Getting the Cybersecurity, you deserve

1. Protecting your digital identity.

   As a practical matter, security in our current day and age must include securing social media accounts (Facebook, Tinder, Twitter, Snap Chat, Tik Tok, Instagram, etc...), devices (phones, computers, and tablets), and online accounts (utilities, banks and credit unions, email, shopping sites, funds transfer utility programs, etc.). These along with many other things constitute your Digital Identity. It is extremely important, and growing more so every day, to protect your digital identity.

2. Privacy

   Training I have received stresses the importance of keeping information about yourself and your personal affairs private. Remember, allowing strangers to access your posts, friend list, and photo's makes it easy to create a new "fake" account with your name, birthdate, and photo and then ask your existing friends to 'friend' them. I have received friend requests from fake accounts before. My experience is that the person behind the fake account will start up a chat with those who accept friend requests. This can set in motion requests for money, more information, etc.

   In other words, consider the following when putting your personal information online.

   a. When setting permissions in your social media accounts,
      i. Who do you allow to see your posts?
      ii. Who do you allow to see your photos?
      iii. What personal information do you allow to be viewed?
      iv. Who can see your birthdate?
      v. Who can search and find your account?
      vi. Who can see your friend list?

   b. Do you respond to posts that ask you to reveal 'innocent' information about yourself? I have a cousin who seems to spend her days finding these types of 'fun' posts to share out with family members. Many of these posts ask you to reveal things about you that you wouldn't ordinarily share.

   c. Who do you accept friend requests from? It pays to investigate the profiles of people who wish to be your friend. You could perhaps reach out to the person the friend request is from by another medium, phone or email, asking if they sent the friend request.

Cybersecurity

Cyber Security on a whole is a very broad term but is based on three fundamental concepts known as "The CIA Triad". It consists of **Confidentiality, Integrity and Availability**. Three points

emphasized during cybersecurity training. These are areas that we keep in mind when protecting data and/or systems on a day-to-day basis.

a. Availability – Availability in terms of all necessary components like hardware, software, networks, devices and security equipment should all be maintained and upgraded. This will ensure the smooth functioning and access of Data without any disruption.
b. Confidentiality – Defines the rules that limits the access of information. Confidentiality takes on the measures to restrict the sensitive information from being accessed by cyber attackers and hackers.
c. Integrity – This assures that the data is consistent, accurate and trustworthy over its time period. It means that the data within the transit should not be changed, altered, deleted or illegally being accessed

From An Introduction to Cyber Security Basics for Beginner (geekflare.com)

3. Protecting devices

    a. Rules to follow across the board with all electronic devices

        i. Keep the operating system up to date with new releases.
        This ensures that you are operating with the latest fixes to security fixes.

        ii. Deploy and use virus detection software. Make sure you also keep this software up to date with updates to virus definitions.

        Some of the best rated software packages for 2021. The Best Malware Removal and Protection Software for 2021 | PCMag

        Free Virus detection software 5 Best (REALLY FREE) Antivirus Software for Windows [2021] (safetydetectives.com)

        iii. Acquire and install password management software. In our everyday use of the internet, we have many systems that we need to access. Each of these require a logon id and a password. It is important to use a different password for each account you have. One trick of hackers is when they find your login id and a password on the dark web, they will try that same login id and password in other popular online systems. If you have used the same password all the way through, you have just opened the door to your accounts and identity.

        Compare the Best Password Management Software Solutions of 2021 (top10cybersecurity.com)

            1. Don't use passwords like "password", "00000000","12345678", "qwertyui", "asdfghjk". In other words, don't use some simple sequence of letters or numbers. Hackers often use a dictionary of most often used passwords when trying to break into your accounts or software.
            2. Using a package that manages passwords, makes it so that you only have to memorize the password that gets you into the password manager's data. The software will remember the passwords for all of your online accounts.

