Cryptocurrency scams are on the rise in SA: How crypto cons work and how to protect yourself

Issued by ESET

22 Apr 2022

"The digital gold rush is here. As more people attempt to make money from cryptocurrencies, criminals and con artists aren't far behind. Make sure you know how to recognise the biggest schemes that want to part you from your digital coins," says Carey van Vlaanderen, CEO of ESET South Africa.

Carey van Vlaanderen, Chief Executive Officer (CEO) of ESET South Africa

The world seems to have gone ‘crypto-mad’. Digital currencies like bitcoin, Monero, Ethereum, and even Dogecoin, are all over the internet. Their soaring value promises big wins for investors (if you’re “buying the dip”, that is). And the ‘fortunes’ to be made by mining for virtual money have echoes of gold rushes that formed the first mining towns in South Africa back in the 1800s. Or at least, that’s what many, including a long list of scammers, will have you believe.

In reality, if you’re interested in cryptocurrency today, you’re quite possibly at a major risk for fraud. In many respects, in this new unregulated world, bad actors often have the upper hand. In 2021, South African-based Africrypt was reportedly hacked, effectively wiping out a staggering R51bn of investors’ money. While the apparent hack made global headlines, the founders of Africrypt vanished as international investigators scrambled to piece together what happened in what is now suspected to be a completely fraudulent cryptocurrency investment platform.

The good news is that normal rules of fraud prevention apply too. Everything you read online should be carefully scrutinized and fact-checked. Don’t believe the hype, or buy into something that seems too good to be true, and you’ll stand a great chance of staying safe.

Why are cryptocurrency scams on the rise?

Fraudsters are masters at using current events and buzzy trends to trick their victims. And they don’t come much more “zeitgeist-y” than cryptocurrency. Headlines and social media posts are partly to blame, creating a feedback loop that only adds to the hysteria over virtual currencies.

- There are few if any regulations governing the cryptocurrency market for investors, versus the traditional stock market
- Huge media interest makes it a regular hook for phishing and scams
- Soaring cryptocurrency prices attract consumers dreaming of getting rich quick
- Social media helps to amplify the buzz, real or fictional
- There's also the lure of mining coins for money which phishers can use as a hook

What are the most common cryptocurrency scams?

If you have virtual money safely stored in a cryptocurrency exchange, it may be at risk from hackers. On numerous occasions threat actors have successfully managed to extract funds from these businesses, sometimes making off with hundreds of millions. However, usually the breached companies will promise to recompense their blameless customers. Unfortunately, there are no such assurances for the victims of crypto fraud. Fall for a scam and you may be out-of-pocket for a lot of money.

It pays to understand what these scams look like. Here are some of the most common:

Ponzi schemes: This is a type of investment scam where victims are tricked into investing in a non-existent company or a "get rich quick scheme," which in fact is doing nothing but lining the pocket of the fraudster. Cryptocurrency is ideal for this as fraudsters are always inventing new, unspecified 'cutting edge' technology to attract investors and generate larger virtual profits. Falsifying the data is easy when the currency is virtual anyway.

Pump and dump: Scammers encourage investors to buy shares in little-known cryptocurrency companies, based on false information. The share price subsequently rises and the fraudster sells their own shares, making a tidy profit and leaving the victim with worthless stocks or coins.

Fake celebrity endorsements: Scammers hijack celebrity social media accounts or create fake ones, and encourage followers to invest in fake schemes like the ones above. In one ploy, some $2m was lost to scammers who even name-dropped Elon Musk into a Bitcoin address in order to make the ruse more trustworthy.

Fake and copycat exchanges: Fraudsters send emails or post social media messages promising access to virtual cash stored in cryptocurrency exchanges. The only catch is the user must usually pay a small fee first. The exchange doesn't exist and their money is lost forever. Copycat sites offer what appears to be legitimate wallet services. Users are encouraged to download wallets which then install malware on the user's device. In these instances, iOS devices have been compromised where in the past the problem was limited to Android.

Impostor apps: Cybercriminals spoof legitimate cryptocurrency apps and upload them to app stores. If you install one it could steal your personal and financial details or implant malware on your device. Others may trick users into paying for non-existent services, or try to steal logins for your cryptocurrency wallet.

Phishing: Phishing is one of the most popular ways fraudsters operate. Emails, texts and social media messages are spoofed to appear as if sent from a legitimate, trusted source with an urgent request for payment in cryptocurrency.

How you can avoid falling victim

The best weapon to fight fraud is a healthy dose of scepticism. With that in mind, try the following to avoid getting scammed:

- Never provide your personal details to an entity that makes unsolicited contact with you, via email, text, or social media. It may even appear to be your friend, but in reality could be a hacker who has hijacked their email or social account. Check with them separately via another contact method
- If something is too good to be true it usually is. Take any investment scheme with a heavy pinch of salt
- Switch on two-factor authentication for any cryptocurrency account you have

- Dismiss any investment ‘opportunity’ which requires an up-front payment
- Never use unofficial app stores
- Download anti-malware software from a reputable provider to your PC and mobile devices

The world may have gone cryptocurrency-crazy. But you don’t need to join in. Keep a cool head and ride out the hype while making good returns.

- **Eset launches solution to address SOHO security concerns** 15 Apr 2024
- **Don’t gamble with your cybersecurity** 29 Feb 2024
- **Avoiding job scams, and finding a job you love** 9 Feb 2024
- **Sharenting and security concerns: Will you be posting that back-to-school photo?** 10 Jan 2024
- **Fighting the digital grinch: Cybersecurity tips for kids and parents for a safe festive season** 8 Dec 2023

ESET

ESET has been helping people protect their digital worlds for more than three decades. From a small, dynamic company we've grown into a global brand with over 110 million users in 202 countries.
Profile | News | Contact | Twitter | Facebook | RSS Feed