Resources

Table of Contents:

How to Avoid Getting Scammed in the Crypto World

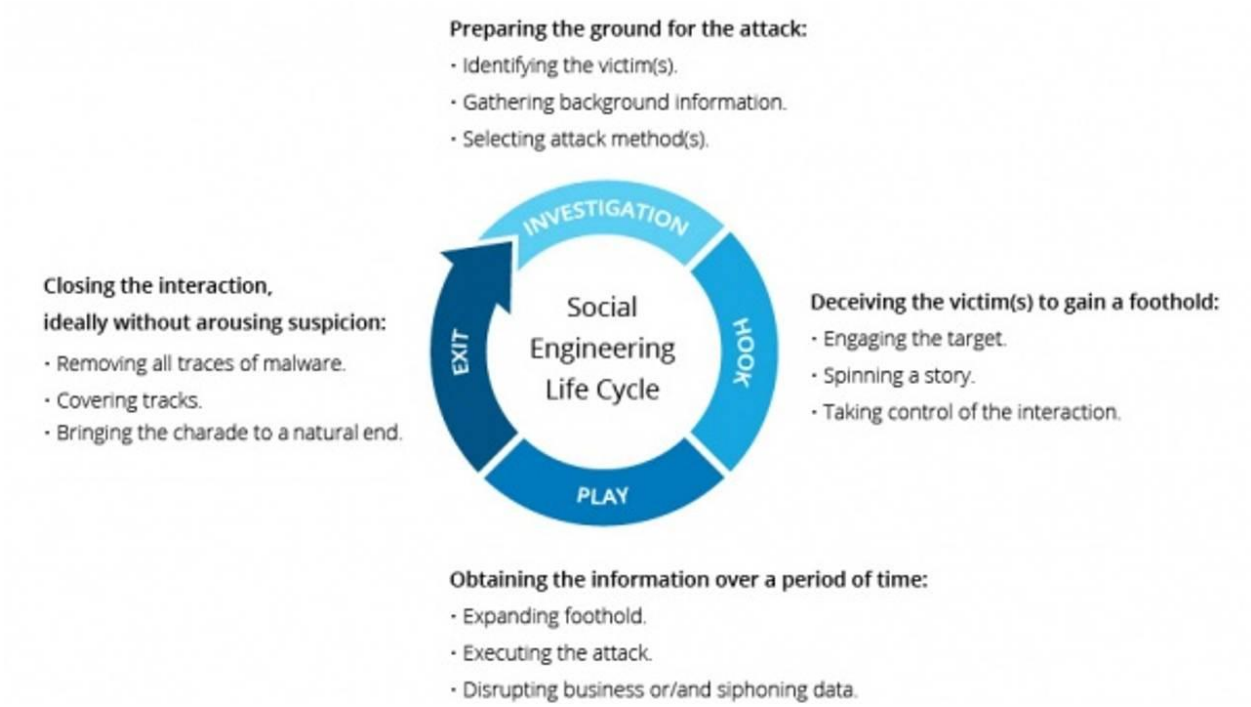
Introduction

So, you've got some crypto but you're not sure what's next? Well, your first job would be to keep it away from scammers and thieves. Just like physical money, there's all manner of people who'd like to get their hands on your crypto. I know what you're thinking –

"How am I supposed to be able to tell if it's a scam or if it's real?"

There are a number of methods which are topical of scammers. Here are some of the most common ways they operate.

Social Engineering Attacks



Social engineering uses human interaction to achieve malicious activity. It uses psychological manipulation techniques to acquire and/or trick you into making mistakes and giving away information that can be used to access your information or even to gain direct access to your account.

They can range from not-very-sophisticated to very sophisticated. Stick with us and read below to make sure you don’t get scammed!

These five techniques are the most common methods of digital social engineering attacks. In the following scenarios, you are the target!

Baiting

As it's name implies, baiting attacks use a false promise to gain a target's curiosity or exploit their desires. An example of one of these desires would be the false promise of easy money. They lure a target into a trap that steals their personal information or infects their systems with malware to steal their information indirectly.

The most reviled form of baiting uses physical media, such as malware-infected flash drives, to disperse malware. These are often left in areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted building or company). The bait has an authentic look to it, such as a label presenting it as important or sensitive information, or even something fun or appealing, like a free trial for a streaming service, for example.

The target picks up the bait (malware-infected flash drive) out of curiosity and inserts it into a work or home computer, resulting in automatic malware installation on the system. Inserting the flash drive into the computer is all that is needed to infect the system automatically with malware. In the past, a target would have had to open a specific file but those days are long gone, unfortunately!

Baiting scams don't rely solely on physical means such as these malware-infected flash drives. Increasingly, online forms of baiting consist of enticing ads, web links to make quick money, and other such psychological manipulations that lead to malicious sites or that encourage users to download a malware-infected application.

Scareware

Scareware is exactly like it sounds. It involves targets being bombarded with false alarms, fictitious threats, or playing on a target's fear of the unknown. Users are deceived to think their system is no longer secure, is infected with malware, or that even that their "*system security is at risk from hackers". This* prompts the target to install software that has no real benefit (other than for the attacker) or is malware itself. Scareware is also referred to as deception software, rogue scanner software and fraudware.

