A Layman's Guide to Cyber Security

Actually, I do not think there is such a thing.

No matter what steps we take to protect ourselves, the bad guys always seem to be one step behind and sometimes two steps ahead. I think the term "Cyber Security" is an oxymoron, at best a false hope.

With all the data breaches (worldwide) from Equifax to Sonic Drive Ins, it is even more apparent that each one of us must take responsibility for our own personal data. From health care to personal shopping habits, all our data is (potentially) exposed to the world. **Having good Internet hygiene habits and strong passwords are no longer enough.**

It doesn't matter if you never use the Internet or live on it. Your data is out there. Recently, my health care data was breached by a company I had never heard of. It seems Group Health used a 3rd party company to process medical claims and **that** company was breached. I received notice that my data ***might*** have been exposed, but they would not tell me what data was at risk. Two years later, I still don't know what personal (private) information about me was released.

Someone recently said, ***"There are two types of companies: those who have been hacked and those that do not know they have been hacked".*** **I believe the same is true on a personal level.**

We hear a lot of cyber security horror stories: Health Care, Financial Institutions, Department Stores, Adult Sites, News Outlets, Government Agencies, and on and on and on. There are two things for sure:

1. No matter what you hear about a breach, it is usually at least twice as bad as originally reported.
2. You only hear about a fraction of the actual breaches.

Unfortunately, data breaches are as much a way of life today as eating and breathing.
Take control of your future financial wellbeing and personal reputation. When (not if) your information has been exposed, what are you going to do about it?

1. Try to find out exactly what data was exposed
2. Contact responsible party and demand mitigation solutions (utilize government agencies to help; Secretary of State for your state, etc.)
3. Determine what you need to do to limit the damage of the exposure
4. Change access methods of data
    a. Have credit cards re-issued
    b. Change PIN numbers
    c. Change passwords (never use same password on other sites)
    d. Alert family and friends (see something, say something)

Take preventative measures to deter exposure:

1. Change your passwords every time you use them. Do not worry about remembering passwords. When you are asked to enter your password, take the ***"forgot password"*** option. This should send a message to your device of choice, asking you to reset your password. This essentially makes each password a onetime use security feature.
2. Do not share your password with anyone for any reason. If you can't remember your password, you can't share it.

3. Always use two factor authentication. This means the site you are requesting access to must send **you** an "invite" with a special code to access your data.
4. Use current virus protection on all your devices.
5. Freeze your credit access with all credit monitoring companies (there is a charge for this).
6. Be aware of the information you share about yourself (and others) on social networking sites. This information can be scrubbed to expose significant information about you. Also, be alert to what others are sharing about you.
7. Keep good backups of the things that are important to you on your personal devices (PCs, laptops, tablets, smartphones, etc.)

I am a Certified Business Continuity Professional (DRII). I have always focused on how to plan for and recover from disasters (usually the catastrophic "acts of god" type). However, it is becoming more and more apparent that personal data breaches may be the most significant personal catastrophe most of us experience. I have always preached "preparedness". We must plan for the worst scenario and pray it doesn't happen. If it does, we must take personal responsibility for our survival.

"Plan well and survive"

Eddy Sherman, PMP, CBCP