HANGING UP ON ROBOCALLERS

December 2021 | Issue 2021:11

Personal Security Practices

As the year comes to an end, many of us take inventory of our possessions. This year, when thinking about what to keep, donate or trash, make sure to protect the personal information on your families' devices.

A sound home data security plan is built on five key principles:

1. TAKE STOCK.
Know what personal information you have in your files and on your computers. Inventory all computers, laptops, mobile devices, flash drives, portable drives, gaming and VR systems.

2.LOCK IT.
Protect the information that you keep. Review, update and change old passwords. Consider two factor authentication for your most sensitive information and accounts

3. SCALE DOWN.
Keep only what you need. Properly clear and dispose of those old cell phones and readers lying around in desks and drawers.

4. PITCH IT.
Properly dispose of what you no longer need. Make certain that any device headed for donation or disposal is wiped clean of all personal information. A factory reset is a software restore of an electronic device to its original system state by erasing all of the information stored on the device.

5. PLAN AHEAD.
Research Password Manager tools to help your family safely change and update passwords frequently. Review your existing anti-malware/spyware tools and upgrade as appropriate.

On behalf of the entire Chief Security Officer staff, wishing you a healthy and happy New Year!

When NOT to Answer Your Phone

Your phone rings and up pops a number from your area code. If you don't recognize the number, chances are you are about to enjoy another robocall. You've tried blocking numbers, which is temporary help at best. You even have signed up on the national "Do Not Call" registry.

"When the pandemic hit about a year ago, we saw the first major drop in robocalls because call centers were closed, but now robocalls are exploding," says Alex Quilici, CEO of YouMail. Robocall volume in the U.S. hit an estimated 5.5 billion calls — an all-time high — in October 2019, then sank to about 2.8 billion calls a month when the pandemic erupted last spring, he says. Lately these calls, many from scammers, have climbed to about 5 billion a month. The FCC has taken aggressive enforcement actions totaling over $450 million in recent years against telemarketers for apparent illegal caller ID spoofing—including so-called neighbor spoofing, where calls appear to be from local callers.

How do you hang up on these annoying spam calls? First, download a call blocker. Try a free solution to see if it does the trick. No-cost services from firms such as YouMail and Nomorobo are carrier-agnostic. (Nomorobo is free for landlines but $1.99 a month for cellphones.) Your mobile carrier has free tools, too. Other popular apps include Robokiller and Truecaller.

There are some privacy concerns when it comes to robocall blocking apps. Some apps require access to your voicemail to identify robocall messages and flag the number, but not everyone is comfortable with sharing the complete contents of their voicemail inbox. Other apps send user or device data to third-party data analytics companies as soon as they are installed. The best way to make sure your privacy is protected is to thoroughly read the app's privacy policies before you install it.

Ask your phone service provider what they do to block illegal robocalls. They may already include certain call blocking options in your current service plan. If so, make sure the functions are activated on your device. Or your service provider may offer additional scam and robocall blocking protection for a reasonable fee.

If you answer an illegal robocall by accident, hang up immediately. Some robocalls ask you to press a button to stop receiving calls or say "yes" in reply to a question. These are tricks scammers use to identify and target live respondents. They may even use your "yes" to authorize charges to which you haven't agreed.

Let a call go to voicemail if it gets through a robocall app and you don't recognize the caller. If the caller claims to be, say, from Citibank, don't call back a phone number left on voicemail. Use a number you know is legitimate, such as one on a statement or credit card. Hang up if it's a live person calling.

Experiment with call-blocking tools, apps and options to strike the right balance between the calls you want — and those you don't. It

Solomon Adote
Chief Security Officer

may take trial and error to avoid a “false positive,” the term for a legitimate call that is stopped.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Information & Technology publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**