Summer 2018 HERSHEYSMILL FRAUD PREVENTION NEWSLETTER

With apologies to Nat it's once again time to roll out those lazy hazy crazy days of summer and plan for a break from work or just the normal routine. Unfortunately, those attempting to separate you from your money never rest. So this issue we'll be looking at what they've been up to lately.

Before I start however, I'd like to take some advice from the Philadelphia Federal Reserve via the Inquirer's Erin Arvedlund. This is probably the most important advice in this newsletter for three reasons.

First, no matter how vigilant we are, there is always a chance to get caught off guard and be fooled, the author included.

Second, the technical capabilities to know about your personal info and the tools they have to imitate legitimate entities is frightening.

Third, your personal data it is for sale on the black market for pennies. Second, sources like Google and Facebook are only too willing to sell it to others no questions asked.

Finally, just FYI these techniques work on business and government as well.

On top of the scammers abilities, your defenses can degrade over time. Dementia, death of a spouse, medication, injury, etc. can make you much more susceptible to their schemes.

So in light of all this I recommend that we follow the Feds advice and add a TRUSTED CONTACT to any account you have involving money or property. This should not put

your assets at risk because they should not have access to your accounts. They are simply there to receive suspicious activity reports from bankers, brokers etc. This is critical if you are incapacitated, hospitalized or just simply not as sharp as you used to be.

If you open any new accounts you should be asked for such a contact. If you are not asked or have existing accounts talk to the company about creating one.

There are more issues here that I can't cover so I suggest you look up her column in the June 18th Inquirer.

Now on to our usual fare. These have been posted on the HM website to get the information out between newsletters. However, the majority of my readers still use the newsletter.

In addition to the Fed Here's a warning from the FBI.

PLEASE HELP PROTECT YOURSELF AND THOSE YOU COMMUNICATE WITH FROM THIS RUSSIAN SPYWARE BY FOLLWING THE FBI'S SUGGESTION

The FBI issued an urgent bulletin for anyone with a home or small office internet router to immediately turn it off and then turn it on again as a way to temporarily thwart the spread of foreign malware linked to Russia. Over 500,000 routers have already been infected.

There are two steps to fully protect your ROUTER but the second step is too technical for the average HM resident without simplifying those instructions which I will not try to do.

However, the first step is very easy to do using the ROUTER which is the piece of Verizon equipment where the cable enters your house and is about a foot high with blinking green lights.

Simply unplug your ROUTER and plug it back in after one minute. Then press the WPS button on top of the router. Then the lights will begin to blink (hopefully green) and you will have your FIOS service back.

You can stop reading here unless you want a little more information about the danger and what the government is doing about it.

The spyware known, as VPNFilter, has been quietly spreading since at least 2016, according to researchers. Once a router is infected, the hackers would potentially be able to use the device as a jumping-off point to launch further attacks. The cybercriminals could also collect personal information, block network traffic — or just turn your router into an expensive brick.

STEP 1 will minimize some of the risk, because some portion of the attack may be deleted after rebooting. This a necessary step, experts said, but they warned that it is not a foolproof fix especially without Step 2.

However, “If this is addressed broadly, it will cause the malware campaign to lose a lot of its access and reduce the broader risk on a macro level,” said a CEO of a cyber security company.

Scammers are Nothing if Not Creative. Below is a list of new (at least to me) scams and a brief description

AIR BNB

This scam involving users of the popular AirBnB site that lets travelers rent an apartment or house. The scam starts with an impostor home or apartment owner directing the renter towards a fraudulent or “spoof” website to finalize payment for the rental.

Those fake sites result in lost money and no place to stay because the rental property being discussed is usually not even available. In fact, the real owners are most likely unaware that their property is being spoofed by scammers.

RECORD YOU SAYING YES

This scam happens when you answer the phone and the person on the other line asks: “Can you hear me?” and you respond, “Yes.” Your voice is being recorded to obtain a voice signature for scammers authorize fraudulent charges over the phone.

You can visit the FCC website to block any unwanted calls. The BBB Scam Tracker received more than 10,000 reports on the ‘Can you hear me?’ scam, but none of the reports resulted in an actual loss of money.

FAKE CAR SALES

The FBI shared information on a growing scam where crooks are targeting those looking to buy cars and other vehicles online. The FBI has received 26,967 complaints with losses totaling $54,032,396 since tracking this issue from May 2014 through December 2017.

This car scam starts with a criminal posting an online advertisement with a low price to get the attention of a buyer, including photos of the vehicle and contact information.

When a buyer reaches out, the “seller” sends more photos and what appears as a logical reason why the price is discounted and indicates a need to sell.

The criminal then instructs you to purchase prepaid gift cards in the amount of the sale and share the prepaid codes. You’re usually told you’ll receive the vehicle in a couple days. Then you don’t hear back from them again you’re left without your money and still in need of a car.

CRYPTOCURRENCY

As the price and popularity of Bitcoin and other cyber-currencies skyrocketed in late 2017, scammers eagerly sought to take advantage of the frenzy.

The Japanese Bitcoin exchange Coincheck was hacked in January and the thieves were able to steal more than $500 million in cryptocurrencies. This is the largest cryptocurrency hack to date.

