**I’ve Been Hacked!**

I don’t need a crystal ball to determine if a particular stock will plummet. All I have to do is buy some shares and down it goes. I don’t need to see an advance copy of tomorrow’s newspaper to see which retailer will be hacked. All I need to do is check my credit card statement. If I shop there they have been hacked or probably will be. Target, Home Depot, Marshalls, CVS and more. The bad guys have hacked my health insurer, Anthem Blue Cross. They hacked American Express in April 2015 (my go to card). They even hacked the IRS. My personally identifiable information has been stolen so many times I can’t even count anymore. I do what I can to protect myself; I check all of my bank accounts and credit cards daily, I subscribe to Lifelock but I have no confidence they can do much to help me. Experian, one of the largest credit reporting agencies who have a tremendous amount of personally identifiable information on all of us, was hacked in 2014. Two hundred million Americans’ had this data stolen (that’s two out of three Americans!). Oops. I’m not a T-Mobile subscriber and that’s a good thing as they were hacked in October 2015 handing over the personally identifiable information of 15 million of their customers. Probably not a big problem since the bad guys already had all of their data from the Experian breach.

I'm not on Ashley Madison, the spouse cheating website, I don’t post nude photos of myself (nobody wants to see that!), I’m not a famous movie star and I’m not a government official. Still, I’ve been hacked multiple times.

The fact that I’ve been hacked puts me in some pretty good company. Last year iCloud was hacked and Jennifer Lawrence, Kate Upton, Kirsten Dunst, Kaley Cuoco and many other had nude photos, many of them selfies, let loose on the Internet for all to see. CIA Director John Brennan had his office email hacked a couple of months ago. Defense Secretary Ashton Carter admitted that the Russians hacked the Pentagon earlier this year.

So what is the average computer person to do to protect themselves? Actually, there’s quite a bit you can do. Of course, you can’t prevent your health insurer or cell phone company from being hacked and sweeping you up along with millions of others. But here’s a few practical suggestions:

1. Remember that everything you do on the Internet is forever. Never mind that some sites claim to dispose of your information at some point. They don’t. Say it and forget it… write it and regret it.
2. Check your bank accounts and credit card accounts frequently. It is common practice for identity thieves to charge a small amount to your credit card, sometimes less than a dollar, just to see if anyone will notice. If the charge isn’t caught and reversed, you’re fair game for much bigger hit.
3. Be careful with emails – your bank or credit card issuer will never ask for your username or password in an email. If there is a link in the email directing you to the “company website” to reset your password, be certain that the link is legitimate. Do this by “hovering” your mouse over the link which will reveal the actual link address. Read the link that pops up carefully as the bad guys need only change a single letter from the actual website address to direct you to website that will look exactly lack the real one (capitalone.com may show as capitolone.com, for example). Once you land on the fake website and are directed to enter your current password and the new password you are toast.
4. Use spatial awareness – know who and what is around you. The guy behind you in line at the ATM may look like he’s chatting on his smartphone. Or maybe he’s taking a video of your finger typing your access code into the ATM. Be sure no one knows your home of office computer password – and be sure someone isn’t standing behind you as you type it in.
5. Purchase a cross-cut paper shredder and use it. In China, there are “teams”, usually young children, picking through the “strips” of paper from cheaper shredders, puzzling them together to find personally identifiable information from credit card and bank statements.
6. Hire the right IT team to help you navigate the dangerous waters of this connected world.

For more information on how to protect your identity on your business’s computer network, visit <www.AnswersNow.com>.