FALL 2016 HERSHYSMILL FRAUD PREVENTION NEWSLETTER

Fall is here and the pace of life picks up from the lazy days of summer. Unfortunately, there is never a lazy time for scammers so let's move on to fall protection.

GARDEN TOOL SCAM

This tip was submitted Marie Villeza of Elderimpact.

Her mother discovered an "amazing" deal on a gardening website. The site would send her free gardening tools in exchange for her honest feedback. All she had to do was to provide her credit card number to verify her identity.

Hopefully, by now readers of this newsletter recognize this as a scam but her elderly mother did not so Marie had to spend considerable time undoing the damage. Remember, there is no free lunch. Or retirement dinner either.

RED FLAGS FOR ELDER FINANCIAL ABUSE

Elder financial abuse has been called the Crime of the 21st Century by the Inquirer's Erin Arvedlund. Annual loses are estimated at $36 billion but it is widely recognized as under reported and prosecuted. Changes in the aging brain (financial acuity declines 1% per year) and the onset of Alzheimer's make them particularly susceptible. On a hopeful note regular exercise can sharpen your mind.

So if you have someone who is at risk here are warning signs of trouble:

Unpaid bills and termination of utilities despite adequate income
Transferring assets to new friends
Sudden unexplained **transfer of financial control**
Checks written to **CASH**
Inability to explain current financial situations
Unexplained disappearance of cash, valuables, or financial statements
Unexplained changes to wills or other estate documents
Sudden appearance of liens or foreclosure notices
Large out of character **expenditures**

If you see any of these and suspect abuse, you can report it to the Philadelphia Corporation for Aging Hotline at 215-765-9040.

DON'T FALL FOR FALL SCAMS

With this particular fall you might see legitimate campaign workers canvasing who might speak to you or leave literature. Never donate money to them directly, just ask for the mail in form if you are so inclined.

School kids raising money for uniforms or charity. Some are legitimate and some are scammers working for adults so only deal with those you know.

Utility employees offering to inspect furnace or water heater are not legitimate if the utility didn't notify you first. Also illegitimate are people offering you a free energy audit as you will get a hard sell for expensive upgrades.
Lastly, don't fall for the courier scam. They will call first or just show up with an unexpected package and ask for a nominal "verification fee" to be paid by credit card. Don't fall for it. (From AARP.)

DON'T GET SKIMMED

Skimming involves crooks fitting a card reader inside a ATM so that they can get your card number and pin when you use the machine. It is by far the most common way for crooks to obtain credit card information. This crime increased 600% in 2015 over 2014. While you usually can't tell if the ATM is skimmed be alert for anything that looks out of place like a misaligned reader or difficulty entering your card. Other ways to protect yourself is to use bank branch machines or well-lit high traffic locations such as Walmart. Avoid ATMs in little used places as non-bank ATM skimming rose from 39% to 60% last year.

So how does skimming actually work? There are three methods:

1. **Skimming Device**. Fits over the top of the card entry slot.
2. **Keyboard Overlay**. A false keypad that fits over the ATM's keys to capture your PIN.
3. **Candid Camera**. A pinhole camera hidden behind a false screen.

Some help is on the way in that your chip cards are much more secure and it is estimated that 75% of ATMs will be upgraded by year end. However, if your chip card still has a magnetic stripe you're still at risk.

AVOID SCAMS TO CHARGE FOR FREE SERVICES

Lower Taxes

This scam involves charging you up to $200 to reduce your property taxes by disputing your current assessment. It may begin with a phone call or mail that looks like a government invoice with words like "tax review" or "tax readjustment."

If you really think you are over-assessed you can file free at the County Assessors Office.

Credit Repair

First, the scam part. They may charge to $5,000 up front or $100 per month but they can't do anything you can't do for free. They will challenge items in hopes that the credit bureau will temporarily remove them giving you a temporary credit increase that will disappear when the items are put back.

Now for the fraud part. They claim they can give you a "New Credit Identity." This is not only a fraud on you but if go along you could face charges.

Your best way to inform yourself is to type in "Credit Repair" at ftc.com.

Your best action is to negotiate directly with your creditors to see if they will remove their negative items if you pay the negotiated (or full) amount.

YOU COULD BE LIVING WITH A FRAUDSTER

Is your spouse cheating on you financially. Could be. 33% of adults with combined finances admitted to hiding a purchase, bank account, bill, or cash from their significant other. Another 13% did worse by lying about their debt or even how much they made.

