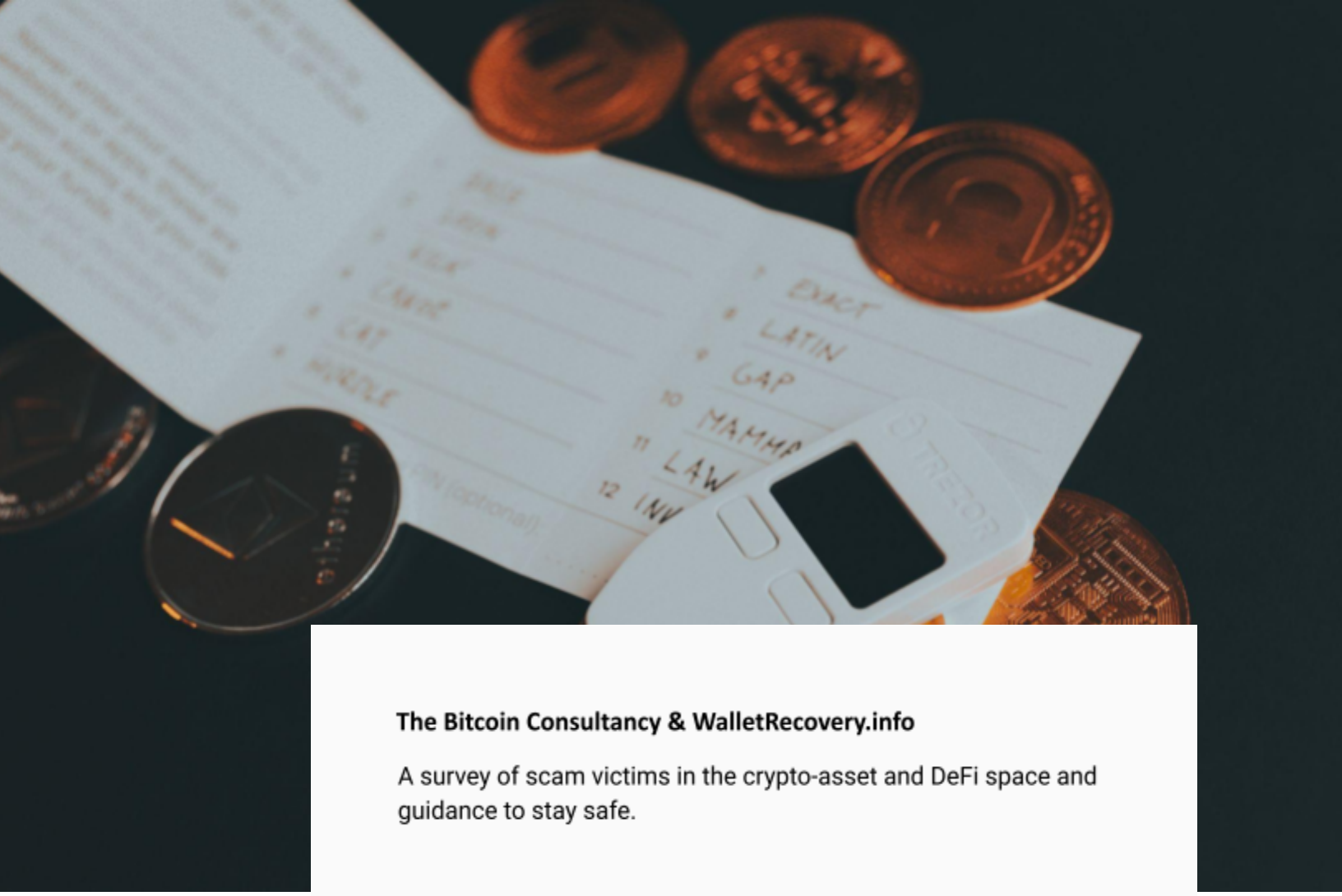


The Bitcoin Consultancy & WalletRecovery.info

A survey of scam victims in the crypto-asset and DeFi space and guidance to stay safe.

2021 Survey of Crypto and Defi Scams

Prepared by

David Veksler

david@thebitcoinconsultancy.com

December 29, 2021

The Bitcoin Consultancy

Introduction

2021 has been another bull market for cryptocurrencies. Unsurprisingly, billions of dollars flowing into an unregulated market have attracted plenty of scammers too.

Besides the risks of theft from platforms and crypto wallets, 2021 has seen a rise in DeFi scams and theft events. While DeFi (theoretically) provides protection against some risks, it also introduces new and complex risks, and we've seen hundreds of millions stolen from DeFi platforms in 2021. 71% of major hacks in 2021 were on DeFi platforms.

This report is based on a survey of about 2500 users of walletrecovery.info, which has helped thousands of customers recover their cryptocurrency wallets since 2017. While we cannot help victims of crypto scams recover their funds, we want to share our findings to improve awareness of common scams in this space and provide guidance for the security of crypto assets.

Key Findings:

- Fake investment platforms were the most common scam (32%), with Bitcoin the most common asset stolen (66%).
- Fake platforms and scammers employ sophisticated techniques like stealing identities of legitimate financial professionals, catfishing romance scams, and elaborate fake trading and gambling platforms.
- 57% of victims filed a report with law enforcement, but 69% did not get a personal response, and only 8% felt that law enforcement took their case seriously. None got their crypto assets back.
- 60% of victims blame insufficient education for falling for the scam, 19% blame their poor security practices, and 7% blame a crypto service provider.
- Only about 10% of victims thought that crypto institutions were doing a good job of educating customers about scams.
- Common signs of scams: unrealistic returns, high-pressure tactics, sales pitches via Telegram, no mention of fees, & lack of reputation.
- Fake "scam recovery" services abound and are sophisticated as well, using complex techniques such as sending stolen funds from other victims to collect their "fee" before the bank transfer bounces.

