

An Ounce of Prevention Will Get You a Pound of Heartache

Eddy Sherman, PMP, CBCP

Living the “simple” life gets harder and harder every day. Living a “connected” life gets more and more complicated every day. What is the simple life, but a memory? Perhaps, for a few of us, it was life without modern conveniences or electricity. For my grandparents, it was candles and outhouses. For my parents it was life without a car or television, or at least color television!

I remember a time without personal computers. Although it might have been simpler, I can't say it was better. When I was 13 years old, man landed on the moon. I'm told it took a large room full of super computers to engineer the safe landing on the moon and return to earth. Now we hold more computing power than that in our hands.

My children might say the simple life was low graphics computerized games or only having a few hundred channels of TV available. My grandchildren will probably be living in the flying car era, and busy colonizing outer space!

Being “connected” comes in many flavors, from not thinking you are connected at all, to being ultra-connected. It could be that you don't know your electric meter is transmitting your power consumption/analytics to your utility company. Or it could mean that your refrigerator is placing replenishment orders with your online grocery store and scheduling deliveries based on your personal electronic calendar. This is part of the Internet of Things (IOT) and usually consists of personal electronic intrusion nobody thinks about (until it goes terrible wrong). The Internet of things is the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to connect and exchange data. *Remember, you can't spell idiot without IOT!* It really can impact our life without our direct knowledge.

And don't even get me started with social media! Well, since you brought it up...

Social media is the source of most social engineering, from targeted advertising to tracking your whereabouts at any time. That said, it's probably our own fault. When

was the last time, if ever, you read and understood the terms and conditions before you clicked “Yes, I agree”? We assume no one wants to harm us, right? And I know that is not the intent of most programs, apps, web sites, etc. we use. But even when that is not the intent of the developer, there are others trolling the Internet that want to do you harm. Hence, the title: An Ounce of Prevention...

The first thing most people think when you discuss electronic security, is passwords. While passwords are the first step to cybersecurity, password cracking has become a competitive art. Always assume that there is NO security in anything electronic: PCs, Tablets, fitness trackers, private or corporate data bases or the Internet. Always assume if it's electronic, the entire world can know about it. Never text, email, chat or otherwise transmit anything that you don't mind being on the front page of your local newspaper. *(Editor's note – A newspaper is the printed media delivered to some homes in the US and posted on the newspaper's web site).*

Just when you think you live the simple life, and things like this are of no concern to me, consider this: Some breaches expose data about us that we didn't even know existed! Recently my medical records were hacked. A company I never heard of was hacked by someone trying to make a buck. This company was a sub-contractor of my HMO. I think they handled the medical billing for my HMO. I was notified by this unknown company that my medical records might have been exposed. They wouldn't tell me what was exposed, and three years later I still have no idea.



This type of data exposure will not stop until those affected, all of us, band together and demand better security from companies that use our data. Many of these companies are, or believe they are, untouchable. We trust these companies with our most valuable assets, our financial, legal, medical, and personal secrets. Until companies handle this sensitive data as if it was their own, we are vulnerable to the worst kind of assault.

I have been describing the potential heartache that could happen in spite of applying an ounce of prevention (passwords). We believe we are protected because we use passwords, even stronger passwords than we've used in the past. However, those who wish us harm scoff at passwords because there are many other ways to get at your confidential information.

There is no single solution to protect all your sensitive information that is stored across creation. Most of us don't know what is stored, or where it is being stored. So, how do we safely live a connected life?

Here's how. Be as vigilant in tracking our data across the world as you are at protecting the data you store on your personal devices. Learn how to monitor your credit, and do it regularly. Think about what you share on social media. Watch for what others share about you on social media.



If you are notified about a potential breach of your personal information, demand to know what was breached, and by whom. This can be hard to do. Engage local and federal agencies to get your answers if the breached company will not cooperate (FBI, FTC, State Attorney General, etc.). Look into what laws might have been broken, either by the hacker or the target company.

This could include privacy/security, trade secrets, Sarbanes/Oxley, HIPAA, Privacy Act of 1974, etc. Use anything you can to find out what was hacked. Then, make a recovery plan to mitigate potential damage. Determine the impact of the breach to you personally. Implement a recovery plan that aggressively addresses your exposure.

You probably will not be able to resolve all the potential land mines waiting for you because of this event. However, with some arduous work you should be able to recover from whatever evil befalls you.

So, whether you're a super-connected commander of the online world, or you just check your email on Fridays, the simple life is no longer possible. Bad guys are attacking our personal information, and most of the time we don't even know it! It is hard to battle an enemy you can't see. When you can't see your enemy, extreme vigilance is our only option. Do your part to protect your online castle, and the data that defines your identity.

Enjoy life—but wear armor!

Eddy Sherman

© 2017 Eddy Sherman