FALL 2018 HERSHEYSMILL FRAUD PREVENTION NEWSLETTER

No scenery this time. Been looking forward to fall since February 4th.

I believe this is the 17th edition of this newsletter. In previous issues I've talked about scams and frauds in general although I've emphasized seniors for obvious reasons.

In this edition I feel the need to take a little different approach and will cover a main topic that is the basis of many of the individual scams previously identified as well an update on spam calls. I want to take this approach for two reasons.

First, people don't realize how serious of a threat Identity Theft can be, especially Medical ID Theft. I want to show how the combination of lax corporate security and a secret version of the web called DARKNET make it easy to do, and how difficult it is to prevent it. Also, I'll talk about how likely your information is for sale on DARKNET and explain a little about where it came from and how it works.

Second, there are some steps you can take to safeguard yourself at little or no cost. It's not worth paying for credit protection services like LIFELOCK.

Also, for those of you who get the AARP newsletter and magazine you will note that I have borrowed freely because they are much better than me at explaining the right technical detail so people understand.

ID THEFT AND THE DARKNET

Let's begin with the first issue. How likely is your personal information for sale? My working assumption is that it is far more likely that it is, than it is not. Why would I say that? Just think of all the data breaches that have occurred at major retailers like Target,

some financial institutions, and the biggest of all – EQUIFAX – which exposed over 50% of Americans. Also, remember that these are only the revealed known breaches. Some companies don't tell. In addition, many successful hacks are never discovered at all. Also, AARP's advice is to assume your personal information has been stolen.

Also, one other brief note. Often the hacked companies say the crooks got this information but not that. If it takes them six months to discover they've been hacked, how can they possibly know what the crooks got.

OK, so now your information has been stolen. How does it actually get sold? Here's where the DARKNET(DN) comes in. The DN mainly differs from the regular web in that people who use it do not want anyone, except the entity they connect with, to ever know who they are or what they did.

DN actually has a legitimate purpose when used by dissidents in a dictatorial country, like China or North Korea. But its primary purpose is to buy and sell illegal goods and services. Sometimes it's drugs, guns or even hitman services. But for our purposes we'll look at stolen IDs.

The DN functions just like the regular web. It has advertising, likes, customer reviews as well as very good customer service. In addition, it follows the laws of supply and demand.

Now you may wonder how it is that between GOOGLE, AMAZON, and FACEBOOK just about everything about you is known, and sold. How can these guys operate in secret? The answer is special software developed by the US Navy in the 90s and publicly released in 2003. It was designed for use by spies, so it makes it impossible to identify who or where the user is.

What kind of stolen personal information can I buy there? The best user data product is a FULZ. A FULZ contains SS#, DOB, Mother's maiden name, address, phone #, driver's license #, passwords, Computer IP address and more.

These can sell for $20 to $30 each as opposed to credit card #s for $.50, or SS#s for $3.00. Those belonging to the elderly cost the most for three reasons. They usually have money, good credit, and most don't check their finances online. In fact, nearly two thirds of seniors do not have on-line account access.

Two final additional things to watch. If you are a really good target, crooks will take one or two more steps to thwart security measures you have taken. Suppose your bank asks you for your brother in law's first name as your security question. The criminal may use your info to get into FACEBOOK where you may have shared that information.

Another, even scarier trick involves something I use called Two Factor Authentication. It simply means that when I log onto Vanguard they send me a code by text to my regular

cellphone which I need to log on. I have to enter this 6-digit code to continue. However, even this method can be compromised by someone cloning your cellphone. An effective counter to this is to also use a security question although this is usually not necessary.

FIGHTING BACK

Before I discuss how to protect yourself, realize that laws and law enforcement agencies will catch some bad guys but never all of them. Also, when caught many cybercriminals go out in a blaze of glory by freely releasing all their stolen information all over the DN.

There are some effective steps you can take to protect yourself as I show below:

Let's start with a simple but not very effective first step. If you go to the EQUIFAX website they will run a DN scan for your name. It will usually come back negative which doesn't mean much because they can only see a few sites. If it comes back positive that means your personal information is everywhere.

The basis of the defenses I discuss below is that most people are really easy marks. If you make it more difficult for the thief he'll simply move on to the next victim.

BEST DEFENSE

Freeze Your Credit Accounts

Implement a credit freeze with ll three major credit bureaus: EQUIFAX, TRANS UNION and EXPERIAN. If you do, you'll be safer than 86% of other adults. See aarp.org/creditfreeze

If this is so easy to do, why haven't the vast majority of adults done it? My guess is inertia or lack of understanding how important it is.

Cost used to be an issue the price was$10 to freeze and unfreeze your account but I believe most states have, or will, remove this cost.

Another reason might be the inconvenience. If you want to apply for credit card or store credit you will have to unfreeze your account before they can verify you. This is usually a simple over the phone process IF you have the Pin # you were issued upon freezing your accounts.

OTHER GOOD MEASURES

Monitor Your Accounts

Sign up for on-line access for every financial account you have and schedule a one-hour time slot each week when you check each one for activity that you did not initiate. If you see any call the institution's 800 customer service fraud line to discuss it.

Use Two-Factor Identification

This extra security step is, or should be, offered by financial institutions and GMAIL. It simply means that when you login, a one-time time limited code will be sent to you by text, E-Mail, or voice. You will have to enter this code to continue. Someone who steals your ID and password likely hasn't stolen your phone.

Use Security Questions

Some financial institutions will offer the option of answering a security question to login. This is an alternative to two-factor identification but not as secure as your answers could be available on the DN.

Use a Password Manager

These commercially available software tools help alleviate one of the worst things people do to compromise their on-line security. They use the same password for multiple accounts, or use passwords that are too easy to guess. The reason people do this is that it's hard to remember all those passwords. With a manager you only have to remember one.

Also, when a company is hacked they will often recommend changing ALL your passwords which almost no one ever does. However, a manager makes this much easier, and therefore more likely to be done.

UPDATE ON PHONE SCAMS

I have personally experienced both the increase in spam calls to my cellphone and neighborhood spoofing using the area code and exchange (first 7 digits.) The only way I have to deal with them is to let them go to voice mail if I do not know the number. Almost all of the spammers will not leave voice mail unless it is the IRS or some other threatening spam call.

Nearly half of all cellphone calls next year will come from scammers, according to First Orion, a company that provides phone carriers and their customers caller ID and call blocking technology

Scammers also trick people into answering their calls with a scheme known as neighborhood spoofing, in which they manipulate caller ID information so that their actual phone number is masked. Instead, the calls appear to have been placed locally. A person looking at their caller ID will see a number that matches their own area code, as if the caller is a neighbor or a relative. Because the number appears familiar, people are more likely to answer the call.

Other prominent spam calls involve fraudsters pretending to be a representative from a bank, a debt collector or cable company.

The Internal Revenue Service has also warned taxpayers about phone scams. Callers use telephone numbers that mimic actual IRS assistance centers, claim to be IRS employees and use fake names and phony badge numbers. The IRS says victims are falsely told they owe money to the government and are urged to pay through a gift card or wire transfer. Scammers may also take advantage of the devastation caused by Hurricane Florence, the IRS warned. Scammers can pose as a charitable organization, preying on the generosity of Americans who want to help those affected by the storm.

Certain apps can block calls from known scammers, but First Orion noted that the tools can be ineffective if fraudulent callers use numbers that aren’t already blacklisted.