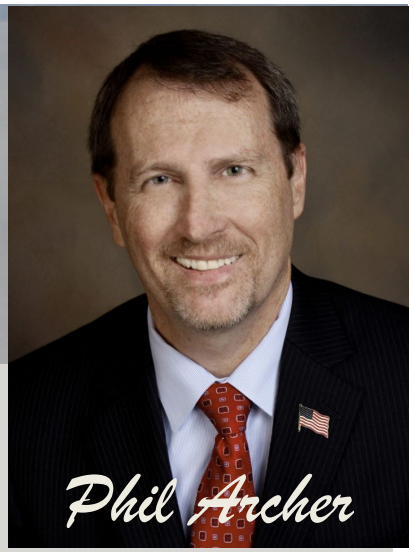
State Attorney
18th Judicial Circuit
Brevard and Seminole County



The Monthly Brief

Volume 12 Issue 1 January 2024

Amazon Security?

You answer your phone and hear "Hi, I'm Jake with Amazon Security alerting you to an attempt to order items on your account." Well it isn't Jake and he's lying. Here's what's really going on.

It's an impostor scam where fraudsters impersonate people and organizations you would ordinarily trust, or at least hear out. Then attempt to convince you to send them money. These scams can also begin with a text message alert.

What You Should Know:

Impostor scams can happen with any brand, service, or government agency. They target everyone, but usually focus on seniors or those who aren't tech savvy.

Government agencies will not call you out of the blue. So, that robocall from the Social Security Administration informing you that your Social Security number has been suspended due to criminal activity is a scam.

Most businesses also won't contact you randomly about some alleged issue. So, the utility company calling to tell you they are about to cut off your power because you didn't pay your bills is also a scam.

What You Should Do:

Never give out your personal, or banking info. Period. **Let unknown callers** go to voicemail. **Don't trust Caller ID**, it can be faked. **Non-personalized messages** should be a red flag.

Learn More About This and Other Impostor Scams by visiting the AARP Resource Center Page and the AARP Fraud Watch Network. *AARP

Follow Us On TwitterX

Visit Our Website: SA18.org

Credit Report vs Consumer Report

Identity Theft is happening at an alarming rate and the stolen info is often used to open credit and bank accounts in the victim's name. Since anyone can buy your private data on the black market, identity theft is easier than ever before. Once it happens, the fix involves locking your credit, notifying all your financial accounts, the IRS, and proving that it wasn't you that ran up the unpaid debt. This can be daunting, time consuming, and very frustrating.

Credit Reports summarize your current and prior borrowing history. With continuous monitoring, they can provide an early warning of identity theft with listings of new accounts you didn't open. Click here to learn how to check your credit reports for free.

But did you know that **Consumer Reporting Companies** also gather and share your personal info? These background type reports are used to make decisions involving employment, residential rental housing, insurance, banking, and other situations. Under the federal Fair Credit Reporting Act all consumer reporting companies must provide you a copy if you request it. You also have the right to dispute information in these reports. The Consumer Financial Protection Bureau identifies these companies, explains what they do, and how to contact them. You can view and search the companies and download the Free PDF list HERE.

For more information on Consumer Reporting visit the CFPB website. For more on free Credit Reporting and Scores also visit their site HERE. *CFPB, Komando .com

Google Voice Authentication Scam

If you're posting on Facebook Marketplace or Craigslist, the FTC is warning consumers about crooks stealing phone numbers to open Google Voice accounts. Scammers target people who post things for sale online listing their phone number. They also prey on people who post looking for lost pets.

How It Works: 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 claim 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. Using your number, they now create a Google Voice account, but that requires verification. Google sends you a text message with a Google Voice verification code and the crook asks you for that code. If you give them the code, they'll use it to obtain a Google Voice number linked to your phone number. Suddenly your number is being used to scam victims, or if the crooks have enough of your personal info, could access your other accounts by redirecting two-step authentication codes and creating new passwords. Similar tricks can be used to defeat 2-step verification for financial accounts.

If you gave someone a Google Voice verification code follow these steps from Google to reclaim 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 *FTC,CBS4