CryptoCurrency Warning

Don’t Let Your Members Be Led to “Slaughter”

By Collen Kelly

The latest crypto-related investment scam, referred to as “pig slaughter” or “pig butchering”, involves sophisticated, yet phony, cryptocurrency investment platforms. Initially, investors invariably see fantastic returns on their investments, which encourages them to deposit additional funds in order to generate increasingly higher “returns.” In some scams, the victim is permitted to withdraw the value increase, with the effect of making them feel comfortable with the phony platform and invest more and more funds.

The trend originated in Southeast Asia, and the name refers to the way in which hogs are “fattened up” before ultimately being led off to slaughter. In this case, the victims get “slaughtered” after the scammer successfully convinces them to “fatten” their phony investment account over a period of time. The “slaughter” involves the scammer emptying the victim’s “investment account” and disappearing with the funds. According to the Secret Service, “once the victims see how easy it is to invest and how well their investments are doing, they can end up investing their entire life savings in a matter of days.”

A majority of victims who fell for these scams said that it started with an advertisement or solicitation posted to social media, usually Instagram, Facebook, or LinkedIn. Dating sites are sometimes used, as well. Curious investors are directed toward elaborate and official-

looking online crypto platforms that appear to have thousands of active investors. Many of these platforms include extensive study materials and tutorials on cryptocurrency investing. New users are strongly encouraged to team up with more seasoned investors on the platform, and to make only small investments that they can afford to lose.

According to the Federal Trade Commission (FTC), Americans have lost over $1 billion to crypto-related scams since January 2021, and a little over half of the money lost – or $575 million – has gone to investment scams, like pig butchering.

The people creating these phony profiles are largely men and women from China and neighboring countries who have been kidnapped and trafficked to places like Cambodia, Laos, Myanmar, and other parts of Southeast Asia. They are forced to work in "industrial-scale scam centers" that work around the clock to find new victims. Law enforcement state that these "dark versions of customer service call centers work similarly to corporate offices, except for the fact that all of the employees have been kidnapped and forced to commit fraud via violent coercion." Survivors of the labor traffickers running these scams describe long hours and abusive treatment. Horrific videos have circulated on social media that show shackled young men being electroshocked in these "customer service centers."

The scammers will work through a pre-set script that is tailored to their prey's apparent socioeconomic situation. For example, a divorced, professional female who responds to these scams will be handled with one profile type and script, while other scripts are available to groom a widower, a young professional, or a single mom. The Secret Service reports that victims "run the gamut from young professionals early in their careers, to senior citizens and even to people working in the financial service industry." Law enforcement report that they "have seen nothing like this before", as this scam is stealing hundreds of millions of dollars from even educated investors. Unlike most other cybercrimes, the FTC notes that younger people, specifically people in their thirties, are the most likely to fall for these kinds of scams.

As a credit union, we must educate our members about this trending cybercrime. Encourage our members to be alert and wary of new acquaintances recommending high-yield cryptocurrency investments.

Red flags include:

- A random test or email from someone you don't know, engaging you in frequent conversations. This could also be a wayward SMS, such as an instant message about an Uber ride that never showed up, or a reminder from an unknown person

about a coffee date. The message is irrelevant, the goal is to simply get a curious recipient to respond in any way.
- The new acquaintance avoids phone or video conversations.
- The conversation quickly turns to an investment that is earning the new acquaintance high returns. The scammer may boast about houses in several locations, or mention owning expensive cars, taking exotic holidays, and having hired staff. Watch out for Instagram Millionaires!
- The conversation if flirtatious and the new acquaintance praises you, mostly when talking about investments. The conversations about other topics are short, and the scammer may threaten to stop communicating.
- The new acquaintance describes what you can do with your new investment returns and how they can improve your life. The scammer may also focus your attention on the return that you made on a small investment and how much more you could have made if you had invested more. This often convinces people to invest more than they can afford to lose.

Unlike typical investment scams that pressure victims to invest NOW, the pig butchering scam relies on priming a victim over time, slowly exposing them to the idea of investing cryptocurrency – then goes for the big "slaughter". This is often referred to as "the long con".

Please let the credit union know if you feel you have been contacted.

A special thanks to Emma Pirlot, BSA Compliance Officer, Forward Financial CU, for sharing her inside knowledge about this type of scam from the member's perspective, which inspired the article.