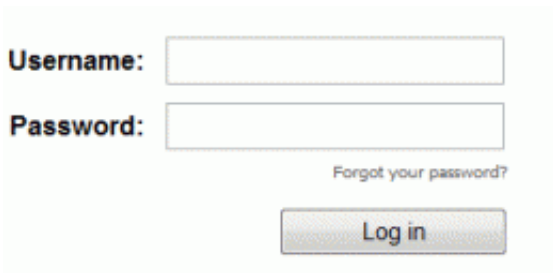


Putting the password problem in perspective

February 11 2015, by Troy Wolverton, San Jose Mercury News



Username:

Password:

[Forgot your password?](#)

Credit: Wikipedia.

Passwords are one of the banes of my life. I bet they are for you, too.

It used to be that we had to memorize one or two - for your ATM, maybe, or for your work computer. But thanks to the Internet and all the online stores, apps and Web services we interact with, we now have to remember dozens. And because sites have increasingly encouraged users to provide more complicated passwords, they're becoming more difficult to remember.

Add in the anxiety of watching millions victimized by data breaches after hackers exposed sensitive information stored by Anthem, Home Depot, Target and others and it's not surprising there's extra attention being paid to creating secure passwords.

Fortunately, there are tips and tools you can use to better protect yourself and make managing your passwords easier.

It's about time. A study by security researcher Cormac Herley of Microsoft Research in 2007 indicated that consumers then on average had to remember about 24 passwords. It's at least double that now, Herley said.

"By the time you get to the order of 50 to 60 accounts, it's not just difficult, it's impossible," he said.

Consumers have responded to the growing number of passwords as you might expect. They often use combinations of letters and numbers that are easy to remember and easy to guess. And they reuse passwords across multiple sites.

Some of the most popular ones are the not-so-secret "123456", "Password", and "abc123", according to a recent report by computer security firm Imperva.

I'm not pointing fingers, by the way; I do similar things.

The problem, researchers say, is that simple passwords are easy to crack. And if hackers or criminals get hold of a password that you've used in multiple places, they potentially can get access to wide swaths of your personal information. All of a sudden it's not just your Facebook account that's taken over by a troll, it's also your bank account, credit card and insurance records.

U.S. consumers filed some 290,056 complaints of identity theft in 2013, according to the Federal Trade Commission, although identify theft could be even more prevalent.

"It happens often enough that people should worry about it," said Lorrie Cranor, a professor of computer science and director of the Usable Privacy and Security Laboratory at Carnegie Mellon University.

According to researchers, the most common ways that passwords are compromised these days are through malware programs that log what consumers type on their keyboards; phishing attacks that lure consumers to type their passwords into fraudulent sites masquerading as legitimate ones; and through large-scale hacking attacks that infiltrate corporate databases of user logon information.

Such hacking attacks have become increasingly common. Just this week, information from up to 80 million customer accounts was stolen from Anthem in a security breach.

While sites have increasingly encouraged consumers to protect their accounts by using stronger passwords that include numbers, symbols and upper- and lowercase letters, those techniques don't provide much protection against the most common security threats. Weak passwords are just as vulnerable to malware or phishing attacks as strong ones. And if sites don't properly protect account information - as appears to be the case with Anthem - the strength of a consumer's password is irrelevant.

Despite all their problems, passwords aren't going away anytime soon, because there's just not a good replacement for them, researchers say. While biometric techniques such as fingerprint scans, iris detection and facial recognition are increasingly being used to protect information, they do require special equipment and have their own security problems. If a logon database gets compromised, you can easily replace any passwords that were stored in it; you can't readily replace the fingerprint records it might have included.

But don't fret. There are some steps you can take to better protect yourself without needing a memory upgrade for your brain.

