Newsletter June 2014

It's finally Spring! I went out with my granddaughter Julia on Saturday to take pictures so we could practice with our cameras for the upcoming trip to Prague and Israel. It was a treat to see things blooming and have warmer temperatures. It's been long overdue!! Collins Park is a great place to go if you want to get pictures of birds, and she got an amazing shot of a red winged blackbird.   We also took pictures of chickens and Oreo Cows! ☺

I had a call from a friend a couple of weeks ago and he asked that I share his story. They're at it again….the so called "Microsoft People". They have changed their approach and are now playing on people's guilt. It went something like this: They call and tell you that YOU'RE RESPONSIBLE for sending out from your computer spam/infections and that you need to have this cleaned up. Right away they're making the person feel like they've done

something horrible and that they're causing other people to be compromised on their machines…..because of YOU! After this approach they convince the person that they need to look at their computer. Of course you want to stop this from continuing, so you allow them to take remote access. Once they get into the machine they actually "SHOW" you all the spam you've been sending and in this case it was around 19,000 pieces of spam. Can you image? And it looks so legit!! They actually put up a screen that they've created and show it to you on your machine. It's all very convincing. In fact, what they've done is to scare you into thinking you've done something bad and that you'll get in trouble if you won't let them help you. What do they do? Once you've given them permission to take remote access of the machine they install malware, remove the dynamic link libraries that run your programs and mess everything up so that your machine won't work. (these are just a few of their tactics) You have to understand that you DIDN'T HAVE THESE PROBLEMS BEFORE THEY CALLED YOU. THEY ARE THE PROBLEM!! Now back to my friend……he called me and was understandably upset and said that after a while things didn't make sense about what they were telling him. He ended the conversation with them, but the damage was done. When he brought the machine to me it would only start in safe mode (the diagnostic mode for the computer), and none of his programs were running correctly. It ended up being a very costly repair for him and we weren't even sure if his information on his computer had been infected. The next step that these people usually take is to call you back in a week or so and offer to fix your computer. The charge? About $500 -$1000! They won't call themselves Microsoft anymore, but you might see them pop up on your computer screen offering to help you or they could call you under a different name. I can't tell you often enough that Microsoft never calls people to tell them that their computers are infected with viruses! The only people who would know that is you or the person that services your computer on a regular basis!

Just this week they called me and I'll tell you how I handle it. If you're still unsure try this. When they called they told me my computer was infected and that they had to remove these infections. I played their game and asked them how they knew. They told me that they could see it from my computer. I said that's impossible and they told me that I was wrong. They said that they had a read out from my machine showing them the problems. Once more I told them it was impossible and that they were wrong. They were starting to get upset with me, and then I told them that I don't have a Windows machine….I have a Mac. They hung up on me without another word. Maybe that's a good way to test them for yourselves! Good news is my friend is up and running and he'll never fall for that scam again. ☺

Have you heard in the news about the hackings that are taking place with the routers that we use to connect to the Internet wirelessly? It's become a very serious issue, and you should be updating the firmware that the manufacturer is providing. It's not something that people just know how to do, and it's not always the easiest thing to accomplish. If you have a wireless router, go to the webpage for Cisco, Netgear, Belkin etc. and look for your router's model. When you find it, download and install the firmware that they're providing. Just look at the box with the flashing lights that you have for wireless, and find the name on it and model number. Some even want your serial number, so get the magnifying glass out and write it down. ☺ I called Time Warner a

couple of weeks ago and asked them if they update the firmware for their customers who rent their routers from them. The told me **"Yes"** if you have the "one box". If you have a separate router, then they don't because they're not able to be updated. So the ones that are really in need of attention are the store bought routers that you've purchased yourself. You might want to call Verizon and ask them if they update the firmware on their devices.

Do any of you do your banking on-line? If so, there are a few things that you should know about how to keep your transactions safe.

Make sure that your anti-virus software and anti-malware software are up to date.

Make sure you make a difficult password for your login on the banks website. Mix numbers, letters, Upper Case and lower case, and use symbols.

Make sure that in the address bar it says https:// before your banks web address. The "s" means secure

Once you've finished with your transactions, Log off, and then go to your history and clear the last hour. Then close out the browser (Firefox, IE, etc) completely before you do anything else on the Internet.

Many banks today are adding on extra security and actually ask you to select a call to your home or a text to verify a code they'll give

you to sign in on their website. It's good to see that they're upping their security measures for you!

Are you an Ebay user? If so, change your password. That's another company that's been hacked. ☹ They have probably been sending you messages telling you to change it, but if you're like me you don't always read everything that comes into your inbox. ☺

When I go to "some" of my clients homes to work, I notice that they're loaded with toolbars in their browser and some of them are actually malware. The number one offender is "Conduit"…another is "SweetPacks. Below is the name of some that will redirect your search to a site you don't want to go to. If you see any of these that I'm listing, so to the control panel, programs and features, and remove them!   Some of these could even be plugins in your browser and should be removed.
Babylon
FunDial
FunMoods
MyStart.incredimail.com or MyStart.incredibar.com
PlusNetwork.com
Search.Conduit.com

SweetIM

SearchNu.com

Delta Search

Pinterest.aot.im

Search.snap.do

Qvo6 or Portaldosites.com

Alott Toolbar

A problem has been detected and windows has been shut down to prevent damage to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen, restart your computer. If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c

Do you ever get this BSoD??? It's the blue screen that comes up in Windows when there's a problem. It's called the Blue Screen of Death! If you get one, look for the numbers that are listed and write them down. They usually start with STOP: 0x00000x0 (or something like that) and you need to write the whole line of numbers and letters down. That's the way that you can trouble shoot what your problem is. This usually happens when there's a hardware or software problem on the machine, and very likely it's driver related.

