**SUMMER 2015 HERSHYSMILL FRAUD PREVENTION NEWSLETTER**

**Newsletter #5**

Greetings fellow Millers. Hope you are enjoying a great summer of 2015.

Now that the annual mailing list update has been issued, for those of you who a are responding for the first time to my annual E-Mail asking if you would like to receive this newsletter as it is periodically issued, you should be aware that there are four previous newsletters that are available if you ask for them when send me an E-Mail requesting to be on the distribution list .Please realize that I try not to repeat myself in new editions but fraud is unlike the news. Nothing ever gets old. In fact, if a scam hasn't been around for a while that's a perfect incentive for crooks to reuse it. Therefore, you should request the previous editions because they will each cover some unique scams.

Now on with the show. recipients

# AOL USER MAILBOX SCAM

**I** want to mention that although this scam is directed at AOL uses the comments apply to all E-Mail providers.

On Saturday my brother-in-law whose in an AOL user received the following message a person named khadijagasang sent to **undisclosed recipients. That** alone should indicate caution, but the fact that sender is **Service Info** and not **AOL** is pretty much a dead giveaway. The clincher however is the subject **@I N F O**. Note that it makes no sense. It is simply designed to evade SPAM filters.

-----Original Message-----
From: Service Info <khadijagasang@gmail.com>
To: undisclosed-recipients:;
Sent: Sat, Jul 11, 2015 6:23 am
Subject: @I N F O

Your mailbox has exceeded the storage limit 1 GB, which is defined by the

administrator, you are running at 99.8 gigabytes, you can not send or receive new messages until you re-validate your mailbox.

To renew the mailbox,

Click Here

**WARNING!** Protect your privacy. Logout when you are done and completely exit your browser.

Other dead giveaways in this amateurish scam is that it says that the mailbox limit is a billion bytes (1 gigabyte) but it says you have used a hair under 100 gigabytes. Trust me, you would never be allowed to do that on any system. Also, there is no such activity as **Renewing Your Mailbox.** However the valid W**arning** to close your browser is a cute touch.

## IT'S TIME TO GET SERIOUS ABOUT ON-LINE PRIVACY

The former president of SUN Computer Systems (now part of ORACLE) made a very chilling but very accurate statement about on-line privacy a couple of years ago. He said “Get over it. On-Line privacy is dead.” Although the statement caused quite a fuss when he made it, in my opinion it is much truer today than it was then. As an example, below I will show you 12 steps (not the 12 Step Program although that's not a bad comparison) that AARP suggests to protect yourself on-line. Some of them I have already recommended but it's good to have them all in one place for reference. The irony of this is I detected that this AARP web page about privacy was using 19 separate programs to track my visit to the site and maybe more. None of them worked because I use a free, simple program that identifies them and allows me to block them from seeing my activities. If you ask I'll be glad to tell you how you to get and use it.

A further issue that I have heard from my friends and relatives is “Who cares if they see what I'm doing?” There are two answers to this objection. First, everything they see you doing is sold to shadowy company called a DATA BROKER. These companies combine every track you leave on the internet such as Facebook LIKES, discussion groups you belong to, public tax and mortgage data along with your location and probably your age and other data to present a very detailed picture of you

to anyone who will pay them which is usually advertisers but could be unknown others,

The second reason is that such trackers may have the ability to store malicious programs without your knowledge that can steal your passwords as well as other nasty surprises.

So without further ado, here is AARP's 12 Step Program to protect your on-line information which applies ware whether you doing  your banking, shopping, or just checking your email online .

# PROTECTING YOUR ONLINE DATA

**Secure your passwords:** You've heard it over and over, but a strong password is your first defense against scammers. DO use complex and creative passwords: experts recommend thinking of a special phrase and using the first letter of each word as your password, or substitute numbers for some words or letters. Do not use the same password for all your accounts; do not write your passwords down or share them with others; and change your passwords frequently.

**Use two-factor authentication:** Lock down your Facebook, Google, Apple ID, Microsoft, Twitter and other accounts with two-factor authentication. That means that when you log in, you'll also need to enter a special code that the site texts to your phone. Some services require it each time you log in, others just when you're using a new device or web browser.

**Keep your browser secure**: To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

**Keep your device clean:** Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs. You can do a lot more. If you are interested E-Mail me and we can discuss.

