

Encouraging password manager use

Karen Renaud

Verena ZimmermannAuthor

This is the accepted manuscript © Elsevier
Licensed under the Creative Commons Attribution-
NonCommercial-NoDerivatives 4.0 International:

<http://creativecommons.org/licenses/by-nc-nd/4.0/>



The published article is available from

<https://www.sciencedirect.com/journal/network-security/vol/2019/issue/6>

Encouraging Password Manager Use

Karen Renaud & Verena Zimmermann

Password Managers are a marvellous invention – essentially removing the pain that comes from trying to remember multiple, complex passwords. Yet adoption rates are low, which seems strange because no one tries to memorise all their contacts' telephone numbers. There are many free password manager apps, so cost is not a deterrent. So, what is going on?

There is some evidence that many people do not trust password managers but also that they do not know about these tools in the first place, so we ran a small study to find out whether improving awareness would make a difference. We embedded a short video on the enrolment page, just above the password entry field on a website used by a student population. It explained what a password manager is, and how it works. We took note of whether they activated the video. We asked them whether they already used a password manager and, if not, whether they intended to use one. Finally, we calculated the strength of the passwords they chose, using the zxcvbn.js tool: scored on a scale of 0 to 4. For example, 'password' gets a rating of 0, while 'bootlegdrench42' is rated as a 4.

Of 1095 users, only 107 ($\pm 10\%$) said that they already used a password manager. A one-tailed Mann-Whitney U test of the password strengths revealed that the passwords chosen by password manager adopters ($N = 107$, $Mdn = 4$) were significantly stronger than the passwords of users not using password managers ($N = 813$, $Mdn = 3$), $U = 31075.5$, $p < .001$, $r = .17$. Even though the effect is small, this result hints at the real benefit of password manager adoption. When people do not have to experience the pain associated with strong passwords, they are more likely to use them. It is a win-win situation.

What about the video? 61 (6%) watched the video, with only 8 watching it all the way to the end. We asked them if they now planned to install a password manager, and only 43 (4%) said they did.

This outcome, while somewhat disappointing, also holds some lessons.

In the *first* place, our website users accessed a web page where they were asked to come up with a password. This seemed the obvious place to display the video and improve password manager awareness. Yet, in retrospect, a choice to play the video required them to delay their immediate goal of accessing the system. That was probably unrealistic.

In the *second* place, we chose to communicate via a video. This is essentially a “push” mechanism – the viewer has no opportunity to ask questions or otherwise engage with the topic of the video. Such interaction is especially important when it comes to password managers because people need to trust the password manager with all their passwords, and such trust will probably not be easily granted.

Our experiment did not considerably improve intended password manager adoption, but it did highlight the fact that there are no quick and easy ways of improving adoption. Improving awareness is likely to be a long slow process. With respect, persistence and individual contact, we may help people to adopt this very helpful tool. The outcome would be less pain and stronger passwords – who can argue with that!

We acknowledge the contribution of Mario Avramidis, who undertook all the analysis for this study.