Shinn Technology Services Corporation

P.O. Box 173
Fishers , IN 46038

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

Technology Issues Update for 2016

Cloud based storage and sharing… cost and security?

There are many options today of storing your documents, photos and music. For the past few years, Cloud based solutions have offered storage areas and allow sharing of data between your devices. Dropbox, Amazon Cloud Drive, Microsoft OneDrive, Apple iCloud and ShareSync all offer these services.

There is really no "best" service. Depending upon your needs, the companies above have many offerings ranging from a low amount of storage for *free* to $20 per month packages for extended storage and sharing. Below are some general guidelines for using Cloud based products.

If you are totally concerned about the security/safety of your data, do not use these services. *Any information you put on the internet could be compromised*. I can say that all companies listed above use encryption for the data being passed back and forth from your computer… and they employ advanced security schemes for their internal and external operations. However, I'm sure you've heard of recent hacks stealing personal data. Below is a link to a list of data breaches for 2016 to date… scroll down to the bottom of the page for details. You may be surprised who has been hacked and what data has been compromised.

https://www.identityforce.com/blog/2016-data-breaches

Whenever you're logging into an internet based resource (bank and credit accounts, vendor accounts, etc.) always use a separate and rich-text password. If you're bank gets hacked, the hacker will attempt to use that password for other accounts you may have. Here are some examples of rich-text passwords: 1P@ssw0rd#, 2016CurlyBird1, 9WilberPig!@#, Johnny#Five93. Never give your password to anyone--- not even when a vendor support department asks for it (because you may not actually be talking to their support department if you've been scammed---see next article).

Backups: Even if you use online Cloud storage (which should be backed up by that vendor), I would suggest doing a separate backup to an external hard drive once a week and storing it in a fire-proof lock box for an additional archive of your digital property.

Be careful who you call for support- continued warning

It is easy for a user to go to Google and type in, for example, “Epson printer support phone number.” Don’t be surprised that the phone number you are given is not an Epson support center, but a scam center that has indexed their number on Google under “Epson Printer Support.”

I continue to have clients getting 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 Epson because you have a printer issue, look in the documentation that came with your printer… there will be a support number there. This is the same for any support number needed---- utility vendors (look on your statement), computer products (look in the manual)…etc.

Understanding Online Restoration

There are many companies that provide online backup services. Carbonite, BackBlaze, iDrive and Barracuda to name a few. This article is not so much about services offered (those are pretty straight forward)... but the process and time of restoration.

When you setup a program like Carbonite and define your backup set, it may take 3-5 days to upload or “seed” your data to populate the first backup set. The time depends on your internet speed and network traffic in your home or office. From there, the daily backup will upload only the files in your data set that have changed.

Let’s say your hard drive crashes. You get a new hard drive, load the operating system and all programs, and then install Carbonite to restore your data set. *It will take 3-5 days for the data set to be restored!* Please be prepared for this… it is not a fast process.

There are a couple ways to be prepared for this disaster recovery.

1) Create a separate weekly backup of your data set to an external hard drive once a week and store it in a fire-proof lock box for an additional archive. It will be much faster to restore your data set from this hard drive than to wait for the cloud based backup to restore. Then, you only need to restore the cloud files that are newer than your local backup.

2) Use a local cloud based backup service. I use Proxurve Solutions out of Carmel, Indiana. They provide the same type of Cloud based backup--- only their servers are located in Indianapolis at the Eastgate Lifeline Data Center. If you have a hard drive crash, we can meet with Proxurve Solutions and copy the data set directly to an external hard drive for immediate restore.

Cost: Some of the cloud based services are pretty cheap (like $49 per year), but you certainly get what you pay for. Proxurve has packages available that start at $12 per month--- local service—fast support.

Always More Scams

There have been a variety of new scams. Here are a few of them…

1) A call from the Internal Revenue Service announcing that you owe back taxes and that an arrest warrant will be issued if payment is not made immediately by credit card. The IRS will NEVER call you about anything. They will send a letter via US Mail on official IRS letterhead with the issue and provide a number for you to call.

https://www.irs.gov/uac/tax-scams-consumer-alerts

2) A call from Windows that a virus has been found on your computer. They will want remote access to your computer and may ask for a credit card to resolve the issue. "Windows" is not a company, it is a product of Microsoft Corporation. They will NEVER call you.

3) A call from a company indicating that you have won a free or discounted travel package. They are asking for a credit card to secure the package and pay for overnight shipping of your travel information. It's all fake.

4) Onscreen Rogue Notice--- a screen will appear while you are browsing the internet (it often times has sound too) saying that it is a Microsoft warning that a virus has been found on your computer. Call this "800" number for immediate help. It is a scam. If you call them, they will want remote access to your computer and get a credit card number. Immediately restart your computer and run antivirus and MalwareBytes scans.

Never give anyone calling you any personal information… period. Ask for their phone number and call them back if you're tempted to hear their spiel. Chances are they will just disconnect.

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 that 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 software 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 actively using it to backup your data.* 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

Domain Name Expiration

If your domain name registration expires, you will know pretty quick as your website and email will no longer function.

You have up to 30 days to contact your registrar and make payment to retain your domain name. After that, the registrar could either return it as available to the public to register or they may roll it under their umbrella of domains owned (and make you pay a high price to get it back later).

Anytime to you get a renewal notice and you aren't quite sure…. call us at 317-545-3650 and ask. We'll be glad to lookup the correct renewal company and time.

Domain Registry of America is a scammer that may send you a renewal notice close to your normal renewal period. If you pay the invoice, they will transfer your domain out of the US and continue your service. You really won't know what has happened until you get a high renewal fee the next year. It takes about 3-4 hours labor for ShinnTech to recover the domain and move it back to the US where you have control.

Free Public Wireless… is it safe?

Most of the public wireless networks at Starbucks, Panera Bread, Hotels, City Centers, etc. are minimal security or wide open networks. Although it is fine to do general internet surfing, I would suggest not logging into bank, credit card or any other critical accounts. I would even suggest not logging into Facebook or LinkedIN. Someone attached to the wireless network could intercept your login credentials.

A really good article to review…

http://www.networkworld.com/article/2904439/wi-fi/is-it-safe-to-use-public-wi-fi-networks.html

Facebook Fraud

The latest scam has to do with hackers creating a new profile in your name… using photos they steal from your real profile. They will then start sending friend requests to your friends posing as you. If you find out that this has happened, immediately post a message on your wall alerting your friends not to accept any new requests from you. Then report the fraudulent account to Facebook at *phish@fb.com*.

General Facebook Security Info

Every user should review their security settings to see "who" can see their information

1) You can adjust settings so that no one can see your friend list (friends, manage, edit privacy, "Only Me")

2) You can adjust settings so that no one sees your photos, albums or videos accept your friends.
   Note: Your profile and cover photo images are public—everyone can see them.

3) You can limit what your friends see. Go to a friend and change the status from friend to acquaintance.
   When you post something, make sure the setting for that post is "Friends except Acquaintances".

4) Change your password frequently /use rich-text passwords. 9WilberPig!@# or Johnny#Five93 for example.