**Lock down your hardware:** Set up your PC/laptop to require a password when it wakes from sleep or boots up. Same thing with your mobile devices; not only should you use a pass code to access them every time you use them, but also install an app that will locate your phone or tablet if it's lost or stolen.

**Treat your phone like a computer:** Smart phones have access to your email, address book and many other sensitive pieces of data yet rarely include any privacy controls. And always read the fine print before installing any new apps: security software on your phone can't protect you if you ignore security warnings and install the app anyway.

**Avoid phishing emails:** Make sure you know who is getting your personal or financial information online. Don't open files, click on links, or download programs sent by strangers via email**.** Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service to ask whether the company really sent a request. I've covered this often in previous newsletters.

**Watch what and how you share online:** If you post too much about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your

accounts, and get access to your money and personal information. Never post personal details like your address or phone number on a social networking website, or anywhere else online. Set your social media profiles to the strictest privacy settings available, and share information only with people you know and trust.

**Be careful of free or open Wi-Fi connections:** Any time you connect to the internet using unprotected Wi-Fi, anyone on that network can see your data. Before you send personal information over your laptop or smart phone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

**Know privacy policies:** Privacy policies tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere. There is significant problem with this advice. Basically, privacy policies are useless. Fraudulent sites publish iron-clad policies they have no intention of following. Others have published but have violated them. Finally, sophisticated web sites like Apples have such over-lawyered, densely worded privacy policies that essentially allow Apple to do whatever they wan. My overall advice is to ignore privacy policies and assume they do not provide you any protection. You will almost always be right.

**Dispose of personal information:** Before you dispose of a computer or mobile device, get rid of all the personal information it stores. For your computer, use a "wipe" program to overwrite the entire hard drive; and for a mobile device, check your owner's manual on how to delete information permanently, and how to save or transfer information to a new device.

**Log-off and lock up:** Always log-off of your device when you're finished and don't depend on an automatic login feature that saves your user name and password; so, if your laptop is stolen, it will be harder for the scammer to get your online information. And although this may be basic, lock up your computer/laptop when it isn't in use and keep it out of prying eyes

Not everyone will follow all 12 steps all the time but the more you do the safer you'll be.

# YOUR DIGITAL AFTERLIFE

Whether or not you believe *you* will have an afterlife, you will have a *digital* afterlife. After all, you probably have on-line financial data,a Facebook account, possibly a music collection and probably others.

While most states have laws that cover the disposition of your physical attributes, almost none have laws to cover your on-line assets. As a resultt they could be

lost, stolen, or simply not handled the way you wanted.

Furthermore, the time of your death is no time to burden your spouse or children with the hassle of trying to discover what on-line accounts you had and the sometimes fruitless attempts to get the repositories to turn over your passwords.

Since many people never think about this issue, **NOW** is the time to handle this issue.

So here, again from our friends at AARP is a plan extracted from a book you may want to read called *Your Digital Afterlife* by Evan Carroll.

1. Note all the web sites you use in a month. Also try to think of others you may use that require user-ids and passwords
2. Write down the user name for each site and the password for each. Best to use paper and pencil for this.
3. Put this list away in a safe place.
4. Only put the location of this document in your will, not the information itself because your will is a public document.
5. As an added benefit to your heirs and to avoid possible lawsuits, specify beneficiaries on all your financial accounts.

## HOW MUCH WOOD COULD A WOODCHUCK CHUCK?

By now, hopefully, you are aware of out of town repair scammers who blow into a community like ours and offer free inspections and low initial prices and call the police. But there is another type of repair scammer who specifically looks for signs of the elderly such as a wheelchair ramp. Unlike the first group, many of these folks are local. Their first ploy is to offer to trim trees for free, hence the name woodchucks. If they believe they have someone who has diminished capacity they strike. They may wet the attic insulation to prove the roof leaks.

If the person is sufficiently cognitively impaired, they may return in a week to

resell the same job.

The solution here is the same as above. Call the police. But the issue is that the victims are often not able to do that but you can help protect them. If you have a vulnerable neighbor and you see a contractors truck parked outside ask questions and ask to see the contract. If you have any doubt, call the police. Even if it's not a scam the police will enforce the requirement for a solicitors permit.