

Tech Tuesday: Building a Digital Defense Against Crypto Romance Scams

September 28, 2021

A graphic with a dark blue background featuring a circuit board pattern. In the center is a large, faint circular seal of the Federal Bureau of Investigation. Overlaid on the seal and background is the text "TECH TUESDAY: Crypto Romance Scams" in bold white letters. Below this, there is a bulleted list of four items. 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" in bold white letters.

TECH TUESDAY: Crypto Romance Scams

- Never invest with someone you only know online.
- Don't provide personal or financial info to those you only know online.
- Be wary of promises of extraordinary profits with online traders.
- Report online crimes 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 crypto romance scams.

The FBI's **Internet Crime Complaint Center** is seeing a rapid rise in the number of people who are falling victim to a new-style romance fraud. In just the first seven months of this year, more than 1,800 people have reported online romance scams resulting in losses of about \$133 million.

Romance frauds have been around for a long time, and they usually start in the same way. The scammer's initial contact is typically made via dating apps or other social media sites. The scammer gains the confidence and trust of the victim – convincing the victim that their virtual love match is the real deal.

The new twist comes when the bad actor claims to be an expert cryptocurrency investor. He offers to help the victim make big money, too. Once the victim invests, the scammer allows the victim to withdraw a small amount of profit from the alleged account.

After the successful withdrawal, the scammer instructs the victim to invest larger amounts of money, and he often pushes the victim to "act fast." When the victim is ready to withdraw funds again, the scammer creates reasons why this can't happen. He tells the victim that there are additional taxes or fees that need to be paid, or the minimum account balance has not been met. This entices the victim to provide additional funds. Sometimes, a "customer service group" gets involved, which is also part of the scam.

The harassment – and the “relationship” – usually end once the victim stops sending funds.

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.