



Secure Your Crypto For Life in 15 Minutes

The ultimate guide to prevent your crypto from getting hacked, stolen, or frozen. **Truly own what is yours.**



Why NGRAVE

NGRAVE empowers people to master their wealth so they can live the life they want. Founded in 2018, **NGRAVE** is a digital asset security provider offering user-friendly maximum security solutions for blockchain and crypto use cases. Its flagship product — crypto hardware wallet “**NGRAVE ZERO**” — is the only financial product in the world with a custom operating system featuring the highest security certification: EAL7. NGRAVE partnered with the world’s top tier in nano- and chip technology, cryptography and hardware security. Among its advisors, it counts several blockchain pioneers such as Jean-Jacques Quisquater, famous cryptography professor and second reference of the bitcoin paper.

NGRAVE’s product suite is a 3-tier solution. [ZERO](#), the offline touch-screen hardware wallet allows users to securely store and transact their crypto. [GRAPHENE](#), the stainless steel encrypted backup solution ensures that users never lose their



keys. It is not only made to withstand extreme conditions, but also designed to be recoverable in the event of loss. Last but not least, [LIQUID](#) is the convenient mobile app that connects users real-time to the blockchain without ever exposing their private keys.

We are passionate about making the world of crypto a safer place. We eradicate the chance of loss and malicious hacking of your crypto, giving you complete control of your digital assets. We believe we are all in this together. Join our movement at <https://www.ngrave.io/>

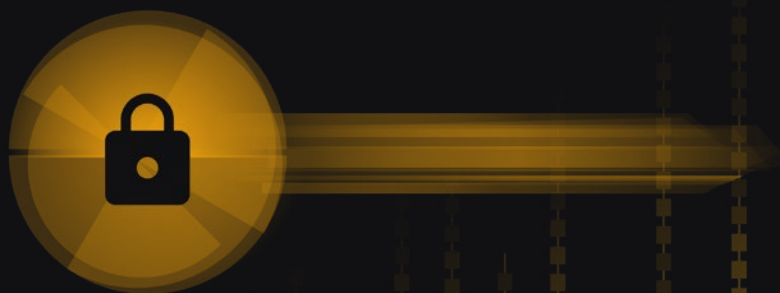


Table of Content

Keeping Your Crypto Safe — Solving the Private Key Paradox	1
Safest Way to Start Investing in Crypto	7
4 Common Phishing Attacks and How to Avoid Them	18
5 Ways to Improve Your Cybersecurity Hygiene	25
5 Mistakes to Avoid With Crypto Hard Wallet Safety	30

Keeping Your Crypto Safe

Solving The Private Key Paradox



How your private key is both unbreakable and hackable and what to do about it.

1. The Core Of A Blockchain Wallet

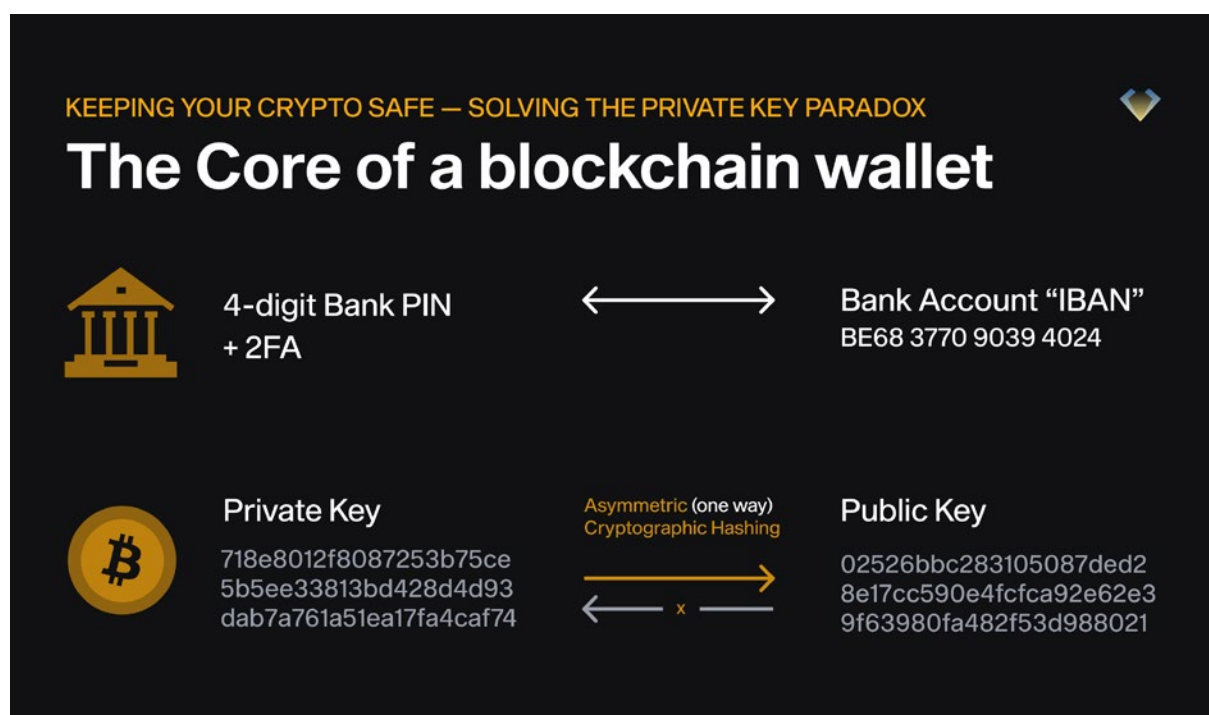
In a previous blog post, we wrote that:

