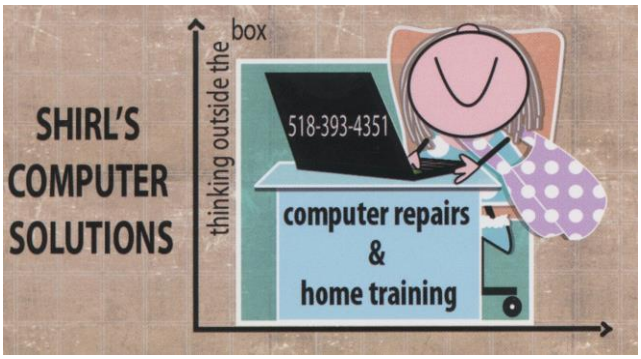



# *July 2017 Newsletter*

It's been a while since you've heard from me, and since I'm still on the mend I'm going to keep this newsletter on the light side. I always say that, so we'll see how it actually goes! ☺ So much has been going on that I felt I **had** to get some of the news out to you. It's a time of frightening **attacks** that come out of nowhere, **changes** needing to be addressed regarding the security on machines, and the **uncertainty** in the voices of those of you have called me with questions that has prompted me to take the time to get some answers for you.


Just today they had another attack that spread a new ransomware attack that is infecting airlines, banks, and utilities across Europe. And in our country there was a hack on a nuclear power plant. One U.S. official called it an "ongoing matter" that is being investigated. No public authorities have issued word on who may be responsible, but agencies are looking at the possibility that another country may be behind the hack. This kind of news has to be a wakeup call for all of us who feel that what we do in our homes on our computers is "different" from what's going on in the big picture of things. The truth is, we're all at risk. This isn't to scare you but to make you aware of one thing….you need to be more up to date with the way you protect your machines. Below is a list of the software you NEED to upgrade now. The days of free are behind us now.

- **Anti-Virus** software should be the premium versions that they offer
- **Malwarebytes** free isn't going to stop ransomware or rootkits with the free version. It's time to purchase their software.
- A **VPN** is a good idea to protect your identity and scrambles your IP address (or gives you another one) so you can't be tracked. I use **Windscribe** and if you're interested in getting a lifetime subscription you can get it for about $70. I have it on all of our machines. This offer won't last for long!! https://stacksocial.com/sales/windscribe-vpn

- **Dashlane** or some other password manager is a good idea to protect your passwords and save them.
- **Backup services** for your computer files are critical. Today with the attacks with ransomware they'll encrypt your files and believe me, they won't give them back to you. They will ask you for money to get your files back, which is usually by a request to give them bitcoins, and they'll keep your money and you'll be stuck with an inoperable computer. **Don't pay them no matter how tempted you are…these people are criminals!!** Below see two cloud services that I recommend.
    - **IDrive** - this has a better pricing plan and will backup multiple computers and devices. They also have a plan that's free for 5GB which will work for many of you. https://www.idrive.com/pricing

    - **Carbonite** – the pricing is for 1 computer only. https://www.carbonite.com/en/?catid=&mkwid=sUu0L2OYR%7Cdc&adnumber=154363752604&c3apimn=154363752604,carbonite,e&pkw=carbonite&pmt=e&pct-network-name=marin&pct-network-pid=Uu0L2OYR&utm_medium=paid-search&utm_source=google&utm_campaign=10378&utm_content=2387&c3placement=2387&crb-cid=&gclid=CJqk7Jmh4dQCFUKUaQodqngFPA

I copied the following article from Kim Komando's website and hope that you'll read it through. If you get an email with one of the following subject lines listed below, DO NOT OPEN IT!! Immediately delete it from your email inbox!!!

**How to spot Jaff ransomware**

The new ransomware is called **Jaff** and it is spreading at a super-fast rate. It's being delivered by the Necurs botnet through a malicious email campaign.

People from all over the world started receiving these malicious emails on **May 11, 2017**. In just the first few hours of the Jaff ransomware campaign, over 13 million emails were discovered.

The malicious emails contain one of the following subject lines:

- **PDF_{four or more digits after it}**
- **Scan_{four or more digits after it}**
- **File_{four or more digits after it}**
- **Copy_{four or more digits after it}**
- **Document_{four or more digits after it}**
- **Receipt to print { if you haven't just purchase something don't open it!}**

The criminals have attached a PDF document to the email that contains an embedded DOCM file with a malicious Macro script. If the recipient runs this Macro, the ransomware is executed and files on the victims' gadget are encrypted. Impacted files are renamed and end with .jaff.