3. This allows you to use different passwords with your different online accounts.
4. If the password management software includes a password generator, use it to generate random passwords that are harder to break.
5. If you decide not to use a password generator, use special characters such as "!@#$%^&*()", numbers, mixed upper and lower case letters.
6. Another strategy is to think of a song title, then use the first letters of each word in the title. Remember to use mixed case in the letters and include special characters and numbers.

iv. Use a VPN service when you use WIFI away from home. VPN stands for Virtual Private Network. A VPN encrypts data that is being transmitted between your device and the receiving computer.

vpn software for windows - Google Search

This will make it so that if you are using your phone or tablet to access your bank account while at the grocery store or another public location, anyone who is trying to intercept WIFI traffic with the intent of capturing account names, logins, and passwords, won't be able to read the data. It is encrypted.

v. When you install new software, do not use the default password that the software came with. Hackers know all about default passwords.

b. Phones – People don't often think that phones also need to have virus detection software installed. This is especially important for Android and Windows based operating system phones. It is also good for Apple phones, but Apple seems to do a better job of screening software that it allows to be installed on their phones.

c. Computers
   i. Create two accounts on your computer. One will be the administrative account. This is the one that you use to install new software with. It will have all access to your machine. Then create another account that has less in the way of permissions. This way, if someone is able to hack into your machine, they will only have the access that was given to the lesser account. It will make it hard for the hacker to mess with your machine settings.
   ii. Do not create a file that contains your account names and passwords and store it on your desktop. One friend of mine, who works as a white hat hacker, told me that it was unbelievable how many machines that he had hacked had such a file like that on his desktop.

   If you must have a file like this, put it someplace several levels down in the directory. Perhaps use a name that doesn't give a clue as to what the file contains.

d. Tablets, i.e., Apple iPad, any non-phone Android operating tablet – The same suggestions as given for phones, desktop, and laptop computers apply here. Especially as many tablets are equipped with WIFI capabilities.

4. Text Messaging

   Use caution when looking at text messages. Especially when the message contains a link to a website or a video to watch. This applies to all messages you receive.

   a. Hackers love to put links to corrupted websites into text messages and email. Usually, the text that is displayed in the message is totally innocent looking, but will take you to a corrupted website.
   b. When you receive a message from someone that contains a video to play, that video can contain code that will do bad things to your device, such as create a new account that the hacker can then use to access your device. Once the hacker has access, he can do anything to your machine without your knowledge.
   c. I personally do not watch any videos that get sent to me. Even if it was sent from a friend. It is just too risky.
   d. Hackers love to spoof phone numbers in text messages. They are able to disguise the real sender that way.

5. Email messages

   Like text messaging, hackers love to try to fool you into taking an action that you wouldn't ordinarily take. For example.

   a. You could get a message from a shipping service like Fedex or UPS telling you that a shipment is due for delivery today from a well-known vendor. The message could contain a link for you to follow if you have any questions about the shipment. If you were not expecting anything, you could be tricked into clicking on the link. You would be then sent to a corrupted website. To make this better, hackers would copy everything from an authentic email from that shipper and only change the link that you would click if you normally had questions.

   b. You could get an email from a company like Apple or Amazon. Places that you already had an account with. The message in the email could tell you that your order was scheduled to ship on that day. It would look like any other normal email from that vendor. Only the link for you to click if you had questions would again take you to a corrupted website that is controlled by the hacker. They could present a sign on page that looks just like the authentic sign on for the vendor, only this time, when you filled out the sign on and clicked log in, your credentials for that vendor have just been saved in the hackers database.

   c. The message in this fake email doesn't matter. The hacker is just doing whatever he can to get you to click on the link to his webpage.

      If you have a genuine concern over what is being presented to you in the email, use a browser that you open and a URL that you know is authentic to sign on to that vendor. Then look for messages that tell you what is going on in your account. Never use the link that is provided in the email message.

6. Spotting fake URL's and email messages – Access official websites to learn how to recognize dangerous email

a. Here is a link to the Federal Trade Commission. How To Recognize and Avoid Phishing Scams | FTC Consumer Information
b. Another link that contains specifics from Executech. How to Read URLs and Prevent Phishing Scams | Executech

The bottom line for this presentation is that even though it doesn't cost much to access the internet, you have to exercise as much caution as you would in non-internet activities. Use common sense. If it doesn't sound right, it may not be. If it is too good to be true, it may be.

As with all things in life, you get the protection you deserve. In other words, just like with your home and your vehicle, you will need to make an investment in your online security.