SPRING 2017 HERSHEYSMILL FRAUD PREVENTION NEWSLETTER

Spring is just around the corner and it's giving us a nice preview these days. When spring comes a young man's fancy turns to love but so can unattached seniors as well. Unfortunately, our scammer friends are always on the alert for new opportunities so we'll start with some advice on protecting yourself.

AVOIDING THE SWEETHEART SWINDLE

Although this is an ancient con, modern technology -online dating- makes it much easier to find victims. The scam remains the same though. Pose as the perfect suiter, start a romance, steal the victim's money.

To protect yourself, know the warning signs. First, they want to leave the dating site and communicate directly to talk by phone or E-Mail so they have personal information. Second, they will always avoid meeting you or cancel if they do. Third comes the pitch. This happens at some point with a plea that your sweetie (who you've never met) is in a jam out of town (jail, lost credit cards, etc.) and needs money ASAP.

In addition to the signs, be proactive. Search their full names. See if their photos or claims match what you find. Check photos carefully because they are often models or publicity photos.

CAN YOU HEAR ME NOW?

This one has two basic threats but the first one has multiple disguises.

Say YES

This one may or may not cost you money based on how much the scammer already knows about you. The caller may say anything from they're a home security service to Social Security. They will then ask a question like "Can you Hear Me?" If you say YES they record and attach to their script that asks you if you want buy something. That's usually not enough, but if they have, or get credit card information they can play the recording to prove to the credit card company you said yes. They can also intimidate people by playing the recording to get you to pay.

ANSWER The Phone

For this one to work you don't have to say anything. It is a Robocall that will record the fact that you answered. This increases the price the scammer will get for selling your phone number.

Protect Yourself

There's no perfect way to protect yourself but I use a pretty simple method. I look at the caller ID. If it's not someone I know I let it go to the answering machine figuring that any legitimate caller will leave a message.

SCAMMING YOU WITHOUT YOU

Scammers and other criminals continue to evolve. In the latest iteration they can scam you without your involvement. This can take many forms. Here are a few examples.

Loans or Withdrawals

Your credit card and other personal information may be available via data hacks of merchants or banks, or as a result of being scammed previously. As I've noted before the most valuable name for sale is someone who has fallen for a previous scam. With sufficient information, the crooks contact a bank or credit card call center and take out a loan or open a credit card in your name.

Checks

This one is pretty straight forward. If you put your name address and phone number on your checks along with your account number that might be enough to enable crooks to simply order a supply of checks drawn on your account. To help prevent this I only put my first initial and last name on my checks.

PHYSICAL THREAT SCAMS

These threats can be quite frightening. Here are two:

Hitman Hoax

In this one a tough sounding guy says he has a “hit” contract on you but he will cancel for a payment.

Virtual Kidnapping

In this scenario, the kidnappers have a loved one who is being tortured. Because of the noise and screams you can’t really identify if the voice is really who they say they are as they plead with you to pay the kidnappers.

HOW THE SCAMMERS WANT TO BE PAID

Scammers used to ask you to WIRE them your payment or send a PREPAID CREDIT CARD. But two things have happened to stop this. First, consumers became aware that these requests usually signaled a scam. Second, the FTC made it illegal for telemarketers to ask for payment that way.

Of course, scammers always adapt. The new method is for you to purchase an ITUNES (or other) GIFT CARD and load money onto it. They then ask you for the 16-digit code which allows them to drain the card.

ARTISANAL SPAM

We live in the artisanal age (customized, specialized products) so why not spam?

What is It?

Traditionally, spammers relied on sending out vast numbers of E-Mails needing only a small number of replies to make money. Artisanal spam works differently. They send out a small number but expect a very high percentage of replies. They can do this because the spam is customized for the recipient. They collect information from public sources like LINKED-IN, FACEBOOK and corporate websites. Also, sometimes they have hacked an E-Mail account that had you as a contact.

How to Protect Yourself

Nothing new here. Follow standard safety practices. Don't click links. If it seems different than your friend's normal E-Mails call them to make sure they sent it. If not, be sure to tell them the account has been hacked and to send an E-Mail to all contacts warning them.