This is a list of tips to keep your computer's security tight and as strong as possible. If you have not followed some of these tips before, this information can function as a security checklist. For instructions on how to implement these steps, follow the links.

Portable CIO's Safe Computing Tips

1. **Keep your computer up to date: Patch, Patch, PATCH!**
   Set up your computer for automatic software and operating system updates. An unpatched machine is more likely to have software vulnerabilities that can be exploited.

2. **Use the right web browser.**
   Our recommendation is to use Google Chrome. It does a better job of preventing access to sites with bad code.

3. **Install protective software, MAC or PC. EVERYONE gets infected – Macs are NOT special.**
   Sophos is available as a free download for Windows, Mac, and Linux from IS&T's software grid. When installed, the software should be set to scan your files and update your virus definitions on a regular basis. We recommend AVG and Webroot for PC's.

4. **Use Ad Blockers**
   Bad guys are using advertisements to insert malicious code into your system. If you block the ads, you block a whole category of threats from accessing your system. The best way to do this is to use Google Chrome (download here), and go into the settings, then into Extensions, and search for and add the extensions called "**Ad Block**" and "**Ad Block Plus**". These are free, and do an excellent job of preventing those pesky side-bar ads that can sometimes spell doom for your computer.

5. **Use AntiMalware and AntiRansomware**.
   AntiMalware works together with your antivirus to create overlapping layers of protection for your system. They all cover different threats, and yes, there will always be overlap. We only recommend 'Malwarebytes AntiMalware' Do not be cheap and use the free product, because that does not stay resident and protect you all the time. Only the paid product protects your 24x7.

6. **Use Email services with Top Notch SPAM and Virus Filtering**.
   Email services are not created equal. Older services such as Comcast, ATT, Pacbell, SBCGlobal.net, AOL, Hotmail, MSN, do not have good SPAM and Virus filtering. That means you are receiving a lot more possibly infected JUNK than you should. Google (Gmail) uses a world-class Spam and Virus filter called Postini, and people who use their system have a far lower volume of SPAM and Viruses than any other service. Outlook.com (Microsoft) is also a good

system, and of course having your own private domain (like your family-name.com) is a great way to limit SPAM and Viruses.
--- Don't be afraid of the switch-over process. It's easy, we can help you, and you won't lose track of everything. Make the change!

Email services we recommend: Gmail.com, Outlook.com, or your own private domain hosted through Office365.

Email services we recommend against using: Hotmail.com, Msn.com, me.com, mac.com, sbcglobal.net, Pacbell.net, Att.net, Comcast.net, covad.net, astound.net

7. Choose strong passwords.
Choose strong passwords. Your passwords should be AT LEAST 12 characters. Use phrases – MUCH easier to remember—and augment them by changing O's into 0's, i's into 1's, and adding $ for the letter S.

- Remember the phrase generator we discussed here: http://preshing.com/20110811/xkcd-password-generator/ -- there is a cartoon on this site that explains why long passwords are so much more important than "complex" passwords.
- Do NOT use the same password for all your internet accounts. Remember – if the bad guys hack a server and capture that amazing password you've been using on all of your accounts, they can break into anything and everything you have online.
- Keep an XL spreadsheet on your PC, or a written diary of your passwords at your desk. The threat to your bank account is "out there"; it's not someone in your living room seeing your list.
- If the website you are using offers "two-factor authentication", do it. When you use two-factor authentication, the extra verification step ensures only you can access your account. It's great security.

8. NOBODY IS WATCHING YOU. Hang up the phone. Please, do not ever fall for the unsolicited telephone call, telling you: "We're from "Windows" and we're monitoring your computer and you're system has an infection." MICROSOFT WILL NEVER, EVER call you. Nobody legitimate will ever call you to access your computer, unless it is for technical support that you first requested from Portable CIO or another service firm.
Bad guys prey on folk-lore and our fears that "big-brother is watching" to scare us into making bad choices. If someone calls you and says they are from "Windows" and they want you to work with them on your computer. HANG UP ON THEM. They are thieves, liars, scam artists, and do not deserve a bit of respect or your time. Do not be nice: THEY ARE BAD GUYS.

