8/9/16

Reprinted from July 28, 2016 post on Credit.com by Adam Levin, Co-Founder of Credit.com and IDT911

Most of us in our “instant gratification isn’t enough” society assume that the potential fallout from transmitting sensitive information via text, fax or email is outweighed by the convenience of getting something where it needs to be fast. After all, becoming the victim of an identity-related crime isn’t the end of the world, right?

Define “End of the World”

While it’s not technically the end of the world, you may find yourself wishing for it. There is nothing quite like that maddening feeling you get while reading a notice from a collection agency informing you that you owe money for goods or services that you never purchased.

The next order of business is where people tend to really lose it: Getting a credit report riddled with identity theft-related errors. If you are lucky, whoever used your information to make the purchases that eventually hit your mailbox in the form of a collection notice only perpetrated that one incursion on your financial reality. That said, look closely at your credit report(s) because indices of identity-related fraud can be similar to spotting a cockroach — for every one you see, there may be more you don’t.

Whether your identity has been ransacked or cherry-picked, that collection notice is often the starting gun for a marathon of annoyance and emotional turmoil that can take months or even years to finish. The mess left behind by an identity thief is like a home burglary, minus the physical clutter. Someone has invaded your private space, in this case the parts associated with finance, and committed crimes using what they found. And, while identity theft is a third certainty in life, you can make it harder for fraudsters to get ahold of your personal information.

Don’t Make It Easy

So, you are about to send some sensitive piece of information — something that can be used to steal your identity — by way of email, text, voicemail or fax. It needs to get there, and your only other option is to go in person, or try to get someone on the phone.

Can you send it? Of course you can, but understand the risk: You don’t know what’s happening on the other end with your information. Who has access to the mail that comes in, the voicemail, the fax machine, the email (include in here hackers who have successfully phished malware onto the computer on the receiving end)?

Let’s make it more nerve-wracking: When you call to provide that information, who are you talking to?

Always ask yourself these questions.

While it may sound simplistic, when you’re on the phone with a representative of a large organization and you know the number that you called is correct, you’ve done pretty much everything you can to be careful. Increasingly, large organizations are practicing safer information storage and have a number of procedures in place to protect you from fraud. These practices are not fail-safe, but they are as much as you can expect.

But let’s say you’re sending that information to your general practitioner, an M.D. who works solo or in a small group. And let’s not pick on your doctor. There are countless professionals, organizations and small businesses out there who have enough of our personally identifiable information to open us up to the risk of identity theft.

A short list would include: your doctor, your dentist, your lawyer, your accountant, your children’s school, your church, your favorite charities, your gym, your alma mater, and many of the services and people you hire to make life easier.

How do you know that they are practicing good information security? The answer: You don't. That's why it's a good idea to be stingy with your sensitive personal information.

Things You Should Not Send

1. Social Security number. This is the skeleton key to your financial life. It can be used to open accounts, steal tax refunds and commit many other kinds of fraud.

2. Your credit card information. There is too much malware out there for this to be a safe practice. Don't send this information via email or any other electronic means that is not secure (look for https:// and the Padlock on websites before hitting submit).

3. A copy of your driver's license. Remember, fraudsters are not big on in-person transactions, but they are very good at talking their way around security protocols. If they have your Social Security number already (this can often be found online through shady websites), and they have enough other pieces of your personal information to convince you they are an official organization, they can dupe you into sending your photo ID — or steal it from someplace you do business — they can do a lot of damage.

4. Your PIN codes or passwords. These should never be shared, period, but if you are sharing that information in a pinch to someone close to you, do it on the phone. Malware is too prevalent to risk communicating that information electronically.

While all of this may sound like common sense, the myriad mistakes people make on a daily basis is beyond the ken of understanding. The key to staying safe is staying vigilant. Always practice the Three Ms: Minimize your exposure, monitor your accounts and manage the damage the minute you discover a problem.

While there is no preventing identity-related crime , you can avoid becoming an unwitting volunteer.