BIZCOMMUNITY

Prioritise keeping your Bitcoin safe, secure, and available

By Claude Schuck

16 Mar 2018

When I was a child, the prospect of going to a theme park was a wild and exhilarating experience, however now it doesn't quite stir up the same feelings! Similarly, the ownership of cryptocurrency isn't the rollercoaster ride it used to be even though it is still perilous.

While the trading of a cryptocurrency is still full of massive ups and downs as the market volatility continues, the instability and risk of your digital wallet is a consistent threat. These aren't just abstract or theoretical; new scams crop up, and old ones resurge, all the time.

Whether it's a fake wallet set up to trick users, a phishing attempt to steal private cryptographic keys, or even fake cryptocurrency schemes, there’s something to watch out for at every turn.

So, what would happen should someone lose access to their virtual wallet or it becomes unavailable?

Availability of data has become a priority for businesses across industry sectors, indeed it’s an area we built our business around. It is now common for digitally savvy consumers to have some method of backup or a duplicate copy of their key documents, photographs, and other important information. Yet, there is seemingly not much thought given to what the damage will be if a digital wallet gets ‘misplaced’.

Just consider the financial consequences if one is unable to access thousands of rands of Bitcoins (if not more) because you cannot remember where the password is stored, or the wallet is being hosted, or even lose a local drive containing your currency.

Just as it pays to put your watch or other jewellery in a safe deposit box, so too does a little effort into how you manage your cryptocurrency.

Lost cause

A recent article shows just how significant the extent of this can be.

An IT worker in the UK kept 7,500 Bitcoins (almost R930-million) on his laptop. However, after it broke he sold the computer for spare parts but kept the drive. Unfortunately for him, he mistakenly put the drive in a waste bin at a local landfill site while cleaning his house in 2013.

Following the surge in the currency in recent months, he now wants to go find it. Needless to say, the health and safety regulations of trying to dig around four years' worth of landfill has seen the council reject his requests for trying to locate the drive.

Inundated with data but not gaining enough insights?
JP Smith 23 Feb 2018

This and many other examples on the internet should spur even the most sceptical of people into action. Even though the financial impact is significant (and potentially devastating), one should take care of applying the same availability rules to digital wallets and cryptocurrencies as is done to all important data.

Don't bank on an online backup

The most critical of these is the 3-2-1 principle. It states that you should have at least three copies of your data, store the copies on two different media, and keep one backup copy offsite and off the internet. You might even consider making a backup to leave in a safe deposit box with your watch – just make sure you encrypt it first!

For obvious reasons you cannot duplicate your digital wallet or cryptocurrency, but you can still ensure you do not keep it at your physical location and off the internet.

Going with a reputable service provider for the safe storage of your cryptocurrency (there are several sites in South Africa that does exactly that) is the best way of avoiding loss if your drive gets stolen or compromised.

> *"Despite it being digital, if cryptocurrency is lost, such as in the case of the hard drive in the landfill site, it is gone forever. Imagine it as real cash left in a burning house."*

Difficult market
But it is not only data that needs to be kept safe. South Africans recently joined thousands of people from around the world in falling prey to a Bitcoin scam that resulted in losses of more than $50m. Promising unrealistic weekly returns of 14% in exchange for an investment of close on R12,000, this turned out to be too good to be true.

Even before news of the scam broke, the South African Reserve Bank (SARB) stated its intention to review its position on private cryptocurrencies. This entails assessing the growth of fintechs and to consider the regulatory implications of

cryptocurrency.

Your guide to the top three cloud computing trends of 2018

Brett St Clair 8 Feb 2018

Beyond that, investors should consider the consequences if exchanges should go down and they are left unable to trade their cryptocurrencies. One such recent example is the Kraken exchange that was taken down for scheduled maintenance but was only up and running after a delay of more than 48 hours, with investors unable to trade during a highly volatile period on the market, meaning they lost out on significant returns.

Just imagine something like this happens on a real exchange operating in pounds, dollars, and a myriad of other currencies.

Maintaining your strategy

Returning to our aforementioned IT worker, he might eventually be able to find the drive and access those coins but the chances of that happening are close to zero.

> *"However, if the cryptocurrency had been stored in the cloud then he will always be able to access it – as long as he hadn't lost the wallet seed or access key to do so too."*

Cryptocurrencies, very much like our reliance on data, are here to stay. It's not just the trading aspect that poses a risk, it is about how best you approach your investment's accessibility and backups. Putting the appropriate steps in place and ensuring the availability and continuity of access to your digital wallet will rely on proven strategic principles that big businesses adopt with their critical data.
Much like the IT bubble of the 90s, users must resist the temptation to blindly adopt the 'shiny and new' if it is at the expense of traditional operating procedures. It is best to combine the strengths of both elements to keep that cryptocurrency safe.

Thankfully you don't need to be a cryptography expert to take some of these basic security steps to protect yourself against most attacks. And if nothing else, don't lose that wallet seed or access key, or risk taking a ride on not just a financial rollercoaster, but a security one too.

ABOUT CLAUDE SCHUCK

Claude Schuck is the regional manager for Africa at Veeam.

- Compliance requires an evolved availability approach - 16 Apr 2018
- Prioritise keeping your Bitcoin safe, secure, and available - 16 Mar 2018
- #BizTrends2018: Welcoming a new era of availability - 22 Jan 2018
- PoPI requires effective data management structures - 31 Oct 2017
- Addressing the risks of data loss - 11 Sep 2017

View my profile and articles...