A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, *"Your computer may be infected with harmful spyware programs."* It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.

Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless / harmful services.

These are similar in nature to another version of this that many of us have encountered before. Those are the infamous phone calls from fake Tech Support / Customer Services representatives supposedly calling from *“Comapny X”* and that “*they’ve detected a problem with your computer / account and that in order to fix it they need to take a credit card number”.*

Just as you wouldn’t give those people your credit card number, you never give your personal information, passwords or crypto information to anyone contacting you in this way.

Pretexting

Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by an attacker pretending to need sensitive information from a target so as to perform a critical task.

Effectively, the attacker is creating a fake story that you, the target mistakenly believes, thus making the you trust the attacker and giving them your information or access to your information.

The attacker usually starts by establishing trust with their target by impersonating co-workers, police, bank, and tax officials, or other persons who have right-to-know authority. They may also attempt to

gain your trust by being extra-friendly and personable with you. *“How’s your day going?”*, *“Is it OK to call you by your first name?”* etc.

The pretexting attacker then asks questions that are ostensibly required to confirm the target’s identity, through which they gather important personal data.

All sorts of pertinent information and records are gathered using this scam, such as personal addresses and phone numbers, phone records, bank records and even security information related to a physical plant.

A classic example of this is to receive contact from a person pretending to represent a bank and saying that “*they have detected some unusual activity on your account”.* Often, they then ask you to confirm your identity to them by you providing your name, date of birth, email address, address, phone number and perhaps even other highly personal and valuable information such as a social security number.

Phishing

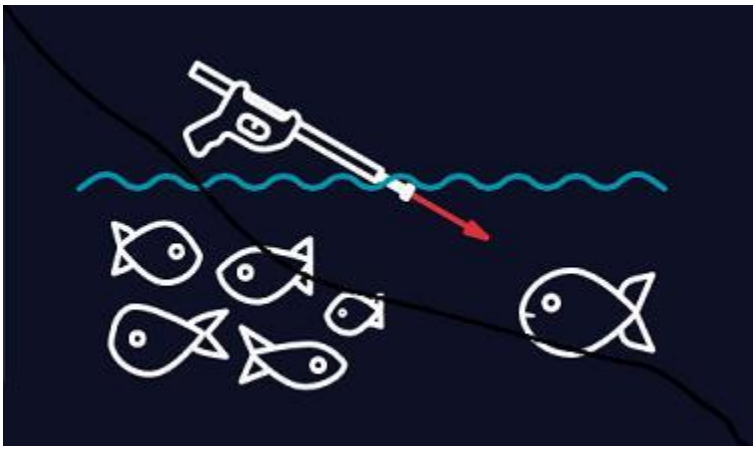
As one of the most popular social engineering attack types, phishing scams have traditionally been email and text message campaigns, sent to thousands of people. However, increasingly in recent years, scammers and thieves have been using the popular messaging apps such as WhatsApp and Telegram, as well as others to send their phishing attacks.

Phishing attacks are aimed at creating a sense of urgency, curiosity or fear in a target. It then compels them into revealing sensitive information, clicking on links which appear legitimate but that actually lead to malicious websites, or opening attachments that contain malware directly.

An example is an email sent to users of an online service that alerts them of a potential security breach, requiring immediate action on their part, such as requiring a password change or to login into their account with a provided link. In either of these scenarios, by asking the target to log into the website, the attacker then steals the target's login credentials.

The provided link is to an illegitimate website (controlled by the attacker) – nearly identical in appearance to its legitimate version – prompting the unsuspecting target to enter their current credentials and existing password, or in the case of a password reset, a new password. Upon completing the form the target submits the information which is sent directly to the attacker. The attacker then has access to the target's account.

Spear Phishing



This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Attackers often use freely available social media posts created by targets themselves. Posting on social media about how *"I've just made a bundle on X crypto"* is tantamount to placing a large target on your back and should never be done, regardless of how successful you may have been!