Contents:

The Top 5 Most Common Scams in Crypto

Here are the six most common scams, as reported by study participants:

1: Fake Investment Platform

A fake platform (32% of scams) is a fake trading service that takes your money with the promise of high returns from “trading.” However, it’s impossible to withdraw your “profits.” In 2021, scammers have been concentrating on dating websites, social media, and Telegram groups. Varieties include airdrop schemes, romance scams, pump and dumps, and counterfeit tokens platforms.

2: Phishing and Fake Wallet Validation

Phishing services impersonate a legitimate platform to steal wallet seeds or login credentials. Varieties include wallet “validation” services, “airdrop” scams, coin “forking” services, and dusting attacks. Recent phishing attacks involve stealing identity documents and hijacking phone numbers to gain access to cryptocurrency exchange accounts.

3: Exit Scam/Rug Pull

Exit scam: a project sells a coin in an ICO, but instead of using the funds to build a project, the promoters take the money and disappear

Rug Pull: a DeFi scam where a coin is released and promoted, then all the value is stolen from the liquidity pool.

4: Scam Coins

Projects that don’t have a legitimate business model and whose promoters simply try to collect as much money as possible without delivering anything of value. By far the most common scam in terms of economic value. Of course, the team behind all coins will claim that their coin is legitimate, but an objective analysis shows no economic value behind these projects.

5: Counterfeit Tokens

A counterfeit token is a DeFi scam in which a worthless token impersonates a real token. Smart contract chains allow anyone to create a token without any restriction on the name, so scammers impersonate real tokens with fake tokens and sell them on both fake and legitimate DeFi platforms. The victim does not discover the fraud until they try to sell their token and realize the knockoff is worthless.

The Four Most Common Defi Exploits

Whereas the previous category covered scams, these scams or hacks are the most common ways users lose their funds on DeFi platforms. This data is based on CryptoSec's survey of 75 DeFi exploits.

1: Rug Pulls

A coin is released and promoted, then the project team drains all the assets from the liquidity pool. According to Chainanalysis, DeFi rug pulls stole $2.8 billion in 2021.

2: Liquidity Pool Drains

A liquidity pool is drained by someone other than the project team. Usually, this is done by finding an exploit or unlimited arbitrage opportunity in the smart contract. For example, a hacker exploited a complex transaction involving 68 different assets to steal $260 million.

3: Front-end Exploits

An exploit not of a smart contract but of the website hosting the DeFi platform. BadgerDAO users lost $120 million when the hackers injected malicious code that granted them access to users' wallets into BadgerDAO's application platform.

4: Bank Run on Peg

Synthetic stablecoins are vulnerable to a bank run that leaves them worthless. Usually, this is due to their tokenomics being fundamentally unsound. For example, the crash of Iron Finance's Titan Stablecoin saw the stablecoin fall from a market cap of over $2 billion to zero.

Why Are There So Many Scams In Crypto?

For every crypto scheme which is outright theft, there are ten trash crypto-assets created mainly to take your money and run. Each project has a story of why they are a great investment. But dig deeper and the business model is a mirage. What the founders really want to do is create as much momentum as possible and sell at the top before the illusion of value vanishes.

Sometimes you don't have to dig very deep. For example, "BabyCake" is an explicit Ponzi scheme, if you look beyond their promises of "bringing passive income into people's lives." It's one of the first tokens to have a Ponzi scheme built right into the smart contract. I count 63 other "baby" named pyramid schemes.

Usually, though, the catch is buried deeper and requires understanding the crypto ecosystem. Let's review why there are so many scams and trash coins in crypto and how to avoid them.

Why are there so many crypto scams?

Anonymity

Cryptocurrencies are only pseudo-anonymous. It's impossible to know who owns some coins from an address alone. But if you interact with the legacy financial system, for example, by cashing out your gains for fiat, your identity can sometimes be found. If you commingle your funds by moving them together, it's possible for a chainanalysis algorithm to link activity to an identity. When I try to help victims of fraud, I can often follow the transaction trail to the cold-wallet of some exchange where the crooks traded Bitcoin for a local currency.

The bigger problem is that our legal systems aren't adapted to deal with crypto fraud. Our legal institutions don't take small-scale crypto fraud as seriously as fraud with "real" money. Lack of international cooperation means that even if I know which exchange was used to cash out stolen crypto loot, they are unlikely to cooperate with local law enforcement.

Bleeding Edge Technology

Bitcoin and cryptocurrencies are still very new. The tools needed to secure Bitcoins are still evolving and rough around the edges. I predict that in a few years, we will carry credit-card-sized devices with biometric readers that make storing and using Bitcoin both safe and foolproof. Until then, the tools for storing and transacting cryptocurrencies are rapidly evolving. There are safe methods to keeping your crypto safe (like hardware wallets, multi-sig,

and steel seed backups), but many people aren't aware of the proper techniques. Accidental and malicious loss of funds is, unfortunately still common.

Transaction Finality

A bigger reason for fraud in crypto is that crypto transactions are irreversible for almost all coins. In the legacy financial system, a fraudulent credit card charge, bad check, or unauthorized wire transfer can usually be reversed. If the theft is big enough and your lawyers are good, the legal system will tend to intervene on the victim's side. In the crypto space, however, no matter how unjust the theft, there is nothing that can be done.

(Keep in mind though that government theft of savings through inflation and taxes is a far bigger problem than theft of crypto. While this is unfortunate for victims of theft, transaction finality is one of the primary reasons why Bitcoin is so revolutionary: it is impossible to conduct legal plunder of people's wealth.)

A Free-Market Alternative to Wall Street

"Wall Street" (i.e. traditional securities markets) is often portrayed as the epitome of capitalism. The reality is that the government has regulated most of the profits out of securities available to the non-elite. Crypto-assets and exchanges allow novice investors access to venture capitalism for the first time since the Securities Act of 1933 limited investments in unregistered securities to "accredited" investors. Initial Coin Offerings offer normal people the ability to invest in startups without having to be worth or put up millions of dollars. DeFi (decentralized finance) exchanges operate using smart contracts, without any centralized entity to regulate. With DeFi, anyone to mint and create a market for a new token, outside the ability of any government to regulate.

