FALL 2017 HERSHEYSMILL FRAUD PREVENTION NEWSLETTER

Fall is upon us. If you can believe it the school buses started running this morning. So while the kids begin their new yearly school cycle, I have to return to the quarterly cycle of passing along news of the latest frauds to help keep the readers safe.

This leads me to couple of points that readers have asked and I think everyone should know. First, you don't have to give up your subscription if you move elsewhere. So long as I have a current E-Mail address your subscription will continue. Second, I have been asked to allow other communities to distribute this newsletter. I have absolutely no problem with that. Third, although most of you are already aware of this, a quarterly newsletter is too slow to protect you so for those who use the internet I put alerts out on the Hershysmill web site as I become aware of them. The web address is http://hersheysmill.org/.

And now to the news of what our scammer friends are up to.

Debit Cards Don't Provide the Same Protection as Credit Cards

The problem is that there has been a recent increase in debit-card fraud. From 2015 to 2016, the number of debit cards compromised at ATMs and merchants nationwide jumped 70 percent, according to FICO Card Alert Service.

Here's an example. A woman had simply wanted a free sample of face cream and agreed to pay the shipping cost — $5.99. But the day after she used her debit card to place the order, the on-line company put through two different and unauthorized charges, one for $92.92 and another for $89.95. The fraudulent fees made her account overdrawn, which resulted in a $39 penalty from her financial institution.

Although this theft wasn't at an ATM, it was yet another reminder of how vulnerable consumers are when using a debit card connected to a bank account holding their household money.

Keep in mind that with a debit card there is not much of a delay from the time of your purchase until the funds are withdrawn. This means fraudulent transactions can quickly do a lot of damage. And you may not get a refund soon enough to cover any bills you have coming due.

The credit card company logo affixed to their debit card doesn't translate into the same protections offered by a credit card. If you want to get further information, read this post from the Federal Trade Commission: "Lost or Stolen Credit, ATM, and Debit Cards" (https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards)

In summary here is your liability:

●Zero dollars if your debit card is reported lost or stolen *before* an unauthorized transaction;
●$50 if, after you learn about the unauthorized transaction, you report it within two business days;
●$500 if the fraud is reported after more than the two business days but fewer than 60 calendar days from getting your statement.
If you fail to report a fraudulent charge more than 60 calendar days after

you receive your statement, you cede all protection. All your stolen money could be gone.

Here's a good tip from a bank. They recommended opening a second checking account just for your debit card and keep a few hundred dollars in that account and replenish as needed, from your regular checking account.

Bank Fund Recovery Scam

Here's one recently received by a resident who checked with me about this E-Mail she received. It is a fraud but it's a fairly clever one. In PA if you leave money inactive in a bank account for a defied period of time the money must be turned over to the state. The state then enters the money in a database with the owners name. This database is searchable and if find money in it that is yours you can claim it. The important point here is that the state does not reach out to you.

Our resident received the E-Mail shown below. There are two parts to it. The first is the alleged amount of money they have discovered for her which she claims is not true. The second is the 15% fee they charge.

The first issue here is that you can go on the PA website and collect the money (if it exists) yourself at no charge. The second, and more significant part, is that you have to return the claim forms to them for submission. Those forms contain all the information scammers need for identity theft so don't do it.

This next one is courtesy of our AARP friends.

Government Grant Scam Hits Facebook

The federal government grant scam has been around for years. But now, scammers are finding targets through social media.

- You see posts from people on Facebook claiming they have been awarded tens of thousands of dollars in a grant from the federal government, and that you could be eligible, too.
- You call the listed phone number, give some personal information, and are told you qualify—all you have to do is send a money order or provide your bank account information to cover processing fees.
- You never get the grant.

- Government grant applications and information about them are free.
- The "Federal Grants Administration" – the agency the scammers say they work for – does not exist.
- If you didn't apply for a federal government grant, there is no way you would receive one. If you're offered a grant you know nothing about, it's probably a scam.
- Never pay money for a "free" government grant.
- If you think you may be a victim of a government grant scam, report it to the Federal Trade Commission at www.ftc.gov/complaint or 1-877-382-4357.

When it comes to fraud, vigilance is our number one weapon. You have the power to protect yourself and your loved ones from scams.

