Cyber Security – Revised 10-23-2019

We live in an increasingly electronic and connected world. Our personal, professional and financial relationships are vulnerable to attacks by bad actors at individual and international levels. We learn of data breaches affecting millions of persons. Many of us have had to get new credit/debit cards or new Social Security numbers. Personal and corporate data have been stolen for ransom payments. Entire industries have arisen to offer us monitoring and protection for our activities. We must prepare to protect ourselves.

From Wikipedia: "Cyber security is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide…Due to its complexity, both in terms of politics and technology, cyber security is also one of the major challenges in the contemporary world."

<u>Computers, laptops, tablets, phones</u>

1. Turn them off at night. This clears, resets and updates critical data while you sleep and protects from concerted hacking.
2. Turn off the computer camera. It's a two-way device and may be used to spy on you. In 2017 Facebook announced a setting to let people turn off its facial recognition feature. You should go to the top right corner of Facebook and choose **Settings>Face Recognition>Edit>No**. If you don't have that feature, then go to **Settings>Timeline and Tagging>Who sees tag suggestions…?>No one**. Do it.
3. Not paranoid about those cameras? Consider your oh-so handy digital assistant in a smart speaker such as Alexa, Amazon Echo, Google, or Siri. Isn't it nice and convenient to talk to that patient object and get a polite response? And it's always listening, unlike some spouses, children or grandchildren. Not only listening, but recording. But, you say, it only responds with the "wakeup" word. Yeah, sure. Or it may respond to a word or phrase that sounds like the wakeup word: election or I like some (Alexa); Petco or pickles (Echo); good girl or goofball (Google); seriously or hey, sir (Siri). But we are assured that the digital listener will soon stop recording when it realizes (through computer algorithms or repetitious training?) that it's been fooled into listening. Don't say you weren't alerted to in-home spying.
4. Is your phone listening? Experts studying this say there's probably no cause for such concern. Apparently the technology required to mine such data is of poor quality. Today, OK. Tomorrow, technology marches on.
5. Be sure you have strong computer firewalls activated. You know this, don't you?
6. Get backup protection. Use "the cloud," professional services, or an external drive. "Stuff happens" and you need to be able to recover your critical data. You need to do at least as much to protect your personal computer as you would for your office or business computer—which probably doesn't contain your financial information…or grandchildren photos.

7. Use secure passwords. You know this, so do it. The longer the password and greater variety of characters they contain, the more difficult it is for programs to hack your passwords. Use random strings of upper and lower case letters, numbers, and those symbols above the numbers on your keyboard. Never use the same password for any other accounts. Change the most critical passwords on a regular basis. Don't keep your passwords in a list on your computer—Hello? Consider keeping all your passwords (we currently have 58 unique passwords!) in a paper notebook, away from prying eyes, digital or otherwise. Then there are password managers, some free, some with a monthly fee. About 1/3 of us use a password manager, so you be the judge. But to repeat: It's most important to have strong, unique passwords for every account.
8. Do you think you can outwit a password thief by changing your easy password by slipping in "@" for A and "3" for E or "GR8" for Great? It works for license plates. Thieves work at this a lot harder than we do and they have software to crack these weak codes. Again: It's most important to have strong, unique passwords with long, random strings of characters for every account. How many times must you hear this before complying?
9. When you use Google or most other search engines, they save your search details in order to target you with specific ads (where did you think they came from?). A search engine that doesn't track your history and target you afterwards is DuckDuckGo. They generate their revenue by showing ads related only to your query. Limited to that instance and not forever after. Pretty neat, I'd say.
10. From Wikipedia: "Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details directly from users. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. The fake website often asks for personal information, such as log-in and passwords. " Your bank, business and government agencies will not request such information via Internet or telephone. You'll get a mailed request.
11. From Wikipedia: "Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer…In early 2016, the FBI reported that the scam has cost US businesses more than $2bn in about two years." Contact the company or agency before responding, if you doubt the legitimacy of the request. Don't be bullied into creating a problem.

Vulnerabilities

Lest you think that life can go on more or less normally under a concerted cyber attack, here are some of the vulnerable systems we all use (ignore at your peril):

1. Automobiles. The newer the car, the more computers available to hack; autonomous vehicles (currently and incorrectly called self-driving) will be particularly attractive to interfere with.
2. Medical. Diagnostic equipment and devices (pacemakers, pumps, etc.) have been attacked and vulnerabilities exploited. "Be still my heart" takes on new meaning.
3. Energy production and distribution. Our electricity is "wheeled" far and near on the grid; a cyber attack could disable all or portions of the grid for weeks at a time.
4. Banking. Financial institutions (government) and banks are ripe targets that have been repeatedly compromised. Credit cards and bank accounts are bought and sold on the black market and produce immediate financial gain…for the black market operators. Credit cards with a high limit can have their information sold for hundreds of dollars a card, but most seem to go for under a dollar, due to old data breaches that invalidated many cards.
5. Identity theft is a growth industry, with the capability of ruining your credit and causing you aggravation, inconvenience and money over many months while you scrub all your accounts and plead your case. Your digital profile consists of name, Social Security number, date of birth, and current billing address and may sell for $50 to $300. Infants' information is particularly valuable, as its fraudulent use may be undetected for many years. Aren't we glad that children now (seem to) need an SSN?
6. Aviation. We've seen problems with ticketing and security processing with innocent software problems that cause delays lasting hours. Imagine a concerted attack on those systems and/or control of airborne aircraft and radar.
7. Government. If you despair of an inefficient government now, imagine a government without its memory or operating systems or communications when computers are down and the GSA has stopped printing notepads and regulations. Good luck to the Department of Homeland Security, where they'll light their notepads with flashlights.
8. Consumer devices. We could stop using (or trusting) our computers, tablets, smart phones, smart watches, FitBits, and other devices tracking our communications and movements. WiFi, Bluetooth and cell phone networks could be turned against us. Not to be paranoid, but who is watching (and listening) to us, to you, now?

National cyber attack, satellite outages, Electromagnetic Pulse (EMP)

We're all in trouble in this scenario. ATMs won't work, gas pumps won't take your card, cell phones may be useless, and Google won't answer your questions. We're back to pencil and paper…if you have any. So:

1. Have cash ready in small bills for small purchases. Coins will be useful.
2. Landline phones may work, so keep yours.
3. Radios and television may still operate, at least on a local basis.
4. This is when an extended food supply (one or two weeks) is necessary.

If there is a nuclear air burst (EMP), we've been attacked by a hostile power and most everything we use to communicate or to drive will be useless. Every device with solid state electronics will be fried. Your ancient tube radio may work, if anyone is transmitting and the power grid hasn't gone down. We will be at war.

At this point, knowing and trusting your neighbors may be the life-saver. For you and them.