BIZCOMMUNITY

Why cybersecurity needs to tighten up as cryptocurrencies plummet

By Dan Thornton

22 Jun 2022

Cryptocurrencies are surely living up to their description as 'volatile'. It is indeed dark days for all things crypto with the valuation of currencies, NFT prices, shares in public crypto exchanges and investment funds plummeting. Crypto investors, traders and miners are understandably, anxiously focused on the tumbling prices and the dire talk of a 'murky' future. However, there's never been a more important time to be concerned about cybersecurity and the widespread cybercrimes that flourish in the 'Wild West' territories of cryptocurrencies and crypto mining.

Image supplied

The latest crash in the crypto market might mark an ending for some, but for others, it is seen as an exceptional opportunity to get into the game. Many will sit tight, gripping their crypto wallets with white knuckles. What's important to know is that cybercrimes in the crypto market are real, and whatever your activities in response to the current situation, you need to make decisions and choices to optimise your cybersecurity and properly safeguard your digital assets.

Multi-million dollar crypto heists, crypto laundering and other money crimes take place across the sprawling, decentralised and unregulated cryptoverse. There are crypto hackers and scammers on every virtual corner. Crypto-jacking, phishing and crypto-malware attacks abound across illegal trading platforms and unregulated crypto exchanges. It's not surprising that cybercrimes thrive in a terrain that is so complex that even seasoned players are often perplexed.

These cybercrimes happen so easily because users most often secure their digital assets with a 'private key'. It might be a long, complicated password code, but if you keep it on your computer, it is so simple for a hacker accessing your computer to find it and log into your digital account. If your private key is stolen, there is no way to recover it, and there are no ways to redress your losses because you are solely responsible for keeping your private keys safe from hackers.

Hacker group RansomHouse threatens to sell Shoprite data
21 Jun 2022

If you are active on a well-known, large crypto exchange, you may think you have adequate protections. Many investors have a false sense of security that decentralisation means 'safer'. Some invest their life savings into these crypto exchanges even though they patently do not have the capabilities and accountabilities we take for granted in traditional banking and investment institutions.

The list of significant crypto exchange hacks is testimony to the dangers of believing 'it won't happen to me'. For example, in January this year, 483 customer accounts were breached on one of the world's most popular exchanges, Crypto.com, resulting in the theft of 4,836.26 ETH, 443.93 BTC and around $66,200 in other currencies. It is reported that over the past decade there have been more than 125 major cryptocurrency breaches leading to losses of more than $3bn.

Protecting your digital assets

In the current turmoil of the crypto market, it is essential to be especially vigilant about your cybersecurity, which ranges from how you protect your router, computers and mobile devices, to where you keep your crypto-keys. More often than not, cryptocurrencies and keys are kept in online or mobile wallets that make it easy to connect swiftly to exchanges and other services.

Many of these so-called hot wallets are provided by your crypto exchange so that you can link seamlessly to access your cryptocurrency or trade. However, this is the least secure way of holding your cryptocurrencies and presents the greatest vulnerabilities to hackers.

Manage your cryptocurrency risks better by:

- Using multi-factor authentication to access the exchanges you use
- Taking your wallets off-line
- Exporting your crypto keys to an external USB drive or storing them physically in a safe

Yes, these actions will somewhat compromise the speed and ease of accessing your digital assets, but they will also create important roadblocks that can prevent hackers from stripping your wallets bare.

It's important to keep in mind that like crime spikes during tumultuous times in the real world, exactly the same happens in the cyber world. Cryptocurrency volatility has gone stratospheric, the appropriate response is to be more protective of your digital assets than you have ever been.

ABOUT DAN THORNTON

Dan Thornton, CEO and co-founder of GoldPhish Cyber Security Training, is a former Royal Marine Commandos Officer. During his seven years of service, he was deployed all over the world including multiple operational deployments leading teams in both Iraq and Afghanistan. He then transitioned from the military into a career in Corporate Security Risk Management helping international oil and gas companies operate safely and securely in some of the most high-risk locations around the world, including West Africa, North Africa, and the Middle East.

- SA shoppers warned of online scams ahead of shopping season - 20 Oct 2022
- Building cyber-savvy workplaces in SA - 3 Oct 2022
- Cyber savvy parents keep kids safer online - 22 Aug 2022
- Cyber fraud has steep collective costs - 27 Jul 2022
- Why cybersecurity needs to tighten up as cryptocurrencies plummet - 22 Jun 2022

View my profile and articles...