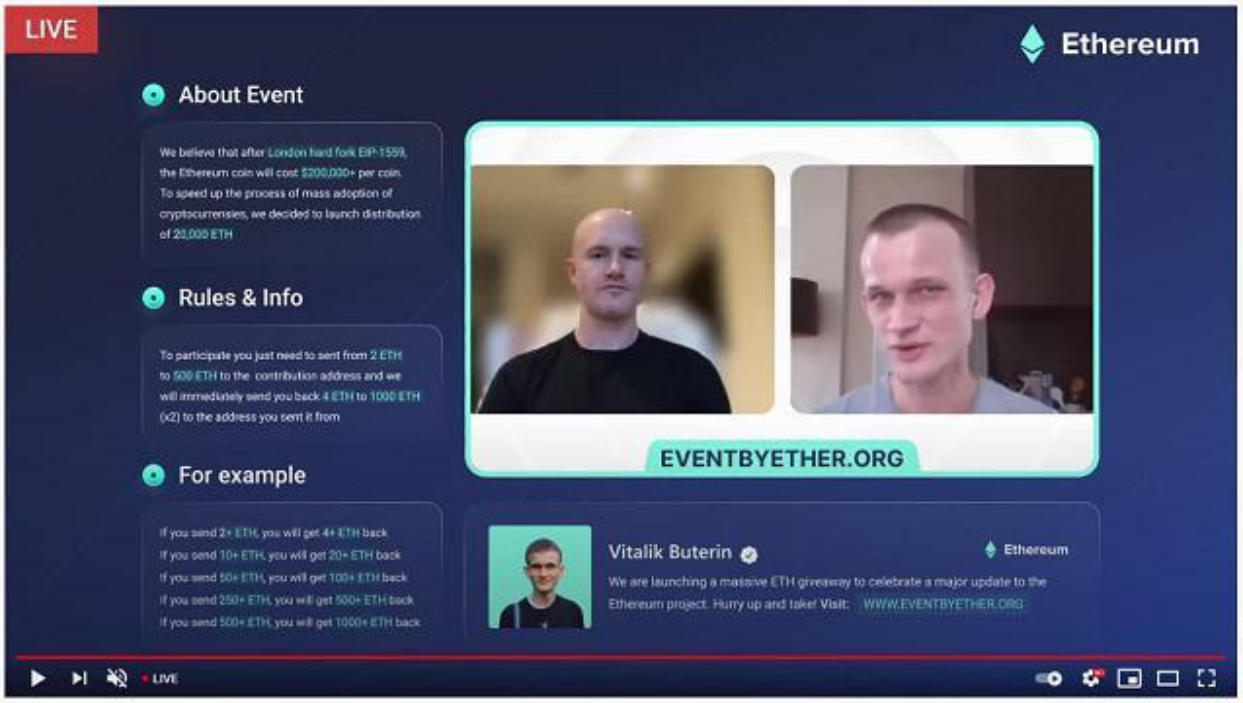
Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skilfully.

A spear phishing scenario might typically involve an attacker who, in impersonating a person such as an authority figure (a manager, executive or an IT department), sends an email to one or more targets. It's worded and signed exactly as the person normally does, thereby deceiving the recipients into thinking it's an authentic message from the authority figure.

A crypto-related example might be a message appearing to be from a crypto exchange. The message prompts recipients to login or change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

Special Event Scams

These types of scams often pop-up in number around the time of a particular coin's special event or anticipated update. Here's an example using the anticipated update of Ethereum's move from proof-of-work to a proof-of-stake concensus mechanism.



- As you might be able to see from the above image, under the '*About Event'* heading there is the first bait, which is that *"We believe that after London Hard Fork EIP-1559, the Etherium coin will cost $200,000+ per coin."* and also in the bottom right hand box is the second bait: *"We are launching a massive ETH giveaway".* There's your promise of riches! **Scam!**

- While there's no Admin or Tech support representative here, it is using a video still which looks like it's from YouTube and it appears legitimate. However, it's just a graphic which is quite simple to create. Even though it looks like there's a video, there is no *actual* video. **SCAM!**
- Under *'Rules and Info'* is where you can be sure and without a doubt this is a scam. The implied promise of *"You just need to **sent** from 2 ETH to 500 ETH to the contribution address and we will immediately send you back 4 ETH to 1000 ETH (2x) to the address you sent it from."*

The promise of doubling your ETH, just like that. **SCAM!**

- Notice they used "*sent"* – a typo, it should be *'send'.* These small mistakes while not very obvious can help you spot a scam. When you add this mistake to the two above baits you can be sure it is 100% a **SCAM!**

Simple Rules to Follow To Avoid Being Scammed

Now that you know all that I hear you say, ***"What should I do or not do so I don't get scammed?"***

We've got you covered so you're always one step ahead of the attackers!

There a few simple rules which you can apply to any contact you may receive from someone who may be an attacker. Establish answers to the following questions and you'll sidestep their attacks and avoid getting scammed.

1) Did they contact you first by direct message (DM)? If so, it's almost certainly a scam!

These are very common attacks, perhaps even the most common. The attacker will send you a direct message via either email, test message or increasingly, one of the various popular chat apps (WhatsApp, Signal, Telegram, Facebook Messenger, Viber, Skype etc.).

They may add you as a friend/contact and try and start chatting with you. They may appear over-familiar and friendly in an attempt to build trust. Once trust is built they will attempt to gain information from you, which is where things can quickly go wrong.

If someone contacts you directly, and you have not reported a problem at all, or at least to them, it is highly likely that they are after your information and/or your crypto. Give them nothing!

2) Are they claiming they are an Admin / Tech Support / Helpdesk / Customer Service representative? If so, it's a scam!

