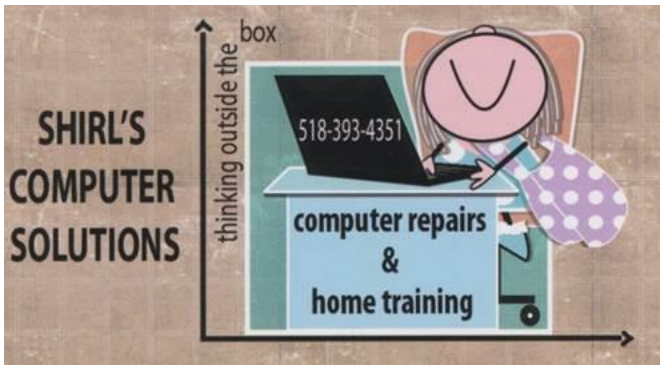


April 2017 Newsletter

Good News! It's Spring and winter is finally behind us, but not without mother nature giving us a major storm to remind us that we live in the great Northeast! Computers have also had a stormy time the past month and yet there's "good news" that I'm hearing that I want to share with you.

SPECTRUM

Spectrum is now official! You probably know by now that that they're taking over Time Warner (since they bought them out) and as of mid-January they've implemented their new packages, and upgraded the services that Time Warner had provided. This includes a 5G upgrade for their Wi-Fi speed. It's 10 times faster than the 4G you've been using! Check out this link to read more or hear a video about it.

http://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g I spoke with Bill Goetz yesterday and he said that they actually upgraded everything for him and gave him a substantial break on his monthly payment. I'm hoping this will continue! The one thing he mentioned was that with the new modem that they installed, he now has Wi-Fi in rooms of his house where they couldn't get a signal before. So, are we going to be happy with the switch? This all sounds good, but then there's another friend (also named Bill) who told me that they wanted to raise his payment to a rate that was unheard of! I guess time will tell, but it does sound like Time Warner was behind the 8 ball with upgrades to give us the best service. If you have any experiences with Spectrum, I'd really like to hear about it.

Latest News…..

Trump to sign bill rolling back internet privacy protections
This is not good! The White House signaled Tuesday that President Trump will sign a controversial bill rolling back Obama-era internet privacy rules, drawing the ire of online advocates who said he is failing his first major drain-the-swamp test by allowing broadband companies to "**sell users' personal browsing histories"**. If Mr. Trump follows through on signing the bill, **consumers would still be allowed to opt out, but they would have to do so explicitly, and advocates said companies could impose a surcharge on people who wanted their data kept secret**. (**article from the Washington Times**) So how do we handle

this? One way is to make sure you clear your browsing history every time you're done surfing the Internet, but the better choice is to run a VPN on your computer. I use Windscribe and purchased a lifetime subscription from a website called Stack Social. They have many options to choose from and the lifetime price is much better than a yearly price. Another way is installing browser add-on's. Some are listed below.

Firefox

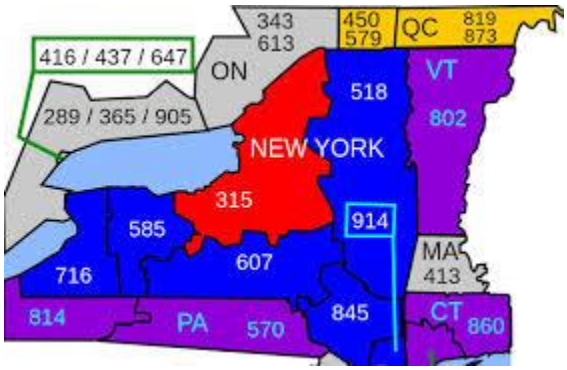
https://addons.mozilla.org/enUS/firefox/addon/hoxx-vpn-proxy/

Google Chrome

https://chrome.google.com/webstore/detail/setupvpn-lifetime-free-vp/oofgbpoabipfcfjapgnbbjjaenockbdp?hl=en-US

Opera – has a built-in VPN

What is a VPN? A VPN or Virtual Private Network is a method used to add security and privacy to private and public networks, like WiFi Hotspots and the Internet. VPNs are most often used by corporations to protect sensitive data.



