Nudge me right: Personalized nudges for enhanced computer security

Eyal Pe'er (Hebrew U), Serge Egelman (UC Berkeley), Marian Harbach (UC Berkeley), Nathan Malkin (UC Berkeley), Arunesh Mathur (Princeton), Alisa Frik (UC Berkeley),

Abstract

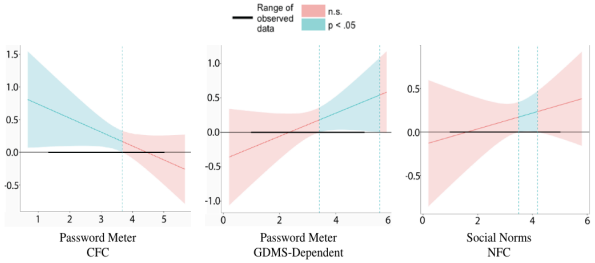
Effects of nudges are constrained to local maxima, as they are almost always designed with the "average" person in mind. Focusing on the ubiquitous area of computer passwords, we present a novel approach that provides evidence of how targeting nudges can lead individuals to create passwords that are four times stronger and more secure than administering regular "one-size-fits-all" nudges.

Background

- Nudges have been found effective in many domains.
- However, in some cases they were found to be ineffective on some populations (e.g., electricity social norms on conservatives, Costa & Kahn, 2013) or even conuter-effective on others (e.g., tax letters on high debtors in U.K., Halpern, 2015).
- Several scholars (e.g., Sunstein, Carroll, Costa & Kahn) already advocated for personalized nudges.
- But currently there is neither a valid method on how it can be done or evidence on how much it can increase nudges' effectiveness.

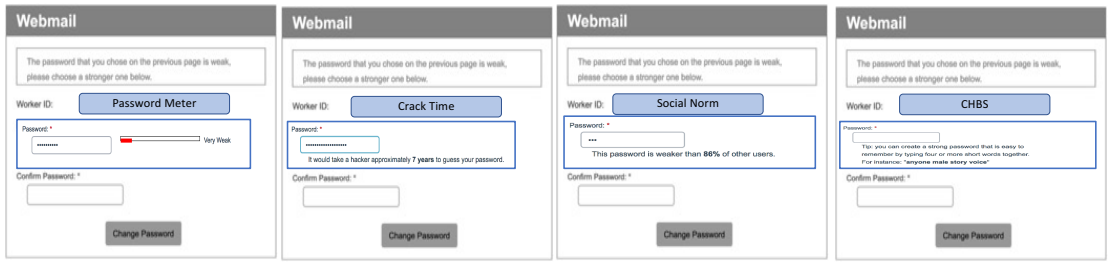
Study 1 – Exploring nudges-traits relationships

- Participants (N=1842, Mturk) did a 2-stage study.
- In the 1st stage they completed trait measures and created a password needed to access the second bonus part of the study.
- We then explored the interactions between nudges and traits using Johnson-Neyman technique to find the regions of significant effects.
- Figure shows three such examples and table shows all significant regions.



Nudge / Trait	Meter	Crack Time	Social Norms	CHBS
Numeracy		>8.59		>6.29
CFC	<3.68	2.11, 4.1		1.92, 5.8
NFC		3.02, 5.2	3.5, 4.18	1.41, 5.71
GDMS:				
-Intuitive		2.79, 4.63		>5.14
-Dependent	>3.41	2.79, 5.7		>2.1
-Rational		3.63, 4.85		2.68, 5.83
-Avoidant		1.96, 5		>5.64
-Spontaneous		2.11, 7.64		>4.35

The Nudges



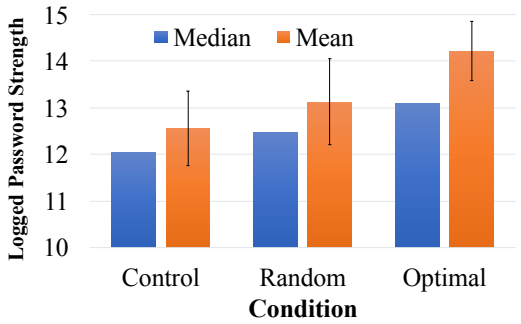
Study 2 – Testing personalization effect

Participants (N=923, Mturk) invited to complete all traits and then created a password (as in Study 1) in one of three conditions:

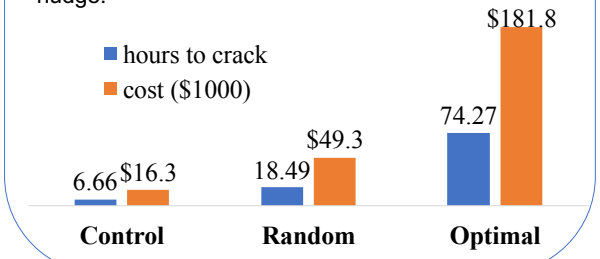
1) Control (no nudge at all)
2) Random nudge (meter vs. crack-time)
3) Optimal nudge (personalized)

Allocation was done using Monte-Carlo simulations based on Study 1 effects. In the Optimal condition each participant got the nudge that was expected to produce the largest effect.

We found that the **optimal nudge led to strongest passwords**, F (2, 920) = 5.201, p = 0.006



Estimates showed personalization increased password strength **by 4 times**, compared to random nudge, or by 10 times compared to no nudge.



For more info contact
eyal.peer@mail.huji.ac.il