Information from Evan Corstorphine, owner of the "Portable CIO"

Website is www.theportablecio.com. Telephone: 925-552-7953

1)   New System Recommendations sheet. Click Here for Details. This is our bible for purchasing new systems. If your members read this they will understand our recommendations and philosophy for buying new systems.

2)   Check out our Facebook page for updates and interesting tidbits. I'm working on updating it more regularly with information about what is going on, things to avoid, good articles on security or exploits that people should know about. Just go to Facebook and 'like' Portable CIO – https://www.facebook.com/pages/Portable-CIO-Inc/112259638810195

3)   Antivirus – We recommend AVG and Malwarebytes. Kaspersky is also a good antivirus. Avast – someone asked about it – it's OK too – there are many decent brands out there, and if you google 'antivirus ratings' or 'antivirus comparison' there's a lot of good information available. Stay <u>away</u> from all-in-one Internet Security versions of Antivirus. Under no circumstance let any McAfee product on your system, particularly the garbage 'Mcafee Virus Scan' that is downloaded alongside things like Flash and Java. "Friends don't let friends drive McAffee." It's junk software in my opinion.

4)   WWW.NINITE.COM – this site is completely legitimate and offers a plethora of useful software. Check it out!

5)   "Classic Start" – the tool that gives you a useful Start Menu for Windows 8 / 8.1 – available at ninite.com

6)   Brands – we do not believe in building computers – it is a complete waste of money to try to build a better computer than companies with seven-digit R&D budgets. We recommend Dell and Lenovo. The only exceptions would be an HP business-class workstation, but those are pretty expensive and inaccessible to the ordinary consumer.

7)   Costco is the best deal around for buying computers. They offer computers better configured for less money than I can buy at Dell with my Partner discount. This is buying<u>online</u> – not in the store.

8)   Get a system with an i7 processor and <u>at least</u> 8gb RAM. 12, 16 or 24GB RAM is just fine, and eventually you'll use it.

9)   Backup your computer! We are firmly against using a local hardisk backup as the primary/regular backup. After seeing thousands of people and their habits, it is my firm belief that internet backups are superior, because they actually <u>get done</u>. Local hardisks die, the USB is flaky, and everything overheats. And that is if you actually ***remember*** to do the backups every week. Local hardisks are fine, <u>only</u> if you want to use a product like Acronis True Image Home to make a full image copy of your hardisk, and then

store that local hardisk away in a drawer. Use www.crashplan.com for your day-to-day backups to ensure all your important files, pictures, geneology, etc. is backed up. Carbonite and Mozy are fine too – we just prefer Crashplan because of some of their features are better. Budget about $6/month max for internet backups. And, no, we are not concerned about the security of the stored data.

10)   You have no privacy.

11)   Use Google Chrome for your web browser. It has built-in predictive web-page analysis that will warn you if the website you're trying to visit has malicious code.

12)   Add the 'extension', called "AdBlock" to your Google Chrome to block the annoying side-ads that are so prevalent on the webpages we visit.

13)   Use GMAIL for your email. Avoid using email provided by your DSL or cable provider, because their spam and virus filtering is nowhere as good as Google's system. Google bought and operates a firm called Postini, which has the best spam and virus filtering available. If you're using an email address like: sbcglobl.net, pacbell.net, att.net,Comcast.net, astound.net, msn.com, Hotmail.com, etc. etc., consider switching over to Google. You *do* care about this, because the less SPAM and Viruses you are exposed to, the higher probability you'll avoid infection by one of the nasty exploits in circulation.

14)   Cryptolocker is a nasty piece of malware provided by the Eastern European computer community (Russian mafia), which attacks your computer by encrypting all of your data files. It cannot be cracked, and you can either wipe off your computer to start over, or you can try paying the ransom. It's 50/50 whether they'll even give you the decryption key after you pay the ransom, so the best medicine in this case is to avoid the illness by keeping all of your defenses in top form. The FBI calls the Cryptolocker/Cryptodefense exploit "The Perfect Crime", because they can't track it, and even the payments which use "Bitcoins" are untraceable.