

Tech Tuesday: Building a Digital Defense Against Ride Share Scams

August 3, 2021

A graphic with a dark blue background featuring a circuit board pattern. In the center is a large, faint FBI seal. Overlaid on the seal is the text "TECH TUESDAY: Ride Share Scams" in white. 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 white.

TECH TUESDAY: Ride Share Scams

- Be wary of anyone offering you free money.
- Don't give anyone the login credentials to your work or personal accounts.
- If someone gains unauthorized access to your financial accounts, call the bank right away.
- 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 ride share scams.

Oregonians are reporting a new kind of scam to the FBI's Internet Crime Complaint Center these days – and given the massive growth of ride share services in the past couple of years, it's not surprising.

Here's one driver's story. When he arrived at the pickup point, he received a call that he believed was from his company. The person on the other end told him he was a great driver and was receiving a \$250 bonus.

Using the driving app, the bad guy asked the driver to message him some personal info, including his sign-on information for the ride share app, his Social Security number, his debit card number, and his PIN number. The driver noticed almost immediately that the fraudster was attempting to drain money credited to his ride share account and his bank account. He realized the scam at this point and immediately started working with his bank to stop the transactions.

How can you protect yourself?

Be wary of anyone offering you free money. If you work for a company such as one of the big ride share operations, they do not need you to give them your bank account info to pay you. They should already have it.

If anyone asks you to give your login credentials to any of your work or personal accounts, don't do it.

If you feel as though you may have been scammed, be sure to notify your bank right away.

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