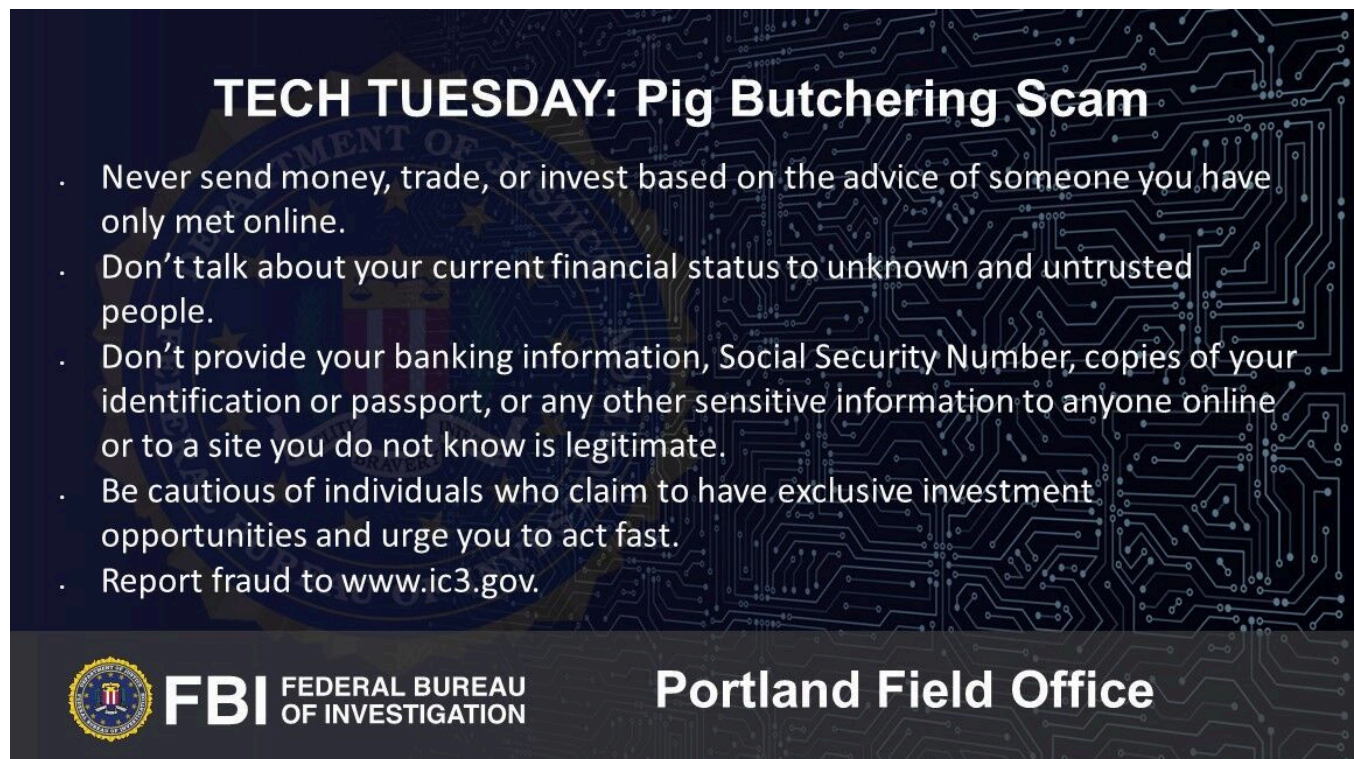


Tech Tuesday: Building a digital defense against a new cryptocurrency scam called Pig Butchering

April 6, 2022

A graphic with a dark blue background featuring a circuit board pattern. In the center is a faint, circular seal of the Federal Bureau of Investigation. The text is white and bold. At the top, it says 'TECH TUESDAY: Pig Butchering Scam'. Below that is a list of six bullet points. At the bottom left is the FBI logo and the text 'FBI FEDERAL BUREAU OF INVESTIGATION'. At the bottom right is the text 'Portland Field Office'.

TECH TUESDAY: Pig Butchering Scam

- Never send money, trade, or invest based on the advice of someone you have only met online.
- Don't talk about your current financial status to unknown and untrusted people.
- 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 you do not know is legitimate.
- Be cautious of individuals who claim to have exclusive investment opportunities and urge you to act fast.
- Report fraud to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Welcome to the Oregon FBI's Tech Tuesday segment. Today: Building a digital defense against a new cryptocurrency scam: Pig Butchering.

The Pig Butchering scam pulls on heartstrings and purse strings.

The fraud is named for the way scammers feed their victims with promises of romance and riches before cutting them off and taking all their money.

It's run by a fraud ring of cryptocurrency scammers who mine dating apps and other social media for victims.

And the scam is becoming alarmingly popular.

In 2021, the FBI's Internet Crime Complaint Center received more than 4,300 complaints related to crypto-romance scams, resulting in more than \$429 million in losses.

The scam started in China in late 2019, but, as those numbers indicate, it's now becoming more prevalent in the United States. Scammers are using translation programs to communicate seamlessly with their victims.

Victims have very similar stories: Meeting someone on a dating app, the scammer gains the confidence and trust of the victim, and then claims to have knowledge of cryptocurrency investment or trading opportunities that will result in substantial profits. The victim is then directed to transfer large amounts of cryptocurrency from the exchange account to cryptocurrency wallets controlled by fraudsters, ultimately losing it all.

Here's how to protect yourself:

Never send money, trade, or invest based on the advice of someone you have only met online.

Don't talk about your current financial status to unknown and untrusted people.

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 you do not know is legitimate.

If an online investment or trading site is promoting unbelievable profits, it is most likely that—unbelievable.

Be cautious of individuals who claim to have exclusive investment opportunities and urge you to act fast.

If you are the victim of any online fraud, you should report the incident to the FBI's Internet Crime Complaint Center at www.ic3.gov or call your FBI local office.