8/20/2015

By Adam Levin

The other cufflink fell on the Ashley Madison hack Tuesday.

According to Wired, 9.7 gigabytes of Ashley Madison data were dumped on the dark web, and the collection appears to "include account details and log-ins for some 32 million users." Where we go from here is anyone's guess.

According to the Wired article, the hackers left a note with the quarry of ill-gotten files of marital listlessness: "Avid Life Media has failed to take down Ashley Madison and Established Men. We have explained the fraud, deceit, and stupidity of ALM and their members. Now everyone gets to see their data." The data includes names (many presumably aliases), email addresses, street addresses (harder to fake because these are tied to billing), amounts charged on credit cards and potentially enough credit card information to re-identify an account with a particular user (the last four digits of an account number or a transaction ID).

There is a mad dash now to rummage through that Dumpster-full of names on the dark web, with the first tack a search for email addresses tied to government accounts. According to U.K.'s Sky News , "15,000 US military and government email addresses are registered on the database, including executives in high-level positions." It also reported "email addresses linked to the White House and NASA, as well as the Vatican and the United Nations."

Among the horde in the coliseum of moral schadenfreude and the media companies that feed the public's insatiable appetite for tales of other people's woe, news of this or that now-public indiscretion will be greeted with glee. For those exposed by the hack, the news will create a spontaneous bouquet of shrugs, denials, tortured apologies and long explanations that no one really wants to wade through, but most will read with rapt attention.

The hack of Ashley Madison and Established Gentleman is of course part a bigger story. There are more than a billion records with significantly more personally identifying information out there. Data breaches have become the third certainty in life, right behind death and taxes. Up to now, the kind of information most often exposed in a breach was of concern because it could be used to harm our financial lives and even our well being (like medical identity theft). What differentiates the ALM hack is that it has moral ramifications. Of course, the damage is also of a material stripe, since it could spur costly life changes due to extinct relationships that might otherwise have survived a rough patch, and even a stray act of cyber-wandering.

The Real Damage Is Emotional

Impact Team, the hackers behind the Ashley Madison hack, provided some advice when they dumped the files on the dark web: “Find someone you know in here? Keep in mind the site is a scam with thousands of fake female profiles. See ashley madison [sic] fake profile lawsuit; 90-95% of actual users are male. Chances are your man signed up on the world’s biggest affair site, but never had one. He just tried to. If that distinction matters.”

The tone of the Impact Team is decidedly of the Somebody Done Somebody Wrong variety. But while that makes for a good song, it’s not how the world works. No one can argue that the Impact Team hasn’t lived up to its name. But with the extinction of privacy upon us, what did it actually accomplish beyond creating a very good example for those who make it their business to help others navigate the post-privacy world— both on- and offline? One could argue not much. Their goal was to make a moral point, but the result may well be a de-sensitization to morally fluid behavior. In a world where no one’s perfect and there is no meaningful privacy, who really cares who knows what?

What Do You Do in a World Without Secrets?

The same rules apply whether you are using social media of the more socially acceptable variety or the verboten kind: Lie. Prevaricate. Dissemble.

You have to tell a bank, and of course your employer, the particulars of who you are. They need your real name, your Social Security number (SSN) and your date of birth. (After all, providing them with fake information can constitute fraud.) You have to tell other organizations,

like doctors and the IRS, certain facts about your life, and of course the act of doing business with a retailer is synonymous with telling the world about it, since breaches are so prevalent. But creating an online alias and protecting some of your most valuable pieces of personally identifying information (PII) on social media and other sites can go a long way in helping you operate on the Web without becoming exposed. Here are some tips to do just that:

1. Never use your real name. Use a nickname that your acquaintances know or create an alter-ego.
2. Never share your date of birth.
3. Create a unique email account—or what's commonly referred to as a burner account—not the one you use for personal correspondence and managing your finances.

4. If you pay by credit card, bear in mind you potentially just blew your alias in the event of a hack.

If your financial details or SSN get exposed in a hack, you don't want it to destroy your credit (on top of everything else). Keep an eye on your financial accounts – look at your statements online every day – and check your credit reports and scores regularly. You can get your free annual credit reports on AnnualCreditReport.com
.

In a world where there are no secrets, you either have to be a saint, very careful … or have no shame.

This story is an Op/Ed contribution to Credit.com and does not necessarily represent the views of the company or its partners.