“Every crypto wallet consists of two things: a private key and a public key. You can consider the public key as your “address” or “account” on the blockchain. When you request a payment to someone, they will send the funds to your public key. The private key on the other hand, is the secret cryptographic password that grants the party who knows the value of the key, complete



ownership of any funds on the associated public key. So if you have crypto on one or more public keys, it is imperative that you protect the associated private keys as much as possible.”

But so why is that private key so important? And can we quantify it?



2. The Private Key Paradox

At NGRAVE, we call the issue at hand the “Private Key Paradox”. The private key or secret cryptographic access key to your crypto wallet is the reason why your crypto is so secure: if I don’t know your private key, I can’t break it or brute force it with the existing computer power available. Therefore, I cannot steal the funds you have on your public key: the address on

which you have your crypto. It's interesting to know that the **public key and thus your so to speak “account number” is actually cryptographically derived from your private key** in the form of a **one-way hash function**. This basically means that while you can calculate your address from your private key, it is near impossible to do the reverse calculation, i.e. calculate your private key from your public key. So, yes, the private key is a crucial pillar in blockchain wallets. **It's also the Achilles Heel. If I can simply look over your shoulder (e.g. when you have your key stored somewhere online) and see your key, it's game over. I can steal your funds.** Also, if you lose your private key yourself, there is no way of getting access again to your crypto. The morale: above all, **generate your private keys out of sight, and keep your private keys out of sight!**

Let's have a look at the numbers.

3. Quantifying The Difficulty Of Guessing Your Private Key

The first thing you see on this graph is that winning the Lottery suddenly doesn't seem such a big feat. Obviously you know better. And it gives a great perspective on how difficult it actually is to guess my private key and get access to all 0.01BTC on my account. Whereas winning the Euro Millions is an odd of about 1: 1.39×10^8 (or 1 in a hundred and thirty nine million), it's nothing compared to guessing one of the richest men on Earth's bank account number, PIN code, and two factor authentication



$\times 10^{69}$, which is billions of billions of times harder to achieve. That finally brings us to you guessing the private key of my Bitcoin address, which is of an order of magnitude of 256 bits, basically equal to you trying to guess which atom I am thinking about right now, of all the atoms in the universe.

4. Implications

So...THAT's why if you don't know my private key, you cannot brute force it. The computational requirements simply don't exist today. Now imagine that you generate your private key offline, and never need to expose it when signing transactions (or any other kind of wallet management for that matter). How can a remote attacker then possibly break into your account?

Now, here is where it becomes tricky. OK, your private key needs to be generated offline. But this generation process itself has to adhere to some crucial conditions. It has to be able to generate the whole range of 2^{256} possible keys. For example, if it were to generate only one of two values all the time, you still would have a private key but it would be easy to guess it. So the generation process itself must ensure that it can generate a key that is statistically unique and unbreakable (the process needs to be able to generate a gigantic range of keys), it needs to be unpredictable (i.e. random, so that nobody could ever just implement the same process and calculate your key from it anyway), and of course it needs to be offline.



5. The Solution

And that's exactly where NGRAVE comes in. We have developed a product suite that not only generates strong private keys 100% offline, but also keeps them unexposed at all times.



Safest Way to Start Investing in Crypto



For any newcomer, finding the safest way to invest in crypto might feel like trying to navigate an obstacle course. We'll help you chart a path to safe crypto investing.

How much should you invest, what crypto should you buy, where should you safely store it? You might feel overwhelmed by all the options, and concerned about the potential pitfalls, but it should help to realise that they all boil down to understanding and mitigating risk; from a purely financial perspective, as well as the risks from a security point of view.



Begin with realistic expectations

If you are thinking about investing in crypto, your inspiration might well have been a friend, colleague, or social media notification, describing massive gains made buying early into some exotic animal-based meme coin, that they are convinced are going all the way to the moon.

Well crypto is as much of a jungle as it might sound, so our first recommendation is that you park the spaceship, and start your crypto journey with your feet firmly planted on the ground, and unrealistic expectations in check.

Yes, there are plenty of people who have made life-changing sums investing in crypto, but that is likely because some, or all, of the following apply:

- they invested very early
- they started with a significant initial investment
- they already had experience investing in volatile assets
- they did insane amounts of research & understand the technology
- they were lucky enough to be in the right place at the right time

Though many analysts feel that the crypto sector as a whole is still in its infancy, it is probably fair to say that if you are reading this article, most of the above don't apply to you (yet).

Unless you have a spare flux capacitor lying around, you cannot



turn back time, nor can you directly influence fortune, though landing on this page, could well be considered to be in the right place at the right time.

