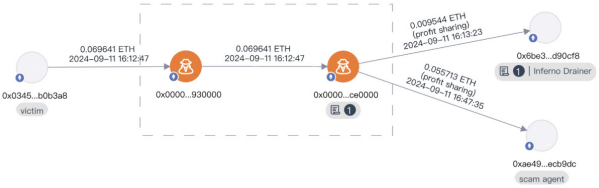
Independent Deployment Solutions for Larger Affiliates: In this model, large-scale affiliates can deploy and operate their backend infrastructure. They are responsible for the entire process, from promotion and lead conversion to managing the theft and ultimately transferring the stolen assets. Affiliates who choose this model have full control over the backend operations and can further subcontract lower-level affiliates, earning additional commission fees.

These models offer varying profit-sharing schemes, and the types of affiliates involved differ significantly. This variety indicates a well-developed and thriving stolen wallet SaaS market.

The Phishing Affiliate Model

Similar to the stolen wallet schemes, many phishing scams targeting token approvals, social media impersonations, and arbitrage traps are also backed by professional Crypto Drainers, who provide technical and sometimes even operational support to fraudsters.

Take **Inferno Drainer**, a well-known phishing service provider, as an example. This group promotes its services through Telegram channels and supplies scammers with the phishing websites needed to carry out their activities. Once a victim scans a QR code on one of these phishing sites and connects their wallet, Inferno Drainer immediately scans the wallet to locate the most valuable and easily transferable assets. It then initiates a malicious transaction targeting these assets.



Drainer's Sharing Model

When the victim unknowingly approves the transaction, their funds are swiftly drained. The stolen assets are then divided, with a portion going to Inferno Drainer's developers and the rest to the scammer.

The "Make Money" Phishing Schemes: One classic example is the "Help You Make Money" scam, where the scammer approaches potential victims through short video platforms, media outlets, or social networks. They establish contact by claiming to have access to high-yield investment opportunities, using tactics such as pig butchering, fake mining pools, and other schemes discussed earlier. Once the victim suffers financial losses, the proceeds are split between the scammer and the SaaS provider.

Because these schemes require lower technical expertise and rely more on persuasive social engineering tactics, some Drainers go a step further by providing their affiliates with complete fraudulent SOP (Standard Operating Procedure) manuals to streamline the scam.

OTC Fraud:
The Weakest Link in Crypto Transactions

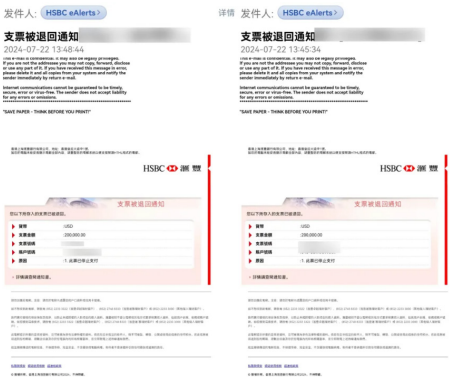
In certain countries and regions, over-the-counter (OTC) trading is the most common way for cryptocurrency investors to convert between fiat and crypto assets. OTC transactions can occur through centralized platforms, online groups, or even in person. However, regardless of the scenario, OTC trading always carries risks, including but not limited to losses of fiat or crypto funds, and in some cases, even personal safety threats. Below, we outline some of the most common OTC fraud tactics.

Exchange Merchant Fraud

For most ordinary investors, conducting C2C (Customer-to-Customer) trades with a merchant on a centralized exchange is the most common method for depositing or withdrawing funds. In such cases, the exchange acts as a guarantor, managing and overseeing C2C merchants on its platform and establishing a secure trading process.

The typical process is as follows: the seller deposits the tokens to be sold into the platform's custody. Once both parties confirm that the payment has been received, the platform releases the tokens to the buyer. Even with these security measures in place, there is still room for fraud. Consider the scenario of selling tokens to a merchant:

Fake Payment Records: The merchant might falsify payment records using technical means, such as modifying the information displayed on the payment tool, or even by creating a fake screenshot that shows the payment has been made. They then pressure the seller to quickly confirm the transaction. If the seller believes the merchant and releases the tokens without independently verifying the payment, they lose their funds.



Bad Check Fraud

Reversible Payment Methods: Another scam involves using reversible payment methods, such as bank checks. The buyer claims to have made the payment using a bank check, and the seller, believing the funds have been deposited, releases the tokens. However, the buyer then cancels the check, effectively reversing the payment and taking the tokens for free. This tactic often targets individuals in countries where bank checks are not a commonly used payment method, making it easy for victims to overlook the risk.

