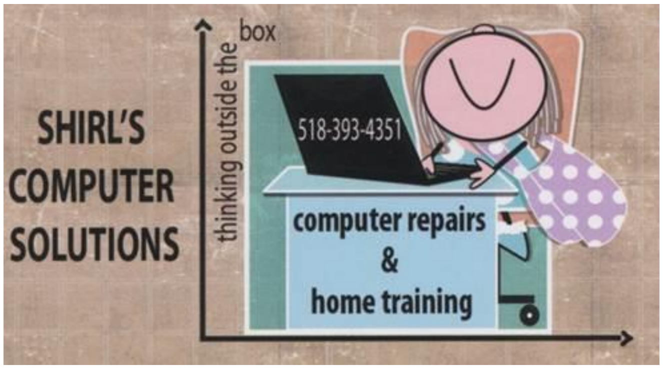

April Newsletter 2016

Every month I start reading and collecting all kinds of news articles as soon as my last monthly letter is mailed to you. I make notes of things that I find to be alarmingly serious threats to all of us and offer that information to you in hopes that it will prevent you from being a victim of fraud. One thing that I noticed when working on some client's computers this past month was that they leave a copy of their tax returns on their desktops. This is just the kind of thing that hackers are looking for because it allows them to steal your identity by finding your social security number. If you're one of the many who do this, remember it's not safe. It's not just in your home and available only to your eyes!! Place the tax return on a flash drive or backup hard drive and then make sure it's removed from your computer.

Users may encounter "Ransomware" through spam or malicious links. Once installed, it will limit access to the user's system and display a pop up message threatening the user to pay to have access to their information.

When I taught at Schenectady County Community College, one of the hardest things I had to teach students was how to copy and paste information from one document to another! We've come a long ways with computers, and copy and paste is simple compared to what I'm about to share with you. Because of all the security news this month, and in order to keep it as simple as possible for you to understand, I'm going to just list what to be aware of with a brief explanation. Keep this in mind when reading the information below; *"Ransomware in particular, has been a very lucrative scam as one security firm estimates that over $325 million was generated just last year. The expectation is that more variations of ransomware will continue to proliferate this year."* With this in mind, I hope you'll at least look at the information below.

- **Security alert! New ransomware found inside Microsoft Word** - You'll receive a Microsoft Word document, possibly an invoice. You click on it and it unlocks a macro that opens cmd.exe. That triggers Microsoft's PowerShell framework to download the PowerWare ransomware. PowerWare was discovered about 10 days ago. If you open a Word or Excel file and it says it needs you to turn on macros, close the file and delete it immediately.

- **Hackers exploit security flaws with Chrome, Safari and Adobe Flash in national competition** - This was found out at a “hackers” contest. If you aren't familiar with this contest, hackers and security researchers at the CanSecWest security conference compete for prize money by breaking into computers using previously unknown exploits. To do that, they exploited flaws in Safari, Microsoft Edge, Adobe Flash and Google Chrome (Firefox wasn't included this year). Once they were into the system, they then attacked unknown flaws in Windows and OS X themselves to take full control. That's the bad news. This shows the importance of needing to keep your software updated all the time! It also shows the importance of your security software. The machines in this test had no anti-virus or anti-malware software installed. ☹

- **Updated ransomware can't be cracked, costing people thousands –**

  If you get TeslaCrypt on your computer, you'll either have to pay to get your file back or wipe the computer and start over. You better hope you backed up your files! The FBI is warning that new versions of ransomware are starting to seek out and destroy local backups, so make sure you have an off-site backup as well. TeslaCrypt is a ransomware trojan which targets computers with **specific computer games installed**. Newer variants of the malware also infect computers without these games.

"Smartphones & Tablets!"

- With smartphones and tablets increasingly becoming the average person's go-to computer, it's no wonder many hackers are moving their focus away from computer attacks toward mobile attacks. After all, your smartphone or tablet can have your banking information, email, text messages, contacts, photos, location history and more in one spot. Over the years, hackers have figured out better ways to sneak on to gadgets and steal your data. And an Android Trojan called Acecard is the latest and most dangerous one yet. Acecard is a phishing app, and works by showing you "overlays." **When you load up a banking app, Facebook, Twitter, Instagram, popular instant messengers like WhatsApp or Skype, PayPal or Gmail, Acecard overlays its own form on top of the app.** The overlay looks just like the sign-in screen or "add credit card" screen for that app. However, when you type in the information, it goes right to the hackers. To avoid this threat, you should avoid downloading apps from third-party app stores, and only install apps from reputable companies in the Google Play store. It also helps to have a security app that can detect Acecard. I use Avast Mobile for my security app.

