SPRING 2019 HERSHEYS MILL FRAUD PREVENTION NEWSLETTER

ROBOCALLS

All of us have been annoyed by unwanted robocalls interrupting dinner, naps, etc. causing us to hesitate to even answer our phones especially if we have Caller ID and it displays an unknown number.

Unfortunately, this problem is growing and not just an annoyance. It is also being used to bilk people out of their money in new deceitful ways.

To review, in past issues I have discussed fear-based scams. For example, the IRS calls that you owe back taxes and will be arrested immediately if you don't pay up RIGHT NOW.

But because of virtually everyone's private information has been compromised the bad guys are now using at least two new approaches.

New Robocall Scams

Fear Techniques.

Reputation Risk. The first is targets mainly seniors because they value the reputations

they have built over decades. The hook is that they have your E-Mail address and password (stolen) which they claim they have from a porn website you viewed which they will make public if you don't pay their fee. This approach has been more successful than some others.

Foreign Language. The second is more exotic. The call is in a popular foreign language like Chinese Korean or Indian. You, of course, hang up but with enough calls they reach a native speaker. When they hear the threat (IRS, Jury Duty) they assume it is from the government because the message is delivered their language it appears legitimate and are thus victimized at a higher rate.

Three Newer Ones.

Don't Say Yes. You get a spam call. The person apologizes and asks if you would like to be on their Do Not Call List. You say yes. Your response is then recorded and inserted into a recorded phone session in which you say yes to their "offer." Best advice. Neve say anything, just hang up immediately. Also, this marks your phone number as a live number so you'll be unwittingly encouraging more calls.

Don't Call Back. Next, this is one I experienced personally a couple days ago. A heavily accented Spanish speaking woman left a message for my wife by name. I can speak some Spanish but I only understood "call back." As this was an unknown (to me) area code I Googled A/C 529 and read many accounts of people calling this number and seeing hefty charges.

Scam Recovery. Burned Once, Burned Twice. The scammers who got money from you know who you are, what you lost and how you were fleeced. It's a perfect setup to send you an E-mail, or call you offering to help you get your money back. There is no legitimate service that does this so delete the E-Mail and let the call go to voice mail.

A Couple Worth Repeating From the Winter Newsletter

Neighborhood Spoofing. Spoofing is when the caller displays a fake ID like "IRS." Neighborhood spoofing involves showing a fake number with your area code and exchange followed by four random numbers. So if my number was 610-265-3571 their Caller ID would be 610-265-nnnn.

Name Spoofing Same for this one. The Caller ID will show a person's name, not just where the call came from. This is especially effective with seniors who may think they forgot the name and pick up.

SOME BASIC WAYS TO REDUCE THE RISK OF FRAUD

These tips are from our friends at AARP with my comments.

Use Electronic Statements Not only does this reduce the risk of financial documents being stolen, it also eliminates the risk that crooks will change your address to theirs, and you might save a few bucks from your financial institution for using electronic statements.

No Shredder? Buy one tonight but spend a few bucks more for a CROSSCUT model

Oldie but Goodie. Freeze Your Credit. It's easy to unfreeze, but the credit bureaus make try to talk you out of it because they only make money if someone can see your credit report.

Don't Enter Sweepstakes. I disagree with AARP here. Why ask them what they will do with your information? Do you really expect an honest answer?

Don't Ask Why They Need Your SSN Simply don't provide it. Let them initiate the request and don't accept "it's our procedure."

Use a Credit Card Instead of a Debit Card. First, your exposure is limited to 50 bucks (usually waived) Second, many top credit card issuers have methods whereby you can be immediately informed of questionable activities or predefined transactions. I don't think this is available on debit cards.
Also, on a personal note I made a substantial purchase with my AMEX card which I decided to cancel because the deal was not as good as claimed (but not fraud.) My card had been charged by this company headquartered in Panama. AMEX took care of this for me for a full refund. I don't think that I could have done anywhere close to that myself with a debit card.

AARP Recommends Paying With Your Phone. To me, this is good advice if you're tech savvy. If you're not I recommend sticking with credit cards.

Don't Answer Calls from Numbers You Don't Recognize. This is excellent advice, but their method will only work with certain cellphone brands. They suggest turning on your phones DO NOT DISTURB feature which will still allow calls from your CONTACTS. However, if your phone doesn't work like that (mine doesn't) I use a two-part strategy. First, I assign the same non-default ringtone to any contact who I haven't given a unique one. Then, my voicemail message says "I don't answer phone numbers I don't recognize. If you still wish a call-back please leave a message."

Then I simply don't answer any default ring tone calls.

Add Your Name to the National DO NOT CALL LIST. Not worth doing.

Avoid Public WIFI. Good advice. Do searches, check E-Mail on your phone. If you need to work with your laptop learn to use your cellphone as a HOTSPOT if it supports that. If you still need to use Public WIFI install VPN software. Don't worry that it's too technical. I use HOTSPOT SHIELD and all I do is click the Icon.

Try to Limit the Personal or Location Info You Post on Social Media.

This provides scammers with the ability to make their pitches much more believable.

Older Phone Scams That Are Still in Use Because They Work.

Social Security

The caller wants to convince you that you are being accused of a criminal act involving Social Security and you will be hauled into court unless someone else has been using your SSN in which case he will try to "Help You Fix This Problem." Ignore the call.

Health Insurance

These calls say that the Open Enrollment deadline has passed but they can still provide good insurance at an affordable price if you press 1. This will either connect to an insurance salesman or a scammer. You don't need either. If you need insurance start at healthcare.gov. Also, you don't want to be identified as a future scam target.

Jury Duty

You failed to show up for Jury Duty and owe a big fine that they (local police) are authorized to collect. Not a word of this is true so hang up or delete the voice mail.

Pain Center

You are receiving this call because this number called seeking information about a pain-relieving brace which you may qualify for at no cost. Press 1 to speak to a product specialist. Amazingly, you qualify for the free brace they will send you. You get a piece of junk and they bill Medicare for lots of green. I don't see this as you being the only contributor. Medicare is terrible at policing these frauds.