PIG BUTCHERING SCAMS PROLIFERATE

BY JAY BORDEN

Let's begin with a simple definition of pig butchering - a romance scam and an investment scam combined.

It begins with scammers finding likely targets on dating apps or social media by pretending to be attractive young women. VPNs are used to mask the scammers' locations to circumvent any country restrictions of the dating app or SM platform.

Once they get a target interested they will often switch to video using young models on their payrolls to convince the target they are really speaking to an attractive young woman. The backgrounds used for the dating app or social media always indicate wealth with luxury condos, locations, and automobiles.

Once the target is convinced, the model will then suggest switching to a messaging service like WhatsApp or Telegram and get the dating app or SM out of the conversation. This is done to prevent the platforms from attributing too much traffic to the scammers and banning them.

With video out of the way, the conversation reverts back to the scammer and the target. This interaction will continue for a while with the target still believing it is the attractive model he saw. At some point the scammer will mention that a friend introduced them to a way to make a lot of money and they want to share it with the target who is now a "friend."

The method involves using an app to trade cryptocurrency and take advantage of different prices on different platforms. The target doesn't need any knowledge or experience because the app they suggest downloading takes care of it all. The target just needs to make an initial purchase of crypto using the app. The app will then make suggestions on when to buy and when to sell and of course where to do it.

PIG BUTCHERING SCAMS PROLIFERATE

CONTINUED

The app offers reports and graphs to show how investors are doing. But the scammers manipulate the graphs to indicate profits. Then encourage the target to add more money to the account to make even more profit.

When enough people become aware of the app name and its reputation, the scammers delete it and issue it again under a different name.

Really, the target owns little to no crypto. The money they invested went right into the scammer's wallet.

If the target wishes to sell crypto to realize the profits, the scammers will often send money to the target if the amount requested is small enough. But if it is too large or requests too frequent, they won't send anything and the target will quickly realize they've been scammed and walk away. They probably won't admit it to anyone out of embarrassment.

Dubai is a popular location for the scammers. To give an idea of how lucrative this is, an entire building complex was used by the scammers with hundreds or even thousands of scammers living and working there. The scammers are often migrants who are lured in with promises of legitimate jobs. Their passports are held by the operators of the scam to prevent escape.

The scammers use sophisticated computers with a program that manages multiple WhatsApp and Telegram conversations and automatically translates between the language used by the scammer and the one used by the victim. There is also a Google Translate window just in case the other translation program doesn't understand something.

Another window is Telegram messaging to communicate with their supervisor and the other scammers.

Be very careful!

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.