TechXplore

'Inconsistent and misleading' password meters could increase risk of cyber attacks

December 19 2019, by Mr Alan Williams

Credit: CC0 Public Domain

Password meters are frequently made available to help users secure their personal data against the threats posed by cyber criminals.

However, the 'inconsistent and misleading' advice offered on some of the world's most popular websites could actually be doing more harm than good, according to new research.

A study by the University of Plymouth assessed the effectiveness of 16 password meters that people are likely to use or encounter on a regular basis.

The main focus was dedicated password meter websites, but the study also sought to assess those embedded in some common online services (including Dropbox and Reddit) and those found as standard on some of our devices.

Published in *Computer Fraud and Security*, the research says there is a clear level of variation in the advice offered across the different websites.

And while some meters do effectively steer users towards more secure account passwords, some will not pick them up when they try to use 'abc123', 'qwertyuiop' and 'iloveyou' - all listed this week among the worst passwords of 2019.

The study was conducted by Steve Furnell, P rofessor of Information Security and Leader of the University's Centre for Security, Communications & Network Research.

He has previously suggested that global IT giants including Amazon and LinkedIn could be doing far more to raise awareness of the need for better password practices.

He has also shown that over the space of a decade, most of the top ten English-speaking websites had not expanded the password guidance they offer consumers amid the increased threat of global cyber-attacks.

Commenting on the latest research, Professor Furnell said: "Over the festive period, hundreds of millions of people will receive technology presents or use their devices to purchase them. The very least they should expect is that their data will be secure and, in the absence of a replacement for passwords, providing them with consistent and informed guidance is key in the quest for better security.

"What this study shows is that some of the available meters will flag an attempted password as being a potential risk whereas others will deem it acceptable. Security awareness and education is hard enough, without wasting the opportunity by offering misleading information that leaves users misguided and with a false sense of security."

The study tested 16 passwords against the various meters, with 10 of them being ranked among the world's most commonly used passwords (including 'password' and '123456').

Of the 10 explicitly weak passwords, only five of them were consistently scored as such by all the password meters, while 'Password1!' performed far better than it should do and was even rated strongly by three of the meters.

However, one positive finding was that a browser-generated password was consistently rated strong, meaning users can seemingly trust these features to do a good job.

Writing in the study's conclusion, Professor Furnell added: "Password meters themselves are not a bad idea, but you clearly need to be using or providing the right one. It is also worth remembering that, regardless of how the meters handled them, many systems and sites would still accept the weak passwords in practice and without having offered users any advice or feedback on how to make better choices.

"While all the attention tends to focus on the replacement of passwords, the fact is that we continue to use them with little or no attempt being made to support users in doing so properly. Credible password meters can have a valuable role to play but misleading meters work against the interest of security and can simply give further advantage to attackers."

More information: Steven Furnell, Password meters: inaccurate advice offered inconsistently?, *Computer Fraud & Security* (2019). DOI: 10.1016/S1361-3723(19)30116-2

Provided by University of Plymouth

Citation: 'Inconsistent and misleading' password meters could increase risk of cyber attacks (2019, December 19) retrieved 25 April 2024 from https://techxplore.com/news/2019-12-inconsistent-password-meters-cyber.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.