Does your password pass muster?

March 25 2015

New research from Assistant Professor Mohammad Mannan and his colleagues has exposed the weakness of password strength meters. Credit: Christian Fleury

"Create a password" is a prompt familiar to anyone who's tried to buy a book from Amazon or register for a Google account. Equally familiar is that red / yellow / green bar that rates the new password's strength. But when those meters give the go-ahead to passwords like Password1+, their effectiveness is called into question.

New research from Concordia University exposes the weakness of

password strength meters, and shows consumers should remain sceptical when the bar turns green in order to create strong passwords.

For the study, forthcoming in the journal *ACM Transactions on Information and System Security*, researchers Mohammad Mannan and Xavier de Carné de Carnavalet sent millions of not-so-good passwords through meters used by several high-traffic web service providers including Google, Yahoo!, Dropbox, Twitter and Skype. They also tested some of the meters found in password managers, allegedly designed with the relevant expertise.

"We found the outcomes to be highly inconsistent. What was strong on one site would be weak on another," says Mannan, who is a professor with Concordia's Institute for Information Systems Engineering.

"These weaknesses and inconsistencies may confuse users in choosing a stronger password, and thus may weaken the purpose of these meters. But on the other hand, our findings may help design better meters, and possibly make them an effective tool in the long run," adds PhD student de Carnavalet.

So what can companies do? Start by emulating Dropbox, the researchers recommend. The popular file-sharing site had the most robust password strength meter—and the software is open-source.

"Dropbox's rather simple checker is quite effective in analyzing passwords, and is possibly a step towards the right direction. Any word commonly found in the dictionary will be automatically be caught by the Dropbox meter and highlighted as weak," explains Mannan. "That automatically prompts users to think beyond familiar phrases when creating passwords."

"Some checkers are very strict, and assign scores only when a given

password contains at least three character sets—that is, a letter, a number and a symbol; other checkers are ok with the use of letter-only passphrases. Such a discrepancy is not explained to the user and is hardly justifiable," says de Carnavalet.

"We've contacted most of the companies we examined in our study but so far our results are falling on deaf ears," Mannan says. One company dropped their meter while another one fixed a simple bug. No other changes were observed even after a year.

For now, it's up to individuals to ensure their passwords are strong by using full characters set random passwords. Of course, remembering those passwords is easier said than done.

As an alternative, Mannan suggests another tool for creating web passwords from private images (SelfiePass/ObPwd for Android and for Firefox). But using such tools may not solve the password problem for all use cases, he warns.

Provided by Concordia University