The flip side is that just because everyone can create and sell their token does not mean they have a viable business model or any technical skills. All you need to be able to do is market your coin, not do anything useful with it. The vast majority of crypto projects trend back to a value of zero.

Bitcoin's Success Inspires Copycats

Most crypto scams are *not* outright theft but an attempt to make a quick buck by riding on Bitcoin's coattails. Profiting from Bitcoin's rise requires an initial buy-in and patience. Want to make billions with an investment of zero? Too impatient for a mere doubling of your money each year? Just copy Bitcoin's code, change a few parameters (invent some justification why they are needed) and launch your own altcoin. Repeat the scheme a few more times and get 12,881 crypto-assets tracked by CoinMarketCap.

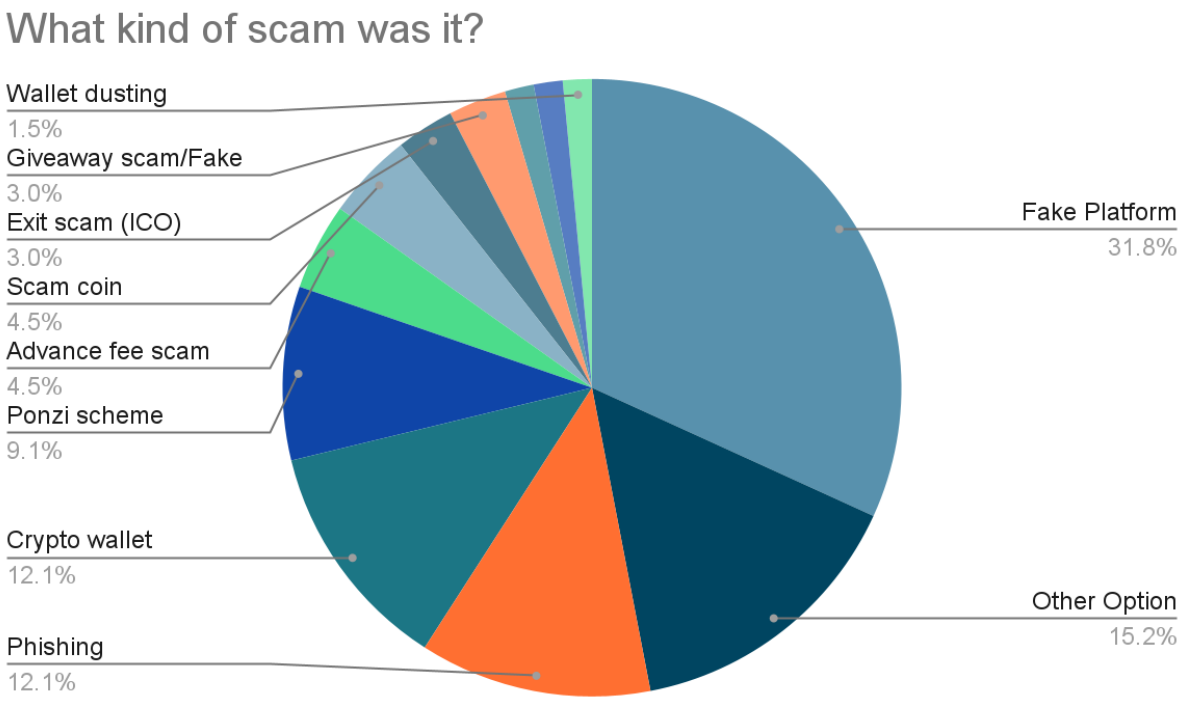
Many projects start out well-intentioned. The founders may want to be revolutionaries just like Satoshi Nakamoto or they might have some justifiable disagreements with the team that maintains Bitcoin. However, the decentralized nature of crypto assets means that once a coin is out there, speculators will run with it. Quite often, the founder exits early with a small fortune and the project evolves in a completely different direction. The founder of Dogecoin sold everything to buy a used Honda Civic. His coin now has a $32 billion market cap.

Today, the crypto-asset market has a market cap of $2.5 trillion, 48% of which is Bitcoin. Many beginner crypto investors are branching out into altcoins hoping to see the same astronomic returns as Bitcoin in the early days.