In-Person Trading Scams

A large number of OTC transactions take place in person. Some novice investors, believing that online trading carries a higher risk, have more faith in face-to-face interactions. This perception sometimes leads to extreme cases where individuals drive hundreds of kilometers to a specific location for a transaction.

Typical In-Person Scam Scenarios:

Fake Cash Payments: The scammer agrees to buy the victim's tokens and claims they will pay in cash. Upon receiving the tokens, the scammer hands over a bag that appears to contain the promised cash but is filled with counterfeit bills or even ceremonial "hell money" used in funerary rites.

Using a Decoy for Cash Payments: The scammer pretends to buy tokens using an online payment tool but sends an unsuspecting third party, hired via anonymous platforms, to act as the buyer in person. The victim, being cautious, may complete a series of smaller transactions successfully. However, once they become comfortable and transfer a larger sum of tokens, the scammer disappears, and the victim never receives the final payment. Attempting to detain the decoy and report the incident to the police is futile, as the decoy is unaware of the scam and the scammer will have erased all communication records by the time the fraud is discovered.

Cash Robbery: The scammer pretends to sell tokens at an attractive discount, requesting the victim to bring cash for the transaction. Upon arrival, the victim is ambushed by a group of assailants who rob them of their cash. This method is essentially a premeditated robbery disguised as a discounted token sale and can pose serious physical risks to the victim.

In-Person Multisignature Fraud

Earlier, we discussed how fake wallet apps can steal victims' seed phrases or private keys. Recently, a variation of this scheme has emerged, involving in-person multisig setups.

How the Scam Works: The scammer arranges to meet the buyer in person at a specified location. During the meeting, the scammer claimed that the buyer's current wallet address was compromised or that the wallet may have been infected with malware. They insist that the victim create a new blockchain wallet for the transaction or else refuse to complete the deal.

The victim, having already invested significant time and effort driving to the meeting location, usually agrees. While the victim is setting up the new wallet, the scammer covertly takes photos of the seed phrase from behind and sends it to an accomplice. Once the accomplice receives the seed phrase, they immediately set up a multisig configuration for the victim's wallet address.

The transaction then proceeds smoothly. The victim receives the agreed-upon tokens, and the scammer receives the payment, either in fiat or cryptocurrency. However, after the meeting, the victim discovers that they cannot make any transactions from the new wallet. The scammer, holding one of the multisig keys, has complete control over the address and can prevent any funds from leaving the wallet.

This scam is fundamentally similar to the fake wallet attack in that it prevents the victim from transferring their funds, leaving them helpless as the scammer eventually drains the wallet.

Security Recommendations for Navigating the Crypto Space

Don't Let Emotions Like Fear and Greed Control Your Decisions

The Web3 industry has a high entry barrier compared to other sectors. This barrier includes not only understanding complex technical principles but also the initial learning curve for using foundational infrastructure and accessing accurate information. Newcomers who underestimate these challenges and overestimate their abilities often find themselves falling into traps.

Emotional manipulation is a common tactic used by scammers. The fear of missing out (FOMO) or fear of losing funds can drive impulsive decisions that put your assets at risk. For instance, a common scam known as the "**Illegal USDT Check**" preys on users' fear of regulatory actions. Victims may have heard of illicit actors using cryptocurrencies for money laundering and know that law enforcement agencies track these funds. Out of fear, they click on a phishing link claiming to check whether their address is blacklisted. In the process, they inadvertently grant permissions to drain their wallet.

However, legitimate address risk assessment tools, such as KYA (Know Your Address) and KYT (Know Your Transaction), do not require users to connect their wallets; inputting the address alone is sufficient for analysis. This is a classic example of falling into traps due to fear and a lack of understanding.

For new investors, the safest approach is to operate within their comfort zone and make small, low-risk transactions to gain experience. Continuous learning and cautious experimentation can help minimize the impact of mistakes.

Don't Blindly Trust—Always Verify

Overconfidence is not the only source of loss—blindly trusting others can be just as harmful. Many investors fall victim by trusting seemingly legitimate sources, such as:

- Download links from search engines
- Airdrop links shared by influencers on social platforms
- Promises of profit from strangers who approach them online

While the forms of fraud may vary, the root cause is a lack of proper verification. If you maintain a list of authoritative Web3 data platforms, official social media accounts, and websites, you can cross-reference at least three different sources when downloading a wallet app or verifying a link's safety. If you cultivate good transactional habits, you will check a contract's history of interactions in your browser before confirming an important transaction, allowing you to detect anomalies in advance. If you join a group where everyone is bragging about their earnings and pushing you to participate, you should use KYA or KYT tools to investigate the addresses involved before rushing in.

