Cyber Security

Cyber Security is your responsibility to keep you computer/cell phone/data secure. Sadly today there is a lot of money in your information and there are smart people working everyday to steal it from you.

Here are a few things that can happen to your computer/data/identity. Install a ROOT KIT on your computer that can log every keystroke you make and send it to another computer. With it, your login passwords, email addresses, and all other info that is on your computer. Install a BOT, which are "ROBOTS" that are controlled by another computer. This will enable someone else to use your computer to send spam or viruses.

Whether you turn your computer off after use or not, you also should turn off your modem and router. There should be a button on each that will not turn it off but disconnect it from the Internet. Obviously, the modem should have a good password, this is one of the first point of entry to your computer and information. Too much trouble, well here is what happened to a person just like you that didn't password his modem. A pedophile cruised residential areas until he found an open modem, using it to downloaded kiddy porn. The homeowner gets busted and spends a lot of time and money proving that it wasn't him or his kids not to mention that he is on the front page of the paper and the 6 o'clock news for a few days.

Using CLOUD STORAGE is pretty safe if you use a name brand site. BUT your stuff can still get hacked, so don't put sensitive data on the cloud. AND make sure to have backups of all of your data off site. Keep a copy of your data off premises.

Speaking of BACKING UP, not if but when your hard drive dies, unless you want to pay some big bucks, everything on it is gone. With Windows 7 Pro and above, you can create a exact image of your hard drive. I recommend that you make this image on a portable hard drive and store it out of the house. If you have a fire or burglary and your backup is next to the computer, you lose it too.

Cell Phones/tablets, are mini computers today and if you leave them somewhere or get them stolen, your data is gone too. I suggest a virus program on them also. With some phones and tablets you can install a tracker app and a locking app, so that you can lock the data up and maybe find your item.

Software:

Understand that all FREE software comes with a virus, it might be harmless "marketing stuff" but can be worse. Go to a porn site or a site that has passwords for pirated software, will have an ugly virus most of the time. Even a new version of Firefox or Chrome, you need to make sure that you are at Mozilla or Google's site when you download them. If you are not, you will get a version that has someone else's agenda with it. Usually, you cannot get rid of these "helpers" without deleting the whole thing and download the correct version. If you get Babylon or Condor from somewhere it's a bitch to get rid of

them. They are not dangerous, but send you to web sites that are paying them not where you want to go.

From time to time Java and Adobe Flash will say that there is an update and you need it. Pay attention, there are fake "update recommendations" too. Pay attention to your computer and the notices. One note, on JAVA, Adobe and others they try to upload other people's software, McAfee or others as part of the update. PAY ATTENTION TO ALL CHECKED BOXES during the process. Don't screw up or you have to uninstall the crap you don't want/need.

ATTENTION: From time to time you will get a pop up, telling you that you have a virus and need to upload the fix. THIS IS A VIRUS!!! AND THE WHOLE THING IS A LINK. IF you click on the RED X to close it, you still have clicked on the link and will be given the virus. Instead of clicking on anything, use the power button to shut off your computer to be safe. You might try to save anything that you are working on, but other than that shut off the computer. Make yourself a note which web site you were on, when it popped up.

Software to help you prevent viruses and scams are out there but you must use them. I have a number of them running all of the time and occasionally a virus still gets thru. Each program seems to have a specialty, so you run them at least once a month.

There are free versions and a PRO version.

I use Vipre for the main Anti Virus and Internet defense. It also has Vipre Rescue that you download and run if your computer is acting strange. IMO Norton is too bloated and slows down your computer. Years ago, they messed up an update, and tried to cover it up instead of admitting it immediately. So I switched from them. McAfee and others are probably as good as any. AVG has a free version and a PRO version, some people think that the free version is good enough.

Malware Bytes: https://www.malwarebytes.org/mwb-download/ I like the free version and run it once a month.

SpyBot 2.4 is free but be sure that you are on "THEIR" site. https://www.safer-networking.org/dl/

Windows Defender is by Windows and seems to work good finding Root Kids and viruses.

LastPass (free and PRO) stores all of your passwords. They have a great reputation.

Passwords:

Yes, it is stupid to use 123456. AND to have a list by the computer. Also having just a few for everything isn't a good idea either. Using a program like LastPass will help you keep them straight. Sure for sites that have none of your data on them, you can use something simple and the same. However, anything with real id info should be complex. Banks, Credit Cards etc. Speaking of banks, change your mother's maiden name with them. Your mother's maiden name is on Ancestry.com for anyone to find. You can pick anything under the sun, Peter Pan, Snow White, be creative. In the end you will need to write your

passwords down, but encrypt them when you do. Figure out some type of code so that it would take some time to put it together. Keep the real list in a safety deposit box. Don't let your browser save your passwords, not secure enough.

Free WIFI:

Accept the reality that anything that you type on your computer/laptop/phone using a free WIFI can appear on every other computer/laptop/phone within the range of that free WIFI. DO NOT DO ANY BANKING, CREDIT CARD, transactions PERIOD. Don't even type in a PASSWORD.

Phishing:

Make sure that when you are in a browser web site, and ANY of your info is there or asked for that there is HTTPS:// in the URL (address of site). Usually it will be green and a picture of a locked lock will be there.

In case you are not aware, one method to get your info is to ask you for it. I get 500+ spam emails a day. Many are from banks that I don't even have an account in. Any email that you get there are a number of hints that they are not legit.

I recommend that you set up your mail program to show you not only the FROM column but the TO column too. This way you will see if your name was the first name in the TO box. If you are getting an email from your bank sent to a dozen+ people, it's not from your bank.

Banks, Credit Card and PayPal companies which involve money use your name in the salutation. My first recommendation on any email that wants you to login to their site and you do business with them. Go to the browser and log in the normal way.

What to look for in ALL emails: EVEN THE ONES FROM YOUR FRIENDS: Take a good look at the return address. Here is why I recommend that you and your friends create a signature for your emails. All too often your email address is out there and linked to your friends. This happens more easily when emails are forwarded without removing all the trailing email addresses!!! If you and your friends have a signature, and you get an email from a friend but no signature a BIG warning.

The next thing to look at is any link that they want you to click on. Put your mouse over the link and you will see the actual link address. What you will usually see is Wells Fargo.com, but when you put your mouse over the link, you will see something like this: http://i.am.going.to.infect.you.co.ru.

NO ONE legit ask you in an email for any personal info, nor do they on a phone call. Also don't rely on the 800# being your bank's number. Yes, they duplicate your bank's email/stationary and most of the time they only change what they need to. They also duplicate the bank's web site, but if you really look and understand URLs you will catch that it isn't your bank's URL. BUT you shouldn't be there anyway!!!

ID THIEFT: If this has happened to you, you know what a pain in the ass. I had a credit card stolen on-line but they were only able to buy one thing. One small good thing is that you can get a 7 year fraud

alert on your credit report, so no one can make any change or open anything in your name for 7 years. Otherwise, you can only put a 90 day alert on your report. I use Credit Karma to watch over my credit reports. It's free and you also get a free FICO score.

KID USING YOUR COMPUTERS or have their own: Kids are going to do whatever they want to do and trying to educate them is a real challenge. The safe thing is to NOT let them touch your computers. Set up a guest login in the router so that any virus on their computer can't infect the whole house. I had a friend that every time his grandkids left I had to disinfect his computer.