What is within your control is how much effort you make in understanding what you are getting into, so don't expect to go away with a crypto investment plan on a page - there will be homework set from the [NGRAVE Academy](#).

Most of the recent crypto investors will have made very modest returns, and a significant number will have jumped in without knowing what they are doing and got rekt - crypto term for losing everything. And those stories of fantastic gains, well, those are true and should be regarded as crypto's lucky lottery winners.

If you want advice for sensible and safe crypto investing that doesn't rely on a Powerball Win, start with your feet and focus on the ground - rather the moon. With your expectations back on Earth, we can think about the first practical step, which is deciding **how much you should consider investing in crypto**.

Don't invest what you can't afford to lose

The key phrase to understand when deciding how much to invest is something called discretionary income. This is the amount of income you have left over after all your fixed monthly commitments have been accounted for. This must be money you can afford to lose and not incur debts, or any material



impact on the essentials of your day-to-day living.

You should only consider investing from your discretionary income. If you already have a large lump sum to invest from savings or inheritance - which doesn't involve taking on debt or leverage - then you should only consider crypto as one element in a wider balanced portfolio that will include less riskier investments - such as share ETFs or mutual funds - because investing in crypto carries considerable risk.

Not only are cryptocurrencies very new technologies, but they are also a direct challenge to governments' authority. That creates enormous uncertainty around future adoption and potential value; in the context of great economic uncertainty for a host of other reasons (not least the Covid Pandemic). That uncertainty translates into extreme short-term volatility and longer-term risk that your investment will lose value over time. So never invest what you cannot afford to lose.

Start by investing in crypto Blue Chips

Saying that crypto is inherently risky is a generalisation, because just as you can define a portfolio of investment categories with a range of risk, with crypto being at the extreme, you can categorise crypto into a risk spectrum.

Bitcoin and Ethereum can be considered crypto's blue-chips - the term given to established and trusted publicly traded companies tracked by the Dow Jones Industrial Average or



FTSE 100 Index. They have the longest track-record of proven and effective technologies, with large enough user bases to create network effects which are very hard to disrupt. For that reason, they are the most sensible place to start investing in crypto.

Neither guarantee a future return on your investment, but the table below shows you historically how they have performed. For newcomers, they should form the majority of your initial investment:

At Jan 1st.	Bitcoin		Ethereum	
	Price	% Change	Price (USD)	% Change
2012	5.27	1,655.90		
2013	13.3	152.56		
2014	770.44	5,690.96		
2015	313.92	-59.25		
2016	434.46	38.4		
2017	997.69	129.64	8.2	
2018	13,412.44	1,244.35	752.46	9,076.34
2019	3,869.47	-71.15	139.61	-81.45
2020	7,188.46	85.77	130.75	-6.35
2021	29,391.78	308.87	729.12	457.64
2022	47,743.00	18351.22	3765.67	516.47



Follow a Cost Averaging strategy

If you have done enough research, and feel that Bitcoin and Ethereum will continue to increase in price over the long term, you face the difficult task of choosing the right time to pull the trigger on your first investment, given short-term volatility.

Interpreting short-term market behaviour isn't an exact science. There are many schools of thought around what exactly drives short term price movement, which focus on different aspects of **technical analysis** - interpreting price movement, chart patterns and volume - as well as analysing actual transactions and segment behaviour - known as **on-chain analytics**.

It is totally unrealistic for you as a novice crypto investor to wrap your head around those concepts, but luckily there is a sensible and simple investment strategy to get you started, called **Cost Averaging**.

Cost Averaging simply means making regular, recurring purchases of equal value spread over time, instead of one lump sum investment. This approach will allow you to average out the short-term volatility, and if your overall premise is correct, build a net-positive investment over time.

The benefits of Cost Averaging

- Simple strategy that can be automated at most exchanges
- Removes the stress & uncertainty of timing purchases



- Has proven successful in the long run for Bitcoin & Ethereum
- Allows you time to learn as your investment grows
- Doesn't require an initial lump sum

The downside of Cost Averaging

- Works best when pursued through a Bear Market
- Recurring purchases will incur more transaction/trading fees
- Requires patience & discipline as takes time to build a meaningful position
- Doesn't guarantee success

Cost Averaging isn't a magic bullet for successful crypto investing, but it is the most sensible approach for someone without experience and with modest discretionary income. It is a really good idea to build a Cost Averaging tracker - in excel or googlesheets - to both give you a clear picture of your profit and loss, as well as keep you grounded.

Over time, a Cost Averaging approach can be modified as you build up your knowledge and experience, using external data to adjust the size of each purchase, and can also be reversed to sell fixed amounts at regular intervals, if and when your patience pays off.



Use Cold Storage to avoid the temptation to impulse trade

Warren Buffet, one of the world's richest men, and most famed investors, once said:

'The stock market is a device for transferring money from the impatient to the patient'.

This is equally true of investing in cryptocurrency, which is one reason why Cost Averaging is sensible for inexperienced investors, because it enforces a level of self-control.

If however, you leave your funds on the **exchange you use to facilitate the recurring purchases**, you could be tempted to abandon your plan when the rollercoaster ride is at its most extreme, trying to catch a short term spike, or bail out when price plummets.