Jill Davis has been writing me and mentioned that a good topic to include in my Newsletter is the fact that we who live in the 518 area code will now have to dial 518 + the phone number we want to call after it. Right now, Spectrum is changing things over for it work on their system, but come **August 19th** we'll all have to be doing this if we want to call someone!! To test this new procedure, add a 1 before the area code and number. Example with my phone number 1+518 393-4351 Jill always gives me good suggestions. ☺

SCAMS SCAMS SCAMS!!

This is right from Microsoft's webpage and I would ask that you take a moment to read it through. It's very important to be forewarned about this so if it happens to you, you won't panic.

Avoiding technical support scams

Cybercriminals don't just send fraudulent email messages. They might call you on the telephone and claim to be from Microsoft. They might also setup websites with persistent pop-ups displaying fake warning messages and a phone number to call and get the "issue" fixed. They might offer to help solve your computer problems or sell you a software license. Once they have access to your computer, they can do the following:

- Trick you into installing malicious software that could capture sensitive data, such as online banking user names and passwords. They might also then charge you to remove this software.

- Convince you to visit legitimate websites (like www.ammyy.com) to download software that will allow them to take control of your computer remotely and adjust settings to leave your computer vulnerable.
- Request credit card information so they can bill you for phony services.
- Direct you to fraudulent websites and ask you to enter credit card and other personal or financial information there.

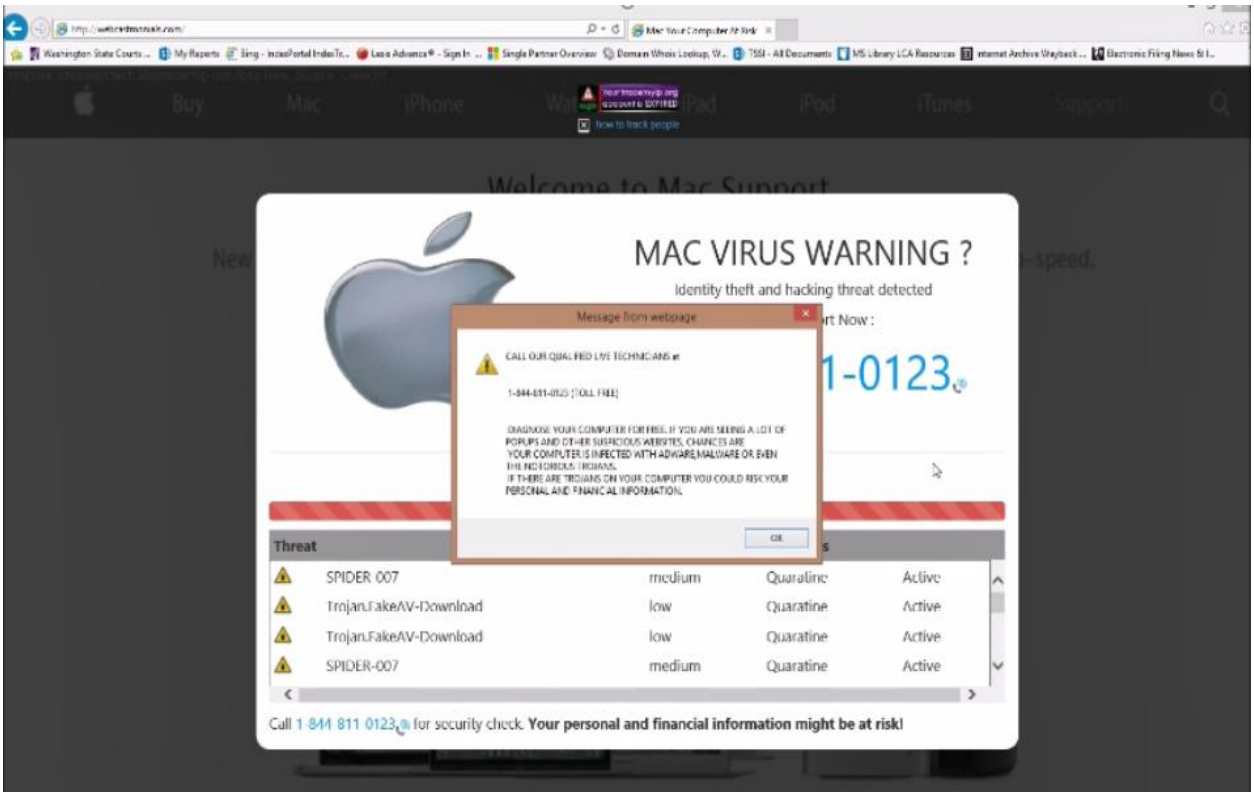
"Remember, Microsoft will never proactively reach out to you to provide unsolicited PC or technical support." Any communication we have with you must be initiated by you