Red Flags

1. Your spouse changes the subject or becomes argumentative when you try to talk finances.
2. They want sole control of your finances or keep passwords secret.
3. You find cash in your house or your bank account that you didn't know about.
4. You discover new credit cards or credit lines in your spouses' name.
5. You spot unexpected or unexplained withdrawals from joint accounts.

If you see these try to discuss them calmly and see if your spouse will truthfully explain what has happened and agree to real joint control. If not meet with a financial planner to see if they can mediate and arrange a working plan going forward. If not, you may need to see a lawyer.

ANOTHER PHISHING ATTEMPT TO AVOID

An E-Mail arrives in your inbox with a variant of the following message:

We suspect an unauthorized transaction on your account. Click on the link below to ensure your account has not been compromised and to confirm your identity.

Even if the E-Mail shows your bank logo DON'T CLICK. Just call your bank's 800 number to see if there is an issue. There won't be.

DON'T HELP SCAM MEDICARE

Criminals who scam Medicare can start the process by simply calling and saying "I'm from Medicare and we need to update our records." Just hang up especially if you don't know any reason your personal situation needed updating. Wait for Medicare to write to you.

Another way they work is by setting up sham clinics for "Free Screening."

Once they have your Medicare info, it is fed into a large network of druggists and doctors who submit phony bills in your name. If they get paid they will also sell your name for a high price.

So what should you to prevent this activity?

Review all your Medicare documents and report charges for any services you didn't receive.
Shred unneeded medical information and don't recycle prescription bottles with labels still on them. Trash them instead.
Hide or lock up your meds if strangers are coming to your house. It's too easy to take a cellphone picture of your labels.
Never give out your personal medical info to people you don't know.

SAFER HOLIDAY TRAVEL WITH YOUR DEVICES

Here are some travel cyber security tips from our friends at AARP.

Before You Leave

1.to those you can carry on your person. This makes it less likely for your devices to get stolen or compromised.

2. **Update your mobile software before you go.** Keep your operating system software and apps on your mobile device updated, which will improve your device's ability to defend against malicious software also known as 'malware'.

3. **Turn off Wi-Fi and remote connectivity when idle**. Some devices will automatically seek and connect to available wireless networks. Bluetooth, for example, enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment systems. Disable these features so that you only connect to wireless and Bluetooth networks when you want to.

4. Create strong passwords. Before you leave home, make sure you have strong passwords on all of your electronic devices. Passwords should be at least eight characters in length with both numbers, letters and special characters (@!$?). Create unique passwords for each device.

5. Enable stronger authentication. Stronger authentication (also known as two-factor or multi-factor authentication) adds an extra layer of security beyond using a password to access your accounts. Most major e-mail, social media and financial platforms offer multi-factor authentication to their users. Be sure to ask your service provider if you can activate this feature before departing on your trip.

While Travelling

Be mindful of your Internet activity and how you can protect your privacy as well as your device:

1. **Keep your phone locked**. Always lock your device when you are not using it. Even if you only step away for a few minutes, that is enough time for someone to steal or destroy your information. Use strong PINs and passwords for your accounts and lock screen.
2. **Think before you connect.** Before you connect to any public wireless hotspot such as those in an airport, hotel, train/bus station, or café be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. Many fake networks have seemingly legitimate names.
3. **Protect your money and your information.** Do not conduct sensitive activities, such as online shopping, banking, or sensitive work, using a public wireless network or a public computer.
4. **Delete your cookies and cache**. If you use the Internet on a public computer (such as at a hotel or café) while you are traveling, be sure to delete your cookies in the web browser after you have finished. When you are on the Internet, a browser saves your information and this saved data is called a “cookie.” This data, which can include login credentials or other personal information, can then be accessed by other individuals that may use the computer

5. **Don’t broadcast your location**. Many social media platforms offer location-tagging as part of their features, which allows users to include their location when they post online. Avoid using these location features and do not announce on social media that you will be out of town. You could be telling stalkers exactly where to find you or telling a thief that you are not home.

BONUS FEATURE

How to See Everything Google Knows About You

For those who request it, I will forward an illustrated eight-page document that will guide you through the process of accessing the information Google has on you that they admit to. I’m sure there is more but this is a good start.

Finally, I am curious to know if the **URGENT WARNING** on the **YAHOO Hack** was of any use to anyone. Please let me know for future warnings**.**