

Letter

# How to Create Memorizable and Strong Passwords

Pietro Cipresso<sup>1,2</sup>, MSc, PhD; Andrea Gaggioli<sup>1,2</sup>, MPsych, PhD; Silvia Serino<sup>1,2</sup>, MPsych; Sergio Cipresso<sup>3</sup>; Giuseppe Riva<sup>1,2</sup>, MA, MPsych, PhD

<sup>1</sup>Applied Technology for Neuro-Psychology Lab, IRCCS Istituto Auxologico Italiano, Milano, Italy

<sup>2</sup>Psychology Department, Catholic University of Milan, Milano, Italy

<sup>3</sup>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](mailto:p.cipresso@auxologico.it)

(*J Med Internet Res* 2012;14(1):e10) doi: [10.2196/jmir.1906](https://doi.org/10.2196/jmir.1906)

**KEYWORDS**

Privacy; security; passwords; psychology

## *How to Create Memorizable 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 method, 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.



©Pietro Cipresso, Andrea Gaggioli, Silvia Serino, Sergio Cipresso, Giuseppe Riva. Originally published in the Journal of Medical Internet Research (<http://www.jmir.org>), 10.01.2012. This is an open-access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/2.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work, first published in the Journal of Medical Internet Research, is properly cited. The complete bibliographic information, a link to the original publication on <http://www.jmir.org/>, as well as this copyright and license information must be included.