Forbes

Beware The New Crypto Scam Floating About

By Erik Sherman
Freelance business, economics, finance, and tech journalist.
July 31, 2022

Aside from all the problems regularly appearing in the cryptocurrency space, there are also many crooks ready to relieve people of the coins they are holding, no matter how much the value has dropped.

The line of break-ins, exploits, and scams is never-ending. Plus, no matter how much someone like Senator Kirsten Gillibrand (D-N.Y.) says in an interview with Bloomberg Technology that "the interesting nature of blockchain technology is that it's a hundred percent transparent, so if you want to trace who bought or sold something through cryptocurrency, you can do that pretty easily," you can't. Having an online address is not the same as having someone's identity.

It's up to the consumer—that is you—to be careful and know when something might smell fishy and require being wrapped in old newspaper and tossed into the trash.

But as happens with technology, the scam use of it also continues to advance, as is apparent in a forfeiture filing by the United States Attorney's Office for the Central District of California. The defendant: "Approximately 40.997711 EthereumETH -1.1% Digital Currency."

As the complaint reads, “P.M. is a resident of, and does business within, Orange County, California, within the Central District of California. P.M. controls an investment vehicle which invests in digital currencies, including Ethereum.”

So, there’s an owner of Ethereum cryptocurrency, whose identity is being protected, that maintained a cryptocurrency wallet with Coinbase.

“On or about December 21, 2021, the victim, P.M., received a pop-up message identifying an error while attempting to log into the Victim Account held at Coinbase on his laptop,” the complaint continues. “The pop-up message stated, ‘Due to a recent activity your account has been blocked. Please contact our support team at +1-810-420-8046 to remove account restrictions.’ P.M. called the identified telephone number and was connected to someone purporting to be a Coinbase representative. The individual P.M. spoke with identified himself as Ankit Anwaral (‘Ankit’). Ankit knew P.M.’s log in information and P.M.’s current location. Ankit stated to P.M. that, in order to authenticate his information, P.M. needed to transfer his cryptocurrency balance from his Coinbase account to a Coinbase Pro account, which was a more sophisticated account designed for investment professionals. Ankit directed P.M. to download a remote desktop application called ‘Anydesk’ onto his laptop to allow Ankit to remotely control P.M.’s computer. Once P.M. did so, persons unknown began to transfer P.M.’s funds. Shortly after, P.M. noticed that 40.997711 Ethereum, valued at $165,145.40 at that time, had been transferred out of the Victim Account. Due to Ankit’s misrepresentations, P.M. did not realize he had been defrauded until the full contents had been transferred out of the Victim Account.”

The cryptocurrency then went through “numerous transfers before being reassembled in other wallets in order to conceal the corrupt source.” (Again, when someone says that all blockchain activity is “transparent” and that people’s identities are easily discovered, you can disregard the individual as someone who knows far less than they think.)

“The thing that struck me about this, I was impressed by the fact that the DOJ was filing such a civil enforcement action,” says Tal J. Lifshitz, a partner in Kozyak Tropin & Throckmorton 's complex litigation department and co-chair of the firm's cryptocurrency, digital asset, and blockchain group. He adds that “999 times out of a thousand,” the Department of Justice answer to someone filing a complaint would be, “We understand you Mr. Victim were defrauded but it’s your own fault.”

But there’s a federal lawsuit instead, very possibly because the person who was defrauded is well-connected.

Commonly, people get duped by scams that prey on fear or greed. There’s typically a red flag. Giving a phone number to call is one of them. You always call the main number of the company and asked to be transferred to the person or something like a fraud department.

However, in this case the fraudster had some significant information about the victim. Was it malware that was on the person’s computer and providing data that would be convincing? Some kind of penetration of Coinbase’s systems? Maybe it was a different type of mechanism.

Whatever it was, reputable companies will not have someone online giving you a phone number to call because it’s too redolent of a scam.

Be aware that when there’s a lot of money potentially changing hands, there are people who won’t blink twice at trying to confuse you into doing something foolish. Take your time to do the basics like calling the company through an independently provided number, ask questions. Anyone trying to push you past the speed to intelligent consideration is someone not to trust.

Follow me on Twitter or LinkedIn. Check out my website.