Letter

How to Create Memorable and Strong Passwords

Pietro Cipresso[1,2], MSc, PhD; Andrea Gaggioli[1,2], MPsych, PhD; Silvia Serino[1,2], MPsych; Sergio Cipresso[3]; Giuseppe Riva[1,2], MA, MPsych, PhD

[1]Applied Technology for Neuro-Psychology Lab, IRCCS Istituto Auxologico Italiano, Milano, Italy

[2]Psychology Department, Catholic University of Milan, Milano, Italy

[3]Freelancer, Milan, Italy

Corresponding Author:
Pietro Cipresso, MSc, PhD
Applied Technology for Neuro-Psychology Lab
IRCCS Istituto Auxologico Italiano
Via Pellizza da Volpedo 41
Milano, 20149
Italy
Phone: 39 61911 ext 2892
Fax: 39 619112892
Email: p.cipresso@auxologico.it

(J Med Internet Res 2012;14(1):e10) doi:10.2196/jmir.1906

KEYWORDS

Privacy; security; passwords; psychology

How to Create Memorable and Strong Passwords

In a recent JMIR article, El Emam, Moreau and Jonker highlight the importance of using strong passwords to protect personal health information in clinical trials [1]. An important implication that was not fully discussed is the potential problem people may have to create passwords that are complex but at the same time easy to remember.

To address this problem we propose the PsychoPass methord, a simple way to create strong passwords which are easy to remember. This method relies on mental practice and is not an hardware or a software to download. The idea is that a password can be created, memorized and recalled by just thinking of an *action sequence* instead of a word or string of characters. To be more specific, the method consists of the following steps (see Figure 1 and 2): (1) begin with a letter on the keyboard; (2) memorize a sequence of actions (something like “the key on the left, then the upper one, then the one on the right”, and so on); (3) memorize the sequence (not the letters used); (4) create as many passwords as you want by remembering only the first letter and the sequence. Using different types of sequences it is possible generate thousands of different passwords. Using sequences' combination is possible to create an infinite number of passwords. Moreover the created passwords will be a nonsense sequence of letters, numbers and symbols, resilient to any attack.

Furthermore the password communication among colleagues maybe done just by using the first letter and on the base of a common knowledge of the sequence (e.g., sequence 3, letter j).

El Emam and Colleagues state that more sophisticated collaboration tools are required to allow file sharing without password sharing, and provide several recommendations to implement these practices. We think that more awareness and new practices among users may represent the correct way to implement security beyond the technological issues. In particular, future research needs to focus on the processes that make technology a powerful tool for security.

Figure 1. The same sequence to generate different passwords (about 15 minutes to memorize the sequence).

Figure 2. Another sequence to generate other passwords (about 15 minutes to memorize the sequence).

Conflicts of Interest

None declared.

Multimedia Appendix 1

Movie demonstrating the method.

[MOV File, 7MB - jmir_v14i1e10_app1.MOV]

Reference

1. El Emam K, Moreau K, Jonker E. How strong are passwords used to protect personal health information in clinical trials? J Med Internet Res 2011;13(1):e18 [FREE Full text] [doi: 10.2196/jmir.1335] [Medline: 21317106]

Edited by G Eysenbach; submitted 06.08.11; peer-reviewed by K El Emam; accepted 07.01.12; published 10.01.12

Please cite as:
Cipresso P, Gaggioli A, Serino S, Cipresso S, Riva G
How to Create Memorable and Strong Passwords
J Med Internet Res 2012;14(1):e10
URL: http://www.jmir.org/2012/1/e10/
doi:10.2196/jmir.1906
PMID: