Welcome to Securing Your Digital Footprint-

Basics of Cyber Security-

In this new year I wanted to talk about a few things to hopefully make 2017 safer and more secure.

Security - is where it all starts. I just finished a class (https://www.futurelearn.com/) on Cyber Security. Let's talk about security for your digital life.

You have an iCloud account, and you haves stored some very personal photos there. The next thing you know, you can't access your account, your password isn't working. Then you hear from all of your friends on Facebook/Social Media, that these naked pictures of you have been popping up all over the web. That's what happened to those celebs that were in the news recently. It wasn't a lack of security on the iCloud site it was Bad Guys getting a hold of information that they used. Information that was out there from interviews, yearbooks, Facebook/Social Media, web sites. Once they asked for the password to be changed, the Bad Guys were asked those 'personal security questions' which they were able to answer and gained access to the account.

***Personal Security Questions** - Make up answers to those questions, put the 'fake' answers someplace secure so that you can refer to them - and use THEM and only THEM.

***Passwords** - it used to be thought that a password that was at least eight character was OK. Now the thinking is the longer the better, fifteen characters is the minimum length now. Of course you want to have upper and lower capitals, numbers, symbols AND a saying is more secure than something random. Example would be: #IwEntToThe%Z00~ . Using a password generator is something that you can employ if you are having a hard time thinking something up.

NEVER use the same password more than once.

Change your passwords, yes all of them, at a minimum of every three months.

***Password Safes/Managers** - are certainly a good idea, I know I suddenly have a password for nearly any place I go on the web, impossible to remember them all. Some good ones are 1Password and LastPass both work with Mac, Windows, Android, iPhones. There are many other similar products out there. What's old is new, writing down passwords on a piece of paper and keeping it in your desk, is now an acceptable secure thing to do. In addition to all the pertinent info for each account, I also put a date that I last changed the password and what the last password was. If you try to use a previous password with some security systems it will lock you out.

Make sure that the master password to get into your password safe/manager is very strong. One of the new hacker attacks is to go after that password. (http://arstechnica.com/security/2014/11/citadel-attackers-aim-to-steal-victims-master-passwords/) Alarm bells went off for me when I recently heard someone keeping the password for his password safe/manager on Dropbox. Putting something so valuable onto a cloud seems foolhardy to me.

:(You're mileage may vary.

***Pin Numbers** - When you're out shopping and you swipe your CC/Debit Card - and you are presented with the option of debit or credit - ALWAYS, always use credit. NEVER, type in your pin number, if you don't have to. After the hack attack at Target, then Staples and most recently Home Depot, obviously our debt/CC systems are not a safe as we were lead to believe.

***Online purchases** - I highly recommend that you have one debit/CC that you use. Something not traceable to your checking or savings account(s). I suggest you go to your bank open an account with fifty dollars in it. Have a debit/CC issued. Make sure that there is no way that card/act. can be associated to any of your other accounts. Use this account without fear to shop online. Yeah it can kind of be a pain in the bottom, but if you've suffered through Identity Theft - this is a better way of spending your time and resources.

***Paypal -** is really the only "secure" way to purchase online. (PayPal is committed to protecting the privacy of our users. When you send or request money using PayPal, recipients never see your bank account numbers or credit card numbers. They only see your email address, date of sign-up, and whether or not you have completed PayPal's Verification process.) Of course there is no such thing as 100% secure, anymore.

***Email** - Phishing - "attempted by attackers to steal valuable info by pretending to be trustworthy party." The Bad Guys are betting that you will click on the link in the email they sent so they can do bad things. NEVER, EVER, click on any links in emails that come from 'trustworthy parties' like banks, PayPal, Ebay, iTunes, etc.. If you are being told something is wrong with your account, get out of email and go to the website of the entity/company that sent the email. From there check your account. These types of emails have spelling errors and often address you as dear sir or madame for a personal email.

If you do receive one of these emails, contacting the fraud department of said company to report the incident is helpful in tracking down the Bad Guys.

If it is a true email from a legitimate company it won't have any private or personal info in, nor will it have any links, and it will in general terms tell you why you are being contacted.

Spearphishing - "Spear phishing is an email that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your computer." Recently it was revealed that more than 100 Wall Street companies fell for this type of attack. (http://arstechnica.com/security/2014/12/phishing-scam-that-penetrated-wall-street-just-might-work-against-you-too/)

***Microsoft Technical/Support Calls** - I just heard from someone on one of my mailing lists that they received one of these calls. I have been hearing that this OLD scam has been very active last year. This phone call claiming to be from Microsoft Technical or Customer Support purports they've

detected something wrong with your computer and would you like them to fix it for a fee. When was the last time you heard of a company actually offering to provide customer service?

***VPN** - Virtual Personal Network, "is a great tool to protect your privacy and security while you use the internet." How this works is you have an account with a VPN company. While you are on the internet either at home or away, you engage the VPN network and use that. Think of it as a safe tunnel you crawl into while you are on the web. How many of us use wifi at home? Find out if the Bad Guys are listening: (http://www.wikihow.com/Secure-Your-Wireless-Home-Network). Many of the VPN companies don't keep logs of what you are doing, so you can surf, without fear of Big Brother watching your every move. This is a safe way for you to surf those 'free wifi' spots at the coffee shops you do your writing in.

Cyberghost and OpenVPN are a couple that are free and recommended. You can find more here:(http://lifehacker.com/5935863/five-best-vpn-service-providers).

***Virus Software** - All of you PC/Windows folks know about these and use them every day, right? As a recent Mac person, I was told that I would not need to bother with this. However, I was using a free wifi spot that left me feeling like my computer needed to shower. I installed Avast, it was free and recommended. I've already had two popups telling me that a suspicious email and a suspicious cookie were both stopped. These days it is better to be safe than sorry.

***Social Security Number** - how many of you know that your Social Security number is not to be used for identification? (http://www.ssa.gov/history/hfaq.html Q21.) **STOP USING IT!!!** If someone/company asks for it refuse to use it, and site the provided link. Trust me, I've done it. It usually sends them for a loop for a second and then they will start asking you those personal security questions.

I did not intend to scare the pants off of you. What I did want was to open your eyes to the threats that are lurking out there in our digital, ever more connected world. The hackers are getting smarter and better organized which means we have to be ever vigilant. Complacency with your security with the web is the quickest way to end up the victim of Identity Theft. 2014 was filled with lots of stories of hack attacks, I'm sure 2015 will be no different, but hopefully all of you won't be caught unawares.