Those are the moments when your patience will be tested to the max, and it helps if you take an out of sight, out of mind approach, by moving your funds after each recurring purchase into what is known as Cold Storage.

Cold Storage means placing your crypto assets in a completely offline state, safe from any malicious online threats, but with the additional benefit of making it less likely that you'll make a hasty trading decision.



The recommended form of Cold Storage is a cryptocurrency hardware wallet, which is what NGRIVE manufactures, so we have a huge amount of additional resources to help you understand their benefits and function.

- [Do you need a cryptocurrency hardware wallet?](#)
- [What is a cryptocurrency hardware wallet?](#)

This moves us on from the simple and sensible ways for newcomers to manage and mitigate the financial risk elements of investing in crypto - that might see it decline in value - to keeping that investment secure from threats that might simply try to steal it.

Understand the nature of crypto custody

With such an emphasis on security, you can be forgiven for thinking that crypto is a Mad Max style lawless wasteland. It isn't. Illicit activities have been estimated to account for less than [1% of all crypto transactions](#), but the threat is real.

Just as you should research the fundamentals of crypto to appreciate its potential future adoption and value, the best way to ensure the security of your personal funds, is taking time to understand how crypto works, and in particular, the concept of custody.

Banks custody your fiat money; they look after it, and grant your privileged access. This trust-based relationship is at the



core of modern centralised money, and what crypto - with a decentralised model - was created to fix.

The [NGRAVE Academy](#) is a great place to learn more about this, but it boils down to one key phrase: Not your keys, not your coins. This means that the safest way to store your crypto is by being in possession of the information that ultimately enables it to be spent - Private Keys, represented in most modern crypto wallets by a Seed; a collection of 12-24 unique words.

The ultimate way of exercising that control in a secure and convenient way, is by using a crypto hardware wallet like the [NGRAVE ZERO](#).

When you purchase crypto from an exchange - for example through the recommended Cost Averaging approach - they have custody of your Private Keys and therefore your funds. This is known as counterparty risk, as a third party - and any of its security weaknesses - becomes the point of failure, not you, but unlike the funds held in custody by your bank, exchange balances aren't insured.

Banks Insure Funds, Exchanges Don't

Traditional money functions with a trust model. That trust extends to regulation and compliance, which includes measures to compensate for theft of funds, up to a maximum amount, depending on your location.



This isn't the case with custodial crypto services - like exchanges or wallets. There is no safety net. Some exchanges maintain an insurance fund, to cover losses from hacks, but that isn't compulsory. Your funds might be at risk.

There is no such thing as a free lunch, so you will have to accept the risks associated with investing in crypto. There are certainly things you can do to minimise that risk. We've tried to introduce you to the most obvious and practical way to safely get started investing in crypto. But that is just the start of an ongoing journey of education and awareness that you should continue to make, in order to stay safe, as you look to grow your crypto investment.



4 Common Phishing Attacks & How to Avoid Them



Empower yourself, don't be next in line.

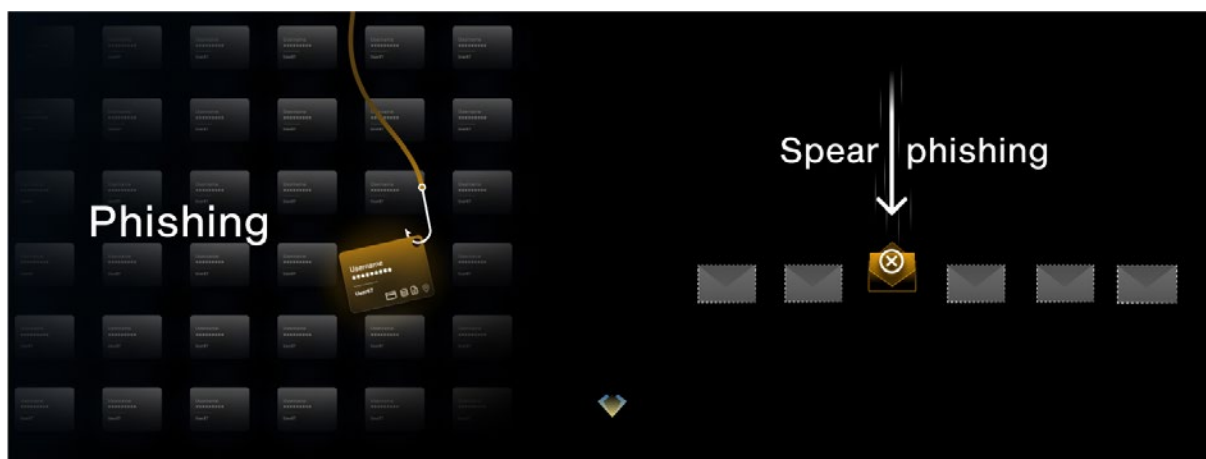
Phishing scams predate the cryptocurrency industry, with the first documented attack believed to have been carried out in the mid 90s.

Though the overarching goal of phishing is simply to defraud unsuspecting victims of money, the fact that such ploys are executed by tech-literate hackers means they're increasingly used to steal digital assets. Not least because cryptocurrencies confer greater privacy protections than fiat, meaning hackers can vanish into the night with their ill-gotten gains.



