NEWSLETTER #2

Before beginning this issue of the newsletter I'd just like to explain where the material comes from and what I hoped to accomplish. First, the material in here is not original with me. It comes from a variety of sources that I use for research such as Consumer Reports, the Inquirer and news items. Second, other material comes from security industry publications and web sites as well as conversations with people in the field.

My objective for this publication is help you understand the scams, why the crooks do it, and how to protect yourself. With that, off we go.

This issue deals with three scams and a potpourri of tips to help keep you safe . The first is one that the New York City Prosecutors Office and the FBI consider an epidemic - The **PAY UP or ELSE** fraud being perpetrated by illegal bill collection agencies.

The second is the **MICROSOFT or OTHER VENDOR TECH SUPPORT SCAM**. I am especially glad to present this one because I have received inquiries on it from HM residents who have been contacted. Please call or E-Mail with suspicious contacts you receive so we can cover them in this newsletter.

The final scam in this issue is a come-on to **ELIMINATE YOUR TIMESHARE FEES FOREVER**. Too good to be true? It is.

ALERTS AND TIPS TO PROTECT YOURSELF FROM BEING SCAMMED

THE PAY UP NOW OR ELSE SCAM

In a moment I'll describe this scam but you should know that because it involves the claiming of frightening consequences from legitimate agencies, it is working very well for the scammers. For example. a recently closed Georgia company collected $4,000,000 from 6,000 people who did not owe anything through the combination of threats described below and illegal debt collection tactics.Also,since scammers copy anything that works, it is spreading so rapidly that the US Attorney in New York city described it as an epidemic a week ago at a news conference to warn people. And just to show no one is immune the FBI Agent in Charge of NYC said that they had even tried to scam him.

How Does it Work?

The scam itself is pretty simple. You receive a call, voice mail message, or E- Mail from a "Debt Collection Agency." They say that you allegedly owe money to a scary Federal Agency (IRS), law enforcement (Police, Courts, Attorney General), or your utility company.

The basic pitch is that you owe money and if you don't pay up or call back IMMEDIATELY terrible things will happen to you. You will be arrested, your car will be repossessed , or your gas or electric will be turned off immediately.

The people running these shows were trained in the high pressure penny stock boiler rooms of the 1990s so they are relentless and shrewd. They will use legal sounding phrases the best of which is "the

statute of limitations has run out on your civil and legal rights." Truly a classic.

They will also send fake documents that look quite legitimate.For example, they may name government criminal collections task forces that simply don't exist.

Signs That It's a Scam

This section is really unnecessary. This approach is always a scam. First, real government agencies and utilities will almost always contact you with registered mail and try to collect before turning you over to a Debt Collection Company.

Second, the legitimate agencies first attempt may ask for money and spell out consequences, but the demands are not immediate on first contact. And, since using the postal mail for fraud is a serious offense, scammers use E-Mail or phone calls. Also, don't be fooled by the official-looking caller ID. Using computer-based calling, scammers can display any caller ID they want.

Finally, another sign of the scam is the payment method. Either they want you to wire them the money or let them deduct it from your checking account. ABSOLUTELY NEVER do this.

What Should You Do if They Call?

The answer is pretty simple. Tell them to put their claim in writing with ID and phone numbers as well as physical addresses for everyone involved with this case so you can discuss it with your attorney. Most likely they will hang up. If not, do so immediately and whenever they call again. If they were legitimate they would have no problem complying with your request.

While the response above sounds simple you might need to be prepared for an arduous battle.Keep in mind that this is their job and they work on commission. Just keep on ignoring them and eventually they'll realize they are wasting their time with you, and time is money to them. If it becomes too difficult, talk to the police department for suggestions.

THE MICROSOFT (OR OTHER VENDOR) SCAM

I especially appreciate the opportunity to discuss this one because several HM residents have called or E-Mailed me on this one.

How Does It Work?

There are actually two versions of this deception. The first is not so much a typical illegal scam but an attempt to sell you something you don't need from a somewhat legitimate vendor. The second version is more insidious in that they charge you for stealing your identity.

Version 1 - The Vendor Scam

You place a technical support call to the 800 number for a software product installed on your computer. A very polite person offers assistance which usually works. However, in working on your computer he

has found there are some significant issues affecting your computer's performance that he can fix remotely for usually $100 to $300. Alternatively, he has discovered that your computer is infected with malware with the same fix pitch. If you refuse, he will offer to show you error logs that prove his claim, but of course they wouldn't mean anything to you and are almost always normal anyway. If you still refuse, your polite technician can become quite pushy.

What Should you Do?

Actually, quite short and sweet. Reply **No Thanks, if I need help I'll call back. Bye.**

Version 2 - The Real Scam

In this version, identity thieves have gotten hold of a software vendors customer list which is quite easy to do. The difference here is that the scammer is not interested in stinging you for a couple hundred bucks. He's after your identity so his approach is different He will call you and to describe a scarey bug or infection in their software that he will fix for free. All he needs is for you to allow him to have remote access to your computer and everything will be fine. If you allow this, everything will be fine for him because he will have infected your computer with invisible software that will silently send him every account number and password you enter.

What Should I Do?

In this case, if you didn't initiate this call just follow the old 70s line and **Just Say No** and hang up.If you are still concerned, call your software company's hotline and ask if they are aware of any such issue.

TIMESHARE FEE ELIMINATION

How Does it Work

Scammers are acutely aware of your pain points. One of the biggest regrets many people have is the yearly fee for a timeshare they no longer want or use. Therefore they are vulnerable to a letter like the one I recently got. It was specifically addressed to me at HM. It even said "Dear Allan" They nicely informed me that I was eligible to eliminate all future timeshare fees including 2015 if I acted by 12/1/2014. They also said this was my last opportunity because they had unsuccessfully tried to contact me previously. They even gave me a reference number for when I called them.

What they didn't explain was how they would get the Timeshare management company to drop fees I was legally required to pay them.

For those who get this letter the sender is **Property Management Services in Rockville, Md.**

What Should I Do?

Most HM villages provide paper recycling. This should go there immediately.

A POTPOURRI OF LITTLE TIPS TO MAKE FOR A SAFER HOLIDAY

1. Never post your travel plans on social media. You can do that along with pictures and descriptions after you're home. Burglars and scammers love to know when you're house is empty and your mail will be uncollected.

2. Open a **PAYPAL** account and use it instead of your credit card wherever it's accepted. It's always a good idea to not give out your credit card number, expiration date, but especially your security code.

3. Sign up for on-line account access at your bank and credit card company and check charges weekly. If you're compromised the less time you give the scammers the less you will have to undo.

4. To avoid receiving credit card applications that can be stolen from your mailbox and used, sign up to opt out credit card mailings by going to **optoutprescreen.com** or call **888-567-8688**. Scammers frequently steal these from mailboxes and open credit cards in the recipients name.

5. Put your landline and cellphone on the National Do Not Call List at **donotcall.gov** or call **888-382-1222**. That way solicitation calls can usually be assumed to be scams.

That's it for this newsletter but there's much more to come as scammers never rest.

Have a great Holiday and stay safe. See you in the next issue.

Allan Pomerantz