Scam Pop-Ups: What You Need to Know

Another well-known trick is the website pop-up, that little browser window that sometimes appears while you're searching the Web. Cybercriminals set up websites with scam pop-ups with messages and phone numbers. These pop-ups usually are not easy to close.

While some pop-ups are useful and important, others are traps that attempt to mislead you into revealing sensitive personal or financial information, paying for fake anti-virus software, or even installing malware and viruses onto your device.

Do not call the number in the pop-up. Microsoft's error and warning messages never include a phone number.



The graphic above shows that they're even showing up on a Mac

Here are some of the organizations that cybercriminals claim to be from:

- Windows Helpdesk
- Windows Service Center
- Microsoft Tech Support
- Microsoft Support
- Windows Technical Department Support Group
- Microsoft Research and Development Team (Microsoft R & D Team)

How to report tech support scams

- Help Microsoft stop cybercriminals by reporting information about your tech support scam.
- In the United States, use the FTC Complaint Assistant form.
- In Canada, the Canadian Anti-Fraud Centre can provide support.

- In the United Kingdom, you can report fraud as well as unsolicited calls.
- In Australia, you can use the ScamWatch website to report a scam.

Whenever you receive a phone call or see a pop-up window on your PC and feel uncertain whether it is from someone at Microsoft, don't take the risk. Reach out directly to one of our technical support experts dedicated to helping you at the Microsoft Answer Desk.

How to protect yourself from tech support scams

If someone claiming to be from Microsoft tech support contacts you:

- Do not purchase any software or services.
- Ask if there is a fee or subscription associated with the "service." If there is, hang up.
- Never give control of your computer to a third party unless you can confirm that it is a legitimate representative of a computer support team with whom you are already a customer.
- Take the person's information down and immediately report it to your local authorities.
- Never provide your credit card or financial information to someone claiming to be from Microsoft tech support.

What to do if you already gave information to a tech support person

If you think that you might have downloaded malware from a tech support scam website or allowed a cybercriminal to access your computer, take these steps:

- **Change your computer's password**, change the password on your main email account, and change the password for any financial accounts, especially your bank and credit card.
- **Scan your computer** with the Microsoft Safety Scanner to find out if you have malware installed on your computer.
- If you are using an old version of Windows (Windows 7, Vista or XP), Install Microsoft Security Essentials. (**Microsoft Security**

Essentials is a free program. If someone calls you to install this product and then charge you for it, this is also a scam.)

Note: In Windows 8, Windows Defender replaces Microsoft Security Essentials. Windows Defender runs in the background and notifies you when you need to take specific action. However, you can use it anytime to scan for malware if your computer isn't working properly or you clicked a suspicious link online or in an email message.

Microsoft does not make unsolicited phone calls to help you fix your computer.

In this scam cybercriminals call you and claim to be from Microsoft Tech Support. They offer to help solve your computer problems. Once the crooks have gained your trust, they attempt to steal from you and damage your computer with malicious software including viruses and spyware.

Although law enforcement can trace phone numbers, perpetrators often use pay phones, disposable cellular phones, or stolen cellular phone numbers. It's better to avoid being conned rather than try to repair the damage afterwards.

Treat all unsolicited phone calls with skepticism. Do not provide any personal information.