Here are four of the most common phishing attacks, plus useful tips for protecting yourself from cybercriminals.

1. Spear phishing



A recent [report](#) by data protection firm Barracuda Networks highlighted the growing prevalence of spear phishing attacks, whereupon attackers target specific individuals with customized messaging — typically a phoney email purporting to be from a trusted sender.

Oftentimes the aim of the attacker will be to compel recipients to reveal sensitive information, or induce them to visit a malware-ridden website. According to Barracuda's report, the average organization is targeted by over 700 such social engineering attacks every single year.

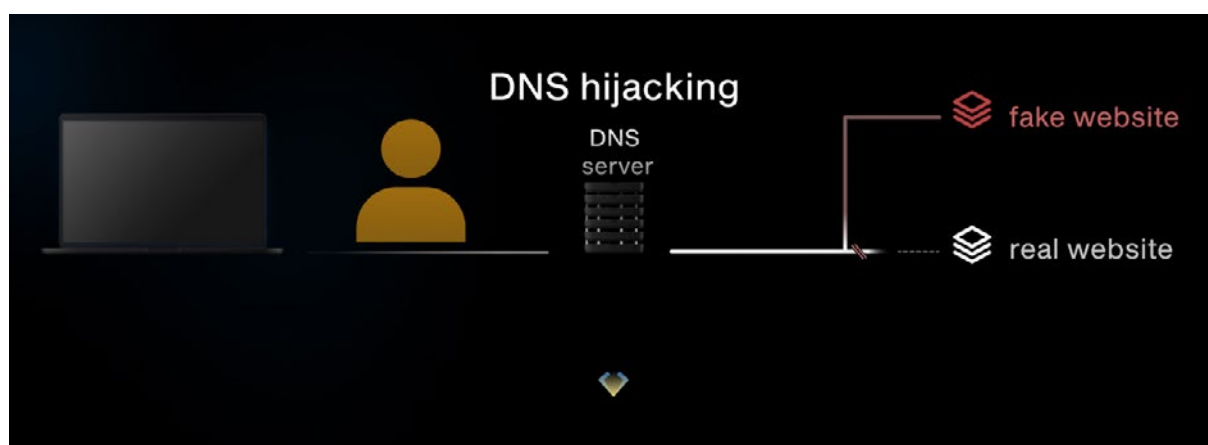
As far as crypto is concerned, phishing emails and text messages purporting to be from hardware wallet providers such as Trezor — or even cryptocurrency exchange platforms



— attempt to induce the recipient to ‘update’ their seed phrase or change their password, after which the thief can steal log-in credentials and drain the wallet in question. Another tactic is to entice users with plausible promotions, as was the case with [the attack on Celsius users](#) earlier this year.

So, how can you immunize yourself from spear phishing? At a company level, there are myriad solutions: staff training to increase employee awareness and reporting; machine learning utilization to analyze communication patterns; AI tools to ensure account-takeover protections. Individuals, meanwhile, should take steps to verify the legitimacy of senders, carefully vet links and sender email addresses, avoid open Wi-Fi networks, and have 2-Factor Authentication in place. Above all, be extremely wary about any email from which you are asked to enter a log-in and password.

2. DNS hijacking



Some phishing schemes are more sophisticated than others. Take DNS spoofing attacks, for example. With this decades-old scam, cybercriminals hijack legitimate websites and replace them with a malicious interface, before phishing users into entering their private keys on the fraudulent domain. Earlier this year, two major defi projects built on Binance Smart Chain — namely PancakeSwap and Cream Finance — fell victim to such an attack, although it was unclear how many users had been duped.

One of the most effective ways of protecting yourself from a DNS attack is to use a VPN, since it bypasses your router's settings by sending traffic via an encrypted tunnel. You should also be diligent about checking the URL in your browser to ensure the website certificate is trusted, and heed any warnings that indicate your connection to a site is insecure. Of course, storing your crypto offline in a tamper-proof hardware wallet like NGRIVE, rather than interacting with funds online, is also good practice.

3. Phishing bots

Five years ago, we were told that an army of 'bots' influenced both the Brexit referendum and the U.S. Presidential election. Whether these claims had merit is beyond the scope of this article, as we're interested in a different kind of villain: the sort created to steal our precious seed phrases.



“The phishing request comes from an account that looks ‘normal’ (but few followers), helpfully suggests filling out a support form on a major site like Google sheets (hard to block), [and] asks for your secret recovery phrase” - **MetaMask**



Back in May, Ethereum-based crypto wallet MetaMask drew users' attention to a phishing attack perpetrated by phrase-stealing bots on Twitter. “The phishing request comes from an account that looks ‘normal’ (but few followers), helpfully suggests filling out a support form on a major site like Google sheets (hard to block), [and] asks for your secret recovery phrase,” explained MetaMask, before dispensing some sage advice on how to protect oneself: “ONLY seek support from WITHIN the app you want help on.”

