Shinn Technology Services Corporation

P.O. Box 173
Fishers , IN 46038

(317) 545-3650
http://www.ShinnTechnology.com

Urgent issues in technology 2016 to date

Windows 10 Virus?

Recently Microsoft has gotten very aggressive about loading the Windows 10 operating system on your computer. Months ago they loaded KB3035585 as an MS update. That loaded a white icon on your taskbar to provide never ending pop-ups about the upgrade. That alone was a nuisance, but as of two weeks ago, they have been auto-loading the upgrade files on your computer (about 7GB without your knowledge) and auto-installing the Windows 10 operating system. Like a plague, clients have called us-- "I didn't push any buttons-- the computer just loaded the Windows 10 upgrade-- and now I can't _____ (fill in the blank)."

Below is some brief information and Q&A about Windows 10.

Windows 10 loaded on a brand new computer is fine. There can still be problems with devices you want to connect (printers, scanners, NAS drives, etc) and software issues, but at least the base computer and it's device drivers are solid. A new computer was built to run the Windows 10 operating system.

Although I think Windows 7 (supported through Jan 2020) is the most stabile operating system ever produced, Windows 10 is far better than the Windows 8/8.1 series. The Windows 10 upgrade is free through July 29, 2016.

1) Why is the Windows 10 upgrade a problem?
Windows 10 upgrade try's to detect and load device drivers for all functions of your computer—hardware and software. The older your computer or software, the more problems will occur after the upgrade. I have had everything from complete hard drive failure… can no longer print… can no longer access the internet… to software programs that no longer function. Call Microsoft support--- they will tell you they are not responsible for support of your computer or their upgrade.

2) What if Windows 10 got loaded and I don't want it?
You can uninstall the upgrade and go back to your previous operating system within 30 days of the upgrade. If you got caught in the auto-upgrade scam, allow Windows 10 to finish loading (do not just turn off your computer). After the upgrade has loaded, open the Start menu and select Settings. Click the Update & Security icon and select Recovery. You will see a "Go back to Windows X" option. Click the Get Started button.

3) What if I want to disable the ability of Windows 10 to auto-load?
Never10 was developed by Gibson Research as a free utility to remove the 7GB of windows files and disable the ability of the computer to be upgraded. You can read about and download the utility from here. It is safe to use.

https://www.grc.com/never10.htm

4) I would like to install the free upgrade to Windows 10—how do I proceed?

- Research all devices and software in your environment. Make sure there are device drivers (or work arounds) for all your printers, scanners, etc…. then check with manufacturers of software to make sure your version will work under Windows 10 (there may be patches needed or upgrades required).

- Perform a complete data backup to an external hard drive (maybe even two backups).

- The upgrade can take up to two hours depending on your internet download speed and processor speed. Windows 10 will attempt to get you to "login" to a Microsoft account as part of the installation. There is a skip (very small at the bottom of the screen). I would suggest using Windows 10 in local mode due to privacy issues. See *Security Refs* below for additional reading.

- After you finish the upgrade and login, immediately test everything in your environment. Access to network server, printing, scanning, software (and all functions you use in that software). Make sure everything works. At that point you have 30 days to uninstall the Windows 10 upgrade if something comes up and no solution can be found.

Security Refs:
http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself

http://bgr.com/2015/07/31/windows-10-upgrade-spying-how-to-opt-out

5) I am using Windows 10, but having problems with Edge.
Microsoft came out with a new browser with Windows 10--- The Edge. Because Internet Explorer is such a targeted browser for hackers, The Edge was developed to combat these issues. The problem is The Edge is not an industry standard browser. Banks for example, may only support Internet Explorer, so The Edge will not work with many online accounts. You can go back to Internet Explorer as it is loaded (but kind-of hidden).

- Click the Start Menu, then All Apps, then Windows Accessories--- you will find Internet Explorer
- You can go into the default program manager and make IE the default browser as well

Safely remote USB devices--- Eject

When using a USB device, like an external hard drive, it's a good idea to properly eject the device rather than just unplug it from the computer. Please click the link below to learn how…

http://windows.microsoft.com/en-us/windows7/safely-remove-devices-from-your-computer

Domain Name Registration & Image Licensing

Whenever you register a domain name for your use, make sure it is registered in your name with your contact information. After your web developer sets the DNS, go in and change the password so that only you have access. Also make sure you have a written agreement with your developer/advertiser that you own the domain and the website (and all images on the website)… otherwise if the relationship goes bad, you may find that you own nothing and have to start your corporate branding all over again.

Image licenses

It is very important in today's litigious environment, that you purchase licensed images to use on your website and internet marketing. Just "taking" an image off the internet can get you sued. A matter of fact, Getty Images sells licensed images--- but they make a lot more money finding and suing people who are using their images without proper license. They prey on people without good legal knowledge and it's a huge business.