Many sites now allow users to log in using Facebook or Twitter instead of creating a whole new account and password. Two-factor

authentication - a technique that involves using a second code in addition to a password - can protect you even if you reuse passwords. And password managers can store your secret code in a kind of digital locker that's accessible on all your devices and even generate unique and strong passwords for you on the fly.

Jason Miller, a product manager at Next Issue Media, uses a password manager called 1 password. After a friend's retirement savings were stolen in a case of identity theft, Miller, 44, saw the importance of getting on top of his passwords.

"They're not really the greatest method of securing something, but given that that's what we have, you've got to do something to manage it all," said Miller, a San Jose resident.

Even without those techniques, researchers suggest that users can simplify things by prioritizing their accounts, such that they worry about having strong and unique passwords only on those that really matter, and by using personal codes that allow you to generate easy-to-remember but unique passwords for each site.

"It's good to try and have a couple strong passwords and do your best," said Joseph Bonneau, a technology fellow and security researcher at the Electronic Frontier Foundation, who says it's even OK to reuse passwords - at least on sites that don't store any of your personal or financial information. "Rather than try to have a bunch of slightly different, but not very good passwords, it's better to just acknowledge that on most sites, your passwords don't really matter."

PUTTING UP WITH PASSWORDS

Too many passwords in your life? There are no perfect solutions. But there are some techniques and tools that can make them easier to

remember or more secure:

Use a [password manager](#). Programs such as 1 password and LastPass keep all your passwords in a kind of locker that's secured with - what else? - a password. Such programs often have mobile versions and allow you to store your passwords in the cloud so that you can access them across devices. They can also generate passwords for you that are unique and strong. But they can be inconvenient to use with mobile apps. And if your account is compromised, all of your passwords could be exposed.

Turn on [two-factor authentication](#). Many sites provide extra security through this technique, which requires a second code or bit of data, in addition to a password. That code, which is often sent via text message or can be a randomly generated number on a small keychain token, provides protection even when users reuse passwords. But using two-factor authentication can be inconvenient, because it requires an extra step and not all sites offer it.

Rely on Facebook. Many sites now allow users to log in using their Facebook, Twitter or Google credentials. That can greatly reduce the number of passwords you have to memorize, because the single one for your social networking site replaces all of the ones you would have used for individual sites. But not all sites allow you to log in with Facebook or Twitter. And there are privacy concerns also: Do you really want Facebook or Google monitoring your activities when you aren't on their sites?

Create your own code. Some security researchers suggest that users create passwords with a root-and-extension model. With this technique, your passwords would all have the same base, preferably one that wasn't an easy-to-remember word or number. Then you would extend that password with extra, but unique, characters using the same algorithm for every site. So, your base might be "D0YKtw2SJ" - a truncated version of

"Do you know the way to San Jose." And to that, you might add the second, fourth and sixth characters of the domain name of the site you visit - a, e and o, in the case of Facebook. The result is a password that's both unique and relatively easy to recall - if you can remember your code.

Prioritize. Not all accounts and passwords are of equal value. It's much more important to protect your bank account or other financial information than your ability to log in to a news site you rarely use or a random forum [site](#). Researchers suggest users save their strongest and unique passwords for their most important sites. If you're going to reuse passwords, do that only with less important sites - but do so with the knowledge that if that password is compromised, it could affect your access to multiple sites.

Write them on a piece of paper. It's long been thought that writing passwords down on paper was one of the dumbest things you can do. But it turns out that it's not so bad, at least compared with other solutions. Handwritten passwords aren't vulnerable to hackers. And if you keep them in your wallet, they'll nearly always be with you. You can be even safer if instead of writing the passwords themselves, you write simple hints. Of course, you can't easily search through [passwords](#) on paper. And if your wallet's stolen, you could be in big trouble.

©2015 San Jose Mercury News
Distributed by Tribune Content Agency, LLC

Citation: Putting the password problem in perspective (2015, February 11) retrieved 24 April 2024 from <https://phys.org/news/2015-02-password-problem-perspective.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.