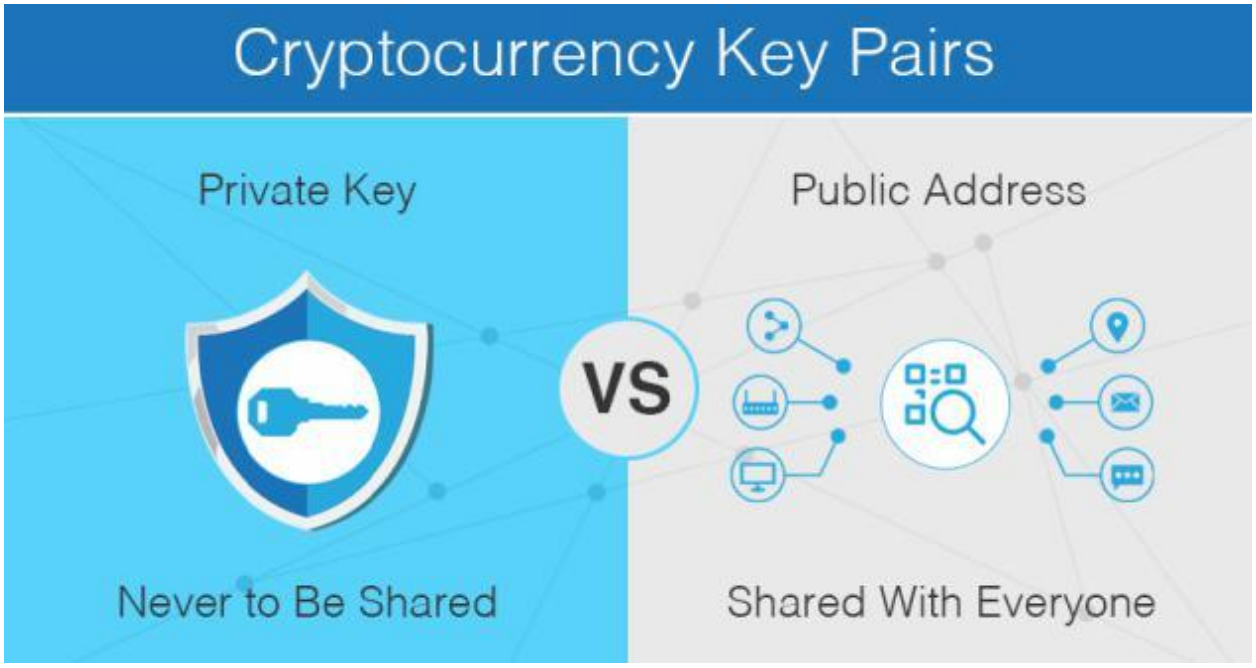
This is another very common tactic. Again, unless you've specifically had a problem that you have reported, you should view all contact from them as a potential scam and be very careful about what information you divulge.

Examples of this might be that they offer you *"the chance to invest in a high yield / lucrative opportunity"* or *"a guaranteed winner"* and that perhaps it is *"available for a limited time only"* to try and pressurize you into making an on-the-spot decision or reveal some information you otherwise would not have. These are common tactics. They are relying on your natural wish to *not want to miss out* so they can take advantage of that to scam you out of your crypto. Don't fall for it!

If they are pretending to be from a company or crypto exchange, these companies have dedicated teams to combat these types of scams. A simple search on your preferred search engine should turn

up the company webpage you need and/or their email address which you can often forward dodgy emails to for them to further investigate.

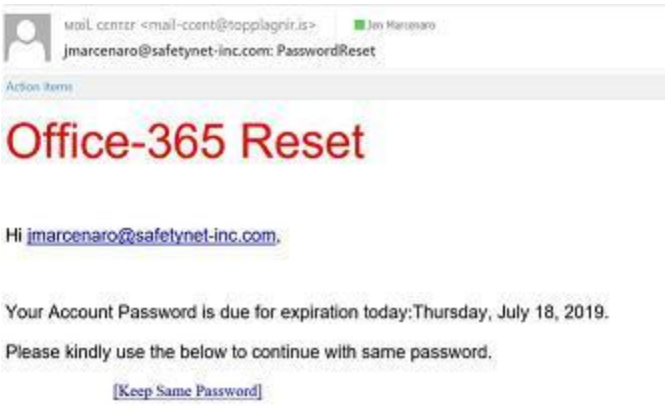
3) Are they asking for your Seed Phrase / Words / Private Keys / Email address?



A seed phrase or seed words are a series of words generated by your cryptocurrency wallet that gives you access to the crypto associated with that wallet. Consider a wallet as being similar to a password manager for crypto, and the seed phrase as being like the master password. As long as you have your seed phrase, you'll have access to all of the crypto associated with the wallet that generated the phrase – even if you delete or lose the wallet.

If they are asking for any or all of these then it is guaranteed to be a scam. Period. No company or representative would or should ever ask you for these. They are effectively asking you for the keys to the bank vault! Never give them or anyone else this information – ever – for any reason whatsoever.

4) Are they sending you a link for a website, live chat, or form?