Is your Mac getting slower all the time? If so it could be an easy fix! Your Mac could have disk errors. It takes time for it to work around these. Fortunately, you can fix them.

Go to System Preferences and run Disk Utility. Select your hard drive and click the First Aid tab. Then click the Repair Disk button to run a full disk scan and repair.

These steps should get your system back up to speed. However, in some cases, you might need a hardware upgrade.

Perhaps you're using more powerful programs than you used to. They could be overwhelming older hardware.

Consider installing more RAM. Macs tend to run best with a minimum of 4 gigabytes of RAM. If you use creative professional software, consider upgrading to 8GB or 16GB.

RAM is easily installed on 2010 or newer Mac minis and most other Macs.
Not sure how much RAM you have? Go to the Apple menu and select About this Mac. ☺
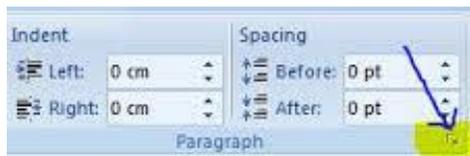
Tip of the Week: Double Space a Document in 2 Keystrokes

If you create a lot of documents, invariably, you will use the double-space formatting for either a paragraph of an entire document at some point.

Or you may find the need to use the 1.5 space option to let the text breath a little more and make the document easier to read (great for legal documents or school assignments).

Instead of going into the Paragraph menu to format the text, give this a try:

Select the text you want to change (or use Ctrl-A to Select All)

Press the Ctrl+2 to double-space

Press the Ctrl+5 to 1.5 space

Press the Ctrl+1 to return to single-space

Does your family post a lot of photos on Facebook? Do you ever wish you could save them to your computer? Here's a website that you'll want to visit to download batches of photos. Windows OS

http://www.fbdownloader.com/

I don't mention Facebook very often, but these are scams that you should be aware of. You may already know them, but if not these can help keep you safe while working on this social media. Mention this to your friends too!

Four Facebook Scams

1. Free giveaways
The easiest scam to fall for on Facebook is a free giveaway. You'll see everything from gift cards to free tablets, laptops and smartphones. Who doesn't like free?
Just one catch! You have to give the "company" your information. Or you have to download a program to qualify.
This is a variation on a classic survey scam. These trick users into giving out their information or downloading malicious files onto their computers
If you check the company's page or website and don't see the giveaway, steer clear. Even if it's real, only enter through the company's official page. And only if it's a company you trust. Scammers like to set up fake sites and pages that mimic the real thing.

2. Viral videos
Almost as exciting as free gadgets is seeing the latest viral video. However, many supposedly salacious celebrity "videos" posted on Facebook aren't videos at all.

When you click to watch, you'll be asked to update your video player first. You'll even be provided with the updated program file. How helpful!

Of course, the program is really a virus. Plus, it will automatically share the scam with all of your friends.

This one is easy to avoid. Type the video's title into Google. You should see a link to it on YouTube. If the video isn't on YouTube or a legitimate news site, it's a scam.

3. Custom profiles

Another common scam offers to change your Facebook profile look or layout. A famous version was the Facebook Black scam. It supposedly gave you a slick, black color scheme.

These scams try to trick you into installing a rogue Facebook app. If you do, you give the scammer access to your personal data. It will also spam your friends to try and trick them.

Again, this scam is easy to avoid. Just remember that there's no official, or unofficial, way to change your Facebook layout. A program like Social Fixer can change the way you see it, but nothing will change the way other people see it.

4. Who viewed your profile?

Knowing who views your profile is the Holy Grail of social media. Who doesn't want to know who is cyber-stalking them?

That's why this scam has been around almost as long as Facebook. No matter how often Facebook says it isn't possible, people still want to believe it is.

So they gladly download apps or visit websites that turn out to be malicious. And they give full access of their Facebook profile to strangers. No good can come of that.

The best you can do is see who has unfriended you. Of course, that only works after you've activated one of the tracking services.

If you want to keep track of every scam happening on Facebook, the site Facecrooks is up.

**Courtesy of Kim Komando

Computer Term of the Month – We all know what hacker means ☺ Here's one that you probably never knew existed!

Technoplegic   A person who feels paralyzed mentally when faced with technology. Technoplegia is an equal opportunity affliction, affecting those great and small, sharp and dull.

The count down has begun! It's just 22 days until we leave for Prague to see our son John. Now I'm getting excited and overwhelmed with all that there is to do. Just remember that I'll be gone from the 25th till the 11th of July. If you have any computer problems now, I'm free until the 24th for appointments.

Happy Father's Day and Happy 4th of July….. I think that covers it all until next time! ☺

Warm Regards,
Shirl