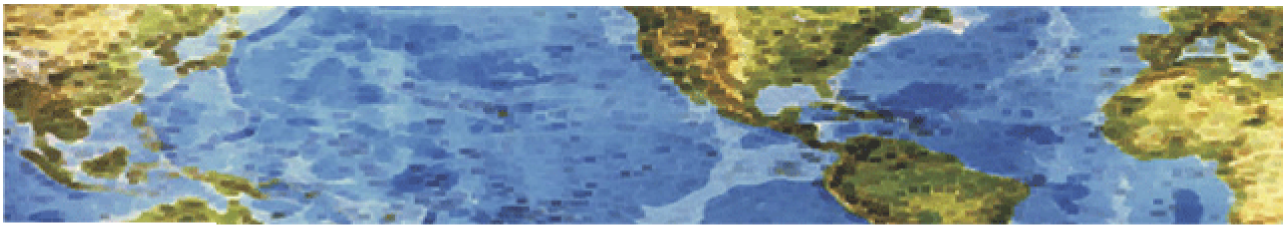
HALL ASSOCIATES



Risk-Based Decision Making Commentary
8 August 2014 Newsletter

Here's Looking at You: How Personal Health Information Is Being Tracked and Used

People who use cell phones, credit cards, websites, store coupons, and medical devices leave a trail of data that are often harnessed by third parties, sometimes without consumers' knowledge.

Every day, in the course of using cell phones, credit cards, search engines, websites, and medical devices, we leave digital "footprints." Aggregated and analyzed, these data flows, which occur with and without our knowledge, have the potential to paint a detailed health profile of individuals, as well as to describe whole communities based on location, health conditions, or other factors.

The proliferation of extremely large databases of health information challenge regulators' and society's ability to ensure individuals' data rights and privacy. A report by the California Health Care Foundation (http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/H/PDF%20HeresLookingPersonalHealthInfo.pdf) provides an overview of some of the emerging issues related to consumer-generated health data. It is based on numerous interviews with technology and health care experts, several of whom offer strategies for protecting privacy in the future.

Among the issues discussed:
Most people are unaware that they are leaving their personal data behind and that some of this information is not protected by HIPAA. Data brokers are able to build dossiers on individuals to sell to marketers, while consumers lack recourse to obtain or correct their information.
Clinical researchers, health plans, and others use the information to enhance individuals' health as well as to benefit public health. Larger and speedier clinical trials are made possible by the quantity of data available.
Different types of information — such as historical claims data and consumer-generated data — can be combined and used for statistical modeling for health or financial risk-profiling. Such information is purchased by hedge funds, hospitals, large provider networks, payers, pharmaceutical companies, and others.

Even when given an opportunity, most consumers are not vigilant about protecting their data; many are willing to share data to further their own health or to serve public health goals.

Read more: http://www.chcf.org/publications/2014/07/heres-looking-personal-health-info#ixzz39GdSpmN2

HALL ASSOCIATES

Over One Billion Passwords Served

It was recently reported in the New York Times **- and many other places -** that a criminal gang in Russia has a massive collection of usernames, passwords, and email addresses. It's truly a massive collection of user information, over one billion usernames and passwords and over 500 million email addresses.

How does this happen?

While this gang seems to have been very successful, there is nothing new about how they obtained this information. They started with some a small set of passwords (which they seem to have bought), and then worked their way through one website/company after another, gaining access, installing phishing redirects, and finding other vulnerabilities. Part of their activities also involved the use of a botnet to gather information directly from people's computers. In the end, apparently, data was taken from over 420,000 websites.

What does this mean to you and me?

In short, your usernames, passwords, and email addresses may have been exposed. Right now it's not known how many passwords were in the clear and usable or were in encrypted forms. So it's hard to assess exactly how much risk there is, but, given the scope of this dataset, it's safe to say that there is a good chance that passwords you use have been compromised. And doubly so if you (like many people) are in the habit of re-using the same passwords at many different websites.

What should you do now?

Right now, you should change the passwords for all of your critical accounts. While you are at it, if possible, set up two-factor authentication for your critical accounts such as your online banking account, PayPal, your primary email account, etc. Note that access to your primary email account often lets people reset passwords to get access to all your other accounts.

What should you do to get/stay safe?

1. **Change your passwords and be sure to use a different password on every site**. You should never reuse passwords across websites. Some services like Gmail will even let you make several passwords so you can even use different passwords on different devices (laptop, smartphone, pad etc.)
2. **Try and make your passwords complex.** Definitely don't just use dictionary words (I'm talking to you "my wife's/kids birthday"), instead try passwords that combine letters and numbers, such as "r3ds0x". However there's a debate on what's best for passwords right now, since unless you're using a password system you will have trouble remembering "932ujsdo8u23knsdf". Passphrases that are long but also easy to remember such as "1 2 3 take me out to the ball game 1 2 3" seem to be best right now.
3. **Use two-factor authentication for your critical accounts**. Two-factor authentication, like receiving a text to login, makes your online accounts much safer and is the second most important thing to do (besides not using "puppy" as your password.)
4. **Consider a password manager**. Using a system to manage your passwords lets you easily use unique and complex passwords for every website. You'll have more secure accounts and you'll still be able to access your accounts from any device. Plus it has the benefit of using a unique email address for every website, so you can control spam if (or when) that website is cracked. Don't forget that they got 500 million email addresses as well. **However, some password management systems have been hacked, so check first and then pick with care.**

http://www.abine.com/blog/2014/one-billion-passwords-served/ is one site but this information is all over the web. Try Google.

8 August 2014