Data Doctors' Ken Colburg had this to share on March 9th.

- “Protecting Your Mac from Ransomware - If this nasty malware sneaks its way into your computer, it silently grabs all your personal data files and locks them down with military grade encryption. Once the files are encrypted, the only way to open them is with a special key that the hackers demand payment for, hence the term ‘ransomware’. The ransom amounts can range widely and generally double within a few days if you don’t pay quickly. The discovery of the first ransomware scam specifically targeting Mac users should be a wake up call for anyone that still thinks Macs are somehow infallible. Making sure you keep all your software updated, only downloading apps from Apple’s App Store, installing a solid Internet security package and using an online backup service such as Carbonite (http://goo.gl/wKaqLP) are the best ways to avoid ever becoming victimized. “

- **How to tell if your NetFlix account has been hacked**

Has your Netflix account been hacked? There have been several recent reports about hackers selling Netflix, HBO and Spotify streaming accounts for as little as $0.25 for a lifetime subscription on the Dark Web. Could you be one of the victims? There are a few ways to tell. First, you'll want to check your account using these steps:

1. Click on your account icon in the top right hand of the screen.
2. Select "Your Account."
3. Select "Viewing Activity." If there are titles showing up that you didn't watch, that's the first red flag - but everything could appear normal.

Don't stop there. Select "Recent Account Access." Here, you should see only your locations. If it's just your devices you're all set, if not you know you've been hacked. What should you do if you've been hacked? Head back to the "Your Account" page and under "My Profile" click on "Sign out of all devices." According to Netflix, "This method of deactivation will disconnect all devices currently connected to your Netflix account, but may take up to 8 hours to take effect. Next, you will need to reset your Netflix password.

Clicking on a Link that looks suspicious can get you in BIG trouble! Here are 5 things to ponder before you click on that tempting link!

1. **Where did the link come from?** If a link is unsolicited, you don't want to click on it. Hackers send them out in emails and texts all the time.
2. **Why am I Clicking on the link?** For example, an email might say your bank account has been hacked and you need to click right away and enter your information so the bank can get your money back. Maybe you see a post on Facebook saying you could win the lottery or get a brand new expensive tech gadget for free. If it looks "funny" to you, go with your instincts and don't click on it.
3. **Does the link look right?** If not, don't click on it.
4. **Is there a second opinion?** Check out your antivirus software's URL checker to make sure it's not a bogus link. This is added as a toolbar on your browser.
5. **What's on the other side?** If you're even a little suspicious of a link, you shouldn't click on it. Better safe than sorry. And if it's information you really need, you can usually visit a company's site directly to find it, or look it up in a Google search.

I hope you can stand one more because it has to do with the popular Facebook. ☺

facebook

One critical thing to know before you click 'like' on Facebook

For example, you might not like the announcement that your friend's pet just died, but you might click "like" to acknowledge that you've read the post and that you're thinking of them. In fact, liking posts is something of a reflex for many people, and it's a reflex that scammers are taking advantage of. Welcome to **"like-farming."** Only after the post gets a certain number of likes and shares does the scammer edit it and add something malicious. In fact, if you go back through your history of likes, you might find that some of them have changed to something you wouldn't have liked in a million years. So, what kinds of stories do scammers start with to trick people into liking and sharing? One popular type of story is the emotional one. You've definitely seen posts showing you rescue animals and asking you to like if you think they're cute. Or maybe it was a medical story where you're asked to like that the person was cured, or to let them know they're still beautiful. There are also the posts that ask you to like to show that you're against something the government is doing or disagree with something terrible happening in the world. A popular one, for example, is posts that ask you to like or share so you can win something. This happens especially whenever Apple launches a new iPhone or iPad.

What about brain - teaser posts, such as the ones that have you like or share if you can read the words backwards or solved a tricky math problem.

It isn't just posts either; it can also be pages. A scammer might set up a page for "I love puppies" or what appears to be a worthy company or organization. It puts up enough content to get a lot of likes, then switches the content for spam and scams. Once you've liked the page, everything new the scammers put up goes on your News Feed, and in some cases your friends' feeds as well. Your best bet is to be very judicious about what you like and share on Facebook. Don't just reflexively click "like" on everything.