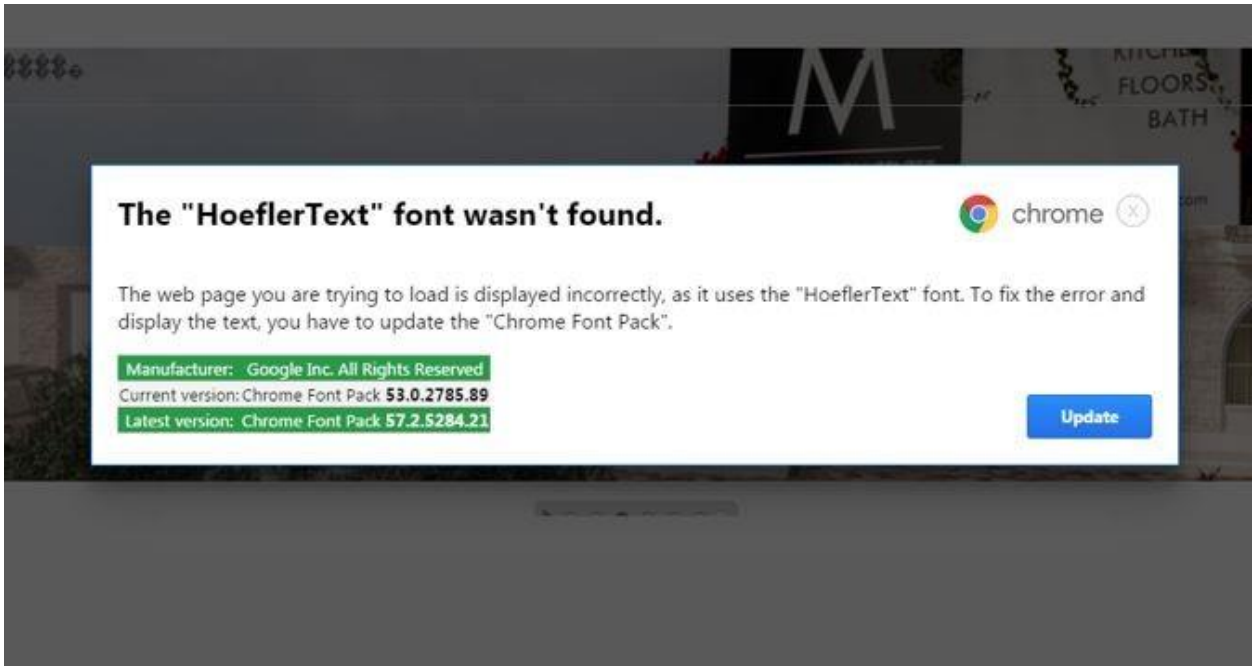
If you receive an unsolicited call from someone claiming to be from Microsoft Tech Support, hang up. We do not make these kinds of calls.

Another Scam – please watch this video on identity theft.

https://www.youtube.com/watch?v=78MnQbKB9-E

Google chrome

Google Chrome scam continues to spread Watch out for this fake pop-up warning



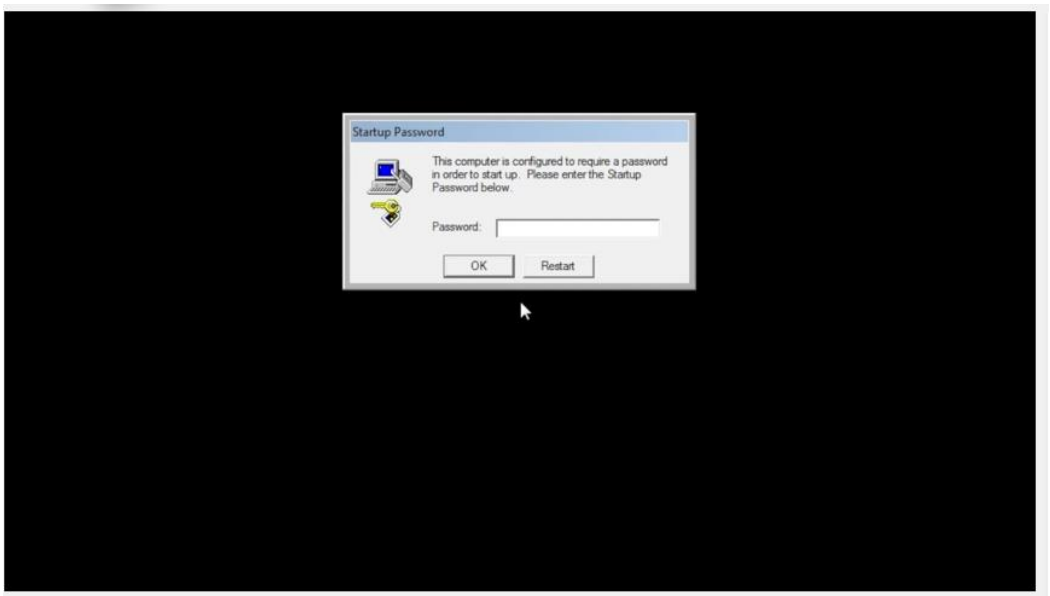
Clicking on the Update button on this message will infect your gadget with click-fraud adware. **Do not click on Update!!**

