AUGUST 2021

VOL. 13

SFST Bulletin

TECH SUPPORT SCAMS

Kristen Orr, Tech Paralegal

New data from the FTC Consumer Sentinel Network shows that as of June 30, 2021, about 1 in 5 people have lost money to imposter scams; and when older adults are the victims, their median loss is much higher. Seniors age 80+ reported losing nearly four times as much money as victims age 20-29. One of the more popular imposter scams is the **tech support scam**. In these situations, bad actors impersonate well-known businesses –Microsoft, Norton, Best Buy's Geek Squad, etc. – using these familiar names to lend credibility in an attempt to get the victim to trust them.

The scam can play out in a few different ways; a pop-up might appear on the computer screen stating that there is a security risk, or that the anti-virus software is out of date. A potential victim may receive an email or a phone call from what appears to be a legitimate company, claiming that their computer has been compromised, or their anti-virus subscription has been auto-renewed and they need to call if they want the charge removed. If the victim calls the number provided or clicks the link, they can be prompted to release personal and financial information under the guise of accessing their account.

Sometimes, the scam stops there; victims are convinced to send money or personal information to the scammer; they think they are paying to protect their computer from nonexistent security risks, or providing information to process a refund in order to correct an invented billing error. People can lose thousands of dollars before they realize they are being scammed.

However, the scam can go even further when victims are convinced to allow the scammer to remotely access their computer in order to rectify the alleged problem. **Remote access** to a computer involves the holder of the device downloading software which allows someone else to view and operate the computer screen as if they were sitting in front of it. The scammer may convince the victim that remote access is necessary for them to diagnose the issue or work on the computer; however, once the connection is established, the scammer can do whatever they want, and the victim may not be able to regain control.

The Center for Elder Law & Justice operates a Legal Advice Helpline to answer legal questions, and provide referrals to additional services.

During the COVID-19 outbreak the Helpline will accept phone calls from individuals regardless of age. Helpline calls are free of charge!

The Helpline is staffed by attorneys Monday through Friday from 9:00am to 11:00am to take live calls. Individuals can call outside of these hours and leave a voicemail to get a callback from an attorney, or send an email to **Helpline@ elderjusticeny.org**.

To contact the Helpline attorneys by phone, place a call toll-free to **1-844-481-0973**.

If someone you know has concerns about their financial health, a quick self-assessment using the Senior Financial Safety Tool can be conducted at **https://probononet.neotalogic.com/a/sfst**

The scammer may convince the victim that remote access is necessary for them to diagnose the issue or work on the computer; however, once the connection is established, the scammer can do whatever they want, and the victim may not be able to regain control.

The scammer can make it appear that the computer is compromised by sharing their own screen or projecting fake images that make it look like there are security issues. They can show themselves "fixing" the issue and then demand a fee for doing so.

Scammers can fake bank account transactions, and make actual transfers without consent, while remotely accessing the computer. They might have the victim open up their online banking portal to send a refund of $500.00, and then manipulate the screen to make it seem like they "accidentally" deposited $5,000.00 into the account. They will request the victim send back the "overpayment" of $4,500.00, but there was never a deposit into the account in the first place.

They can deny the victim access to their device until they pay a ransom. They can install malware, or "malicious software," on the computer, causing damage to the device and granting access to personal data. They can access documents, pictures, and sensitive information stored on the device, and log-in to any website where the victim has saved the password. They can remotely access the victim's online bank account and transfer the balance anywhere.

If you are contacted by someone offering tech support, or you receive a security warning popup on your computer, you should always take the time to independently verify where that message is coming from. Tech companies do not call clients out of the blue; no legitimate company will ask for remote access to your computer in order to process a refund, or to fix your computer without you first requesting assistance. Do not click on unknown links you receive via email or text, and do not call any phone numbers that randomly pops up on your computer. If you fear you are having security issues, do your own research and contact a reliable computer company. Never pay with a gift card or bitcoin, that is always a scam; no reputable company will require that payments be made via gift card.

For more information on tech support scams and how to protect yourself, visit https://www.consumer.ftc.gov/scams/tech-support-scams.

The Senior Financial Safety Tool project is supported through a cooperative agreement with the U.S. Department of Justice, Office of Justice Programs, Office for Victims of Crime award number 2018-V3-GX-K024. The opinions, findings, conclusions or recommendations expressed in this Project are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice.