

Accepted Manuscript

Title: Enhancing security behaviour by supporting the user

Author: Steven Furnell, Warut Khern-am-nuai, Rawan Esmael, Weining Yang, Ninghui Li

PII: S0167-4048(18)30038-5
DOI: <https://doi.org/10.1016/j.cose.2018.01.016>
Reference: COSE 1278

To appear in: *Computers & Security*

Received date: 18-9-2017
Revised date: 12-1-2018
Accepted date: 18-1-2018

Please cite this article as: Steven Furnell, Warut Khern-am-nuai, Rawan Esmael, Weining Yang, Ninghui Li, Enhancing security behaviour by supporting the user, *Computers & Security* (2018), <https://doi.org/10.1016/j.cose.2018.01.016>.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Enhancing security behaviour by supporting the user

Steven Furnell¹, Warut Khern-am-nuai², Rawan Esmael¹, Weining Yang³, and Ninghui Li³

¹ Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, United Kingdom

² Desautels Faculty of Management, McGill University, Montreal, Canada

³ Department of Computer Sciences, Purdue University, West Lafayette, Indiana, United States

Abstract

Although the role of users in maintaining security is regularly emphasized, this is often not matched by an accompanying level of support. Indeed, users are frequently given insufficient guidance to enable effective security choices and decisions, which can lead to perceived bad behaviour as a consequence. This paper discusses the forms of support that are possible, and seeks to investigate the effect of doing so in practice. Specifically, it presents findings from two experimental studies that investigate how variations in password meter usage and feedback can positively affect the resulting password choices. The first experiment examines the difference between passwords selected by unguided users versus those receiving guidance and alternative forms of feedback (ranging from a traditional password meter through to an emoji-based approach). The findings reveal a 30% drop in weak password choices between unguided and guided usage, with the varying meters then delivering up to 10% further improvement. The second experiment then considers variations in the form of feedback message that users may receive in addition to a meter-based rating. It is shown that by providing richer information (e.g. based upon the time required to crack a password, its relative ranking against other choices, or the probability of it being cracked), users are more motivated towards making strong choices and changing initially weak ones. While the specifics of the experimental findings were focused upon passwords, the discussion also considers the benefits that may be gained by applying the same principles of nudging and guidance to other areas of security in which users are often found to have weak behaviours.

Keyword: passwords, authentication, security nudges, user awareness, human factors

1. Introduction

Over the past few years, the importance of information security has become clear for individuals and organizations. Numerous incidents serve as evidence, demonstrating that protecting information assets is no longer an optional duty. However, despite the advance in security technology, the weakest link in the information security realm still lies in end-users (Crossler et al. 2013).

Although several studies have shown that some users may intentionally abuse the information systems (e.g., Siponen and Willison 2009; Willison and Backhouse 2006), ample evidence

Download English Version:

<https://daneshyari.com/en/article/6883928>

Download Persian Version:

<https://daneshyari.com/article/6883928>

[Daneshyari.com](https://daneshyari.com)