**Info By Justin Ferris*

In conclusion….just be careful on the Web. One key point was made….backup your information and keep it in a safe place. I, personally, have 4 backup drives on my machines that are turned off after each backup and I subscribe to Carbonite. Are on-line back-ups safe? Carbonite and other services encrypt your information and that makes companies like that less attractive to hackers. Most people don't encrypt the information on their computers so that's why they target us. **The ultimate backup scenario uses the 3-2-1 method: 3 copies on 2 different devices with 1 copy off-site.**

Windows 10 is still lurking in the background and waiting to be downloaded. If by some chance you are interested in putting it on your machine, you have until July to make your decision. I put it on one laptop that I don't use so I could learn it, but I'm still happy with my Windows 7 operating system. Here's the latest news that I can share with you about this controversial upgrade.

This is appealing - Windows 10 starts up faster than its predecessors. It comes with Microsoft's voice-activated virtual assistant, Cortana. Plus, Microsoft has beefed up Windows' security.

This is not appealing – Windows 10 (Microsoft) collects tons of personal information on you…including your calendars, emails, location and more.

And least appealing of all - The problem started with the latest round of Windows updates, specifically patch **KB 3135173**. After it installed and the computer rebooted, a number of people discovered that all their default programs and file associations had been reset. The Windows 10 Action Center listed a string of error messages saying that there was a problem with the third-party program or file type and it had to reset. **The reset, naturally, routes everything back to Windows programs like Microsoft Edge, Windows Photos and others**. The update also wiped out third-party options from context menus. So, if you right-click on a file, you won't see any of the options for opening it or using it with your third-party programs. Even worse, users who tried to put their defaults back to the way they were have found that Windows 10 will show an error message and reset it again. So, was this a bug or is Microsoft declaring war on third-party programs? Hopefully it will be fixed. This is why I've said to WAIT! For me I'm waiting until I have to buy a new computer and have no alternative but to buy Windows 10**. I hear that Oct is the cut-off date for buying Windows 7, but it could be a lot sooner.**

Ever wonder if someone is spying on you?

Fortunately, there's a very easy, free way to find out if you're being spied on online. SpyDetectFree is a simple download that you don't even need to install onto your device. When you want to find out if someone is spying, click on the Check Now button. Free for Windows

http://www.worktime.com/spydetectfree/

Recalls Look up by VIN (Vehicle Identification Number) | Saferca

This website lets you find out if there are any recalls on your car. Usually we're notified by the dealership, but sometimes we just don't get them. Check out this link to see if your car is one that needs to be brought in for service.
https://vinrcl.safercar.gov/vin/

During the month I get a lot of questions, and here are the most common ones.

- **My Internet isn't working** - The simplest way to resolve that is to unplug your Modem, then turn off your computer and wait 1 minute. Plug the Modem back in and restart your computer. This resets your IP address (your address for the Internet Provider that supplies your cable).

- **I get a message that "this page cannot be displayed" or "Server Not Found" when I go to a website** – again, it's the Internet Connection. It means that your computer and network are not communicating. Just reset the Modem. It can also mean that the site is down for updates or that there's too much traffic on that site. Try again later. If this is an on-going issue, contact your Internet provider. You might have to ask them to put you on a different channel for your wi-fi.
- **My desktop icons don't work anymore** - Usually it's because a program has "bellied up". If you have a program like AOL Desktop, this happens a lot. Uninstall AOL and resinstall it. That remedies the problem 99% of the time.
- **My Time is off on my desktop clock** - (windows) Go to the bottom right corner of your screen where you see the time and date, do a right mouse click on it and look for Adjust date/time. Click on it and look for the Internet Time tab on the top of the Window. Click, and another Window will open up that will synchronize the time with an Internet Time Server. Click on Update now and then ok. You're all set! You have a CMOS battery inside the machine that runs the clock and other functions. It's not uncommon to lose time on some machines. This is an easy fix. ☺

Computer Term of the Month - CMOS

Alternatively referred to as a Real-Time Clock (RTC), Non-Volatile RAM (NVRAM) or CMOS RAM, CMOS is short for Complementary Metal-Oxide Semiconductor. CMOS is an on-board, battery powered semiconductor chip inside computers that stores information. This information ranges from the system time and date to system hardware settings for your computer. The picture shows an example of the most common CMOS coin cell battery used to power the CMOS memory

I know this was a long newsletter, but hopefully you'll find something in it that will help you. Don't forget your Spring cleanup for your machine. It's really true that an ounce of prevention is worth a pound of cure! ☺

Warm Regards,

Shirl

www.shirlscomputersolutions.com

Specializing in computer repair & training, upgrades, removal of viruses, and instruction in Digital Photography and Photoshop. Other services include scanning of photos, negatives, transparencies and copy of VHS and Cassette tapes to DVD!