What is Ransomeware and How Do you Get It and What Can You Do?

Ransomeware has been in the news a lot lately, so what is it? As the name implies they take something you need and you have to pay them to get it back. In this case the stolen item is your data but it never actually leaves your computer. They simply scramble it using a code word only they know

and you have to pay them to get the decoder ring to be able to use your data again. As an added bonus the price goes up the longer you wait. Since the initial asking price is usually $300 my advice is to pay up. Don’t feel bad. Many big companies have been victimized as well. Also, amazingly, if you have trouble the provide ab 800 support line (how nice.)

Since ransomeware is malware the only defense are the usual tactics. Don’t click on E-Mail links or visit strange sites.

Another From AARP

Be Wary of Door-to-Door Home Security Sales

The summer months unleash door-to-door sales agents in communities across the country. We've received reports of a scam run by con artists claiming to be from home security companies. While many home security companies conduct legitimate business using door-to-door sales agents, be wary of anyone using high pressure tactics or creating a false sense of urgency – common traits of a scam!

It may be a scam if an agent comes to your door offering a great promotion on a home alarm system, but you have to act now to get the deal. Or, if you have a home alarm company sign in your yard, the person may say he is a technician from that company and he's there to install system upgrades.

- Home security scams are hard to spot because scammers work hard to make the deal look legitimate.
- The scam artist may claim you'll get a big insurance discount by purchasing an alarm system, butthat isn't usually the case.
- A legitimate alarm company would never send a technician to upgrade equipment without first making an appointment with you.

- Realize that not all salespeople are legitimate and approach a door-to-door deal with caution.
- Rather than accepting offers at your door, get references from friends and neighbors when looking to buy a home security system and then reach out to the company yourself.
- When you are approached by a door-to-door sales agent, research the company by entering its name into an online search engine, to see if any complaints come up.
- If you do decide to accept a door-to-door offer, read the fine print. The written contract should include everything you agreed to orally.
-

If you do sign up for a home alarm system or an upgrade, and then regret it, you have a three day "cooling off" period during which you can cancel

your purchase, thanks to a rule by the Federal Trade Commission. It applies if you sign the contract at home or a location that is not the seller's permanent place of business.

Don't Fall Victim To Harvey Flood Scams

As Harvey, the largest rainstorm in the history of the continental United States, floods homes in Texas and Louisiana, many Americans want to send money for relief efforts.

The need for that help will be enormous: FEMA Administrator Brock Long has said more than 195,000 people already have registered for disaster assistance.
Many reputable organizations already are delivering food and care to those in need. But experts on charitable giving say donors need to be wary: con artists are also after your money. Scam charities raised hundreds of thousands of dollars in the aftermath of 2012's Hurricane Sandy, and they are likely to try it again now. Here's are tips from legitimate sources, such as the Federal Trade Commission's web site, on how to safely donate to Harvey relief efforts.

Know where your money is going.
Contribute to organizations that have an experience assisting in disaster relief, and be skeptical of charities that pop up solely in response to Harvey or those with unfamiliar names. You can check out charities with the Better Business Bureau's (BBB) Wise Giving Alliance, Charity Navigator, Charity Watch, or GuideStar.

Never give out cash.
Give your donation by credit card or a check made payable to your charity of choice.

Understand crowdfunding.
Scammers may claim to represent legitimate organizations online. The crowdfunding website GoFundMe created a Medium post about safety measures being taken to protect those donating to relief efforts, and all verified GoFundMe Harvey-related campaigns as hosted at an official page.

Check a charity's website before you text a donation.
Confirm that the charity has authorized donations via text message — and keep in mind that your contribution may not reach the charity until after your phone bill is paid. It may be faster to donate directly to the charity.

Be wary of clicking on links or opening attachments in e-mails.
Unless you are sure you know who sent it, don't open attachments that could install malware on your computer. And don't assume that emails you get — or social media messages you see — have really been posted by the legitimate source. They might be fake.

Report suspicious organizations.
Be skeptical if an organization will not send you information about their programs and finances: any legitimate organization will be glad to provide you with this information. The Better Business Bureau Wise Giving Alliance has charity reports on thousands of U.S. charities. If you believe a scam may be taking place, you can contact the BBB to report what you know.