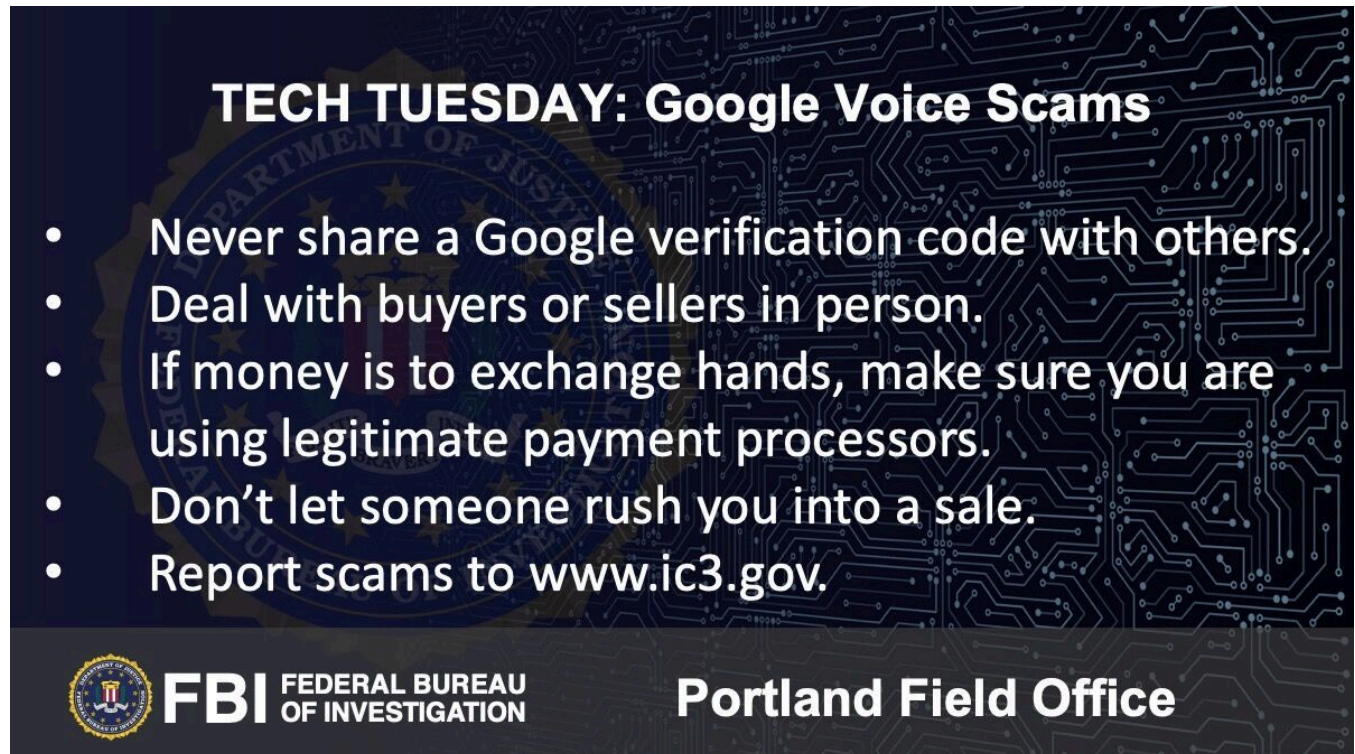


Tech Tuesday: Building a Digital Defense Against Google Voice Authentication Scams

January 4, 2022

A graphic with a dark blue background featuring a circuit board pattern. On the left is a large, faint circular seal of the Federal Bureau of Investigation. The text is in white. At the top, it says 'TECH TUESDAY: Google Voice Scams'. Below that is a bulleted list of five items. At the bottom left is the FBI logo and text, and at the bottom right is the text 'Portland Field Office'.

TECH TUESDAY: Google Voice Scams

- Never share a Google verification code with others.
- Deal with buyers or sellers in person.
- If money is to exchange hands, make sure you are using legitimate payment processors.
- Don't let someone rush you into a sale.
- Report scams to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Welcome to the Oregon FBI's Tech Tuesday segment. This week: building a digital defense against Google voice authentication scams.

What is Google Voice? It's a service – brought to you by Google, of course – that allows you to set up a new virtual phone number that can be used to make domestic and international calls or send and receive text messages.

You don't even have to have a Google Voice account to get scammed in this particular scheme. Here's how it works:

You post your real phone number on some online platform. It's common for scammers to target victims who use popular marketplace apps or websites to post items for sale. Want to get rid of that old couch? Post it on one of those popular re-sale sites, and hope someone likes your taste in style.

Recently, we have also been getting reports of people who are getting targeted in other locations, including sites where you post about lost pets.

The scammer contacts you via text or email. He is really interested in buying that couch or thinks he found Fluffy. He says he just needs to make sure you are legitimate so he doesn't get scammed. He says he will send you an authentication code from Google to confirm that you are a real person and not a bot.

You will receive that authentication code in the form of a voice call or a text message. He asks you to repeat that number to him.

What he is really doing is setting up a Google Voice account in your name using your real phone number as verification. Once set up, he can use that Google Voice account to conduct any number of scams against other victims that won't come back directly to him. He can also use that code to gain access to, and take over, your gmail account.

If you do get scammed, check **Google's website for information** on how to take back control of that virtual voice account.

Here are some ways to avoid getting scammed in the first place:

- Never share a Google verification code with others.
- Only deal with buyers, sellers and Fluffy-finders in person. If money is to exchange hands, make sure you are using legitimate payment processors.
- Don't give out your email address to buyers/sellers conducting business via phone.
- Don't let someone rush you into a sale. If they are pressuring you to respond, they are likely trying to manipulate you into acting without thinking.

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