The Google Voice scam: How this verification code scam works and how to avoid it

October 27, 2021 by Alvaro Puig Consumer Education Specialist, FTC

It's Cyber Security Awareness month, so the tricks scammers use to steal our personal information are on our minds. If there's one constant among scammers, it's that they're always coming up with new schemes, like the Google Voice verification scam. Have you heard about it? Here's how it works.

Scammers target people who post things for sale on sites like Craigslist or Facebook Marketplace. They also prey on people who post looking for help finding their lost pet.

The scammers contact you and say they want to buy the item you're selling — or that they found your pet. But before they commit to buying your item, or returning your pet, they feign hesitation. They might say they've heard about fake online listings and want to verify that you're a real person. Or they might say they want to verify that you're the pet's true owner.

They send you a text message with a Google Voice verification code and ask you for that code. If you give them the verification code, they'll try to use it to create a Google Voice number linked to your phone number. (Google Voice gives you a phone number that you can use to make calls or send text messages from a web browser or a mobile device.)

So, what's the harm? The scammer might use that number to rip off other people and conceal their identity. Sometimes these scammers are after a Google Voice verification code *and* other information about you. If they get enough of your information, they could pretend to be you to access your accounts or open new accounts in your name.

If you gave someone a Google Voice verification code follow these <u>steps from Google to reclaim</u> your number.

No matter what the story is, don't share your Google Voice verification code — or any verification code — with someone if you didn't contact them first. That's a scam, every time. Report it at ReportFraud.ftc.gov.