

Cybercurrency ‘Pig Butchering’ Scam

Introduction

A recent cryptocurrency scam has highlighted a need for fraud awareness. The new scam - called “pig butchering” - includes a sophisticated new twist that combines a romance scam with an investment spin. According to the Federal Bureau of Investigation (FBI), the term “pig butchering” refers to a time-tested, heavily scripted, and contact intensive process to fatten up the prey before slaughter

How it Works

Pig butchering scams originated in Southeast Asia and are spreading globally. This scam is predominately executed by a ring of cryptocurrency scammers who mine dating apps and social media sites in search of victims. It involves a con artist creating a fake profile used to reach out to potential victims often through social media, WhatsApp, Tinder or other dating sites, and even random texts, masquerading as an incorrect number or an old acquaintance. The goal is to initiate a cordial discussion with the victim, attempting to be their “new friend” or “lover”.

The new friend creates reasons to continue a conversation, which leads to multiple calls. They slowly develop a relationship so they can insert themselves into their victim’s daily life. While building trust with the victim, they slowly introduce the idea of making a business investment using cryptocurrency. The new friend employs persuasion rather than requesting money outright because they are aware that individuals are savvy and know that being asked for money by a stranger is a sign of a scam. The victim is gradually drawn into what appears to be benign talk about cryptocurrency investments and earnings, but they are really being manipulated to make an investment.

The new friend slowly convinces the target to invest in cryptocurrency and refers them to a bogus website or app that looks authentic but is controlled by the

scammer. The victims are encouraged to invest small amounts in the beginning and the scammer will make sure to post a modest gain on the investment. They may even allow the victim to withdraw money once or twice to convince them the process is legitimate.

The victim is then persuaded to invest larger amounts on the fake platform, sometimes hundreds of thousands of dollars. Once the money is sent to the fake investment app, the scammer vanishes, taking all the money with them, resulting in significant losses for the victim.

While pig butchering often uses romance as a tactic, scammers can also build other types of personal or professional relationships. They are experts who are trained to manipulate their targets, making it is easy for someone to fall prey to this scam.

Consumers must always remain vigilant and alert for scams, especially as new financial products like bitcoin and other cryptocurrencies become popular. Just as with any major financial decision, consumers should research the investments they are considering; avoid people or entities demanding upfront payment in cryptocurrency; be wary of promises of large, quick returns; and refrain from mixing online dating with any investment advice.

What to Do

Look for Red Flags

- ❑ Strangers sending seemingly innocuous text messages out of the blue.
- ❑ Strangers who quickly try to move the conversation to WhatsApp or another social media site.
- ❑ People who avoid video-calling with multiple excuses or flatly refuse to initiate any kind of video-calling.
- ❑ People chit-chatting about their insider investment knowledge.
- ❑ The URL of the investment platform doesn't match the official website of a popular cryptocurrency market or exchange but may be very similar.
- ❑ The investment app generates warnings of being "untrusted" when launched, or the computer's antivirus software marks it as potentially dangerous.
- ❑ The investment opportunity sounds too good to be true.

Follow these tips to protect yourself:

- ❑ Don't send money, trade, or invest with a person you have only met online.
- ❑ Don't speak of your financial position or investments.
- ❑ Don't share personal information or current financial status with strangers.
- ❑ Don't provide your banking information, social security number, copies of your identification or passport, or any other sensitive information to anyone online or to a site that you cannot verify is authentic.
- ❑ If an online investment or trading site promotes unbelievable profits, it is most likely just that—unbelievable.
- ❑ Be cautious of individuals who claim to have exclusive investment opportunities and urge you to act fast.

Cryptocurrency scams have bilked billions of dollars from unsuspecting investors and most people who lose funds don't recover the money. It is estimated that worldwide losses were in the tens of billions of dollars in 2021 alone, making the pig butchering scam a "super scam."

Work Cited:

Cryptocurrency Scam – Pig Butchering as found at [Cryptocurrency Scam - Pig Butchering \(michigan.gov\)](https://michigan.gov) on September 12, 2023.