“ONLY seek support from WITHIN the app you want help on.”
- **MetaMask**



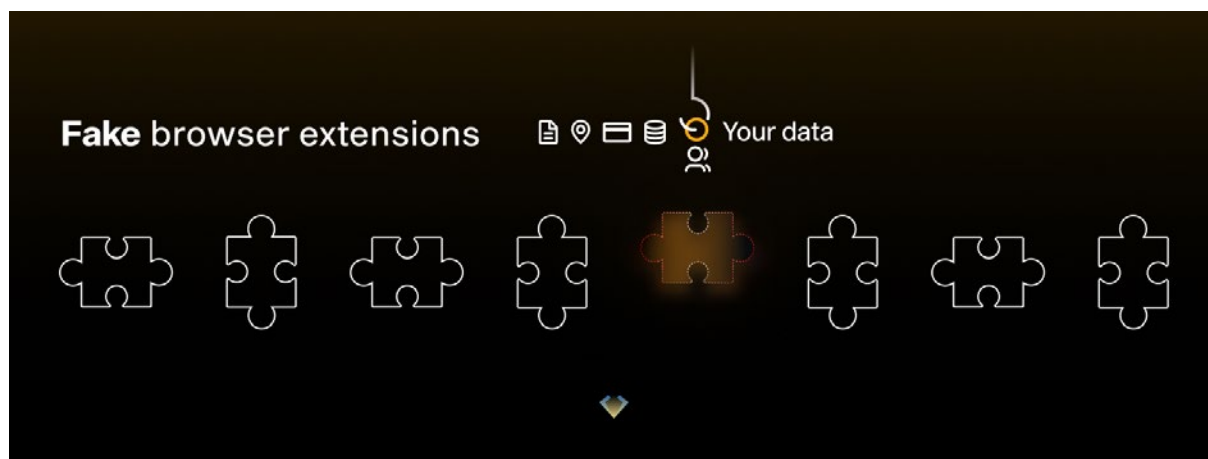
While it might seem like a good idea to verify that correspondence has come from an official account, this strategy isn't full-proof: social media accounts can be hacked like any other, as evidenced by the great Twitter hack of 2020 that [earned cybercriminals \\$121,000 worth of bitcoin.](#)

4. Fake browser extensions

In the cryptosphere, we're accustomed to using all sorts of browser extensions with the aforementioned MetaMask proving especially popular. Unfortunately, cybercriminals are turning this predilection to their advantage by creating fake extensions and stealing funds from users. Last year, a malicious Chrome extension called Ledger Live was downloaded over 120 times before being booted out of the Chrome Web Store. Troublingly, attackers were able to leverage Google Ads to promote the product and attain an air of legitimacy.

The take-home? Don't rely on web stores to properly vet the extensions they make available. If downloading a crypto extension, check its profile page to ensure it has plenty of reviews and comes from a trusted developer. Scrutinize the permissions the extension asks for (Chrome Settings>Extensions>Details) to check that they accord with its features. Oh, and you might want to download an extension directly from a link on the company's website.





Conclusion

There are other general rules you should consider following to protect yourself from phishing scams. For example, it's smart to bookmark verified sites where you typically input sensitive information. Ditto saving contact email addresses from crypto companies with whom you interact. Countless people have also fallen victim to phishing emails or malicious websites that feature a subtle misspelling of a legitimate address. It may seem like a chore, but double-checking URLs is a good habit to get into.

Knowing how phishing scams work is the first and most important step to protecting your crypto wealth. Follow the tips outlined above and the only thing you'll have to worry about... is the market.



5 Ways To Improve Your Cybersecurity Hygiene, Right Now

Don't wait until it's too late. Follow these easy steps to elevate your online security today

Hackers wreak havoc around the world as they go after people's money and sensitive data. They have various tools at their disposal, including automated scripts, that enable them to [attack](#) your computer every 39 seconds, on average 2,244 times a day. And if you are a cryptocurrency owner, then you're giving cyber-criminals one more reason to target you as over two-thirds of [breaches](#) are financially motivated.

That's why it's essential that you adopt the best security practices, known as cybersecurity hygiene, and increase your chances of avoiding an online threat. Read on to explore steps



you can take to protect your devices, online accounts, and digital coins.

1. Install reputable antivirus and malware software

Not having antivirus and anti-malware software means that you're vulnerable even to well-known threats. Having quality software to monitor your devices for signs of suspicious behaviors is a vital part of cybersecurity hygiene. These tools will perform automatic scans, erase malicious codes, and prevent attackers from easily penetrating your device.

Also, using a network firewall is another step to prevent unauthorized users from accessing your websites, mail servers, and other sources of data. If you want to learn more about how antivirus software works, then click [here](#).

2. Update software regularly

Many of your apps, software products, and operating systems will update themselves regularly. You'd do well not to delay these updates as developers might have found security vulnerabilities that require the system to apply urgent patches. Also, developers might not necessarily alert you when they implement a critical patch to avoid giving hackers the heads-up.



3. Use strong passwords and multi-factor authentication

Most people know reusing passwords is risky. They're also aware that relying on simple passwords such as "123456" makes them vulnerable. And yet, they do these things anyway. Surveys [show](#) that two-thirds of people use the same password or a derivate across all their online accounts. This means that if hackers get hold of a person's password, they'll have access to his or her entire 'digital kingdom'.

