September 28, 2015

Because of the Russian gang data breach in 2014, the recent U.S. Government's OPM (Office of Personnel Management) breach resulting in the loss of well over 1 billion, yes, 1 billion people's records, and the smaller security breaches we hear about in the news almost daily, we must all remain vigilant with our online and other financial accounts and activities. Here is a very short list of easy steps you can take now to help thwart cyber threats:

1. Change passwords on critical accounts, use strong passwords, and don't use the same password for multiple accounts.
2. Enable a 2-step login process (aka 2-factor authentication) where after you have entered your userid and password, you receive a text message on your cell phone (or an automated voice call to a landline) with a random 6-digit number that you also have to enter before accessing their accounts.
3. Enable any other type of 2-step (or greater) login authentication measures provided by the website.
4. Be sure to log out of your account when you are finished!!!!! This is critical!!!
5. Call your banks and credit card issuers and place passwords on your accounts.
6. Ensure you have installed the latest security patches and updates to your computers' operating systems (Windows or Apple iOS), Java and Adobe Flash. The latter two can be disabled, if you don't use them.
7. Ensure you are running the latest **PAID** version (buy the new, full version every year) of a software security suite (anti-virus, anti-malware, anti-spyware, firewall) from dependable outfits such as Kaspersky, Bitdefender or Webroot.
8. In certain cases, place fraud alerts or freeze your credit files with the big 3 credit reporting agencies. Clark Howard, noted consumer advocate, has a great page on his website with easy instructions on how to do this. Clark Howard's Guide to Freezing Your Credit.[1]

[1] http://www.clarkhoward.com/news/clark-howard/personal-finance-credit/credit-freeze-and-thaw-guide/nFbL/

9. Monitor your bank accounts and credit card accounts very closely. Get and save ALL receipts and reconcile your credit card statements at the end of every month just like you do your bank checking accounts. If you use a debit card, think again - read these articles: Kim Komando's articles, "5 Risky Places to Swipe Your Debit Card"[2] and "The 1 Essential Thing You Need to Do Now to Protect Your Debit Card"[3] and Clark Howard's 9 Places You Should Never Use A Debit Card.[4]
10. Password protect any devices (tablets, cell phones, etc.) you have that may contain critical personal or financial information. If you are concerned about first responders being able to access your ICE (In Case of Emergency) contact numbers, Kim Komando has a solution for iPhone users: One Thing Every iPhone User Must Do In Case of An Emergency.[5]
11. Do NOT save passwords in your computer's browser. Use a password manager – here are a couple of good articles about them: Lifehacker – Faceoff: The Best Password Managers Compared[6] and Lifehacker – The Five Best Password Managers.[7]
12. Contact your cell phone provider and enable parental controls - set up a requirement for a password anytime you want to send money via text message.
13. Physically secure your computer with a product such as a Kensington Lock or similar type device.[8]
14. If you have been a victim of identity theft, go to the Federal Trade Commission's Identity Theft Resource Center website[9] for a step-by-step guide to help you recover.
15. Don't forget to take steps to protect your children's identities – they are over 50 times more likely to be stolen than adults' identities. Go to the Federal Trade Commission's Child Identity Theft Resource Center website[10] for more information.

---

[2] http://www.komando.com/tips/245380/5-risky-places-to-swipe-your-debit-card/all

[3] http://www.komando.com/tips/247376/the-one-essential-thing-you-need-to-do-now-to-protect-your-debit-card/all

[4] http://www.clarkhoward.com/5-more-places-you-should-never-use-debit-card

[5] http://www.komando.com/tips/312844/one-thing-every-iphone-user-must-do-in-case-of-emergency/all

[6] http://lifehacker.com/lifehacker-faceoff-the-best-password-managers-compare-1682443320

[7] http://lifehacker.com/5529133/five-best-password-managers

[8] http://www.kensington.com/us/us/4480/security#.VfcHA5egyf8

[9] https://www.identitytheft.gov/

[10] http://www.consumer.ftc.gov/articles/0040-child-identity-theft

Want to know more detailed statistics about identity theft? The U.S. Department of Justice's Bureau of Justice Statistics just released (Sept. 2015) its most recent and very comprehensive report on this subject. Here is the link to the summary[11] and the full report.[12]

[11] http://www.bjs.gov/content/pub/pdf/vit14_sum.pdf
[12] http://www.bjs.gov/content/pub/pdf/vit14.pdf