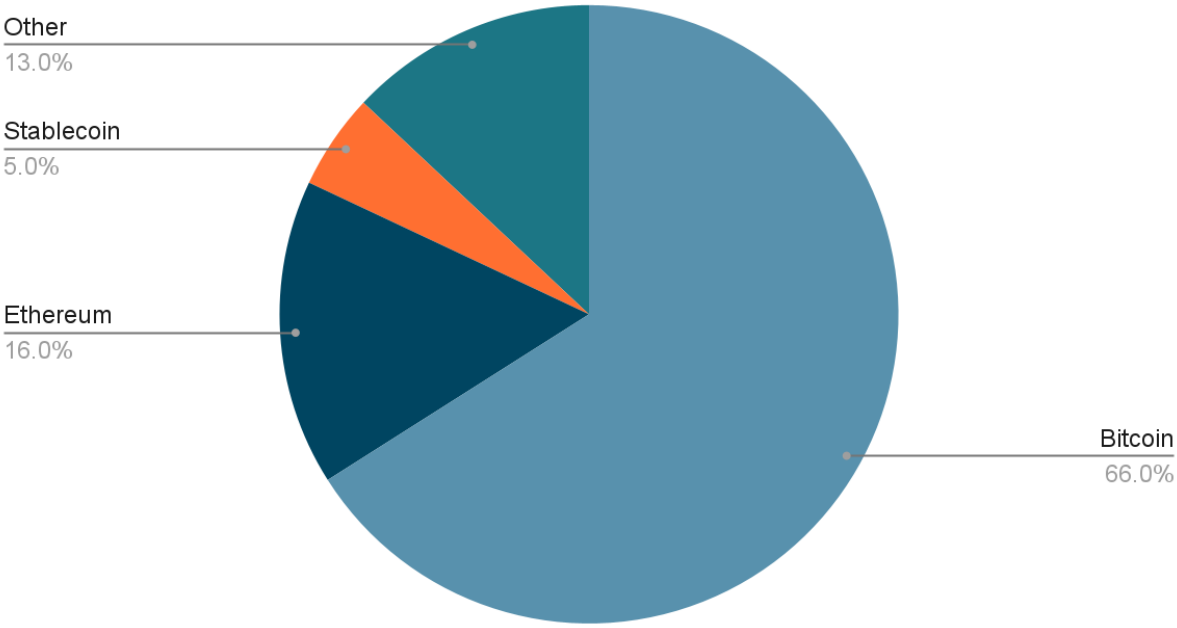
Crypto Scam Victims Survey

The “Cryptocurrency & Defi Scams - 2021 Survey” surveyed 2,500 users of walletrecovery.info to compile this report:

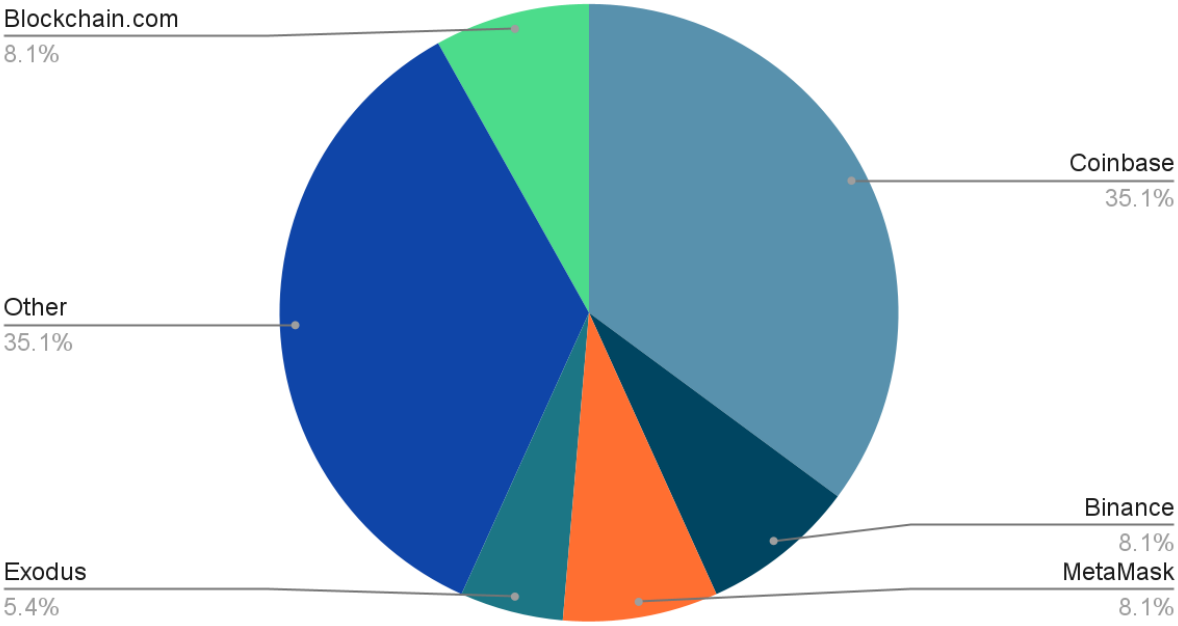
By far the most common scam was the fake investment platform. (See “Appendix: Common Cryptocurrency/Defi Scams” for definitions.)



Which cryptocurrency was targeted by this scam?

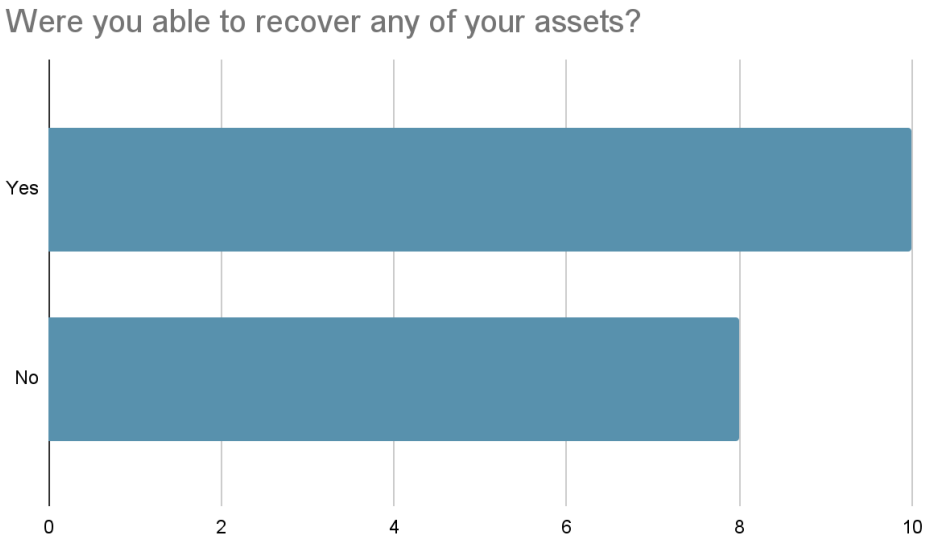


Which wallet or exchange were you using?



Amounts Lost:

- Mean: USD $32,133
- Median: USD $6,000



Note: We believe the actual rate of stolen crypto-asset recovery is zero. "Recovered" assets include reversed bank transfers (when tokens have not yet been withdrawn) and fake recovery services that send victims a small portion of what they lose to justify a larger recovery fee.

- Coinbase, Blockchain.com, Binance, and MetaMask are the most common platforms scammers target.

Recent phishing techniques are highly complex. Thieves have realized that copies of identity documents are a "backdoor" to loot their Coinbase accounts.