Hidden ads will be loaded and clicked on automatically. This is how the criminal gets paid, by ripping off legitimate ad networks. At this time, the risk to Chrome users is their gadget is infected with click-fraud adware.

However, this scheme could change at a moment's notice. The hacker could change the malicious link into something worse, like **encrypting ransomware**. This is why it's so troublesome that this scam is still active.

Ransomware

If you've been hit with Ransomware, you'll see this password prompt. You'll need to call someone you trust with your machine to get you out of a mess if you see this come up. They'll want to charge you from $500 to $2000 to get back into your computer. Don't call the phone number they give you!!!!!!!!!!!!!!!!!!



What happens after you pay "Microsoft Technical Support" scammers(Almost 2 Hours Long!)

Cybercrime – I have a document that Ben gave me to read and it was very well written and published in Money Magazine. If you haven't read it, you should. This is the new terrorism in our country today and you need to be educated about it. I've been trying to figure out a good way to share the information, but there is too much to just write it in a newsletter. If you're interested in reading this, please contact me. If you subscribe to Money magazine, please check it out and share it with your friends.

Apple News!

Change this Setting Immediately -

Stolen Apple IDs are currently hot ticket items for hackers interested in targeting Apple devices. With your Apple ID, crooks can gain access to several connected services, including the Apple Store, Apple Music, iCloud, iMessage and even Find my iPhone. But there's another way your own account can be used against you by clever cybercriminals, and it's much more discreet. It's called "Family Sharing," and it's a setting you may have established a long time ago and completely forgotten about it. Obviously, this feature is great for families and groups that share devices with one another and have similar interests. Just imagine: A single purchase of that movie everyone wants to watch over the weekend or that eBook you've all been anxious to start reading.

Family Sharing gone wrong

Where things get scary is when someone hacks into your Family Sharing service. If it happens, you may not even notice until unexplained charges begin showing up, or credits you've saved disappear from iTunes. Once a crook has invited himself (or herself) into the mix, they can begin downloading apps and content that will be charged to the payment method on file, which is typically the organizer's credit card.

Reclaiming your account

If this happens to you, there are a few options. For those who use the Family Sharing service quite regularly, you'll need to delete the intruder

and reset your login credentials. To delete the unwanted visitor, the group organizer will need to follow these steps:

On your mobile device, head to Settings >> iCloud >> Family. There, you should see a list of everyone who's connected to your Family Sharing account beneath the "Family Purchases" header. Tap the name of the individual you'd like to delete, then tap Remove.

Turning Family Sharing off

For anyone who's not using the Family Sharing service all that much, it's best if you just turn it off altogether. To do this, the group organizer will need to access Settings >> iCloud >> Family (on their mobile device), and click "Stop Family Sharing."

And they said it would never happen because they’re Apple ☹

300 million Apple users at risk of hacks unless Apple pays ransom! Why your iPhone could be at risk

A group of hackers calling themselves the "Turkish Crime Family" claims to have gained access to a massive cache of iCloud and Apple email accounts. Access to these accounts could allow them to wipe everything from the victims' gadget remotely. They could also reset the victims' iCloud accounts. The hackers allegedly have access to more than 300 million Apple email accounts. This includes people using @me and @icloud domains. The cybercriminals are demanding that Apple pay

them either $75,000 in Bitcoin currency or $100,000 in iTunes gift cards. In exchange for payment, the group would then delete the alleged data cache. They are giving Apple until April 7 to make the payment.