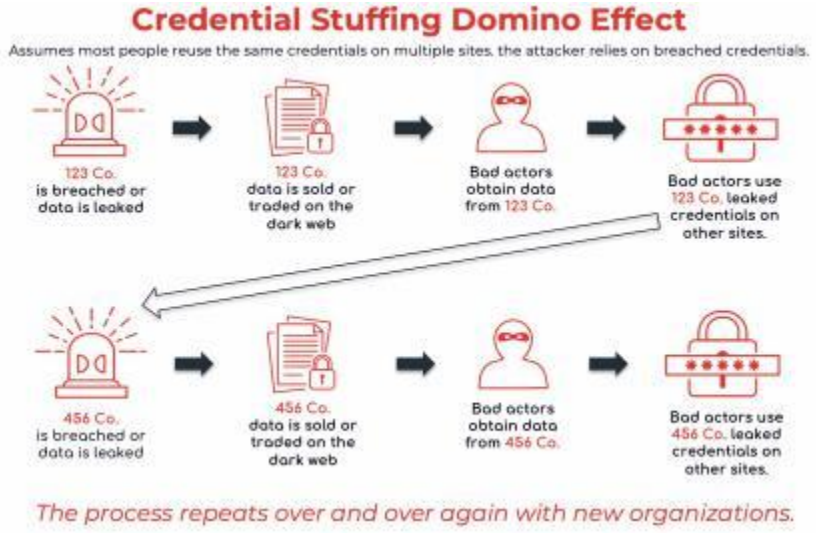


If so – **DO NOT CLICK ON IT!!!** It is very likely this a 'phishing attack', where that link is not a real link to a legitimate website / live chat / form.

If you click on the link, it will either activate a piece of malware deliberately embedded into the fake website / live chat / form to attempt to steal your information or, when you enter your information, it will go directly to the scammers instead of going to a legitimate website. If they are using a fake login screen, and you entered your login information, then yep, you guessed it, they now have your login information!

NEVER CLICK ON ANY UNVERIFIED WEBSITE LINKS / LIVE CHATS / FORMS / LOGIN PAGES – EVER.

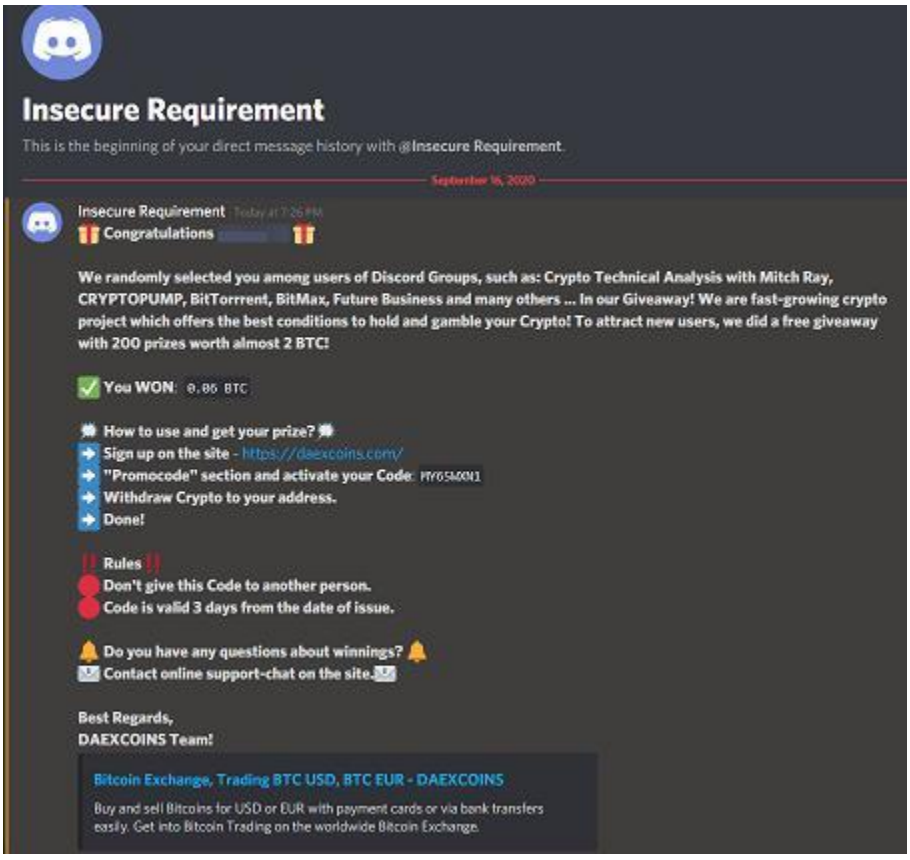
5) Did they say *"You're in our system/database?"* If so, it's a scam.



Email addresses and phone numbers are routinely sold online and scammers, spammers and hackers often buy them to try to target those people whose information has been sold for further exploitation. If you're on a database or a system, that often means your email/phone number has been compromised, then sold and now you're receiving unwanted calls, texts and emails about things you're not interested in or *"amazing new opportunities"* that are only available to you!

If you get a lot of messages or emails of a scam nature then it would be wise to set up a new email address or phone number. Disroot.org and Riseup.net provide reliable, secure email addresses for free, as well as paid options if needed.

6) Are they offering to buy / sell / give away crypto via DM or even on the main page? If so, it is definitely a scam!



Anyone offering to buy, sell or give away crypto via DM is almost certainly a scammer. This is the digital equivalent of the classic conman who feeds on your knowledge (or lack of it), tells you what you want to hear to build trust and then manipulates you into giving them your information and likely crypto. Don't fall for it!

If you don't know them and they've messaged you out of nowhere then those are the two biggest red flags. The safest thing would be to either report them as a scammer while not divulging your personal or crypto information, remove yourself from the conversation and then block that individual.

If this person has suddenly appeared in a Telegram group for example, and you suspect their motives are not pure, it's always good to ask them questions and test them. Doing this is like shining the spotlight on them – and we know how much criminals like that!

Or you can forward their private message to you (which shows them asking for your information etc.) into the main group. Expose them! At best, they'll leave the group and you and others will have been saved from potential loss. At worst, well, you were being diligent – better safe than sorry!

Help! It's too late, I already clicked the link! 😕

Well, if you've done this, the risk ranges from potentially bad to extremely bad but the faster you take action, the better. Follow these actions immediately to minimize the risk of losing your personal information and crypto:

- **Unplug the internet cable or disconnect from the wireless network on your computer.**

Do not delay. You do not have time to think or debate whether you should disconnect from the Internet – JUST DO IT!

If it's not easy to disconnect or access, pull the mains plug from the internet router. Desperate times call for desperate measures but it could save you a small fortune. Your family will understand and can go without internet for a few minutes!

- Install a reputable Internet Security software suite, update the malware definitions in the options and then run a full system scan.

Are you using a Windows or Apple computer? If so, you are much more likely to be exploited with malware. You should already be using a reputable Internet Security software suite with these but if you aren't, install one immediately, run the updates and then run a full scan on your computer. Do not stop the scan until it completes. If there's malware, this software should find it and be able to remove it.

If you find that you're having problems installing this software, that can be a sign that malware is active on the computer and is attempting to block the installation so it can continue to remain. A classic sign of your computer being compromised is that it goes unresponsive.

This occurs because the malware attempts to gather and send a large amount of data from your computer, which is normally quite resource-intensive and causes the system to slow down. If the fans on your computer spin up and the computer stops responding, your system is likely infected.

Minimize the damage by immediately disconnecting from the internet and install the security software suits and scan and disinfect your system. If you can't install the software suite then it's either time to call that techie friend of yours or take a trip to the computer shop. Don't tell your friend or the computer shop owner your crypto info either.

NOTE: Generally, Linux users are less likely to suffer these things because Linux users make up a very small proportion of computer users when compared to Apple and in particular, Windows users. That said, it is still possible though. Keeping one's system software up-to-date is often the best proactive protection. If you're using Linux and you click a dodgy link, the same rule applies – disconnect from the Internet immediately and seek help from someone knowledgeable about Linux.

Driving it Home - Stay Safe Out There!

OK, so I've read all that but what should I do if I'm still not sure?

It's OK, take a deep breath! The safest thing would be to do nothing. By nothing I mean don't divulge any information or crypto. Don't click on any links.

The golden rule is: *"If it seems too good to be true then it probably is!!!"*

Be objective and answer the following checklist questions if you're ever unsure:

1) Have *I* reported a problem? If not, and someone has contacted you out of nowhere? *It's a SCAM!*

2) Are they claiming to be an Admin / Tech or Customer Support / Helpdesk and they called you, even though you've not reported a problem? *It's a SCAM!*

3) Are they asking for your Seed Phrase / Words / Private Keys / Email address? *It's a SCAM!*

4) Are they sending you a link for a website, live chat, or form? *It's a SCAM!*

5) Did they say *"You're in our system/database?" It's a SCAM!*

6) Are they offering to Buy/Sell via DM or even on the main page? *It's a SCAM!*

7) Are they using a special event, a giveaway or other baiting techniques to get you interested? *It's a SCAM!*

Understanding KYC and Alternative Options

Introduction

Cryptocurrency Peeps- Do You Know What KYC Is??

KYC stands for “Know your customer” and it is a regulation that any businesses with a banking relationship have to abide by. **AND Bitcoin exchanges are no exception.** The KYC regulations #1 rule that is imposed worldwide are businesses that act as money exchange and/or transmitters have to have “suitable” information on every customer they serve.

And now within the Bitcoin space, ‘creeping KYC’ is a disease that is slowly spreading. If you have ever or plan to purchase through one of these regulated KYC entities, you are essentially tagging your bitcoin address to your personality.

This means that chain surveillance firms, the companies they work with, or governments can potentially

- Track your spending habits
- Prevent you from using other regulated services
- Confiscate your bitcoin

- Come after you for tax liabilities
- Know more about you than they should

I get it though, auto DCA from a Bitcoin-only company makes ‘stacking sats’ easy. I’m not telling you to stop what you are doing, I just want to provide all the facts so everyone can make a knowledgeable decision.

