EMORY ALLIANCE CREDIT UNION

12 Smart Habits to Protect Your Identity

It's high time we (as in all of us – business, government and consumers) stop making it so easy for scammers, phishers and identity thieves. The best intentions can't really stop these guys, but adopting a best-practices approach to data security can make your online world more secure. Here are some of the things you can do to help avoid the living hell of identity theft and other identity-related crimes.

1. Change Is Healthy, Especially When We Are Talking Passwords.

A growing consensus in the data security community believes that passwords will be a thing of the past in the next decade or so, with new forms of authentication being developed and becoming main stream. But until that joyous day when you can throw your increasingly complex password recall system out the virtual window, please change your passwords regularly: Once a month at the minimum. Make them long and strong, develop your own system (perhaps using a favorite phrase at the core) or use a password manager!

2. Change Your User Names

Too many sites still allow (or require) you to use your email address as your user name. The problem with this is that the (arguably) most public piece of your personally identifiable information is, by very definition, not the most secure way to confirm to a site that you are the right person to gain access to your sensitive information. By using your email address (or name) as your user ID, you're giving the bad guys one half of the front door key. Consider using a complex user name as part of your security protocol.

3. Tighten Your Privacy Settings

If you haven't revisited your social media privacy settings in a while, you may be surprised how much has changed. Did you realize you were sharing your love of Michael Buble, profile pictures and birth date with anyone and everyone? You can change that, and you definitely should.

Check (and tighten at every opportunity) your privacy settings on every site you use! Make sure only trusted contacts can see your posts.

4. Purge Your 'Friends'

Having a ton of friends is one indication that you might be an awesome individual, but for those who believe more is better consider the possibility that someone you don't know might be looking at you as their day job. Since most of us don't (or at least shouldn't) invite strangers to stay in our homes, why would we friend them online?

5. Tell a Few Lies

One way to throw a would-be scammer off the trail of your personally identifiable information is to be less than truthful. Here's where you can truly benefit by making yourself seem younger or using any of the many things people lie about: Change your birthday, your hometown, schools attended, etc. (You get the picture—and by fibbing "they" won't.)

6. Check Your Bank & Credit Accounts Daily

One way to stop (or at least to contain) fraud is to stay on top of things, and there is nothing easier these days than this so-called chore of monitoring your financial accounts. Set up daily reports and transaction alerts with your bank and credit card accounts. This makes checking your accounts part of the morning grind—or whenever you choose to have reports sent. You can also set up alerts that let you know about every transaction, big or small, or only monitor transactions above a certain threshold—all of it sent to a smart device or your email, thus making it easy to know what's what at a glance.

7. Check Your Credit Report

These days there is nothing difficult about checking your credit—many credit card companies now provide free access to your FICO score—and doing so will let you know in short order if anyone has tried to tap into your available credit. You can get a free credit report summary every month on Credit.com, and you can get your free annual credit reports at AnnualCreditReport.com.

8. Consider a Credit Freeze

Another option to help strengthen your identity defenses is the credit freeze. You can actually lock your credit, but don't forget that you will need to unlock it every time you want to open a new line of credit or (for example) allow a current creditor to review your account for a limit increase. There can be a charge for freezing and unfreezing your credit, depending on your state's laws.

9. Stop Using Public WiFi

Sure it's convenient, but do you really need to pay your bills when using public WiFi? You truly never know who might be looking over your shoulder and is able to see the traffic on those accounts. The solution here is simple: Conduct sensitive business on a secure network because, unfortunately, "free access" could end up becoming very expensive.

10. Stop Clicking the 'Remember Me' Box

Let's say your computer is lost or stolen. Do you have a security code protecting the device? Is it a long and strong password? Can you erase or disable the device using a user name and password entered from another device? Even so, there's a chance that whoever finds (or takes) your computer can gain access to what it contains—including the various ways into your financial affairs. So, always type in all user names and passwords for financial accounts. Don't let your computer auto-fill unless you're absolutely certain it's secure, and you use a good password manager.

11. Turn Off Geotagging

Several of us in the security community have been warning about this for years. Unfortunately, lots of people still leave location services enabled when using cameras, and it's still a good way to provide a North Star for those who are looking to figure out how to better identify you, or where they can find you, your family or your valuables. Thieves spend hours every day on social media looking for things to steal, and if you post pictures of your prized possessions online, without disabling geotagging, you are handing a would-be thief all the information they need to show up at your door when you're not at home and rob you blind.

12. Sharing Is Not Necessarily Caring — Share Less

No one really needs to see pictures from your vacation in real time, except of course the burglar looking to empty your home of its most valuable contents.

But that is not the only reason to avoid over-sharing. A study in Science Magazine found that anonymized metadata sets used for research were re-identifiable with specific people using just a few data points provided by the people being re-identified. If you guessed that those data points came from social media, you're right. Every meal you post from a favorite restaurant, or article of clothing from a must-have designer, is potentially correlated with a credit card transaction—from there it's just a matter of the amount of time it takes a computer to find a transaction on a metadata set of purchases that matches your Instagram post.

Identity theft and other identity-related crimes are no longer something you need to think about from time to time. There is no avoiding every scam and fraudster out there, but you can make yourself a harder target. Only through a paradigm shift in the way we view data security will things change. Please consider and put into practice some of these suggestions and maybe in 2016 you can better avoid becoming a fraud statistic.

Article Author: Adam Levin is chairman and founder of IDT911 and co-founder of Credit.com.