COMPUTER PRIVACY OVERVIEW

1. Protect yourself from hackers.

a. Turn off your computer and wi-fi router at night or when away from the computer for extended periods. You can't be hacked when you're not connected.

b. Never click on an email from an unknown source. Phishing is still the most common way individual computers get hacked. If you're not sure, don't click! If, for example, you get an unexpected email from your "bank", call the bank to see if its legitimate.

c. Never click on ads. Criminals buy ad space on legitimate websites, and you'll never know the difference. If you see an advertised product/service that interests you, do a search and go to the website of the product's manufacturer.

d. Use a reliable antivirus app. Windows 10 Defender which comes free with Win 10, is adequate--if you have that, there is no need to buy another app. If you have an earlier version of Windows, do a search for reputable companies and expect to pay a yearly fee. Its definitely worth the money (think of it as insurance).

e. Always use "https" instead of "http" to avoid ending up on fake websites. Download and use the app HTTPS Everywhere.

f. Use a search engine that, by default, does not log your IP address. I use DuckDuckGo for all my searches.

2. Protect your privacy: avoid data collectors who sell your data for big bucks.

a. Never give out personal information online unless legally required to do so. This includes real name, DOB, SSN, current address (you really don't want crooks to find out where you live), phone number, primary email address. If you go to a new website which asks for this info, make up a name, etc. This is called "spoofing" and is NOT illegal or immoral as no one is harmed (but you retain your privacy). Create an alternative email address and phone number for just this purpose (do a search for how to); use "spoofed" info to open those accounts.

b. Anonymous browsing is very important. Always use a VPN when visiting websites online in order to avoid being tracked online. Choose one that opens automatically when you turn on your computer; then you won't forget to use it! Pay for a good one that does not retain any of your traffic or connection logs (read the privacy policy); you can get good ones that cost less than $100 per year. Personally, I avoid the free ones. E.g., NORD, OpenVPN. If you are not familiar with VPNs, research before buying so you understand what you're getting. Again, think of this as insurance.

c. Use a browser that does not keep your info (i.e., a record of all websites you visit). FIREFOX is most often recommended by experts. Avoid the big names like Google, Yahoo, etc.

d. Consider an encrypted email like Protonmail (free or paid versions--I use the free one). Why? Consider this: Google, for example, sends you personalized ads via scanning all your emails to see what products you are interested in and then selling that info to advertisers (and might they

be scanning for other info as well?) . This quote says it all: "Why does Google provide all these great apps for free? You are not Google's customer, you are its product." (Note: it will be to your advantage to research and understand the concept of "end-to-end encryption.")

e. Very insecure, text messages are like post cards--open for the world to see (and usually stored indefinitely). Avoid using the native text-messaging feature (the one that came with your smart phone). Instead use a text-messaging app that uses encryption, e.g. ChatSecure, Signal, also Cryptocat for iphone. Other popular text apps are less secure than advertised, e.g. Whisper, Secret. As always, do your homework before choosing one; apps with OTR and PFS are best.

f. Use a search engine that, by default, does not log your IP address. I use DuckDuckGo for all my searches.

3. Other useful tips.

a. Use Malwarebytes for additional virus protection (free or paid).

b. Consider using a cookie cleaner software tool like ccleaner. (Research "cookies," which can track your activity online.)

c. Not a safety/privacy app but handy: Adblock Plus does what the name suggests--blocks most (but not all) advertising from website pages. (Ironically, this often triggers pop-up pages saying "please turn off your ad blocker!)

4. Continue to educate yourself on internet safety issues. Here are some books I've read that are enjoyable and informative. Some will go beyond what the average privacy seeker needs, but I find it interesting to see just what can and cannot be done.

Future Crimes by Marc Goodman. This blew me away when I first read it soon after it was published. Have re-read it and used it for reference several times since. One of the best non-fiction books of 2015.

The Art of Invisibility by Kevin Mitnick. This book explains all the issues and terminology mentioned above and then some. He tries to keep it simple but sometimes the tech is just complicated. "The world's most famous hacker." Since he did it before being caught by the FBI, he can tell you how to avoid it!

Hiding From the Internet by Michael Bazzell. Great stuff, well written, but has a lot more info than many of us need. Pick and choose the content you're interested in.