SCAM SAVVY

Outsmarting Cybercriminals

By Liza N. Burby

IT HAPPENS TO US ALL. A recent voicemail on my cell warned, "This call is from the Department of Social Security Administration. The reason you have received this phone call from our department is to inform you that we've just suspended your social security number because we found some suspicious activity. So, if you want to know about this case just press 1. Thank you."

I admit my first response was, "Wait, should I be worried about this?" before healthy skepticism kicked in and I pressed delete instead. Yet cybercrimes like these are increasingly impacting people of all ages, and those 50 and over tend to be most vulnerable. The annual report from the FBI's Internet Crime Complaint Center (IC3), reports that in 2018 there were nearly 50,000 complaints of financial and personal data breaches from victims between the ages of 50 and 59, and over 60,000 for 60 and over. Their collective losses were in excess of $1 billion.

According to Nassau County District Attorney Madeline Singas, there are scams that particularly target seniors, like the grandparents hoax where cybercriminals call and say something like, "Your grandchild's been in a terrible accident overseas and if you don't wire this money, the hospital won't treat them." But anyone can be susceptible, she says.

"All these scams prey on basic fears that people have that someone they love is in trouble or that your financial security is at stake," Singas says. "I think they go hand in hand because they create this urgent situation, and that urgency makes people sometimes do things they wouldn't normally do if they had the time to think about it."

Many of these crimes are underreported because victims feel shame that they were duped, Singas says. "Especially if you're an older person, you don't want to tell your family, because you don't want them to worry that you're not in control of your faculties."

Photo credit: Getty Images

According to the FBI, the states with the highest reports of victims in 2018 in order were: California, Texas, Florida, New York and Virginia.

Further, scammers have gotten sophisticated, says Scott Schober, author of "Hacked Again" and a frequent expert guest on news shows. "Cybercriminals do their homework and take that extra step to be convincing, to make it look real," says Schober, who is president and CEO of Berkeley Varitronics Systems, a cybersecurity company in New Jersey. "They're using technology and spoofing text, phone numbers and email addresses, automated tools that even take all the logos. Everything seems legit for anyone that does a quick glance at it."

Awareness about the most common current scams can help, says Steve Morgan, founder and editor-in-chief of Cybersecurity Ventures, a leading provider of data and analytics for the industry, based in Northport. "The most dangerous scams are the ones that are seemingly the most authentic."

Here are seven to watch out for.

Tech Support. Fraud A caller identifies themselves as being from a large tech company like Microsoft or Google. They tell you they need to reset your password because your computer has been exposed to malware.

"Once you confirm your email address and share your password, the tech support scam is successful because they now have access to your device," Morgan says.

Phishing. An email from a disingenuous source claims to be someone you know or a trusted business like

the IRS, your bank or even the hospital where you recently had surgery. They present various propositions, like the hospital telling you something wasn't covered by insurance. Their goal is to fish for information like your bank account or Social Security number.

Vishing. The "V" stands for voice and works like phishing, but through robocalls – a call that uses a computerized autodialer to deliver a pre-recorded message, just like the one I got about my Social Security number.

"It's a socially-engineered, criminal hack," says Morgan, "meaning they use an air of authority to engage you, then ask you questions to authenticate yourself. And depending on how convincing they are, they can get you to reveal personal information like your mother's maiden name."

SIM Swaps. The con works with the scammer knowing your name and phone carrier. They tell them your SIM (subscriber identity module) card is defective and needs to be swapped out, then give a convincing excuse to get them to send it to a different address.

"As soon as they put that new SIM card into a phone, the original card stops working, and then they have access to everything – all your texts and emails, which often include login IDs and passwords to your investment, retirement and bank accounts and more," Morgan says.

Social Media Fraud. Using Twitter, Instagram, Facebook or LinkedIn is an instant way for a hacker to reach out to you. They set up a legitimate looking account with a fake name and image, even creating a business related to your industry.

"They're targeting you directly, so they want to look credible and create a good reason for the two of you to connect, " Morgan says. "Once you respond, they attempt to gain access to your personally identifiable information (PII), which can be used to unlock some or all of your data – and worse they can masquerade as you."

Ransomware. This is cybercriminal activity in which you're unable to log onto your computer or phone and you're asked to pay the company that hacked you to gain access – in effect, they hold your data hostage.

"Our research shows that ransomware is one of the fastest growing cybercrimes and is expected to cost the world $20 billion by 2021," Morgan says.

Romance/Confidence Fraud. They gain their victims' trust by convincing them they're in a relationship through texts, emails, phone calls and in-person dates. The next step is to ask for money for airfare, an item like a computer, help with a sick child, and even to launder money on their behalf.

In 2018, romance/confidence fraud was the seventh most commonly reported scam to the IC3 based on the number of complaints received, and the second costliest scam in terms of victim loss.

Photo credit: Getty Images

THE EXPERTS SHARE

Basic Steps to Protect Yourself

DA Madeline Singas:

- Regularly check your credit report for suspicious activity, including unfamiliar addresses.
- Set alerts to your bank accounts.
- Know that the IRS never calls. Neither does the Department of Social Security.

Steve Morgan:

- Update your device's anti-malware and regularly back up your computer and cell phone.
- Practice multi-factor authentication – adding an extra security step to your email and phone, like a fingerprint.

Scott Schober:

- Don't respond "yes" to any questions; instead ask for their phone number.
- Let calls you don't recognize go to voicemail.

For More Information:

The IC3 website offers tips and a list of common and current scams at ic3.gov/crimeschemes.aspx

AARP's podcast "The Perfect Scam," with fraud expert Frank Abagnale of "Catch Me If You Can" fame, features scam victims, con artists and experts. You can sign up for watchdog alerts, review their scam-tracking map, and call their fraud helpline at 877-908-3360. Visit aarp.org/podcasts/the-perfect-scam

If you feel you're in danger, call 911. If you suspect criminal activity or have been the victim of a cybercrime, call the FBI field office in Melville at 631-501-8600. File a complaint at ic3.gov/complaint/default.aspx

You can also call the Nassau district attorney's tip line, 516-571-7755. In Suffolk, email the DA's office at infoda@suffolkcountyny.gov.