What Information You Will Have to Provide

You will always need to provide personal information if you are planning on buying bitcoin from a KYC exchange. How much personal information you supply will depend on which exchange you are using.

Some only require your name for smaller amounts (which you could easily make up a name), but others may require a lot more like:

- Name
- Address
- Phone number

- Drivers license
- Government ID
- A selfie holding a piece of paper with the name of the exchange and the date
- A video call with the exchange

Why Providing This Information Is A Huge Risk

Number 1: Data Leaks

Since the KYC information ties to your personal identity to any bitcoin you purchase, the exchange will know

- How much you bought
- When you bought it
- Your banking information
- Where you withdraw to

With all of that personal and sensitive information you provided, it is easy for all of it to be stolen due to weak security practices at some of these central party companies.

Let me ask you this: how would you feel if your name, address, photo, and exactly how much Bitcoin you own was stolen from an exchange and being sold to the highest bidder on a darknet market?

Number 2: Censorship

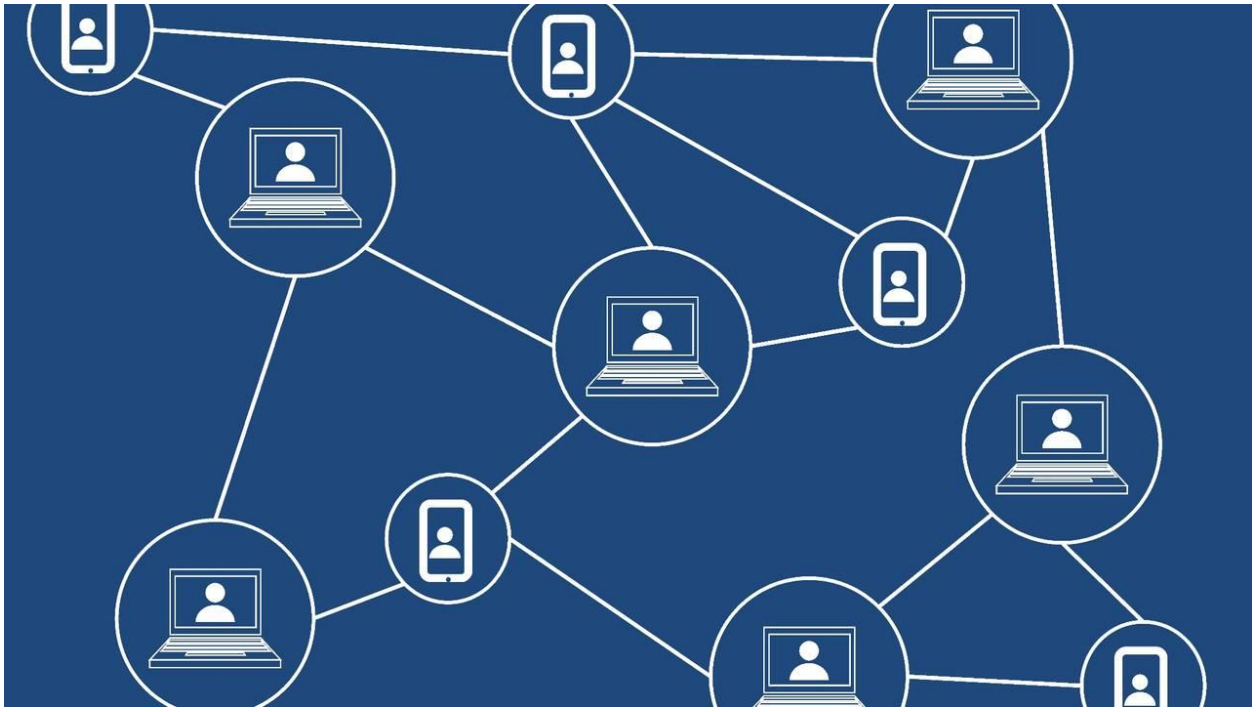
Most of these KYC exchanges work directly with chain surveillance firms (and some directly with government agencies) to remain compliant with their jurisdiction. This completely transparent nature of the Bitcoin blockchain can mean anyone with the right tools can follow your activity. That means if you withdraw to or deposit from an entity that the exchange does not like, they can freeze or even close your account.

Number 3: 6102 type order

Executive Order 6102 is an executive order signed on April 5, 1933, by US President Franklin D. Roosevelt “forbidding the hoarding of gold coin, gold bullion, and gold certificates within the continental United States.”

If the government in your country chose to exercise a similar order against Bitcoin, anyone who bought bitcoin from a KYC source would be an easy target for confiscation. Not to mention the fact that they will know the addresses you withdrew to and could watch those for any movements (The blockchain is completely transparent don’t forget).

What Other Options Do You Have?



There are plenty of options out there to purchase Bitcoin that has no ties with KYC sources. These are all considered to be P2P (peer-to-peer) exchanges, and they work by trading directly with another individual and not a centralized third party. Some of these P2P exchanges do sell other coins as well as bitcoin, so make sure to be extra careful.

