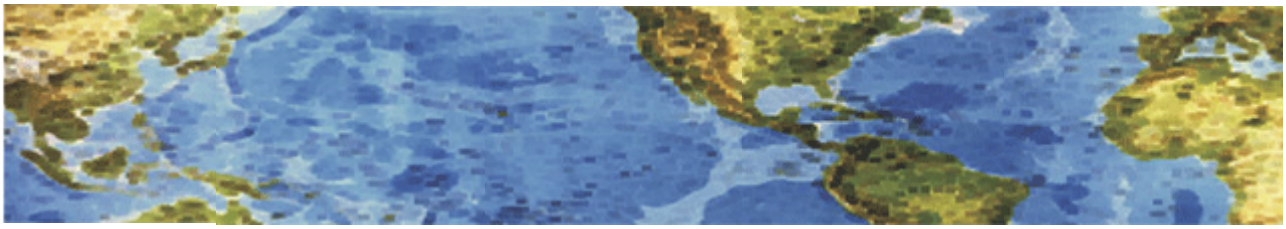
HALL ASSOCIATES



Risk-Based Decision Making Commentary
11 June 2014 Newsletter

8 Numbers Identity Thieves Want to Steal From You

The Star Wars Cantina of cybercriminals targeting your identity, health care, finances and privacy today might seem like a movie you've seen so many times you could lip sync the entire thing. **Nevertheless, cybercrime and identity-related scams change faster than trending hashtags on Twitter, and the fact is nobody knows what's going to happen next.** Who would have thought Apple's iCloud was vulnerable (much less to ransomware)? Or eBay**? Data breaches are now the third certainty in life and sooner or later, you will become a victim.** According to the Privacy Rights Clearinghouse Chronology of Data Breaches tracking tool, at least 867,254,692 records were exposed through data breaches between 2005 and May 28, 2014. The Milken Institute says the number of compromised records was more than 1.1 billion between 2004-2012. The Identity Theft Resource Center reported 91,982,172 exposed records in 2013 alone.

The amount of information out there is simply staggering. You probably realize that identity thieves are after your email addresses and passwords, but that's not all they want. In particular, each of us is attached to various sets of numbers that, when cobbled together, enable sophisticated identity thieves to get their claws into you. The fraudster doesn't need all your information to complete the problem set. They just need enough to convince others that they are you.

Here are eight numbers that they are gunning for:

1. Phone Numbers: You want people to be able to call you; you may even list your phone number on a public-facing site. If you do, bear in mind some companies use your phone number to identify you, at least in part. With caller ID spoofing, it's not hard for a fraudster to make your number appear when they call one of those companies.

2. Dates and ZIPs: Birth, college attendance, employment, when you resided at a particular address, ZIP codes associated with open accounts—these are all numbers that can help a scam artist open the door to your identity by cracks and creaks. Many people put this information on public websites, like personal blogs and social media sites. In the post-privacy era, **it is imperative you (and your kids) grasp the concept that less is more.** Another tactic worth trying is populating public-facing social media sites with inaccurate information—though you might want to check each site's rules since some sites frown upon the practice.

3. PIN Codes: Card-skimming operations use a device to capture your debit card information while a camera records you as you type in your PIN code, making it very easy for a thief to replicate. Cover your hands and be paranoid, because it's possible someone actually is watching you.

4. Social Security Numbers: Your Social Security number is the skeleton key to your personal finances. There are many places that ask for it but don't actually need it. Be very careful about who gets it and find out how they collect it, store it and protect it. Whenever you're asked for your SSN, always consider whether the request is logical based upon the context of your relationship with them.
5. Bank Account Numbers: Your bank account number is on your checks, which makes a personal check one of the least secure ways to pay for something. Consider using a credit card. You get rewards, buyer protection and less of your information will be out there.
6. IP Addresses: Scammers can use malware and a remote access tool to lock files on your computer and then demand a ransom in exchange for access. A message informing a user that his or her IP address is associated with online criminal activity is a common scare tactic used in ransomware scams. Don't fall for it. While it's not difficult to track an IP address, there are a number of browsers that hide your IP address and associated searches from the bad guys, and there are fixes for ransomware.
7. Driver's License and Passport Numbers: These are critical elements of your personally identifiable information that represent major pieces of your identity puzzle and, once you have the number, these documents can be counterfeited. Countless times each day, millions of personal documents undergo major makeovers and suddenly feature new names, addresses and photographs of fraudsters.
8. Health Insurance Account Numbers: Health insurance fraud is on the rise, and one of the biggest growth areas is identity-related health care crimes. This can jeopardize your life -- not just your credit or finances, as the fraudster's medical information can be commingled with yours, precipitating blood type changes, and eliminating certain allergies to meds or presenting new ones. The results can be catastrophic when a course of treatment is prescribed based upon incorrect information in the file**.**

It's time to become a data security realist. Data breach fatigue is the enemy. Every new compromise and scam is potentially crucial news for you, since it may point to weak spots in your own behaviors and ways that your data hygiene might be putting you at risk. So keep reading articles about new threats to your personal data security, and read every single email alert that you receive—though be careful of the obviously fake emails and always verify directly with the institution. **The smartest thing you can do is to assume the worst.** Your personally-identifying information is out there, and, in the wrong hands, you're toast—even if you are really on top of things. That said, by monitoring your bank and credit card accounts and the Explanation of Benefits Statements you receive from your health insurers, you'll be in a better position to minimize the damage.

Most importantly, read your credit reports. You can do that for free once a year, and use free online credit tools, like those on Credit.com, which updates your information monthly, explains why your credit scores are what they are, and give tips for what you can do to improve your credit standing. But then what? It is also vital for you to have a damage control program in place once you suspect that you have an identity theft issue. Contact your insurance agent, bank and credit union account rep, or the HR Department where you work to learn if there is a program to help you recover from an identity theft. You may be surprised that there is and you are already enrolled for free as a perk of your relationship. **While there is no way to avoid cybercrime and identity theft, there is plenty you can do to make sure the damage is minimized and contained, and that no matter what happens, your daily life can go on without too much disruption.**

http://www.foxbusiness.com/personal-finance/2014/06/10/8-numbers-identity-thieves-want-to-steal-from/?intcmp=obnetwork