Crooks have figured out that copies of ID documents can eventually bypass passwords and all other security measures. Facial recognition is much easier to fool than publicly known. SIM swapping is still common, as cell services do not take security seriously.

Did you file a report with a law enforcement authority?

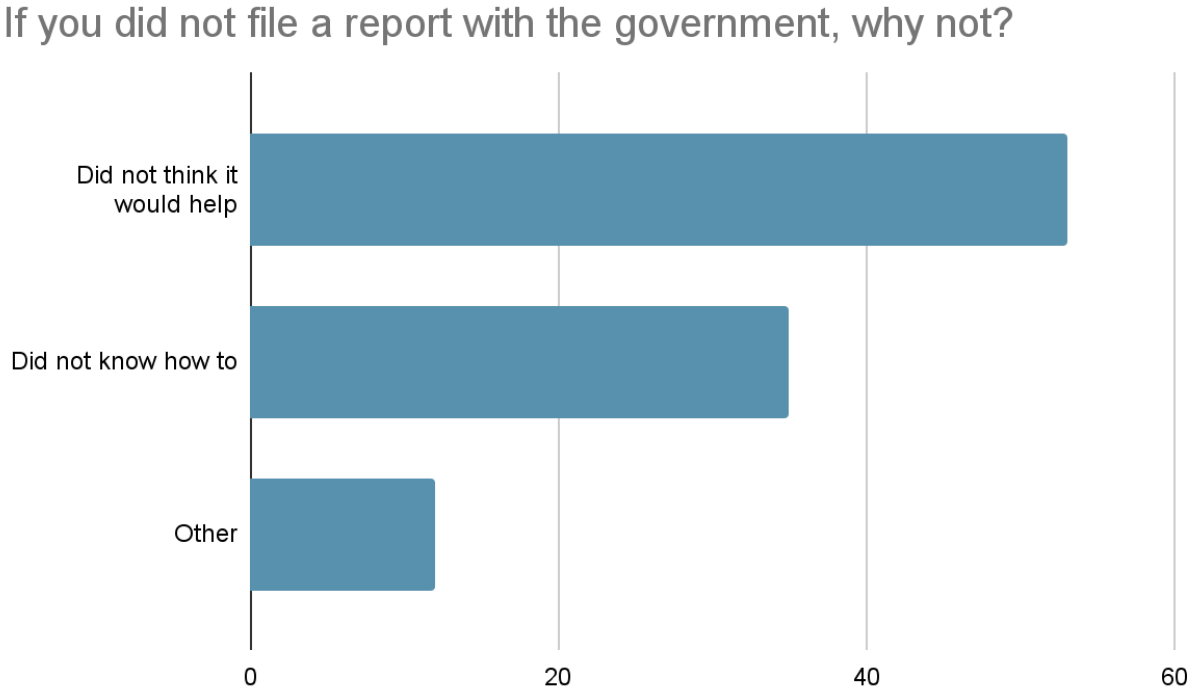
Yes: 57%
No: 43%

If you filed a report, did you receive any response specific to your situation?

No: 69%
Yes: 31%

If you filed a report, do you feel like the authorities took your case seriously?

No: 92%
Yes: 8%



Did you hire (for a fee) a private organization to help you with the scam?

No: 72%

Yes: 28%

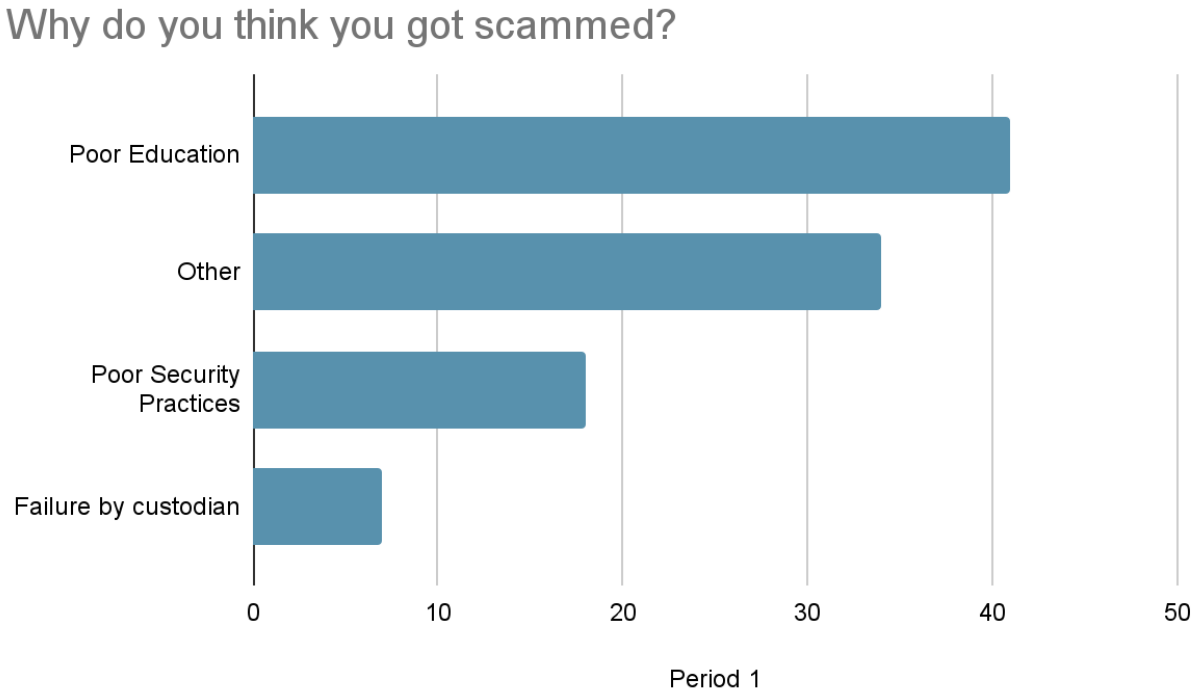
Are you less likely to invest in crypto after your experience?