Here is a list of some of my favorite P2P exchanges:

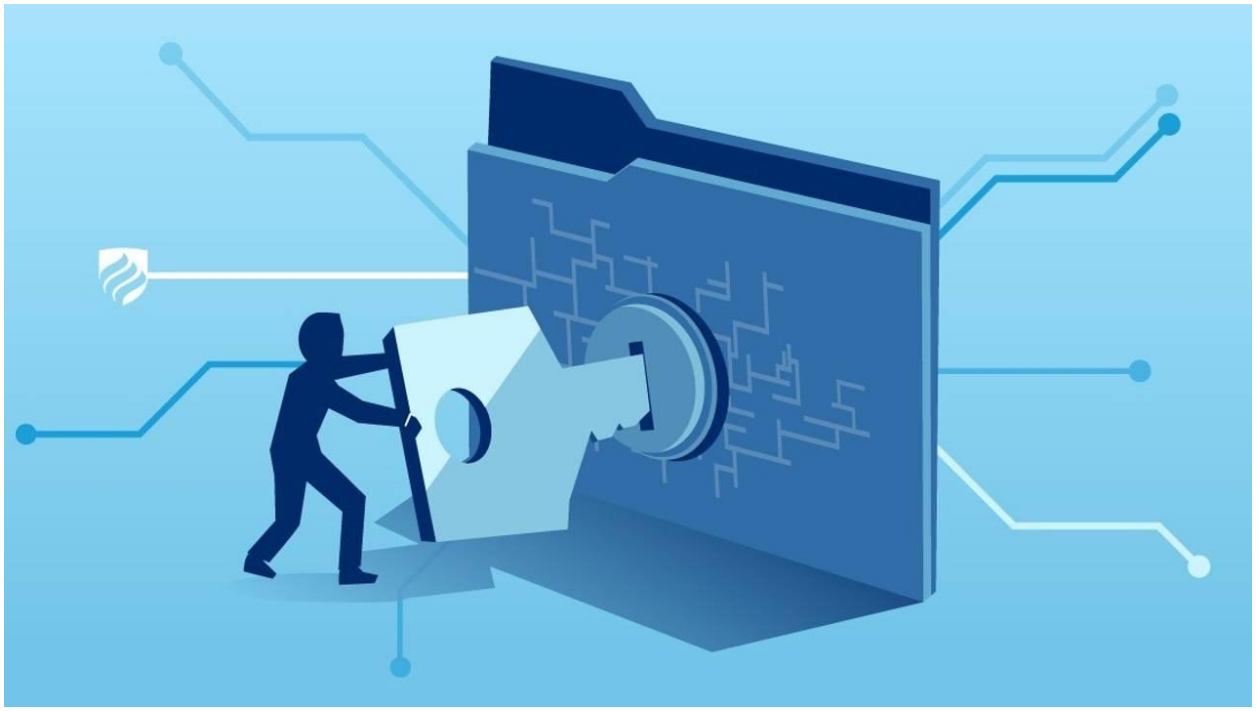
Hodl Hodl

Bisq

LocalCryptos

Local Coin Swap

Doesn’t Buying No-KYC Bitcoin Come With A Hefty Premium?



Yes, some offers to purchase bitcoin on P2P exchanges have some very high premiums over the spot price. However, if you wait for a little you can pick some up at the spot or just marginally (1-4%) above. Both Bisq and Hodl Hodl allow you to create a ‘Buy offer’ where you tell the market that you want to buy ‘X’ amount of bitcoin at ‘X%’ relative to the spot price. All you need to do then is wait for a seller to accept your offer and complete the trade.

We personally take this approach and have never waited for more than a day for someone to accept the offer of around a 2-4% premium.

What Other Ways Can I Get Some No-KYC Bitcoin?

There are plenty of other ways, but each varies with levels of difficulty and complexity.

- Earn it
- Sell unwanted goods for it
- Buy it from a friend or at a local meetup
- Provide value to others and have a donations page

- Pay for dinner when out with friends and ask them to reimburse you via bitcoin

Can I Ever Un-KYC Myself?

No. You can never undo that if you have ever purchased Bitcoin from a KYC source. You do, however, have three options to protect yourself…

Go Back Out The Way You Came In

Sell your KYC coins you bouts at the exchange you bought them from.

Depending on where you are from, this will likely create a taxable event that you will need to contend with. But, now you will have a paper trail to prove you no longer own those coins. Now you have a clean slate to buy bitcoin via a non-KYC source.

Keep Two Stacks

Immediately stop buying bitcoin from KYC sources segregate/label those funds. From now on, start obtaining bitcoin from a non-KYC source, However, this still leaves you vulnerable to some of the risks outlined above but you may be a little safer with smaller KYC amounts.

You should also consider conjoining your KYC stack. This will not erase your KYC history but it would give forward-looking privacy for future transactions. Whirlpool is by far the easiest and most effective conjoining implementation.

Move Jurisdictions

This is the most extreme and not likely to happen. But, you can move to different jurisdictions to free you from future obligations. Of course, this is not a 100% guarantee as certain jurisdictions may have information-sharing agreements (the EU for example).