A ransom note will then appear on your gadget, it looks like this:


Image: Example of Jaff ransomware note (Source: Forcepoint)

The victim is instructed to install the Tor Browser and go to a link on the Dark Web. There, the victim will find instructions on how to pay the ransom to receive a private key that will allow them to decrypt the files.

The criminals behind this attack are asking for a hefty ransom. The demand to decrypt the victims' files is 1.79 Bitcoins, which is about **$3,300**. This is much larger than a normal ransom demand, so you definitely want to avoid it.

How to protect against ransomware attacks

In an effort to help people fight ransomware attacks, the FBI suggests taking these steps:

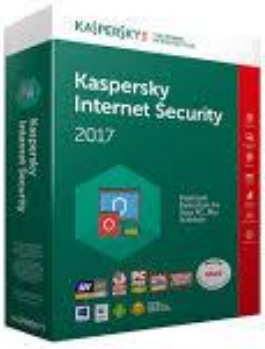
- **Back up data regularly** - this is the best way to recover your critical data if your computer is infected with ransomware.
- **Make sure your backups are secure** - do not connect your backups to computers or networks that they are backing up.
- **Do NOT enable macros** - You should never download PDF, Word or Excel files attached to unsolicited emails to begin with. If you do open one of these documents and it says that you need to turn on macros, close the file and delete it immediately.
- **Never open risky links in emails** - don't open attachments from unsolicited emails, it could be a phishing scam. Ransomware can infect your gadget through malicious links found in phishing emails. Can you spot one? Take our phishing IQ test to find out.
- **Have strong security software** - this will help prevent the installation of ransomware on your gadget.

**Remember, this is something that can't just be fixed! You'll lose everything if you don't have a backup. The main thing is, don't pay any ransomware threats.**

We thought it was just Windows users that were having problems, well now Mac's are on the list to target for malware.

If you like converting your movies and videos to other formats to view on your portable gadgets, you are most likely familiar with this free video transcoding software Handbrake. It's the go-to tool for many a Mac and Windows user for making videos compatible with just about anything. It's that popular! However, if you have downloaded **Handbrake** on a Mac between May 2 and May 6, there's a chance you may have infected your machine with malware instead. According to Handbrake's security warning, hackers have replaced the HandBrake-1.0.7.dmg installer in one of its download mirror servers with a trojan application. The affected mirror server was named as download.handbrake.fr and has already been shut down for investigation. The malware appears to be a remote-access trojan, which allows hackers to take complete control of your Mac and steal passwords and credentials as well. **If you're not proficient with repairs on a Mac, you'll have to have the infection removed by a professional repair person.**

Now a question for you! Do you use **Kasperky Anti-Virus**? Is so read the article below. If you've been watching the news, you'll know why the question is so important. As for me, I'll stick with Avast!!




# Article by Alexander Zemlianichenko Jr./Bloomberg

Russia's growing aggression toward the United States has deepened concerns among U.S. officials that Russian spies might try to exploit one of the world's most respected cybersecurity firms to snoop on Americans or sabotage key U.S. systems, according to an ABC News investigation. Products from the company, Kaspersky Lab, based in Moscow, are widely used in homes, businesses and government agencies throughout the United States, including the Bureau of Prisons. Kaspersky Lab's products are stocked on the shelves of Target and Best Buy, which also sells laptops loaded by manufacturers with the firm's anti-virus software.

But in a secret memorandum sent last month to Director of National Intelligence Dan Coats and Attorney General Jeff Sessions, the Senate Intelligence Committee raised possible red flags about Kaspersky Lab and urged the intelligence community to address potential risks posed by the company's powerful market position. "This [is an] important national security issue," declared the bipartisan memorandum, described to ABC News by congressional sources.

In February, the Department of Homeland Security issued a secret report on the matter to other government agencies. And the FBI is investigating the nature of Kaspersky Lab's relationship to the Russian government, sources with knowledge of the probe told ABC News. The company has repeatedly insisted it poses no threat to U.S. customers and would never be used as a government tool.

Current and former U.S. officials, however, point to company executives who previously worked for Russian intelligence and military agencies. They worry that Kaspersky Lab's software could allow state-sponsored hackers to steal users' files, read private emails or attack critical infrastructure in the United States.