	MUCH LESS LIKELY	SOMEWHAT LESS LIKELY	NO CHANGE	SOMEWHAT MORE LIKELY	MUCH MORE LIKELY	AVERAGE
Rating	8	6	13	0	2	2.38

Have you made any new crypto investments since being targeted by a scam?

No: 70%

Yes: 30%



On a scale of 1-5, with 5 being best, do you think crypto institutions are doing a good job of educating customers about scams?

	1	2	3	4	5	AVERAGE
Rating	12	5	**14**	3	1	2.31

On a scale of 1-5, with 5 being most prepared, how prepared do you consider yourself to avoid future scams?

	1	2	3	4	5	AVERAGE
Rating	0	0	10	12	**13**	4.09

What are the most important signs that you're dealing with a scammer?
(Selected Answers)

- Unrealistically high returns
- Payment to withdraw funds

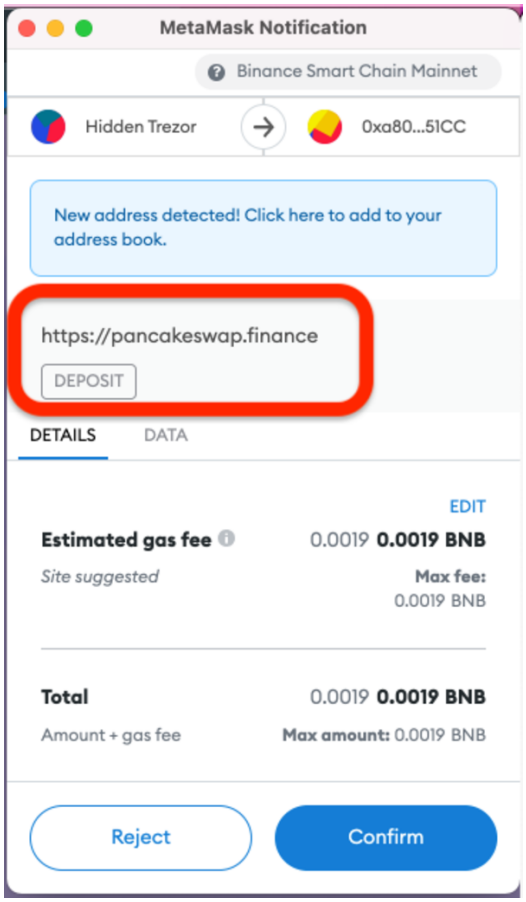
- Communicates by text only
- Asks for payment in gift cards
- Offers to good to be true
- No reputations
- Fees too low or never mentioned
- Poor English

Five Practices to Avoid DeFi Platform Hacks

1: Always Review The Transaction Details

Below, you can see a sample MetaMask transaction confirmation dialog.

Always review these transaction details to confirm the action is what you expected.
Here is a confirmation dialog:

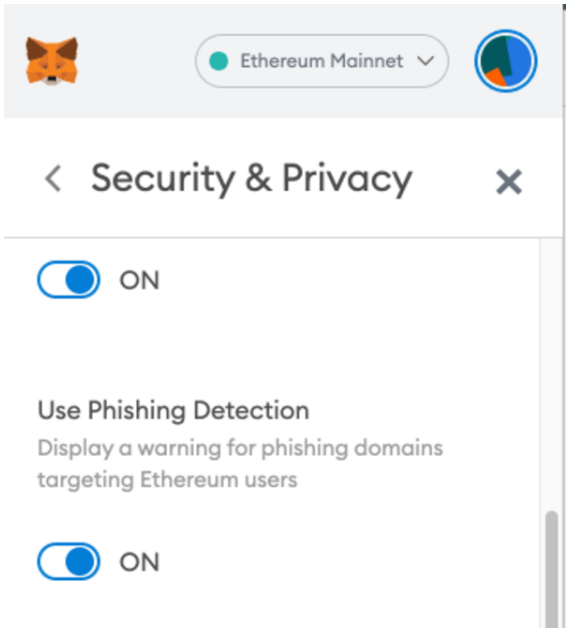


Note that this confirmation is on the Binance Smart Chain, the action is DEPOSIT, and the total amount is .0019 BNB.

Always review the chain, the action, and the amount.

Remember that Defi is just smart contract code, and you can always see the method being executed and the parameters passed to those methods.

2: Use the MetaMask Blacklist



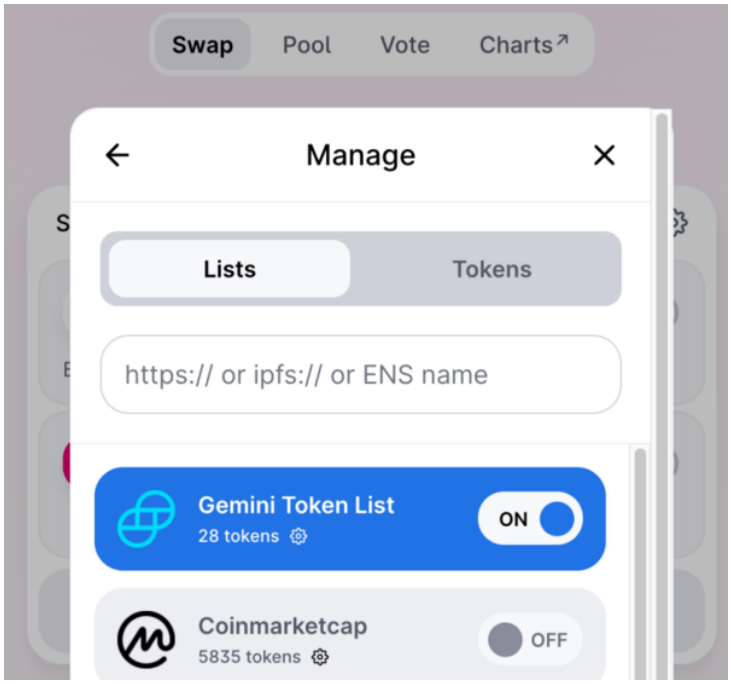
You may not use MetaMask for DeFi. Even if you don't, you should install the extension because it has a built-in phishing blacklist. This blacklist protects against many scams, such as malicious Bitcoin paper wallet sites – not just Ethereum scams.