What you need to do now

In the chance that hackers have gained access to your Apple accounts, take these steps:

- **Change your passwords** - Make sure that you change all passwords associated with your Apple accounts. Also, have unique passwords for every site that you have an account. Using the same password across multiple sites should never be done. Read this article to help you create hack-proof passwords.
- **Backup your iPhone** - You should backup your iPhone onto your computer through iTunes. If your phone ever gets wiped, you can restore it with your backup on iTunes. Click here to learn how to backup your iPhone.

Beware of phishing scams - Scammers will try and piggyback on potential breaches like this. They will create phishing emails, pretending to be the affected company, hoping to get victims to click on malicious links that could lead to more problems. Take our phishing IQ test to see if you can spot a fake email.

Verizon is getting out of the Email Business

Connie contacted me to let me know that she had an email from Verizon saying she had to switch her email client because they were no longer providing email. Not everyone has been notified, so be prepared to see this letter in your inbox if you're a subscriber of Verizon. She chose AOL and now I see this news about AOL! If you're happy with AOL just beware of this news.

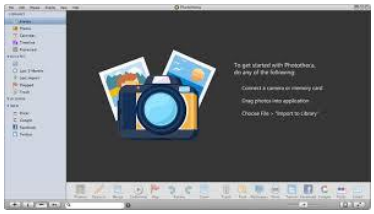
"Most of us probably have an older relative that still uses the AOL Desktop Software. Unfortunately for them (and possibly us as well if you're the one they call when they have a problem) as of April 10th, 2017 the AOL Desktop Software will be seeing a transformation to a monthly subscription based service. A new version of the software, AOL Desktop Gold, will replace all previous versions of the software and all previous versions will no longer function. This new service will cost $3.99 per month. AOL Desktop Gold will be included with their current safety and security bundles that include software such as McAffe and AOL One Point password manager.

Don't type Amen on this viral Facebook post It's a scam!

How the latest Facebook scam works

Like-farming is exactly what it sounds like. Scammers post a story on Facebook for the purpose of cultivating likes and shares. Based on the way Facebook works, the more likes and shares a post gets, the more likely it is to show up in people's News Feeds. This gives the scammer

more viewers for posts that trick people out of information or send them to malicious downloads. The story they originally post normally has nothing dangerous about it. Only after the post gets a certain number of likes and shares does the scammer edit it and add something malicious. There are plenty of Facebook posts that will tug on your heartstrings. Some of them ask you to type **Amen**, then like and share with your friends. The subject of the post could be almost anything. You might see a picture of someone who is ill and are asked to help them get better by sending them well wishes. Sometimes the scammer promises you something positive in return for typing Amen, liking and sharing a post. I found one on my News Feed that claimed I would receive a miracle by doing this in the next hour. As much as you're tempted to reply, don't!



As you can see, it's been a busy month in the computer world, so we'll end with something that will be less stressful. If you have tons of photos like I do, you'll want to sort them out and put them in some kind of order. Here's a "free" program to download for Windows users.
https://lunarship.com/

The magic Photoshop Touch for Mac

The Photoshop Touch interface will have you performing amazing edits and creating fantastic effects in no time.

Designed specifically for tablets, Photoshop Touch is also fully integrated with social networking sites so you can share your creations and view

comments from within the app. For ten bucks, it's a pretty powerful program. (The company's full program costs hundreds.) If you're an advanced user and feel like an image could use more work in Photoshop CS5, send it to the Adobe Creative Cloud and open it up when you're back at the desktop.

App Links

Download for iOS - *$10*

Download for Android - *$10*

Computer Term of the Month

Noob

The word "noob" entered the Concise Oxford Dictionary in the same year as "woot." It refers to a new person who doesn't know what he or she is doing. It often appears in reference to gaming or for computing activities. The word derives from the term newbie and is sometimes spelled as "newb" or "n00b" with two zeroes, particularly in the gaming world.

Every month I say I'm going to write less and it ends up more! To much is happening and this is just a **"few"** of the articles I've put aside to share with you. Hopefully next month can be an easier read. ☺

Happy Easter and Happy Passover!

John 20:16-18

Warm Regards,

Shirl