The obvious solution is to use complex and unique passwords for each online account you create. Password managers, such as Keepass, can make this job easier. They generate a unique password for every account and you only need to remember a master password. **Also, cryptocurrency hardware wallets are well suited to operate as password managers and NGRAVE's [ZERO](#) will have this capability in the near future.**

Another option is to use multi-factor authentication (2FA), whenever possible. Ideally, you'd rely primarily on face recognition- and fingerprints-based 2FA systems as SMS-based ones only move security to your carrier, which might not always be reliable. But if you have to rely on SMS-based authentication, then consider using solutions like those **offered by [Efani](#) that protect you from SIM hacking.** And some apps and software systems even allow setting up multiple 2FAs for different use cases, such as logging-in, signing transactions,



or sending money.

“Crypto hardware wallets such as NGRAVE’s ZERO can be used as true offline password managers.” – Ruben Merre, CEO NGRAVE

4. Encrypt and backup data

Another important cybersecurity hygiene practice is making sure that devices storing your sensitive data — whether it’s your laptop, tablet, smartphone, removable drive, backup tapes, or cloud storage — use data encryption. Many apps have data encryption set by default. And protect your wireless network, too. Use routers with WPA2 or WPA3 encryption and update their default name and password.

It’s also recommended to keep your files backed up either on an external hard drive or in the cloud. This can protect you against data loss or when hackers encrypt your data and demand ransom to give you the decryption key. These ransomware attacks are growing in frequency and it’s estimated that they’ll [inflict](#) up to \$20 billion in damages by 2021.

“Ransomware attacks are on the rise — and they’re estimated to cost global organizations \$20 billion by 2021” – Cybersecurity Ventures 2020



5. Avoid phishing scams

As you go about your online life, scammers will try to trick you into giving out personal data such as your credit card numbers, passwords, and bank account details. Avoiding phishing scams requires constant vigor. To that end, there are many things you can do: access only secure (https) websites, don't click or download suspicious-looking links or attachments in emails, use only secure Wi-Fi networks, and beware of what personal information you share online. There are also Chrome extensions, such as Metamask, that warn you of URLs that are known scams.

Protect your crypto coins

As crypto coins grow in value, their owners are increasingly targeted by hackers. Tackling this threat requires practicing cybersecurity hygiene and protecting your privacy, identity, and investment details. If you happen to be a well-known crypto hodler, for instance, hackers are likely to target you.

Staying one step ahead of this threat also involves using the best wallet technology for safely storing and managing your coins. NGRIVE offers a series of products that ensure your crypto money, private keys, and seed data are all safely stored and protected. Transferring coins is safer, too. You can learn more about our [technologies](#) here and buy the NGRIVE ZERO hardware wallet via our online [shop](#).



5 Mistakes To Avoid With Crypto Hard Wallet Safety



So you've been a very good boy or girl, and Santa's brought you a shiny new crypto hardware wallet. You deserve a pat on the back for taking full responsibility for your crypto.

Now don't shoot yourself in the foot by making one of these five common mistakes of crypto hardware wallet safety.

#1 - Never share your Seed

Cryptocurrency is a hugely disruptive technology. Its potential impact has been compared to that of the internet. If you are an active crypto investor, congratulations, you are early. Your crypto portfolio could be very valuable in the future, so buying a cryptocurrency hardware wallet - the most effective means



of safely storing it - is likely to be one of the wisest investments you could ever make.

But you now own something more valuable than each of the individual coins you may be storing, it's called your wallet Seed. That 24 word recovery phrase provides ultimate access to all your funds, because that is how **Hierarchical Deterministic wallets (HD for short)** work. So consider it to be as valuable as your entire portfolio, and protect it accordingly.

That means never, ever, sharing your Seed with anyone. The device manufacturer has no reason to ask for your Seed; an exchange, wallet, DEFI/CEFI service, DAO has no reason to ask for your Seed; if your future-self travels back in time saying they've lost their Seed, you still shouldn't share it.

There is no circumstance under which you should legitimately need to share your Seed with anyone. Seer that mantra into your brain, tattoo NSYS behind your eyelids, paint it on your bedroom ceiling, so it's the last thing you see at night, and first thing in the morning. Never share your Seed. Hopefully we made that clear.

#2 - Don't store your Seed online or on a piece of paper

You now, hopefully, consider your Seed to be as valuable as your whole crypto portfolio. You know there's no circumstance where you should ever share it (see above), but you have no



choice but to store a copy of it somewhere.

You might be tempted to write it in a word doc, or text file, but that in essence, breaks the golden rule of sharing, because by storing it online, it could be accessed and malicious software could track your keystrokes.

Taking a photo and storing that in the cloud fails the test for the same reason. Don't store your Seed online, store it offline.

Yes, you could try and create a Sherlock Holmes style memory palace and just keep it in your head, but the risks are too great that you'll simply forget it.

Some cryptocurrency hardware wallet manufacturers, who we won't mention, ship their device with pieces of paper on which to write your Seed. Given your Seed is equal to the value of your entire crypto portfolio, are you happy to give it the same level of security that you would to a shopping list?