REF: http://artlawjournal.com/respond-getty-images-demand-letter

Industry blocking more email from spam sources- AOL, ATT, YAHOO

SPAM is a huge problem. No one wants to get a thousand worthless emails a day. There are many resources available today that help your email service provider remove junk emails before you ever see them--- of course it's a balancing act to try not to delete emails you want to see from clients and friends. We see many problems with users of AOL, Hotmail, ATT and YAHOO getting blocked as spammers. This is partly because they are old email services and partly because they do a poor job of policing their outgoing mail load for spamming.

You can get on a SPAM list from a couple points—1) You, the user, are sending out hundreds or thousands of emails a day—even to your clients and friends, would be picked up as a SPAM use. 2) Someone on your shared server is a Spammer and gets the entire IP address/Sever put on a black list. It sometimes takes days to get this problem resolved through the blacklist servers.

A better way to do email marketing or mass emailing is through Mail Chimp or Exact Target. Mail Chimp is free up to 2000 subscribers and Exact Target has great small business packages.

Blocking super cookie with Better Privacy

In conjunction with using Mozilla Firefox as your browser, Better Privacy serves to protect against special long term cookies, a new generation of 'Super-Cookie', which silently conquered the Internet. This new cookie generation offers unlimited user tracking to industry and market research used by Google, YouTube, Ebay and others. Concerning privacy Flash-cookies are most critical. This add-on was made to make users aware of those hidden, never expiring objects and to offer an easier way to view and to manage them - since browsers are unable to do that for you.

Flash-cookies (Local Shared Objects, LSO) are pieces of information placed on your computer by a Flash plug-in. Those Super-Cookies are placed in central system folders. They are frequently used like standard browser cookies. Although their threat potential is much higher as of conventional cookies, only few users began to take notice of them.

Click here to learn more.

https://addons.mozilla.org/en-US/firefox/addon/betterprivacy
https://www.mozilla.org/en-US/firefox/desktop

What is Ransomware?

Ransomware is malicious software that cyber criminals use to hold your computer or computer files for ransom, demanding payment from you (Bit Coin is the currency) to get them back. Sadly, ransomware is becoming an increasingly popular way for malware authors to extort money from companies and consumers alike. There is a variety of ransomware can get onto a person's machine, but as always, those techniques either boil down to social engineering tactics or using software vulnerabilities to silently install on a victim's machine. CryptoLocker and its many variants are probably the most known form reported by the news media.

The best preparation to protect against Ransonware is to regularly backup your data. Note: Never leave a USB device (external hard drive or jump drive) plugged in when not backing up your computer. If you are attacked, the ransomware will move out to all external connected drives as well…. making your backup worthless.

REFS:

http://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker
https://en.wikipedia.org/wiki/Ransomware
http://money.cnn.com/infographic/technology/what-is-bitcoin

Passwords

When we maintenance or rebuild a client computer, it is often times necessary to re-login to resources (email, bank, vendors, etc). Not having your password causes a considerable delay in service. It can take up to 20 minutes to go through the "lost or forgotten password" process for just one password. We're just trying to save you money on the time of a service call. Please store your passwords in a safe place for quick reference.

Backup Options
In today's world there is absolutely no excuse for not backing up your data! There are many affordable options.

1) Remote backup offsite via internet
There are many remote options for backing up. Carbonite is one of the most popular reported by the new media, however there are some negatives when restoring data. We prefer paraDATA offered by Proxurve Solutions in Carmel Indiana. Your backup is encrypted for security and stored on a server in a secured Indianapolis NOC (network operations center). Their rate plan starts at $12 per month for up to 10GB of storage. There is about an hour in labor for setup.

2) External hard drive routine local
In this scheme, you purchase two USB external hard drives and alternate them for daily backups. One is stored in a local fire safe and is alternated daily. We use NovaStor for a backup software solution. The total for this setup is about $400 plus and hour of labor.

Be careful who you call for support
It is easy for a user to go to Google and type in, for example, "Hewlett Packard phone support." Don't be surprised that the phone number you are given is not an HP support center, but a scam center that has indexed their number on Google under "Hewlett Packard."

I have at least two people per week that get caught in this scam. The representative will ask to be remote connected to your computer. From that point you are actively getting scammed. They may tell you that you have a serious virus or that malware is loaded. They will then load tracking software, permanent remote connect software or maybe even a virus so that you DO have a problem.

Make sure you know who you are calling. If you want Hewlett Packard because you own a printer product, look in the documentation that came with your printer… there will be a support number there. This is the same for any support number---- utility vendors (look on your statement), computer products (look in the manual)…etc.