PHYS.ORG

Basic password guidance can dramatically improve account security, study shows

February 28 2018

Technology users should be offered more detailed support and guidance when creating account passwords in order to make them more secure and harder to crack, a study suggests.

Research led by the University of Plymouth found those who receive basic guidance including password meters were up to 40 per cent more likely to make their choices secure.

However, those given feedback such as how likely it was that hackers could guess their passwords – and therefore access private information held in their accounts – were up to 10 times more likely to change their original choice to something more secure.

The research was conducted by the University's Centre for Security, Communications and Network Research (CSCAN), in conjunction with the Desautels Faculty of Management at McGill University and the Department of Computer Sciences at Purdue University.

Published in Computers & Security, it comes at a time when the global cyber security threat is continuing to rise with accounts held by individuals and organisations constantly at risk of attack.

Steve Furnell, Professor of Information Security and the Director of CSCAN, said: "Over the past few years, numerous cyberattacks and security incidents have demonstrated that protecting personal and professional assets is no longer an optional duty. Yet many still occur out of unintentional mistakes such as negligence, carelessness, and human errors. Despite the advance in security technology, the weakest link in the information security realm still lies in end-users so it is essential that more support is offered to try and overcome this in the future."

The research focused on two experiments designed to investigate how variations in password meter usage and feedback can positively affect resulting password choices.

In one experiment, 300 users creating an internet account were offered either none or a range of advice including a standard password meter, emojis or an emotive feedback message. The results showed the number of choices rated 'weak' falling from 75 per cent, where users received no guidance, to around a third when they were shown more emotive messages.

For the second, 500 participants in the United States were presented with more specific security-related advice, including suggestions of how long it would take a hacker to crack their password. Those users had a significantly greater understanding of the risks, and created passwords that were longer and up to 10 times stronger as a result.

As part of the study, researchers also demonstrated that several leading sites – including Facebook, Twitter and Amazon – continue to permit weak passwords practice, allowing combinations of the user's first name and surname, a string of numbers such as "1234567890" and the word "password" respectively.

Professor Furnell added: "If this lack of provision is apparent with market-leading sites, it is unlikely that users are being better served in other contexts, and it potentially goes some way to explaining why bad practices persist. A common weakness in the provision of security is that while relevant features are present and available to be employed, users are often expected to use them with little upfront guidance, or ongoing support. It is therefore hardly surprising to find that users' resulting behaviours are often explicitly insecure.

"These findings provide a lesson not only for passwords, but for end-user security in general, as the combination of effective guidance and enforcement gives users the chance to understand and buy into security right from the start."

More information: Steven Furnell et al. Enhancing security behaviour by supporting the user, *Computers & Security* (2018). DOI: 10.1016/j.cose.2018.01.016

Provided by University of Plymouth

Citation: Basic password guidance can dramatically improve account security, study shows (2018, February 28) retrieved 16 August 2024 from https://phys.org/news/2018-02-basic-password-guidance-account.html