9. If something you receive seems too good to be true, it ~~probably~~ is.
There is *no* free lunch.
You did *not* win a "free cruise."
There is *no* rich uncle.
The bank did *not* make an error in your favor.
You did *not* win a "free cruise."

10. **Pay for your software. Free software introduces risk.**

"Free" versions of software are usually sponsored by people who want to sell you other services or products you don't want. Worst case, they're outright infected. Also, "free" versions of software (particularly protection products) usually have certain key important functions disabled – such as real-time monitoring. If you have antivirus or antimalware, but it's just sitting there and not turned on because it's the "Free" version, what good is it? (It isn't.) The cost of legitimate software is a trifle compared to the cost of expensive repairs, data loss and emotional stress.

11. Stick to professional recommendations. I.E., just because you *can* do something, doesn't mean you *should.*

Yes, there are a lot of good products out there. There's even more bad ones. Avoid following the latest fads, or fancy advertisements, or recommendations from your non-IT-professional friends. We do this for a living, and want you to be safe. If you follow our recommendations, you have done everything possible to safeguard your system. Messing around with the recipe *decreases* your safety, and introduces unintended actions and consequences. Follow good advice, and you are going to be safer and more supportable if and when things do go wrong.

12. **Backup, Backup, BACKUP! Your FIRST backup should be internet-based. Your SECOND backup can be "local USB Hardisk" based.**

Use Crashplan (www.crashplan.com) Backing up your machine regularly can protect you from the unexpected. The service keeps a few months' worth of backups and make sure the files can be retrieved if needed. Download and install CrashPlan and learn how to back up your system.

- Don't trust USB hardisk backups. Based on the experience of fixing thousands of computers, I can say with authority that they don't ventilate the hardisks, which causes them to overheat and fail, and the USB electronics within them are consumer-grade and flaky. Use these only as receptacles of whole-system images using whole-image backup products such as Acronis (www.acronis.com), then put that image in your safe. Do not rely on USB hardisk as your primary backups for daily use – it is a disaster waiting to happen. And, do not leave them plugged into your computer and turned on; use them, turn them off, and put them in your safe. (In addition to the reasons stated above (heat, flaky electronics), if a backup hardisk is attached to your computer and your system contracts Ransomware, the backup hardisk will become encrypted and unusable if it is connected to your system when the infection hits. Then you're sunk.
- Never use a USB Thumb-drive as your primary backup medium. They're ok for short-term secondary storage or for transporting data, but they are not reliable for backups.

13. **Control access to your machine.**

Don't leave your computer in an unsecured area, or unattended and logged on, especially in public

places. This includes Athena clusters and Quickstations. The physical security of your machine is just as important as its technical security.

14. NEVER conduct banking or login to sensitive sites when on public networks

It's almost impossible to tell if the wireless network you are connecting into is legitimate. If you connect to a "spoofed" network at an airport and login to your banking website or check your stocks, or do anything with your passwords or personal information, this information is all being captured by the bad guys. No Bueno. So, if you're in public place, limit your web surfing to those things that have no pecuniary value, such as Google, Yelp for restaurants, Wikipedia, etc.

15. **Use email and the internet safely.**

Ignore unsolicited emails, and don't open attachments, links and forms in emails that come from people you don't know, or which seem "odd" – unexpected or otherwise unordinary. Avoid untrustworthy (usually free) downloads from freeware or shareware sites. Learn more about spam filtering.

16. **Please use OpenDNS Network protection.**

Protect yourself by subscribing to, and using OpenDNS. For $20/*year*, you can add this extremely valuable layer of protection to your entire home network and to all of your PC's, Mac's. This is one of the best layers of protection against Ransomware and "drive-by malware" from infected websites. We recommend it for all of our clients.

17. **Protect sensitive data.**

Reduce the risk of identity theft. Securely remove sensitive data files from your hard drive, which is also recommended when recycling or repurposing your computer. If you travel with a laptop, we suggest you Use the encryption tools built into your operating system to protect sensitive files you need to retain. If the system is encrypted, if it's stolen, the data is useless to whomever ends up with the machine.

18. **Use desktop firewalls.**

Macintosh and Windows computers have basic desktop firewalls as part of their operating systems. When set up properly, these firewalls protect your computer files from being scanned.