SUMMER 2017 HERSHEYSMILL FRAUD PREVENTION NEWSLETTER

Summer is nearly two months away but new and recycled frauds emerge every day so I'm pushing ahead a bit to help you avoid some of them. With that said, I have realized that a quarterly newsletter cannot keep up with the scams that can show up much more frequently. However, I don't want to flood mailboxes with updates to this document so I am partnering with the http://hersheysmill.org/resources/fraud-prevention/hm-fraud-updates/ website which will feature a button for fraud updates that you can choose to view if and when you want. When it is ready I will inform all the subscribers to this newsletter.

FDA Warning for Fraudulent Cancer Treatments

It is a violation of the Federal Food, Drug and Cosmetic Act to market and sell products that claim to prevent, diagnose, treat, mitigate or cure diseases without first demonstrating to the FDA that they are safe and effective for their labeled uses. The illegally sold products cited in the warning letters include a variety of product types, such as pills, topical creams, ointments, oils, drops, syrups, teas and diagnostics (such as thermography devices). They include products marketed for use by humans or pets that make illegal, unproven claims regarding preventing, reversing or curing cancer, killing/inhibiting cancer cells or tumors, or other similar anti-cancer claims. : The products are marketed and sold without FDA approval, most commonly on websites and social media platforms

The FDA's recommendation is that consumers should not use these or similar unproven products because they may be unsafe and could prevent a person from seeking an appropriate and potentially life-saving cancer diagnosis or treatment. Avoid purchasing products marketed to treat cancer without any proof they will work. Patients should

consult with their health care professional about proper prevention, diagnosis and treatment of cancer.

To help the FDA protect others, patients and Healthcare professionals are encouraged to report adverse events or side effects related to the use of these products to the FDA's MedWatch Safety Information and Adverse Event Reporting Program by completing and submit the report Online: www.fda.gov/MedWatch/report.

To see the **list of illegally sold cancer treatments** copy and paste the following ridiculously long URL which I've done and it will work:

http://links.govdelivery.com/track?type=click&enid=ZWFzPTEmbWFpbGluZ2lkPTIwMTcwNDI1LjcyNjg2NzgxJm1lc3NhZ2VpZD1NREItUFJELUJVTC0yMDE3MDQyNS43MjY4Njc4MSZkYXRhYmFzZWlkPTEwMDEmc2VyaWFsPTE3NDA5NTUxJmVtYWlsaWQ9YWMwODQwMUBnbWFpbC5jb20mdXNlcmlkPWFjMDg0MDFAZ21haWwuY29tJmZsPSZleHRyYT1NdWx0aXZhcmlhdGVJZD0mJiY=&&&100&&&https://www.fda.gov/ForConsumers/ProtectYourself/HealthFraud/ucm533465.htm?source=govdelivery&utm_medium=email&utm_source=govdelivery

AVOID CROOKED INSURANCE AGENTS

Pennsylvania is unfortunately one of the easiest states in the US to get a license to sell insurance, especially if you have a relevant criminal conviction. Everyone deserves a second chance and not allowing people convicted of a crime to get employment guarantees their return to prison. But common sense is needed. For example, it's OK for someone convicted of sex with a minor to work in a warehouse but not in a junior high school. The same should apply in PA with regard to insurance salesmen but it doesn't in PA thanks to the 1033 Waiver program. Through this program people convicted of forgery, identity theft, or criminal fraud can get a license to sell insurance and many do.

It's easy to check out your current or prospective agent by doing the following:

Go to www.insurance.pa.gov click on **regulations,** then **regulatory actions,** then **archived actions.** You will then see an alphabetical index of names which will show you what an agent has been convicted of, if anything.

To see what this can show, I did this and picked out Ms. X from Dubois Pa who got a waiver in August of 2015. Her rap sheet: Two counts of felony **theft by deception**.

In addition to protecting yourself from a specific agent, we should try to protect all citizens by getting rid of the 1033 Waiver Program and adopt the New York state rule that agents disclose their commissions on any product they propose to sell you.

TODAY'S MAIL FRAUD

In today's mail I received an offer for a free Android tablet and a $50 VISA card. They pulled out all the stops on this one. They used the Google Play trademark, displayed the Trademark symbol for VISA, used the bank check background, had official looking check numbers and had a return address of Pennsylvania Avenue in Washington DC. This was all very impressive till I checked the office of the Accounting Department and found it was a box in the Pa Ave FEDEX.

