WINTER 2015 HERSHYSMILL FRAUD PREVENTION

NEWSLETTER #6

Greetings fellow Millers. I trust everyone is looking forward to Christmas and New Year's Eve.

Just a quick administrative note to get started. Since the Resident's Directory is only updated annually this newsletter cannot reach new residents if you think they would like to receive it please pass this on to them.

And with that it's Ho, Ho, Ho and off we go.

The Latest Hack

Just a quickie to start off with a topic that unfortunately always has new additions for every newsletter. This time it appears that Staple's has had a data breach, otherwise known as being hacked. If this report is found to be correct, Staples will join the long list of US organizations to have been targeted by hackers, including **JPMorgan Chase, Home Depot, Dairy Queen** and **Target.** So look for notices from them and as always, check your bank statements closely if paper and weekly if you are on-line.

The Grinch is Still With Us

This Christmas over a million E-Mails will be sent purporting to be from a delivery service – FEDEX, UPS, DHL, or the USPS. But they all have the same goal – to install **spyware** on your computer. They also all use the same ploy. They say they are holding a gift for you and you just need to confirm your identity by clicking on the link in the E-Mail. DON'T. If you think you might really be getting a gift, go to the carrier's website yourself.

Who Doesn't Love a Bargain?

There is an old saying. If it's too good to be true, then it isn't. This is especially true when you do a Google search for an item and find it at a price much lower than anybody else's. You will be directed to a website that looks a lot like the real one but the address will contain an extra letter or

two. Once at the website you will likely get **spyware** loaded on your computer. In addition, they probably will steal the credit card you enter. Also, on the slim chance you get something it will be counterfeit.

When Free is not So Free.

If you go to a website you are not sure of you may be offered **free goods**. You merely have to use your credit card to pay for shipping. This is a great example of **Phishing** which is another ploy to steal your credit card.

Beside **Phishing** for your credit card, you may also be offered a free download of a screen saver or ringtone. As before when you download, you will also be downloading **spyware**.

Finally, there is a non-computer version of this scam. It's cold, so who wouldn't like a free warm weather vacation? But when you call you will be subjected to a high pressure boiler room attempt to sell you an over-priced vacation club membership. As a bonus, if you bite, they might just steal your credit card as well.

Hurry Hurry Urgent

I get snail mail scams frequently too. The last one I got was a beauty. It was tightly sealed and marked in two places. They were offering me permanent relief from my time sharing maintenance fee. Of course, they had no idea where my timeshare was but they did offer a 100% guarantee (of what they don't say.) But of course this was a legitimate offer because they are a member of the Better Business Bureau (or maybe they copied and pasted it) and it was sent from a legitimate Washington DC office building address but surprisingly they didn't give a suite number.

However, I did get one to top this. It told me was a finalist in a Ford Escape giveaway despite not entering the contest. It was also the final attempt to reach me. It even had a gold seal from the West Chester Auto Pin Seal and scratch off number and tab to pull to match. Amazingly, my numbers matched.

I just point out these scam signposts FYI.

Your Money for Your Life

Recently, in New Jersey some crooks were ordered to pay $14,000,000 in restitution to the elderly people they swindled but they are very unlikely to see anything. The scheme mimicked a legitimate business whereby the company buys your life insurance policy from you for an amount less than the face value. You then make them the beneficiary and they collect when you die hopefully making a profit. This is the same bet life insurance companies make when they sell you the policy only in reverse.

However, these folks were running a Ponzi scheme by paying off their old investors with new money coming into their company from investors promised a 12% annual return.

Phone Safety

There are two areas of phone protection that I want to cover. The first involves **misdialing** and the other using **public WiFi**.

Misdialing

The problem starts when you fat finger one of the digits when you try to dial a legitimate organization's phone number. No organization is immune from AARP to the NRA.

The way the scam works is that the bad guys buy up the legitimate 7digit phone number in every other area code except the correct one. Then if you dial 866 instead of 800 you will hear a recording that tells you have won something or are eligible for heavily discounted services. The objective is always the same – get your credit card and personal information. Amazingly, this scheme is perfectly legal as long as they don't claim to be the company you called.

The best way to protect yourself is to hang up if:

The recording or operator does not provide the name of the company You called

You are offered something free but need to use your credit card for shipping costs

Asked for any personal information like birth date or SS number

Using Public WiFi

Many public WiFi sites have been infected with Spyware so if you do use one take these precautions:

Make the website starts with https: not just http:

Don’t do banking, E-Mail, or access credit card sites

Make sure your device does not automatically connect to public WiFi. This is a default setting you may need to change

If you must do these things, use your cellphone network