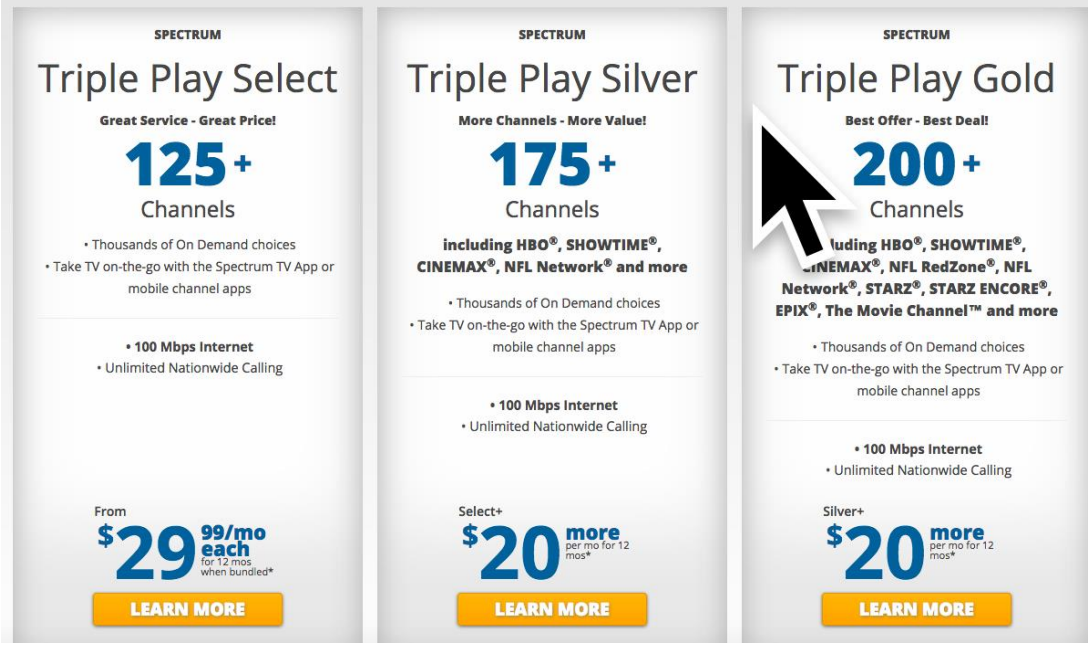
**Kaspersky Lab's possible relationship with Russian intelligence services "makes a lot of people in the national security community uncomfortable," said Eric Rosenbach, a cybersecurity veteran who until January was the Defense Department's chief of staff. In particular, current and former U.S. officials fear Kaspersky Lab products have the potential to facilitate Russian cyberattacks on power grids or other key utilities. "That is something I have followed for a long time and have significant concerns about," former U.S. Deputy Secretary of Energy Liz Sherwood-Randall said.**

There was "widespread knowledge that this poses a huge risk to the U.S. critical infrastructure," according to Michael Carpenter, who until January served as the Defense Department's deputy assistant secretary for Russia, Ukraine and Eurasia.

Last year, FBI officials communicated potential concerns about Kaspersky Lab to a select group of private-sector leaders, including the Electricity Subsector Coordinating Council, an organization of electric company chiefs from across North America, sources said. The Senate Intelligence Committee also received several briefings on the matter.


Did you hear that Cable TV suffered the worst quarter ever? According to quarterly reports, cable and satellite TV services have lost about **762,000** subscribers over the first three months of 2017. That's five times more than the same period last year! Is the cord-cutting movement slowly killing cable TV? I'm not sure about that, but since I've had Spectrum I'd say that it's an option to seriously consider. I talked to Spectrum and this is what I found out.

- There is no longer going to be a "basic plan" for cable. You'll have three choices which are below. The prices are for "new customers". If you already have Time Warner, you're out of luck. The lowest plan starts around $129 a month without boxes and taxes.




They also told me that they require a cable box for every TV you own. They won't use the discounted "little" boxes that they sent out last year. I asked the service rep for a total for my bill, and my bill will go up about $25 a month. So much for Spectrum being competitive! The worst part was that my service has gone downhill…my phone doesn't work half the time, Cable doesn't always connect on the TV's and Internet? Half the time I can't get my mail or get on a website. I'd be interested in hearing your experiences, and also what you have..Verizon, Dish.. and is it working well for you.


**Computer Term of the Month –** Well, I have the perfect example! When I started my business, I needed a name for it. I registered the name I chose with the State of New York, and then I could use that name to list my business and to setup a website to advertise. My domain name is Shirl's Computer Solutions (the name of my business) and when people search they find me by my "domain name".

That's it for this month!  I guess I didn't cut back very much. ☹  I do want to thank all who have made phone calls, sent cards and have offered prayers.  My eyes are healing but the cornea repair is still keeping me from driving and enjoying the sunlight. My eyes are very sensitive to most lighting.  I am working from home, so don't be afraid to call if you need help.  I'm using TeamViewer or accepting machines for repair at my home.

 *Happy 4th!*

Warm Regards,

Shirl