WINTER 2016 HERSHY'S MILL FRAUD PREVENTION NEWSLETTER

Although the temperature has been mostly mild, winter will soon make its appearance and the snowbirds will be heading south. With it the joyful holidays of Thanksgiving and Christmas are also coming and we will all be in a more upbeat and charitable frame of mind. Unfortunately, there are those who would abuse those good feelings so we need to remain at least somewhat vigilant. That said, let's all have a good Thanksgiving and a Merry Christmas,

PACKAGE DELIVERY SCAM

Unfortunately, this one peaks at this time of year. There are several variations including in person or phone versions. Essentially, they say they have a package for delivery to you but there some problem with the address and they need to verify that you are actually the recipient. For that there is a small charge maybe $2.50 or $3.00 for which he is not permitted to take cash, only credit cards. He /she will then "run" your credit card through his card reader which is solely deigned to capture your credit card information. Just tell her you are not interested.

SNOWBIRD WARNING

Actually this is a three-part alert – physical, cyber, and scams at your winter residence.

Physical Protection

Snowbird season is upon us and many look forward to warmer climes but there are criminal organizations who exist just to take advantage of older people who have seasonal residences. So here are some stay safe tips from AARP.

1. Secure your House
   Use timers on your lights. Be sure to stop or forward your mail. But you won't have to worry about snow clearing here at the Mill.

2. Enlist a What If Contact
   Make a list of things that could wrong, and who to call when they do. Examples are a car accident, robbery or running out of medicines. Former detective Joe Roubicek says not doing this is a big mistake. Especially important, share your contact information with police, pharmacy, doctors, and family members. To reduce calls home take copies of your prescriptions with you.

3. Credit Cards
   To avoid credit card rejections and help prevent fraud, notify your card issuers when you're leaving, where you're going and when you expect to arrive. Also, while away try to stick with one credit card to make monitoring easier. Even though your credit card liability is only $50, someone you give your card to can take a cellphone picture and use the information to open other accounts.

4. Home Owners Insurance
   Finally, check with your Home Owners insurance company for any extended away periods.

5. Facebook
   Don't post anything on Facebook that says something like "heading for sunny Florida next week. Also be judicious with your postings while you're away.

Cyber Protection

As always be very cautious using public hot spots. Because information is not encrypted you should always assume someone else can read what you enter so no financial transactions or shopping.

Scams at Your Winter Residence

1. The Condo Sent Me
   Fraudulent contractors show up at your door saying "the condo sent me." If you let them in they might do poor work at exorbitant prices or "case the joint." If they are a team one might distract you while the other one steals. In yet another version the con man may say he's an exterminator. After he "accidentally" sprays pesticide on you he cleans you out while you clean up. To prevent this only let in people that you have asked the condo for.

2. Parking Lot Tricks
   The scammers look for unlocked cars with out of state plates. When you can't start your car they offer assistance at an exorbitant price so keep your car locked.

SMART SPAM

Artisanal Spam

It seems that everything today is artisanal so why not spam? By now all spam filters block BLAST spam from your buddy in Nigeria. Thus, the spammers have turned to artisanal spam which is sent in small batches and semi-customized for you. It's Walmart in reverse. Instead of millions of sales at small markups these guys are after a few "sales" at high prices. And they get them because of data breaches they may know all about you that they need. For instance, if they hacked a large clinic they may know that you went, when you went and your account. In this case an E-Mail with a bill for services is quite likely to be paid.

Facebook Spear Fishing

In this scam the crooks collect personal information from social networking sites like linked-in or pinterest, etc. Once they collate this information they can craft E-Mails from a Facebook friend that looks very legitimate. When you open the E-Mail invisible malware logs every keystroke sending user ids and passwords to the crooks. This scam is very effective and hard to defend but here are some tips:

1. Look carefully at the sender. AmericanExpress.credit.com is not the same as American Express.com.
2. Remember that legitimate companies avoid embedded links that ask for personal information.
3. E-Mails are regularly hacked. If you get one from a friend with a link usually with the phrase "check this out" call to verify first. You may be the first to let your friend know that their E-Mail has been hacked.
4. Credit card scammers make their E-Mails look like your credit card issuer but they will only provide the first four or eight numbers but not the last four. They have the first eight because they are the same for everyone in your region.

SOCIAL MEDIA SELF DEFENSE

Almost half of Medicare recipients use Facebook. Even more in the 50 – 64 group. In fact, young people avoid Facebook for that very reason.

However, many seniors use other social media such as Twitter and Instagram. So here are somethings to watch out for.

- Twitter Tricks
  Cybercrooks create fake twitter accounts to look like customer care reps from legitimate companies. They do this by slipping in an extra character in the Twitter handle or a slight misspelling of the actual name. If you fall for this the scammer is watching and waiting for you to contact "your" company. They will then reply with a sign in link to a copycat website they control and will steal your user ID and password. This works really well because you are responding to a response you requested.

- Fake Live Streams
  Legitimate media companies stream TV shows and movies on line. Always willing to hop on the bandwagon, scammers offer the same thing. By posting fake comments on social websites they promise free access to a live stream. If you click on it you will have to provide credit card information for a free trial you can "cancel anytime. When you provide the information you will be subject to credit card theft, an unwanted monthly charge on your credit card or maybe both.

- Fake Freebies or Discounts
  The purpose of these sites is really FISHING for credit card numbers. Again it starts with a copycat social media page that looks real. The offer is for free or almost free products and services. However, in order to get them you must provide information and a credit card which leads to identity or credit card theft, and not just once because these sites will sell your information to other cybercrooks. If you want freebies go the manufacture's web site.

- Contest and Survey Scams
  If you fill out the survey you will get a prize. If you want to enter the "free" contest you must first fill out an entry form. The objective of the scam is the same in both cases – to give the bad guys information about your income, occupation and spending habits. This is a goldmine for identity theft and a great help in spear fishing people you know.

- Celebrity Based Traps
  Cybercrooks are like bees, they go where the pollen is. In this case, one of the most popular internet searches is "Celebrity+Picture+Video". The scammers pay Google to go to the top of the search engine list and their links take you to websites that promise you anything such as nude pictures or juicy gossip for a fee paid by your credit card. By now, you should know what happens next.

SCAM WARNINGS FROM MASTER SCAMMER FRANK ABAGNALE

Let's finish with two warnings from the master himself.

First one. You write me a check. I take the check and go to an on-line check printing service and order checks in my name but with your account and routing number. By the time your monthly statement arrives the checks have cleared. The only thing I can see to control this is to use on-line banking and check weekly.

Second one. Don't be too social on social media. Especially don't use a straight on photo of yourself because there are devices that can take that photo and match it on line with say a driver's license. Instead, post a photo with friends, preferably doing an activity. Also, never post your real birthdate and where you were born. Follow these tips because these can be the key to identity theft.