3: Use a Hardware Wallet with DeFi

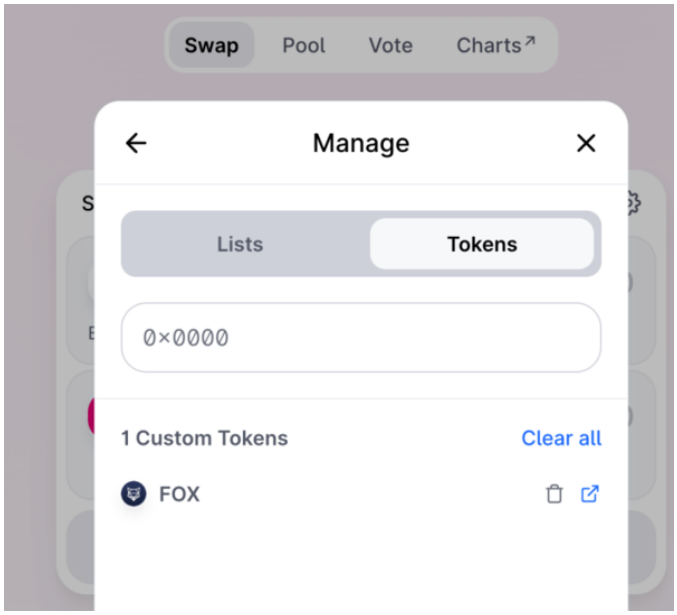
Don't use a browser extension like Metamask to store large sums of money. You can use a Trezor or Ledger wallet with Metamask for DeFi.
Remember that all the software on your computer may have access to your MetaMask keys.
If you reuse your Metamask password, it's trivial to steal your keys.

4: Check the Contract ID on CoinMarketCap

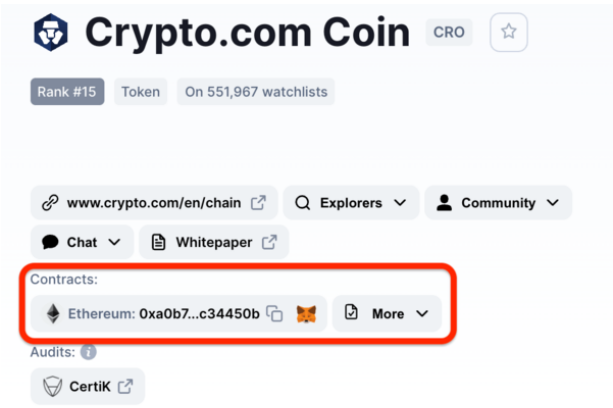
Anyone can create a token on ETH/BSC/AVAX. A common scam is counterfeit copies of real coins.
On Uniswap, you can use the default token list:



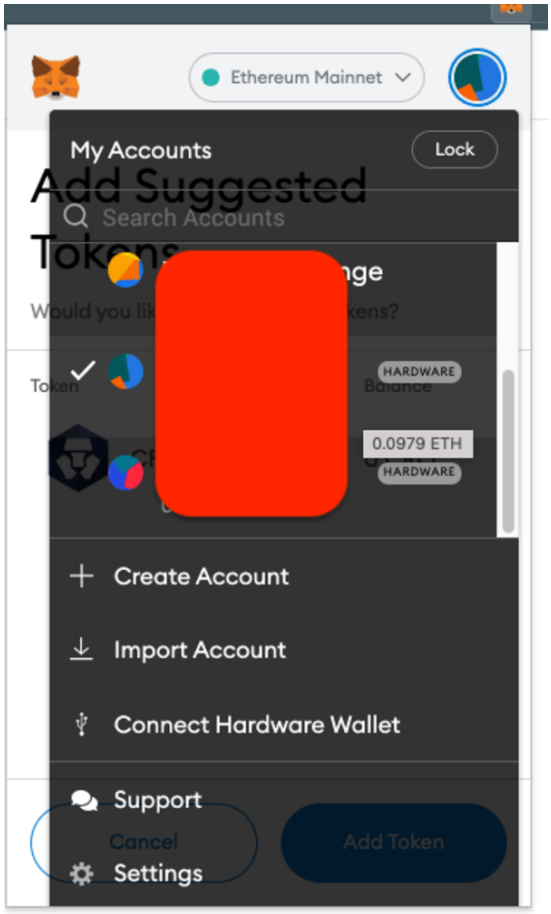
Or specify custom tokens:



Malicious exchanges and token sites may prompt you to add fake contracts to Uniswap or other Dex's.
Be aware that you can name a token anything you want on ETH/BSC/AVAX and other chains.
Double-check that you're buying a real token by checking on https://coinmarketcap.com/
Click the MetaMask icon to add the contract to MetaMask.



5: Separate Trading Wallets from Cold Storage Wallets



If you plan to leave a lot of crypto in cold storage and use a fraction for trading, consider setting up a separate passphrase wallet just for DeFi. This limits your exposure in case of hacks.
In the BadgerDAO hack, a single wBTC address was emptied of 896 Bitcoin. I'm guessing that not all 896 BTC were intended to be used with BadgerDAO. The owner of those coins probably used a shared wallet for multiple platforms. If they limited their balance of the wallet to those intended to BadgerDAO, they could have minimized the loss.

MetaMask makes it easy to switch between different hidden wallets:

Guidance For Crypto Asset Platforms

1: Enable And Encourage Customers To Self-Custody Their Crypto Assets

Crypto thieves are developing expertise in exploiting the security protecting customer accounts. They have discovered that copies of identity documents can eventually be used to bypass almost any security measure. Furthermore, SIM-swapping is still very common and breaks most two-factor authentication schemes. Most retail-oriented financial platforms do not have the resources for extensive transaction verification measures like video calls. This means that all assets stored in non-custodial wallets are at risk. We, therefore, encourage platforms offering crypto services to enable and encourage customers to withdraw crypto assets to non-custodial (self-hosted) wallets, which are not vulnerable to account exploits.