Facebook and Instagram have banned advertisements for certain bitcoin, initial coin offerings (ICOs), and some other cryptocurrency-related products because of deceptive and misleading practices. Several ads were leading victims to sites such as Prodeum, whose only purpose was to take their money and not provide the advertised service.

DEATH THREAT

The FBI came out warning consumers about death threats being made through emails that state “I will be short. I’ve got an order to kill you.”

The email then demands money or bitcoin as a payout from the email recipients. Other versions of the scam could state that a “hitman has been hired to kill” them. This scam is very aggressive and threatening in nature to convince people that they have to pay or else.

DOWNLOADING FAKE BANK APPS

Big banks have scammers posing as them in the form of apps. A recent survey by an Avast, a multi-national cybersecurity firm, found that one in three worldwide users mistakenly believed that a fake mobile banking app was the real thing, putting their financial data at risk. Thieves use the big customer base of major banks to try to get past the secure app stores and collect personal information.

FAILURE TO REPORT FOR JURY DUTY

Another new spoofing phone call scam has popped up and involves scammers posing as judicial officials or police and calling people to let them know they failed to report for jury duty and owe a fine.

Scammers can spoof law enforcement phone numbers or names so people receiving the call may think that the call is legitimate. The FBI in Atlanta has received numerous complaints about the scam from people in and around the Savannah, Georgia area.

GETTING YOU TO GIVE THEM YOUR NEW MEDICARE NUMBER

The Federal Government mailed out new Medicare cards that now have an 11-digit identification number instead of an enrollee's Social Security number to help protect seniors from identity theft. About 59 million people will receive the cards with a requirement from Congress that the Centers for Medicare & Medicaid Services remove Social Security numbers from Medicare cards by April 2019.

Because of the update, scammers are taking to the phones to try trick people into giving them their new 11-digit identification number so they can take over their identity. According to an Allianz survey, the elder financial abuse victims average loss was $36,000.

HOME IMPROVEMENT SCAM

Another common seasonal scam centers around home improvement. As the weather gets nicer, homeowners often look to improve their homes. The Better Business Bureau says in 2017, there were nearly 350 home improvement scams reported to BBB Scam Tracker across the U.S., resulting in more than $600,000 lost.

Some scammers go door-to-door, offering to do improvement projects. They may take a deposit, and then never complete the work If you're not sure the salesman is legit, you can ask for a card and get back to them once you have been able to research the company by visiting the BBB website. These scams can also happen after major national disasters—hail storms, tornadoes, hurricanes, mudslides, and fires, among other things.

NETFLIX PAYMENT FAILURE

The popular service is the target of an email phishing scam featuring the subject line "payment declined," which may get your attention if you are a subscriber. The email wants you to click on a link to update your credit card information.

If you see this don't click on the link because it can be dangerous malware. Visit your Netflix account by typing the address in yourself to check your account as a safer means of verifying your account status.

GETTING YOUR CELLPHONE NUMBER FOR TWO FACTOR AUTHENTICATION (PORTING)

The scam called "porting" involves criminals stealing your phone number and your phone service in order to get access to your bank account through confirmation text messages. Scammers start by collecting your name, phone number and then gather any other information they can find about you such as your address, Social Security number, and date of birth.

Then they contact your mobile carrier and state that your phone has been stolen and ask that the number be "ported" to another provider and device. Once your number has been ported to a new device, scammers can then start accessing your accounts that require additional authorization such as code texted to your phone

SECRETARY OF STATE – MONEY OWED TO YOU

This scam starts when you receive an email claiming to be from Secretary of State Rex Tillerson, who says you're owed a payment he knows about because of an investigation by the FBI and CIA.

The scam reportedly states that you will receive an ATM card with more than $1 million dollars on it, but first you have to send $320 along with personal information to receive it. The Federal Trade Commission (FTC) says this is false—warning Americans to not fall for this—or anytime you're told you have won a prize, owe money, or may go to jail.

STEAING YOUR CHIP CREDIT CARD INFO AT CHECKOUT (SHIMMER)

A shimmer scam is an update on skimming except that thieves are using "shimmers" to target chip-based credit and debit cards. A shimmer is a very thin piece of paper that can read your card number and access your credit or debit card's EMV chip—the chip designed to help make your card more secure.

Did You Know? A shimmer is a very thin piece of paper that can read your card number and access your credit or debit cards EMV chip.

A thief will put a shimmer into an ATM and let it collect information from each card that is used, allowing them to then create a non-chip version or magnetic strip credit card. Shimmers have been showing up more recently despite first being reported on in 2015. In 2017, the number of debit cards compromised at ATMs and merchant card readers—typically via skimming devices that capture card data—rose 10%, according to FICO.

JACKSPOTTING

Jackspotting is a new cyber-attack scam that the Secret Service warned financial institutions in which criminals install software or hardware on ATMs that force the machines to issue large amounts of cash. Criminals have found ways to exploit the standalone machines commonly found in pharmacies, big-box retailers, and some drive-thru ATMs.

It's hard to know the exact financial implications because sometimes these crimes aren't disclosed publicly, but any time money is missing, it's sure to have an impact on the banks and ultimately you, the consumer, in the former of higher fees or more obstacles to accessing your cash.