CRYPTO SECURITY

Our definitive guide to Crypto Security

COIN RIVET

Independent British blockchain and crypto news

PREVIOUS

WHY SECURITY MATTERS IN CRYPTOCURRENCY

THE CURRENT STATE OF SECURITY

BEST PRACTICES TO PROTECT YOUR FUNDS

HOW SAFE IF YOUR CRYPTOCURRENCY WALLET?

HOW TO SPOT A BITCOIN BLACKMAIL EMAIL SCAM

CONCLUSION

NEXT

CONTENTS

WHY SECURITY MATTERS IN CRYPTOCURRENCY

A cryptocurrency is a digital currency that uses cryptography to secure and verify its transactions, recording them in a decentralised and immutable ledger known as **blockchain**. Cryptocurrency can be used as a medium of exchange or a store of value, and can be traded in many exchanges around the world.

Cryptocurrencies operate independently from banks and act as an alternative form of payment to cash and credit cards. As such, it's becoming increasingly popular in countries where banking institutions are unstable, as people would rather have full control of their money in a digital space rather than rely on the banks to keep their money safe. Cryptocurrency offers an alternative, often decentralised, payment method. There's no single authority in charge and single points of failures are eliminated.

The original cryptocurrency, Bitcoin, was perceived as a reaction to the financial crash of 2008. Its intention was to give power back to the people, so the could achieve self-sovereignty over their own money. Sounds great, right?

Well, it could be. But cryptocurrency is by definition virtual. It attracts huge amounts of cybercrimes such as hacks, 51% attacks, and even traditional scam emails.

Not only this, but cryptocurrency is unregulated. With no central authority in charge, you are ultimately responsible for the protection of your own assets. If any instances of loss or theft of funds occur, there is nothing to say that you can get these back. With a lack of regulation comes a lack of protection.

THE CURRENT STATE OF SECURITY

Cryptocurrencies rely on cryptography and trustless, peer-to-peer networks, and consensus. However, that doesn't mean the industry isn't vulnerable to crime.

Your cryptocurrency funds will only ever be as secure as your approach to them. The choices you make, whether it's the exchanges and wallets you use or coins you choose to invest in, all need to be thoroughly researched. Below, we take a look at some examples of where security hasn't been up-to-scratch and the impact it has had on the crypto community.

Two hacker groups behind 60% of all crypto heists

A pair of hacker groups dubbed **Alpha and Beta** are believed to be behind cryptocurrency thefts totalling $1bn over recent years.

Analytics and security firm Chainalysis say the two groups account for 60% of all publicly reported crypto thefts. Alpha is described as "a giant, tightly controlled organisation at least partly driven by non-monetary goals." Beta was dubbed "a less organised and smaller organisation absolutely focused on the money."

Chainalysis wrote on their website that there's "no question" hacking will continue as it's the most lucrative of all crypto crimes.

> "The hackers typically move stolen funds through a complex array of wallets and exchanges in an attempt to disguise the funds' criminal origins. Once they feel safe, they move quickly. At least 50% of the hacked funds are cashed out through some conversion service within 112 days." – Chainalysis

$11 million stolen from prominent exchange

New Zealand-based cryptocurrency exchange Cryptopia suffered a malicious hack in early 2019, with **more than $11 million reportedly stolen** from the site.

The website experienced downtime due to forced maintenance, but the company released a statement on Twitter where they admitted a “breach” had resulted in “significant losses.”

A wallet with the suspected stolen funds was tracked down on Etherscan, with the total balance of tokens sitting at more than $11 million.

Cryptopia is one in a long line of cryptocurrency exchanges to be hacked over the years. In 2018, Japanese exchange Coincheck fell victim to the largest crypto heist in history, with more than $496 million being siphoned out of the site.

Crypto services hit by cyber attacks

MyEtherWallet, a service for managing cryptocurrencies, has experienced multiple hacks in a short space of time.