By refusing to trust others lightly and continually validating information, you can ensure a safer crypto journey.

Most Crypto Scams are Variants of Traditional Scams

Just as most Web3 protocols are not fundamentally different from their traditional Internet counterparts, crypto scams are often just blockchain-adapted versions of old schemes.

To date, most crypto-related scams have direct parallels with traditional internet fraud. The only difference is that scammers have optimized these old tricks using blockchain technology or have merely shifted their target to crypto assets.

For example:

- Impersonation Scams: In the past, scammers would impersonate law enforcement and demand that victims transfer fiat to a bank account. Today, they require victims to buy cryptocurrency and send it to a specific address.

- Double Your Returns Scams: While most people are familiar with “double your money” schemes when the same tactic is packaged with blockchain technology and Elon Musk’s name, many people fail to recognize it and mistakenly believe it to be a technical innovation.

Studying traditional internet scams can greatly enhance your ability to identify and avoid crypto-related scams.

Sunk Costs Are Not Costs

Don't continue down the wrong path just to avoid wasting the costs you've already incurred. Most scammers exploit this psychological tendency.

For example, the **in-person multisig scam** mentioned earlier is a textbook case. The victim withdraws a large amount of cash from the bank and drives with a friend for several hours to reach the meeting place. Everything seems to be in order, but the scammer suddenly insists that the victim create a new wallet, claiming that the old one is unsafe. Despite the suspicious circumstances, the victim decides to comply rather than turn back, not wanting to waste all the effort invested in the journey.

Similarly, in r**omance scams (also known as Pig Butchering Scams)**, victims often continue to invest more money even when they begin to suspect foul play. Scammers exploit the victims’ desire to recover their initial investment, using excuses like “taxes” or “liquidity requirements” to demand additional payments, eventually draining all of the victim’s funds.

Remember, sunk costs are not costs. When faced with a situation that you believe could be a scam, it is often better to walk away and cut your losses rather than let past investments influence your future decisions.

What to Do After Falling Victim to a Crypto Scam

The most critical step to recovering losses after falling victim to a crypto scam is to seek help from law enforcement. Therefore, all actions taken after recognizing a scam should be geared toward gathering evidence to support a formal investigation.

Mitigate Losses Immediately

If you notice a loss of assets, acting quickly can help contain further damage. The necessary steps will depend on the specific type of scam:

- If Your Seed Phrase is Compromised: Quickly transfer any remaining assets to a secure address. This includes not just other tokens or NFTs on the same blockchain, but also assets in other blockchain addresses derived from the same seed phrase or addresses stored on the same device.
- If You've Been Scammed Through an Investment Scheme: Stop any further contributions immediately, and withdraw any remaining funds if possible.
- If You've Granted a Malicious Authorization: Revoke all suspicious permissions for your addresses as quickly as possible.

However, while taking these countermeasures, ensure that you adhere to the security principles mentioned earlier. Avoid falling into additional traps in the process.

Preserve the Crime Scene and Report the Incident

A common reaction for many people after realizing they've been scammed or hacked is to delete the compromised wallet, uninstall the fraudulent app, block the scammer's communication, or even factory reset their device. Such extreme actions are counterproductive and can hinder the recovery process in the following ways:

- Deleting Wallet Apps: If the wallet was a fraudulent app, deleting it could prevent security companies from verifying its legitimacy.
- Erasing Fraudulent App Files: The app files may contain valuable clues that could assist in the investigation.

- Tampering with Evidence: Altering or deleting evidence complicates the process of case filing and gathering critical information for law enforcement.

When mitigating losses, victims must focus on preserving the crime scene. Keeping all evidence intact will aid in future investigations.

Seek Assistance from Relevant Parties

Relevant parties include platforms associated with the stolen assets and security firms that offer investigation services.

Contact Platforms Where the Stolen Assets Were Sent: If you discover that your stolen assets are being transferred to a centralized exchange, immediately contact the exchange's customer support and request that they freeze the deposit address. If you provide clear and convincing evidence, most platforms will initiate a temporary security freeze (typically for 2-7 days) on the account, during which the funds cannot be moved. During this period, you should request that law enforcement agencies formally communicate with the exchange to support the investigation.

Engage Professional Blockchain Security Firms: If you or your associates lack the expertise to track on-chain funds, consider seeking help from professional blockchain security firms or data analytics companies (such as Bitrace) to help you identify the cause and flow of stolen assets, and even provide support during the investigation.

