CIO/CTO Perspective Policy and Regulation Defense in Depth Security Business Insights Voice and Collaboration Solutions IP Solutions Virtualization & On-Demand

Home » Blogs » lippard's blog

Forget passwords!

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

Like 17

5

You may have read one or more of the many recent stories covering the data breach at Gawker Media[1], 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 oxymoron[2]—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
Detailed account of Gawker breach: http://blogs.forbes.com/firewall/2010/12/13/the-lessons-of-gawkers-security-mess/
An alternative method of keeping written-yet-encrypted passwords in your wallet or purse: http://lifehacker.com/5715794/how-to-write-down-and-encrypt-your-passwords-with-an-old+school-tabula-recta

*"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.*

Follow Global Crossing

Subscribe to our Level 3 Blog

Languages

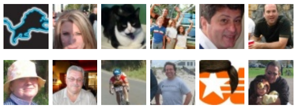
English

Search

Search

Connect on Facebook

Like David Linehan, Michelle Soltesz and 1,809 others like this.



Cloud Services Suite

Click Again for Full Screen

User login

Username: *

Password: *

Log in

Log in using OpenID

Create new account

Like

Request new password

Add New Comment

Login

Type your comment here.

Showing 0 comments

Sort by oldest first

M Subscribe by email S RSS

Trackback URL http://disqus.com/forur

Jim Lippard's blog

Tags: Defense in Depth Security encryption gawker password Security

Recent blog posts

- Global Crossing Genesis Solutions International Events Part 2 of 2 - "Operationalizing the deal"
- Global Crossing Genesis Solutions International Events Part 1 of 2 "Winning the deal"
- IPv4 Addresses for Sale?
- Recap at IBC 2011 - Global Crossing Genesis Solutions
- Regional and global bandwidth expansion boom
- Tips to prevent voice communications systems fraud
- PSN Cost Savings in the UK Government Sector
- Advanced Cyber Attacks Require Sophisticated Technology
- Application management on Data Center critical enviroments
- Crowning glory for Global Crossing (UK) Telecommunications Limited

more

Legal Disclaimer

Disclaimer: Opinions expressed here and in any corresponding comments are the personal opinions of the original authors, and do not necessarily reflect the views of Global Crossing. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Global Crossing or any other party. This site is available to the public. No information you consider confidential should be posted to this site. By posting you agree to be solely responsible for the content of all information you contribute, link to, or otherwise upload to the Website and release Global Crossing from any liability related to your use of the Website.