These guys are getting more sophisticated all the time but the basic rule remains the same: If you get too good to be true offers from people you don't know, they are not true.

SENIOR SCAM PREVENTION - BINGO

As reported in the Inquirer the PA Department of Banking and Securities held sessions in April to help educate seniors to avoid being a fraud victim. This was part of Governor Wolf's Consumer Financial Protection Initiative. Although the scheduled presentations are over, you can request a presentation, perhaps here at Hershysmill.

The program attempts to provide fraud prevention education using something nearly all seniors are familiar with – **BINGO**. Using bingo cards you attempt to spell our FRAUD by answering questions such as "Why are seniors often targeted for fraud?" Answer – "They are too trusting."

The department will also be offering **Cyber Security – Staying Safe on the Internet** during April but you can probably request this session at Hershysmill also.

This is also the Department to report issues to if you or someone you know has been a victim of fraud by calling 800-600-0007.

TODAY'S INTERCONNECTED WORLD HOLDS NEW THREATS EVEN IF YOU THINK YOU DON'T PARTICIPATE

Back in the good old days there were only two things that were certain – Death and Taxes. Today you can add a third – Your internet service will be breached and your computer will be used for criminal purposes. Now you may be the rare someone who thinks they are not connected to the internet but you are if you have a baby monitor, programmable thermostat or a car with Onstar just to name a few. More come along all the time.

So what is the issue? Every day, con artists, semi-legitimate data brokers and even governments (usually foreign) are trying very hard to learn private details about us depending on who we are and who they are. If we're just regular people then crooks are

looking to steal our money. If we are government employees or contractors, the governments may want to use our credentials to hack into military or government networks.

They can use many methods including those we've already talked about in this newsletter but the Inquirer has provided a useful update.

The bad guys are looking for enough data about you so they can convince their targets that they are you to get what they're after. They may also just want to collect a database containing enough information about users to sell. This can also be lucrative and risk free. If you know where to look you can buy databases of social security numbers. This market is very sophisticated. For example, the social security number of someone who has been a victim is worth more because they are more likely to be a victim again

But it's not only stealing data that motivates these folks. Serious damage can be be done by recruiting "dumb" devices that are now connected to the internet with little or no security. One example is the recent attack where the bad guys took over thousands of internet-connected security cameras and their associated recording devices. These were then all used to simultaneously send data to a website that acts as the Yellow Pages for major internet companies such as Twitter (No comment), Paypal, Facebook, HBO, NETFLIX, and Airbnb. The beauty of this attack is they bought down all these major sites by only attacking one site. An Israeli security team provided another example when they showed they could spread a virus to Phillips Hue internet enabled smart bulbs.

So what self-protection tips do they recommend?

1. Try not to reuse the same passwords for multiple sites. I know this a pain but a simple method is to use a word you associate with the site (Shopping for AMAZON) make the first letter a capital and append your phone number. This makes your password easy to remember but very hard to guess.
2. Look into a Password Saver with a single password for it but lets you use very complex passwords for all your sites since you don't have to remember them.
3. NEVER accept the invitation to log into a site using your FACEBOOK account. You're giving away much too much information.
4. Remember that using Public WIFI is like using a postcard.
5. Look out for all the fake store apps on the APPLE and ANDROID STORES. Check the store's website first to get the correct app name.
6. Make sure your device's **firewall** is on. Ask your grandkids.
7. ALWAYS change the password for internet linked devices. Every hacker knows the factory one.
8. Only buy MAJOR brand internet connected devices even if they cost more.
9. You'll definitely need your grandkids or GEEKSQUAD for this one. If possible take non major brand devices off the network and disable the easy to use security disaster known as PLUGnPLAY.
10. Grandkids again. Separate all the Internet connected

INTERNET of THINGS devices on their own separate but equal networks (Zones.)

Chip Cards Are More Secure, But Not Foolproof

Though chip cards are more secure, they can still be compromised. If your physical card is lost or stolen, it can be used by someone else since most cards only require a signature. What's more, the credit card chip doesn't protect against online fraud, so your card could still be compromised by Internet purchases.