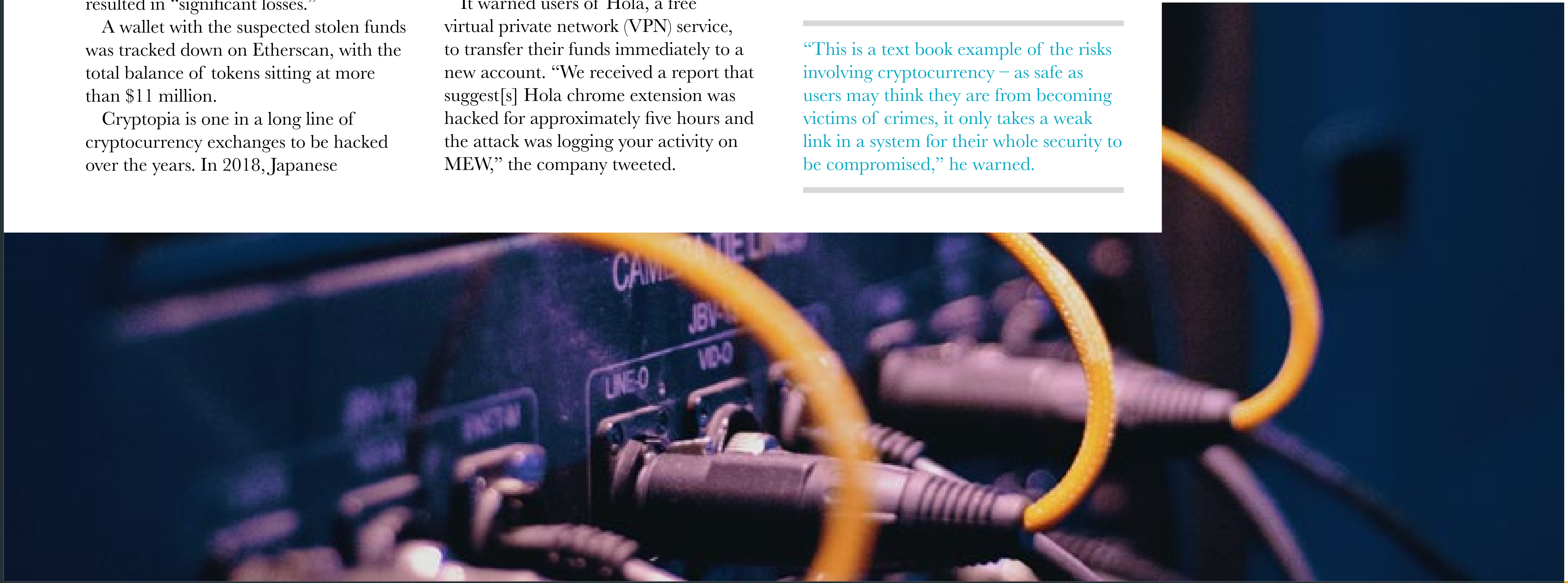
It warned users of Hola, a free virtual private network (VPN) service, to transfer their funds immediately to a new account. “We received a report that suggest[s] Hola chrome extension was hacked for approximately five hours and the attack was logging your activity on MEW,” the company tweeted.

It follows a similar incident in February 2019, when around $365,000 (£275,605) of crypto was stolen from users as a result of a domain name system (DNS) attack.

Raj Samani, Chief Scientist and Fellow at McAfee, said the spike in the value of Bitcoin at the end of 2017 promoted many cyber attackers to extend their activities into the hijacking of crypto wallets.

Samani said everyone, from small and big businesses to individual users, must do their due diligence. “This means making sure that there is a good combination of people, process and technology to effectively protect assets, detect threats and, when targeted, rapidly correct systems to keep cyber thieves at bay,” he adds.

> “This is a text book example of the risks involving cryptocurrency – as safe as users may think they are from becoming victims of crimes, it only takes a weak link in a system for their whole security to be compromised,” he warned.



BEST PRACTICES TO PROTECT YOUR FUNDS

With so many threats lurking in the cryptocommunity space, how can you keep your funds protected? Below, we take a look at everything you need to know about exchanges, wallets and identity management.

Let's look at exchanges. If you use a centralised exchange, you put trust in a third-party to protect your funds. If you use a decentralised exchange, you trade in a trustless environment but take on the responsibility of protecting your own funds.

Either way, be careful. Exchanges have been hacked before and they'll be hacked again. Research from ICO Rated revealed that 54% of all cryptocurrency exchanges have poor security in at least one area. It's important to explore each area and protect yourself as best you can. There are a number of things you can do.

