Forget passwords!

Home » Blogs » lippard's blog

Forget passwords! | Global Crossing Blog Central

Thu, 01/06/2011 - 10:49 | by Jim Lippard

You may have read one or more of the many recent stories covering the data breach at Gawker Media¹, which became known on December 12 when the usernames and passwords of 188,281 accounts used to comment on blogs like Gawker, Gizmodo, Jezebel, and Lifehacker were published to the world (along with source code and internal chats of Gawker employees). Many reports correctly identified a few security lessons to be learned from this breach, such as not using easily guessable passwords and not using the same password for every website. The first point was ignored by many Gawker users—the most common passwords in the file included “12345,” “password,” “qwerty,” “letmein.” Many passwords were also dictionary words, common proper names, or were identical with the username. The second point was also a lesson learned the hard way, as the Gawker breach led to subsequent attacks on Facebook and Twitter accounts.

What I was surprised not to see mentioned in any of the reporting I read on the subject was a much better recommendation on password use than any of the advice offered, which is to forget most of your passwords.

As Bruce Schneier put it over a decade ago, passwords are based on an oxymoron²—they are supposed to be sufficiently random to be hard to guess, yet also be something that is easy to remember. Rather than try to use passwords that meet these incompatible conditions, why not use a tool that allows you to have the former and not bother with the latter? Tools like KeePass (now available as a Droid app), Password Safe, LastPass, 1Password, and Apple’s Keychain mechanism offer mechanisms for generating random passwords for each site you visit, storing them in a strongly encrypted database, and letting the tool do the work of authenticating you when you need to get access. Instead of remembering the password for each site, you remember one stronger passphrase for accessing your password database. You can also take it a step further, and store your passwords on a separate piece of hardware built for the purpose, such as an encrypted USB flash drive from IronKey or Kanguru (or one you make yourself with TrueCrypt).

Now, using a password database tool does have some potential drawbacks of its own. You need to make sure that the system where you are storing your passwords and using this tool doesn’t itself become compromised in a breach that allows an attacker to get access to your password database by intercepting your keystrokes. You also need to make sure you don’t commit a denial of service attack against yourself by forgetting your passphrase or destroying the only copy of your password database—this is a case where it’s a good idea to write the passphrase down and store it somewhere securely (perhaps along with your will), and it’s always a great idea to back up important data. And, when it comes to accounts associated with your job, your options may be limited. But in most cases, the drawbacks are likely far outweighed by the benefits of forgetting most of your passwords and letting a tool take on a task that it can perform better than a human being.

--- References ---

FAQ on Gawker breach: http://lifehacker.com/5712785/faq-compromised-commenting-accounts-on-gawker-media


"The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it’s easy to remember, it’s something nonrandom like ‘Susan.’ And if it’s random, like ‘r7U2*Qnp,’ then it’s not easy to remember."—Bruce Schneier, Secrets and Lies, 2000, Wiley Computer Publishing, pp. 136ff.