SUMMER 2019 HERSHEYS MILL FRAUD PREVENTION NEWSLETTER

A NEW KIND OF FRAUDSTER IS COMING FOR YOU AND HE'S NOT AFTER YOUR MONEY, HE'S AFTER YOUR VOTE

By now we are all aware of the various attempts to influence the 2016 election through fake postings on FACEBOOK and other social media. Hopefully, regardless of your political affiliation you want to cast your vote based on true information and not be manipulated by political actors or foreign governments.

Unfortunately, we can expect more of the same in 2020 so be aware.

However, my point here is to inform you about a new, and more powerful manipulation not seen in 2016. Scammers now have the technical ability to "doctor" videos so well that no person can tell they are faked. I'll discuss the two types below.

Doctored Real Videos

In this scenario a real video is used but is changed with widely available software tools.

One type is inserting a damaging item into a real video. An example would be a speech by Pat Toomey inserting a North Korean flag just behind him.

The other type is simple editing a real video to make the speaker appear to have issues. An example of this type would be the recently released video of Nancy Pelosi changed by simply slowing the speed and a few other tweaks to make her appear drunk and disoriented.

Inserting a Real Persons Face and Voice into a Real Video.

This technique is particularly insidious because it cannot be detected with the human eye.

One example of this would be to show Donald Trump's face in a gay porn video.

Another example would be Bernie Sanders encouraging a group of ISIS volunteers to attack America.

The reason I have chosen such disturbing examples is to show that there are no bounds to this technique.

If Technology Can't Protect Us, What Can I do?

I sincerely hope you asked this question because you want to protect our democracy by protecting our votes from manipulation.

The best defense against these techniques doesn't involve technology and is very simple. Good Old Yankee Skepticism. For example, you know that Mr. Trump would never engage in the activity shown in the video. So in this case, follow his advice that "what your eyes see is not what's happening." Same for Bernie and ISIS.

Also, the same defense applies to "doctored" videos.

You know that Pat Toomey is not a supporter of North Korea.

One final technique. If the video is the first time you are hearing and seeing the accusation about a long time public figure, you should assume it's a fake till someone proves different. The Pelosi video is a good example. As far as I know, no one has ever accused her of being drunk in public before this.

A SCHEME WITH THE OLD PURPOSE – GET YOUR MONEY – BUT WITH A WHOLE NEW APPROACH

For as long as I have been writing this newsletter all the frauds I describe aimed to get the most money they could from you if their fraud succeeded. The new approach is to get small amounts on an on-going basis. The premise is that you won't notice the small amounts, or you may decide that trying to get them removed is surprisingly more difficult than you would think.

Before I explain the scam, I want to give credit for this to the Inquirer and urge you to support real journalists who actually investigate things that need to be looked at.

The scam starts when your credit card has been compromised, which nearly all of the cards have been. The thieves then use that number to open a SUBSCRIPTION in a fake name. Opening a subscription is the key here. It can be a NETFLIX subscription, but more likely a $1.99 per month subscription for additional storage on GOOGLE. They then sell the SUBSCRIPTION to their customers for less than GOOGLE or NETFLIX charge.

At some point you notice the charges and dispute them with your card issuer. Most likely they will cancel the charges and issue you a new credit card. However, that doesn't help because of a credit card industry procedure called the UPDATER. This is a feature intended to give card holders better customer service by automatically notifying your subscription vendors when your card number changes. This allows the subscription to continue uninterrupted without you having to do anything. I have this service used for me and I appreciated it. Unfortunately, now it has the effect of keeping the fake subscription going and you continuing to get charged monthly.

When you recognize these fraudulent charges and try to deal with them it can be a frustrating experience. For example, assume that you need to deal with your card issuer (CAPITAL ONE) and your merchant (GOOGLE). Each may say the other is responsible to fix the problem. At this poin,t not everyone may continue to fight. Some people just decide to keep paying.

By the way, if you think the scammers are making penny ante profits with this scheme that is far from the truth. Some of these scammers may have thousands of such subscriptions, and the top ones make millions.

So how can you deal with this if it happens to you? There are two ways:

First, contact your credit card issuer and ask to be removed from the UPDATER. This means when you get your new card you will have to notify any subscription providers who charge that card.

Second, you can ask the issuer to block payments to the subscription provider, and after a few missed payments they will cancel your account.

WORK AT HOME SCAMS

Because working at home is appealing, especially for seniors, this area is ripe for con artists. They are so common they make the FTC's Top 10 Complaint List.

The key scam indicators are: 1) Higher pay than is reasonable for the "work" you will do and 2) Up Front fees to learn more about the offer.

Four Protection tips to guard against this scam:

- Be a Detective and investigate. Good resources are the Better Business Bureau (BBB), local Consumer Protection agency, State Attorney General and our old friend GOOGLE. Search for the company name and any people mentioned on the website.
- Ask specific questions. What will be my duties? Does the job pay salary or commission? Who will pay me and how often?
- Don't fall for the ADVANCE part of this scam. They will tell you that they will directly deposit an advance into your bank account so they will need your account information. Don't do it.
- Don't give out any personal information. They will say they need your SS # for taxes. They might have a reason they need a credit card. Simple answer – NO!

THIS JUST IN

Too bad France doesn't subscribe to this newsletter or they would have known about the "I've been kidnapped grandma. Send money scheme."

French police are investigating a man who made $90,000,000.00 by posing as France's Foreign Minister and saying he was working with the Defense Minister to free French citizens kidnapped by Islamists. However, he had a leg up on other scammers. He actually had a realistic silicon mask of the Foreign Minister and hat behind an impressive desk on the video calls. Sometimes you just have to admire someone's guts and cleverness even while you send them to jail.

PS although I'm poking fun here, realize that with DEEP FAKES he wouldn't need the mask and could have been anyone he wanted.