BCSI Investigations

April 5, 2022, Volume 12, Issue No. 2

The Investigator Newsletter

A Pandemic of Cybercrime!

by Denis Gagnon LPI - President

Recently hundreds of millions of cryptocurrencies have been stolen at the Ronin Network, which provides the blockchain "Bridge."

The Hack saw 173,600 ether (the native currency of Ethereum blockchain) and 25.5 million USD Coin stolen, totaling US$625 million in value.

This is believed to be the largest cryptocurrency fraud to date.

The Statistics

Canadian statistics for 2022 demonstrate the extent of the problem. As of February 28, 2022, there were 12,252 reports of fraud and 7,922 victims of fraud, and a reported loss of $75.5 millions.

It is believed that the crime is underreported as many individuals feel shame and are embarrassed to report the loss, in some cases to the extent of their life savings.

Due Diligence

BCSI recommends that everyone performs an in-depth due diligence on the companies you are considering managing and processing your cryptocurrencies transactions.

Scams online are getting more sophisticated. Often the scammer will layer the fraudulent activities by accessing the victim under false pretenses on a dating site, for example, and then shift to asking the victim for money. The original approach can be by phone, e-mail, text messages, or through other internet portals.

Due diligence on the party who is contacting you as well as the accuracy of the financial information, is key.

Risk/Benefit Analysis

A risk/benefit analysis is a must. The best approach is to not invest with strangers. It is critical that you do not succumb to the urgency approach.

For individuals, BCSI recommends:

- Do NOT be afraid to say no
- Do NOT give out personal information
- Do NOT invest with individuals you meet on dating sites unless you know them for a long period of time.
- Do extensive research
- Beware of upfront fees
- Protect your computer data and I.P. address with a VPN
- Be careful of posting too much on social media
- Protect your online accounts

For business, BCSI recommends:

- Know your clients (KYC)
- Do NOT give out information on unsolicited calls
- Limit your employees' authority
- Watch for anomalies

Once you have been defrauded

Due to the sophistication of criminals, it is possible that you will still get defrauded, even with the best preventative measures. The first thing to do is document all interactions with the suspect (s) from the day you started communicating, including all text messages and emails.

You can then report it to the Canadian anti-fraud center, your police department and hire BCSI to conduct an in-depth investigation of the fraud.

Feel free to contact us for a complimentary consultation at 604-922-6572.