The Expert's Opinion on Being Proactive With Your Identity Security

Paige Hanson

When it comes to stealing your identity, fraudsters can use tactics – old basic methods, generation zero methods – dumpster diving, shoulder surfing... And then now there are more evolved techniques where they're using fishing techniques over email, they're calling you fishing over the phone, texting, SMiShing you.

So we as consumers need to be aware, have our guard up, that if someone is calling us asking for personal information, texting us, emailing us, initiating the conversation asking for personal information – that is a huge red flag we shouldn't be giving out that personal information.

As a consumer, when you're asked for information, you can ask, "what for? Why do you need this personal information? In order for me to volunteer here do I really need to give my social security number? In order to register my kid for this after school activity do you really need their social security number?" Take advantage and take control of your information and do not blindly give it out.

In order to protect yourself it's important for to monitor certain accounts. The first one is your credit. So you go to annualcreditreport.com and get access to all your credit reports from Experian, Equifax and TransUnion. You can actually do that once a year.

Secondly, you want to go to the Social Security Administration's website at ssa.gov. This will allow you to look at all of what you contributed to social security and you're also able to enable two factor authentication and get alerts if someone's trying to access your Social Security benefits.

Lastly, you want to monitor your medical information. You can do this by one, looking at your explanation of benefits whenever you get the statement but then you can also look at your MIB consumer file. And this will allow you access to any sort of medical operation you had over the past seven years.

A current scam happening is the "Yes" scam. We're typically socially engineered that when somebody calls me and they say, "Hi is this Paige?" I say "yes." And they go on and ask me what they need to.

Well, what the fraudster is doing is they're capturing you saying "yes." Because when you enroll in a service over the phone you have to verbally agree that they can charge your card or open up an account. So now they've captured me saying "yes," because I've fallen for their scam, now they can go and open up new lines and accounts.

So when I say, "hey this is a fraudulent account that's been opened in my name," they go back and they pull the footage or they pull the recording of me opening up the account, it is my actual voice saying "yes."

So this is another scenario where you as the identity theft victim are guilty and you have to prove yourself innocent.

There are many scams happening during the tax season where someone impersonates the IRS pretending that you owe a certain amount of money requiring you to wire them money, send a Green Dot card, or possibly gift cards. But just know, the IRS will never call you, they won't text you and they certainly won't be sending a sheriff down to knock down your door to get their money.

Instead, look for an envelope from the IRS. They will only send you information via postal mail. In the event that you become either a victim of these scams from tax fraud impersonators, or someone has called you but you didn't provide information, there is a section on the IRS's website that'll give you the contact numbers and anything to mail them reporting your issue.