2: Require Multifactor Authentication

Credentials comprising a username, password, and email are extremely vulnerable to compromise. Modern security practices involve three or more credentials: for example, password, email, and TOTP time-based token. Authentication should never rely solely on SMS messages, as they are highly vulnerable to sim-swapping.

One of the easiest multi-factor strategies is using a hardware FIDO2 token (like a Yubikey). It's unfortunate that most platforms still do not support it.

3: Encourage Or Require Whitelists With Cool-Down Periods

Given the reality that all online account credentials can be circumvented with enough effort, a novel approach used by some platforms is cool-down periods. First, the app asks users to white-list pre-registered withdrawal addresses. Making a transfer to any address not specified in the whitelist triggered a cool-down period during which the customer is modified and has a chance to reject the transfer. Platforms like Celsius Networks and Nexo that are focused on long-term storage have implemented variations of this feature. Any platform focused on long-term custody of crypto should offer or require something similar.

4: React Quickly To Customer Feedback To Detect And Respond To Attacks

Today's cryptocurrency theft attempts are highly organized. Criminal organizations look for social engineering heuristics they can exploit at specific platforms, then run them at scale.

Platforms that provide crypto services need to react quickly when they become targets of such attacks.

For example, our customers have reported it is possible to reset many credentials with just an email and copies of a driver's license. Criminal networks are now conducting mass phishing campaigns using social media and paid ads to collect documents. Criminals are exploiting this vulnerability in bulk at certain platforms. These platforms need to conduct regular reviews of customer support requests to identify such patterns and improve customer messaging and security measures.

Unfortunately, most customer service pipelines are highly scripted and not focused on identifying and mitigating new social engineering and phishing exploits.

5: Label Networks And Use The Latest Address Formats

Both Bitcoin and Ethereum now have many forks and clones using the same address format. For example, Bitcoin vs Bitcoin Cash or Ethereum vs Binance Smart Chain. Either accidentally or maliciously, most platforms fail to protect their users against cross-chain confusion. Some users are purchasing Bitcoin Cash thinking it is Bitcoin, while others send their Avalanche or Binance tokens to Ethereum addresses. To prevent accidental or malicious cross-chain activity, platforms need to label what chain they accept transactions on and on what chain transactions will be sent on when facilitating transfers. Additionally, in the case of Bitcoin forks, platforms should switch to the new native address format to prevent cross-chain deposits.

Conclusion: Five Principles To Keep Your Crypto Safe in 2022

1: Avoid Get Rich Quick Schemes

As reported by victims of scams, fraudulent schemes have a few things in common: unrealistic returns, high-pressure tactics, sales pitches via messaging platforms like Telegram, no mention of fees, & lack of reputation.

Legitimate platforms clearly state what they do with customer funds, their fee schedule, and expected returns. Centralized (custodial) platforms should be licensed with a regulatory body such as FINRA. Scammers are impersonating licensed financial professionals, so it is necessary to independently verify their contact information via FINRA BrokerCheck, LinkedIn, etc.

In DeFi, services like RugDoc rate the legitimacy of financial platforms. Social media platforms like Reddit are useful for reviews, whereas Telegram and online review sites should not be trusted, as they are easy to populate with fake reviews.

2: Store Your Cryptocurrency On A Hardware Wallet

A hardware wallet is unquestionably the best way to store Bitcoin and cryptocurrencies. Most victims of scams lose funds by letting someone else custody their assets or granting scammers access to their accounts. Self-custody on an offline hardware wallet is the single best way to prevent this.

3: Independently Verify Identity of Crypto Websites

Most credential phishing and identity theft happen when criminals impersonate either the applications of crypto services or their support services. Users must learn to always access crypto services through their official website and never trust “support” links found through search engines or social media.

4: Use Multi-Factor Authentication

Credentials comprising a username, password, and email are extremely vulnerable to compromise. Use a TOTP time-based two-factor code or a hardware-based FIDO2 token such as Yubikey.

5: Educate Yourself About Crypto Fundamentals

Education is key to avoiding becoming a victim. Learn about the legitimate investment opportunities in crypto (mining, lending, staking, yield farming, etc) so you can meaningfully analyze the offers you come across. Read reviews of legitimate crypto wallets and related services to avoid falling for fakes. Most importantly, do not invest money in projects whose business model you do not understand.

Appendix: Common Cryptocurrency/Defi Scams

- **Fake investment platform/honeypot**: a fake trading service that takes your money with the promise of high returns from "trading." However, it's impossible to withdraw your "profits."
- **Phishing**: a service that collects your logins and/or personal information, then uses that to steal your money
- **Advance-fee scam**: a platform promises to return a multiple of whatever you invested, but disappears
- **Celebrity impersonation**: a variety of advance-fee scam where the scammer pretends to be a celebrity
- **Rug pull**: a DeFi scam where a coin is released, and promoted, then all the value is stolen from the liquidity pool
- **Exit scam**: a project sells a coin in an ICO, but instead of using the funds to build a project, the promoters take the money and disappear
- **Ponzi scheme**: project promises high returns, then pays investors with funds from new deposits
- **Crypto wallet "validation"**: a type of phishing attack that impersonates a real wallet and asks for your seed words.
- **Counterfeit coin**: a Defi scam where promoters sell a fake and worthless copy of a real coin.
- **Wallet dusting**: scammers airdrop a token with a URL in the name of your wallet. When you visit the URL, it tries to steal your money
- **Giveaway scam/fake airdrop**: to claim "free" coins you must turn over credentials that allow scammers to steal your coins.
- **Scam coins**: A catch-all category for projects that don't have a legitimate business model and whose promoters simply try to collect as much money as possible without delivering anything of value.

David Veksler
thebitcoinconsultancy.com
david@thebitcoinconsultancy.com
214-659-1775