Apply two-factor authentication

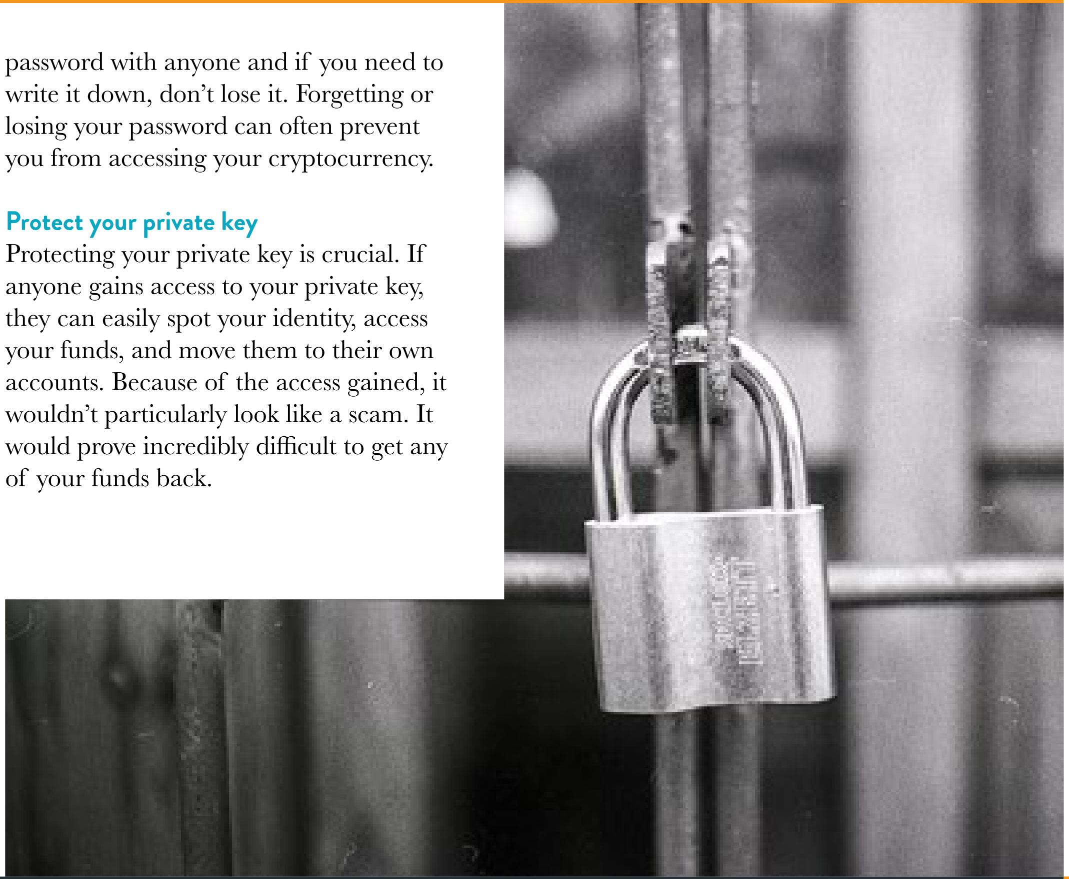
Two-factor authentication, commonly abbreviated to '2FA,' is a must. Most, if not all, the top exchanges utilise 2FA. This practice requires users to enter two layers of identification to access their accounts. This gives users extra assurances about the level of security available, while deterring cybercriminals from malicious activity. In instances where a hacker obtains your password, they would still need a second method of identification to access the account. This second method involves a human element that hackers aren't able to replicate.

Use strong passwords

Despite 91% of people knowing that using the same password for multiple accounts is risky, 59% still do it. Using a weak password or one that is used for another login can leave your wallet exposed to vulnerabilities. Intelligent hacking tools often have dictionaries embedded into them to search through possible password combinations. To strengthen your password you can use an original combination of numbers, letters, and special characters. Don't share your password with anyone and if you need to write it down, don't lose it. Forgetting or losing your password can often prevent you from accessing your cryptocurrency.

Protect your private key

Protecting your private key is crucial. If anyone gains access to your private key, they can easily spot your identity, access your funds, and move them to their own accounts. Because of the access gained, it wouldn't particularly look like a scam. It would prove incredibly difficult to get any of your funds back.



HOW SAFE IS YOUR CRYPTOCURRENCY WALLET?

Your wallet is where you store your keys, making it a huge target for scammers, hackers, and thieves. The type of wallet you choose and how you maintain its security is massively important.

Below, we take a look at the different types of wallets you could use and the benefits on offer.

Software wallets

Electronic wallets can be either downloadable software or possibly hosted on a cloud-based service. These can be mobile or desktop wallets. Hosted wallets more often than not focus on user-friendly interfaces. While they look aesthetically pleasing, you are placing trust in a third party to hold your private keys.

Some software wallets grant you security over your own keys. This is naturally safer than trusting a third party with your private keys, but you then have to make periodic backups. If you don't and your computer/device is compromised or simply stops working, you could lose all of your cryptocurrency. Don't forget that you can still be hacked with this type of wallet.