At the risk of stating the obvious, here are some of the reasons paper isn't a secure way to secure a valuable piece of information:

- It is destroyed by fire¹ (paper's ignition temperature is around 218-246 celsius, dependent on the age & thickness)
- It doesn't mix well with water, either directly, or from a damp or humid environment;
- It can be easily destroyed or discarded by accident



- It can easily be consumed by insects², pets or a rodents³
- It can be easily lost down a crack in a floor board, or just mislaid
- It is easily damaged by exposure to sunlight⁴

There is no easy solution to the Seed storage conundrum, as ultimately you will have to trust an offline medium, but you can do better than paper, such as punching the 24 words into a stainless steel plate.

Better still, if you buy an **NGRAVE COMBO** you'll get a two step stainless steel system - [GRAPHENE](#) - where each element is useless on its own, and only together reveals your Seed.

#3 - Don't use your hardware wallet in public

You are probably used to living your life on the go, thanks to your smartphone. You might want to treat your hardware wallet the same, taking it with you, just in case you need to make transactions on the go. This is a bad idea for a number of reasons:

- You open yourself up to public wifi which isn't secure
- The physical risk vectors to your device multiply on the move; including accidental loss/damage or theft.
- Someone can always be watching you directly, or on CCTV

You could mitigate loss/damage by buying a second device and using your Seed to create a clone, but this essentially doubles



the risk that someone can access the credentials that allow you to access your device.

#4 - Your device is the source of truth

Cryptocurrency hardware wallets are the safest form of storage because they are offline, prioritising security over convenience. Device manufacturers do, however, make every attempt within that crucial parameter to make transacting relatively painless by offering companion mobile or desktop Apps that can be connected to the device.

The NGRAVE ZERO, for example, has an mobile app [LIQUID](#), to sync all accounts and enable transactions, via QR code. The use of a second application layer introduces a security vulnerability known as the [Man In The Middle Attack](#) where the device hosting that secondary application - your laptop or mobile - is compromised.

In order to send or receive transactions using your hard wallet, you need to share address details, often using chat services and/or your device clipboard. The Man In the Middle attack uses the remote access they have gained to intercept/replace the shared address details with details of their own choosing.

If you are using an address for the first time, the only way you can know with 100% certainty that transaction detail hasn't been altered, is by treating the detail on the screen of your hardware wallet as the source of truth, and visually double-



checking it against the original address detail.

Most crypto hardware wallets come with limited screen space and poor quality screen resolution, making it hard to visually confirm the transaction information and rule out this threat.

The [NGRAVE ZERO](#) is designed with this in mind, featuring a large high density colour capacitive LCD touch screen, with high brightness.

#5 - Do a regular device check-in

Crypto hardware wallets are designed to provide cold storage for your coins. They act as secure offline vaults that you can put somewhere safe, providing peace of mind that your funds are safe.

If you are prone to impulse trading, or constantly checking your balance, cold storage has the added benefit of putting your funds out of sight and out of mind. There is, however, a danger in taking that approach too far.

Many hardware wallets require pins or access credentials to enable the owner to access the device. These are separate to the Seed which enables anyone/anywhere to access the funds without being in possession of the device. If you don't regularly use your device, the risk that you forget the device access pin increases, in which case your Seed is your only hope of recovery.



In order to mitigate your forgetfulness, you may be tempted to write down the access pin, which is just as bad as writing down your Seed - breaking rule no.2. You can avoid this by simply doing a device check-in, maybe once a month.

Better still choose a device that uses Biometrics (your thumbprint) for access, rather than a conventional pin. This is the approach taken with the [NGRAVE ZERO](#).

Beyond acting as a memory prompt, the regular check-in will provide the basic visual confirmation that your device is where it should be, and has not been moved by accident or bad intent.

The check-in can also confirm that your device is functioning properly and will recharge the battery. Like any piece of technology, there is always a risk that a component may fail, and though your Seed is your ultimate fail-safe, you shouldn't have to resort to that.

A hardware wallet has its own operating system, known as firmware which gets regularly updated to patch any potential vulnerabilities or to improve usability and support new coins or blockchain upgrades. Your regular check-in should include a firmware update as this will improve function and security, but paradoxically, the act of being online to access firmware updates can, in itself, expose you to threats, depending on the firmware security employed by the device.

Look for the highest level of firmware/OS security known as



Evaluation Assurance Level (EAL). It runs on a scale from 1-7, with EAL7 the highest.

The [NGRAVE ZERO](#) is rated EAL7 - for comparison banks and governments are typically EAL5 certified - and firmware updates will be cryptographically protected and only available through the NGRAVE website.

Owning crypto is a smart move. [Owning a cryptocurrency hardware wallet to store your crypto](#), is an even smarter move, but as we've hopefully demonstrated, there are plenty of pitfalls even once you've made the move to cold storage. The key is to not be complacent. Be aware of the common security mistakes made using, and owning, a crypto hardware wallet device, and your funds will be that much safer.



Get the latest crypto-security tips

Subscribe to the
NGRAVE [Blog](#) & [Academy](#) newsletter

