Secure Passwords You Can Actually Remember!

(Submitted by the CAPLA Systems & Data Committee January 24, 2018)

Forgotten passwords are one of the most common reasons for calls to technical support lines. We do everything we can to avoid having to remember our passwords. Take a look at your monitor. Is there a post-it note stuck on it with a password you always forget because you rarely use it? Or do you use "Password2018" for all the systems you log into (even your online banking site)?

In this article, we're going to show you a technique that will increase your security and let you easily remember a different password for every system you use.

UK media outlet "Telegraph" exposed the top 25 most commonly used passwords. The top 10 of those are: 123456, 123456789, qwerty, 12345678, 111111, 1234567890, 1234567, password, 123123, 987654321. This list of common passwords is what hackers write on sticky notes for THEIR monitors, to try to break into systems! Don't use them!

Some tips they provide for picking a secure password include:
- Don't use the same password for every system
- Make your password as long as possible, but still memorable, by using a phrase
- Use a program that generates random passwords and stores them. Then copy/paste the password from there to the system you're logging into.

That last tip is one of the most secure methods, along with something called "two-factor authentication" or "2FA". However, they both add a level of complication that is not convenient or even feasible for some people (especially if you don't have a cell phone or don't use it's SMS "Text" feature).

Almost all systems have requirements for passwords. Some common ones are:
- must be at least 8 characters
- must have a mix of upper-case and lower-case letters
- must contain punctuation (periods, question marks, exclamation marks)

Here's how to let your IT department sleep better at night, because you're not creating security holes.

1. Come up with a password that meets the most common rules (length, special characters, punctuation, etc.)

    eg. M@ke5ecurityGreatAgain!

2. As you use each new system, change your password to be the common password, PLUS the system name. Be consistent about how you enter the system name. That way you won't have to remember whether you used "Facebook" or "facebook".

    eg. M@ke5ecurityGreatAgain!facebook

3. For added levels of security, try these methods:

    - replace some characters in the system name, AND misspell some of the words.

eg. M@ke5ekurityGraytAgain!f@c3book

- Using a dead or less common language, like Latin or Swahili, for the common part of your password.

eg. EtSecur1tasMagn@!f@c3book

If the example phrase above is too long, or not meaningful to you, make up your own, or use one of these as inspiration. Remember, the longer, the better!

MyBirthd@yI$June22<system name>
Harry&MeghanMay192018<system name>
99%SekoorPa55werd<system name>
IWon'tForgetMy5ecretPa&&word<system name>

I've tried this method personally, and I've found that the common part of my password becomes very easy to type, even though it's fairly complex, because I constantly practice it in my daily routine.

All security methods suffer from the same vulnerability: people. To be effective, security must be easy enough that people will actually use it. If you can manage the process of using a password generator/keeper and/or two-factor authentication, by all means, use those methods, for maximum security.

Some commonly used password generators/keepers include:
LastPass https://lastpass.com
1Password https://1password.com
Dashlane https://www.dashlane.com
Sticky Password https://www.stickypassword.com
LogMeOnce https://www.logmeonce.com/

References:
http://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/
https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/
https://www.pcmag.com/article2/0,2817,2407168,00.asp