However, avoid seeking help from random individuals online. Most internet advice is just noise and won't help you recover your assets. Additionally, some scammers masquerade as digital asset recovery experts, "official customer support" representatives, or platform officials, making the situation even more dangerous.

Final Thoughts

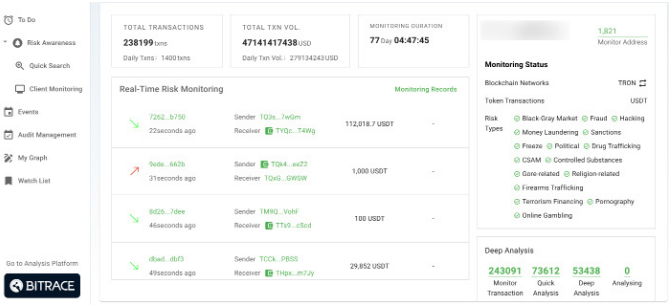
In this handbook, we began by outlining various types of scams that a typical newcomer might encounter at different stages of their investment journey. We then delved into the underlying mechanics and preventive measures for each category of fraud and concluded by listing strategies for recovering losses after falling victim to a scam. The goal is to expose common and highly damaging scams to prevent ordinary investors from suffering avoidable losses.

If you or someone you know has unfortunately fallen victim to a crypto scam, feel free to reach out to Bitrace. We are committed to offering basic analytical assistance to help victims understand what happened and support their next steps.

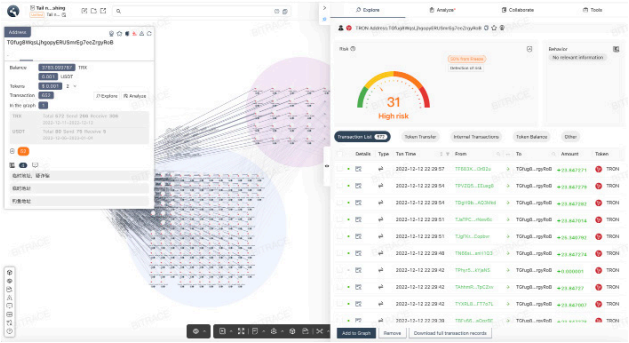
Users with a need for cryptocurrency fund risk detection are also welcome to use our products to better achieve risk identification and prevention.

For individuals, you can visit https://detrust.bitrace.io/detrust-blacklist/ and use the free KYA tool launched by the Bitrace team to quickly check whether the counterparty's address carries any risks. Based on the address's risk score, you can decide whether to engage in financial interactions with them.

For institutions with a high frequency of transactions (such as exchanges, payment platforms, OTC dealers, etc.), the enterprise version of the Detrust on-chain risk fund monitoring management platform can be used to monitor all transactions of the platform's business addresses comprehensively. When risk transactions occur — including risky funds flowing in or out to risky addresses — risk control personnel will receive real-time alerts via email, community bots, and other channels, allowing them to promptly handle ongoing or upcoming user risk activities.



For teams or law enforcement agencies with a need for crypto fund tracking and analysis, Bitrace Pro offers powerful features such as visual analysis, entity identification, address clustering, multi-party collaboration, intelligent monitoring alerts, and more. These tools help you quickly understand criminal patterns, trace fund flows, identify anomalies, and uncover new leads, enabling faster and more accurate investigations.



Feel free to contact us at any time to request a product demo.

About Bitrace

Bitrace is a Regtech company specializing in cryptocurrency risk data analysis. We are dedicated to utilizing AI and big data technologies to more accurately and efficiently identify, monitor, and investigate risks and criminal activities on the blockchain. Our mission is to provide customers with leading regulatory, compliance, and investigative tools and services.

We have collaborated and interfaced with LEs and Web3 enterprises in multiple countries, completing 1000+ case services, monitoring 700B+ USD in risk/criminal funds, and successfully recovering 1B+ USD in losses.

Website: bitrace.io
EMail: support@bitrace.io
X(Twitter): @Bitrace_team
LinkedIn: @Bitrace Tech

Disclaimer

This handbook is provided solely for public education and awareness. It is a nonprofit initiative designed to help individuals understand and prevent cryptocurrency fraud. The information presented is not intended as legal, financial, or professional advice. While every effort has been made to ensure accuracy, the authors and publishers make no warranties regarding the completeness or reliability of the content. Bitrace and its affiliates assume no responsibility for any losses or damages arising from the use of this handbook. If you have any questions, feel free to contact us. Readers are advised to seek professional advice tailored to their specific situations.