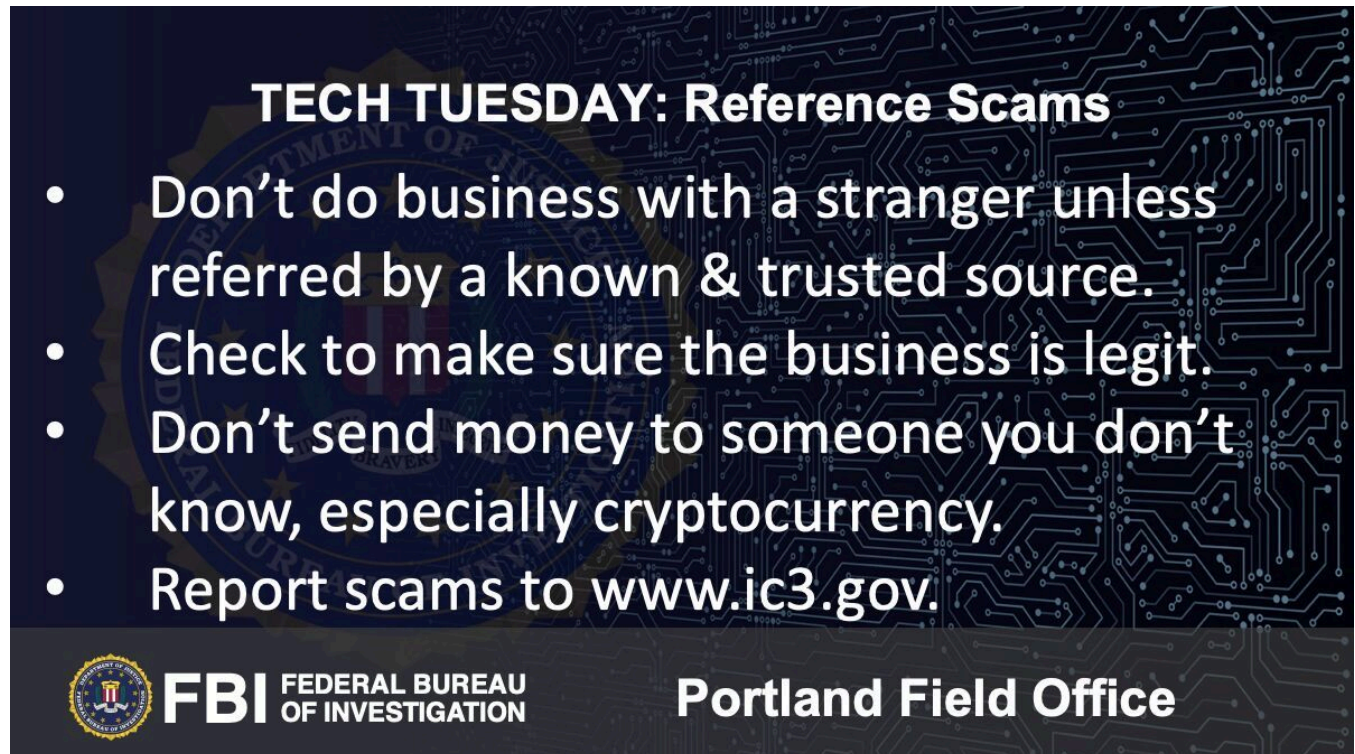


Tech Tuesday: Building a Digital Defense Against Reference Fraud

February 22, 2022

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 this is the text "TECH TUESDAY: Reference Scams" in white, bold, sans-serif font. Below this title is a bulleted list of four items in white, sans-serif font. At the bottom left is the FBI logo (a circular seal) followed by the text "FBI FEDERAL BUREAU OF INVESTIGATION" in white, bold, sans-serif font. At the bottom right is the text "Portland Field Office" in white, bold, sans-serif font.

TECH TUESDAY: Reference Scams

- Don't do business with a stranger unless referred by a known & trusted source.
- Check to make sure the business is legit.
- Don't send money to someone you don't know, especially cryptocurrency.
- Report scams 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 reference scams.

In Oregon, we've received several reports of this kind of scam recently through the FBI's Internet Crime Complaint Center. This is simply a new twist using old-style techniques.

Here's how it works. You post something on social media. You, for instance, are venting about how your car got stolen or your bike is missing. Someone contacts you. The person may claim to be a private investigator or just a "guy who knows a guy." He says he has had success fixing your kind of situation or finding whatever it is that you lost... or he knows someone who does. In the case of a "guy who knows a guy" he vouches for Guy #2.

You get in touch with your new friend the private investigator or the previously-vouched for Guy #2. You pay him – maybe a couple hundred bucks – to get your bike back. The payment could be through a payment app or, maybe, even a cryptocurrency ATM.

You don't have to have a cryptocurrency account or really know anything about crypto – he sends you a code, you walk up to the ATM, insert the cash, and use the code. The money leaves your hand and hits his wallet almost immediately.

Needless to say, your new friend the private investigator – or maybe Guy #2 – disappears faster than your bike, and he takes your money with him.

How do you protect yourself?

- Never do business with someone you don't know or who isn't referred by a trusted source.
- Do your research. Check online for reports of similar activity by bad actors. If the person claims to be a legitimate operator – such as PI – call the company to confirm and check for business records.
- Check references, and not the ones he gave you.
- Don't ever send money to someone you don't know, especially through a crypto ATM.

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