Hardware/offline wallets

Hardware wallets can take multiple forms. They can be as archaic as a piece of paper with a QR code split into two, with each piece hidden in a different location. As you could imagine, it would be a lot easier for a hacker to hack into your software-based wallet than get their hands on the two torn pieces of paper. But, if you lost the paper, or even just one half of it, you would find yourself in an unfavourable situation without access to your cryptocurrency wallet.

Some hardware wallets come in the format of USBs. These are usually small devices that can, if needed, connect to the internet to engage in transactions. In this instance, you would need to be careful not to lose your wallet. Hardware wallets minimise the risk of your wallet being hacked by an external party.

But by no means does this guarantee that your cryptocurrency is entirely safe; you must take care to look after the hardware wallet and not lose or damage it. A way to minimise heartbreak if this occurs would be to make a reliable backup of the keys, such as on multiple hardware wallets each hidden somewhere different but equally safe.

Hardware wallets are arguably safer than software wallets. This is because they are taken offline and immediately eliminate the threat of cyber criminals.

Which type of wallet is the best?

The safety of your cryptocurrency wallet is dependent on two factors:

- Which type of wallet you choose to secure your cryptocurrency
- How smartly you go about ensuring their protection

Serious investors in cryptocurrency may adopt an approach where they utilise more than one wallet. For example, they may have a cold wallet stored for their capital, but then own a spending wallet in which they may trade with or keep a spending balance in the interest of liquidity.

HOW TO SPOT A BITCOIN BLACKMAIL EMAIL SCAM

Scams aren't just isolated to exchanges and wallets. Old-school phishing emails are being brought back into the present date in the cryptocurrency industry.

Internet scams are very common, and they are becoming more difficult to spot every day. Here are some Bitcoin blackmail email scam red flags to look out for to ensure you don't end up having to pay a Bitcoin ransom.

(Note: If a legitimate hacker has gained access to sensitive information and is threatening to release it unless you pay a fee, you should always call the police.)

How do these scams arise?

Hackers may be able to obtain old passwords of yours and use them to try and scare you. They can do this by infiltrating a site you used a long time ago that had weak security. If you haven't used that password in a long time, you might be safe. If it's still your password, then you need to act fast. Hackers can also steal passwords if you've visited a site that had a lot of malicious malware on it. Malware can infect your computer, and this provides a window for a hacker or scammer to target you.

If you are being presented with an old password that is no longer in use, it's likely a scam. This is because if they had actually hacked you and wanted to put pressure on you, they would have chosen to reveal a newer password. If they do present you with your current password, this is where issues might arise and you should change your passwords immediately.

The most important thing to note with these scams is whether or not they have included other personal information. If it is only an old password, it tends to imply the scammer does not have anything else on you. If they do reference anything else about your personal life that can be leveraged against you, call the police.

One example of an email scam may read something like this:

> We have recorded you watching pornography sites behind your wife's back. If you do not want these videos released, then you must pay us $1,000 in Bitcoin.

This is common in Bitcoin blackmail email scams, since the most targeted gender is males (although many women have also been subject to similar scams). The threat may be completely fabricated and the hackers may be playing the odds in the hope that eventually a victim falls for their trap. Another example may read as below:

> You recently logged in to PayPal with the password 123456. If you do not pay us $1,000 in Bitcoin, we will hack your PayPal and take your full balance of $15,348.

Don't follow links from suspicious emails

Remember never to click on any links in suspicious emails, and always check the sender address to make sure any emails you receive that claim to be from reputable sources are legitimate. The level of spelling and punctuation is typically quite bad in these scams.

Make sure you protect all of your personal details. If other personal information other than your password is leveraged against you, and you cannot be sure it is not a scam, contact the police or other authorities.

CONCLUSION

Cryptocurrency is an unregulated industry so you must tread carefully. You are responsible for the protection of your own assets, so we recommend that you thoroughly research potential wallets and exchanges before making a final decision.

It also helps to keep on top of the latest news and keep up-to-date with evolving types of crime. At **Coin Rivet**, we make it easy to keep up-to-date with everything new in cryptocurrency.

Bringing you news, analysis, opinion and insight from the fast-moving blockchain world. Our team of journalists and contributors cover the likes of cryptocurrencies, wallets, exchanges and ICOs across a wide range of sectors including retail, fintech, banking and gaming. We go beyond the press releases and marketing hype to tackle all the industry topics that matter.

Featured in

FOX NEWS EXPRESS coingeek

coinrivet.com