Scary News about Phone Scams and Robocalls

If you think ghosts, zombies and creepy clowns are scary, just wait. Signs point to more phone scams and robocalls haunting consumers – and there's no indication they're going away anytime soon. According to YouMail, an app that blocks robocalls, more than 4 billion robocalls were made in the U.S. in July. Not surprisingly, unwanted calls are the top consumer complaint received by the Federal Communications Commission (FCC).

ROBOCALLS JUST THE BEGINNING

Remember the good old days, when the most annoying calls came from telemarketers who somehow knew when you were sitting down to dinner? Along with the growth in robocalls, there are plenty of other ways scammers use our phones to commit fraud and obtain personal information that they can use to commit identity theft:

- **Robocalls.** In addition to being annoying, robocalls can put consumers at risk for scams. Some of the calls are threatening, demanding money or personal information. Scammers often say the demand is urgent; they realize if someone takes the time to think about what the caller is asking, they may realize it's a scam. According to Consumer Reports, these scams cost consumers millions of dollars a year.

  It's important to note that there are legitimate robocalls, such as appointment reminders and collection calls for debts you do owe. Some utility companies have even used robocalls to warn customers of scams demanding payment or risk having utility services disconnected.

- **Caller ID spoofing.** Have you ever gotten a call from your own number? Or from a number you think your recognize, and answer to find a robocall or scammer on the line? That's caller ID spoofing, also known as neighbor spoofing. Scammers use this technique because they know we're more likely to answer if we recognize the number or think the incoming call is local.

- **Vishing/voice fraud.** Vishing can be similar to phishing, but instead of receiving a malicious email that looks legitimate, the call looks like it is coming from your bank or other organization with which you do business. The caller may be an actual human, or an artificial intelligence (AI) "chat bot," that has enough information about you that the call seems legitimate. A common ruse is the call from your financial institution or credit card company, perhaps letting you know they have detected fraud on your account; in order to issue a new card they need to confirm a piece of information from you, such as your PIN number. It works so well that even tech-savvy people have fallen for it.

Voice fraud can also work **in reverse**: fraudsters contact a call center and ask to change information on a consumer's account. They are able to do this after obtaining personally identifiable information (PII), perhaps through a data breach, which they use to confirm the call is legitimate so they can then access accounts.

Another risk? **A recent article** revealed that Facebook members who provided phone numbers for two-factor authentication were soon targeted by advertisers. While this isn't a scam, it is concerning that Facebook is sharing the very information consumers use to protect their account.

SPOOKY SCAMS YEAR-ROUND

Our Investigators have also seen an increase in phone scams. Members have received calls claiming to be from a number of government entities: the "IRS" is calling to demand payment; the "Social Security Administration" calls to say their Social Security number has been suspended; "local law enforcement" calls saying they've determined your vehicle has been used to commit a crime such as transporting drugs. "Microsoft" or "tech support" calls with a number of schemes, such as: stating they've noticed a problem with your computer and they need remote access to repair it, or calling to issue a refund from a previous tech support scam – if you will provide your account number.

"THIS IS INSANE!"

That's not our opinion. **This comes straight from FCC Commissioner Jessica Rosenworcel**, after she received a robocall during a meeting in which it was announced the FCC had found, and planned to fine, a couple of men who were responsible for making millions of the calls.

The good news: The FCC has made protecting consumers from robocalls a priority, and put a **number of initiatives** in place to not only curb the calls, but track down and punish those behind them. The bad news: it is projected that in 2019, **almost half of calls to our cell phones will be scams**.

There are a few things you can do to protect yourself from robocalls and scams:

- Don't answer calls from numbers you do not recognize.
- Register for the "Do Not Call" registry. This will not stop scammers who don't subscribe to the list, but it can lessen calls from legitimate telemarketers.
- Do not give out any personal information to someone who calls you.
- If you receive a call that appears to come from your bank or another legitimate organization, and the caller asks you to provide personal or account information, hang up and call them directly using a legitimate customer service number, such as the one listed on the back of your credit card.
- When available, use an authentication factor other than SMS for 2FA.

And of course, anytime you receive a suspicious phone call, do not act immediately. Call our Investigators at 888.494.8519, Monday-Friday, 7 a.m. – 7 p.m. CT. They know what techniques scammers use and can help you avoid becoming a victim.