Do Stories Help People Adopt Two-factor Authentication?

Chris Fennell
Michigan State University
East Lansing, MI, USA
cfennell@msu.edu

Rick Wash
Michigan State University
East Lansing, MI, USA
wash@msu.edu

ABSTRACT

Recent research suggests that stories and storytelling can be used to help people make better security decisions. We are interested in using stories as a way to influence users to voluntarily enable two-factor authentication on their accounts. We conducted three studies that each focused on a different story type that would attempt to help users identify with the stories and lead to voluntary adoption of Two-factor. We presented these stories to samples from MTurk and Qualtrics and examined their reactions. We found that overall the stories were effective in convincing users to be willing to adopt two-factor authentication; however, our attempts to narrow in on the mechanism that made the stories effective alluded us.

KEYWORDS

two factor authentication; security; stories; phishing; training

INTRODUCTION

Phishing scams are one of the biggest cybersecurity issues at the moment. Many major breaches begin with a phishing email, and end consumers are also often targets of phishing attacks. The FTC recently warned consumers about phishing attacks pretending to be from Netflix[1], and phishing attacks pretending to be from Apple are also in the news[2]. Most of these attacks are seeking to collect usernames and passwords. The best defense against this is for users to enable two-factor authentication to protect their accounts. The use of a second factor, such as a one-time code via SMS, via an app on their smartphone, or via a dedicated device like a Yubikey, prevents attackers from being

[1]https://www.consumer.ftc.gov/blog/2018/12/netflix-phishing-scam-dont-take-bait

[2]https://krebsonsecurity.com/2019/01/apple-phone-phishing-scams-getting-better/

SOUPS'19, Aug 2019, Santa Clara,CA

	Studies		
	1	2	3
N =	130	98	105
(Ma./Fem.):	(65%/35%)	(53%/47%)	(51%/49%)
No. of Stories:	3	2	2
Sample:	MTurk	Qualtrics	MTurk
Story Type:	Tech. words	1st vs 3rd Per.	Sit.
Pre. 2FA (Y/N):	(85%/15%)	(59%/41%)	(31%/59%)

Table 1: Details of each of the 2FA studies

[3]https://www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/

[4]https://duo.com/blog/state-of-the-auth-experiences-and-perceptions-of-multi-factor-authentication

[5]https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

able to successfully log in even if they steal a username and password. Several studies have examined the impact of 2FA or multi-factor authentication on organizations [2]; however many organizations require adoption of this security service. Most consumer services are reluctant to require users to enable two-factor authentication for fear that it will drive consumers to choose to use a competitor. Instead, use of two-factor is voluntary, and consumer services try to provide training to encourage users to enable two-factor on their accounts. Recently, research has begun to examine ways that stories and storytelling can be used to help users make better security decisions[5, 7].

Literature Review

Popular web platforms like Facebook, Google and Instagram offer 2FA, but have to balance the tension between enticing users to join by focusing on ease of use versus keeping the site and user's data secure. Most of these platforms encourage the use of 2FA, but have low adoption rates; for example, the adoption of 2FA on Gmail is around 10% [3]. In 2017, The security company Duo conducted a U.S.-census-representative survey where they polled 579 individuals about their 2FA usage. They found that around 28% of their participants used 2FA and the majority 54% began using it voluntarily[4]. Continuing to persuade people to adopt two factor is a challenging endeavor. Researchers have created security related messages [6] and video tutorials [1] in attempt to train users to adopt 2FA.

One approach could be to use stories to convince users to adopt 2FA. Stories about security incidents are commonly told among end users [5], and have been used in past research to train users about phishing [7]. Stories are chronological series of events that contain characters, a plot or series of plots, and a situation or context. All of these components allow the reader to immerse himself or herself in the story and as a result, learn the moral or lessons contained within the story. As one example of the power of stories, in the two days after Mat Honan published an article about being hacked[5], almost a quarter million users signed up for 2FA on Gmail[4]. We are interested in helping individuals understand how to have better security practices. Stories might allow us an effective way of helping individuals by appealing to social norms that are part of a users identity[3]

Method

We conducted three different studies in order to explore the different Story types that we could use to train users (See Table 1). The stories were constructed in slightly different ways and represent a different focus within each study. We chose to modify existing stories about 2FA for several reasons. First, we wanted to use natural language that an ordinary individual could relate to and identify with. Second, constructing stories from scratch is a challenging endeavor for researchers because we tend to lean towards the complicated and complex which could make it hard for individuals to relate. Finally, what security practices individuals share or emphasize in a story might be different than what researchers share or emphasize. We created the stories by modifying real stories that we had come

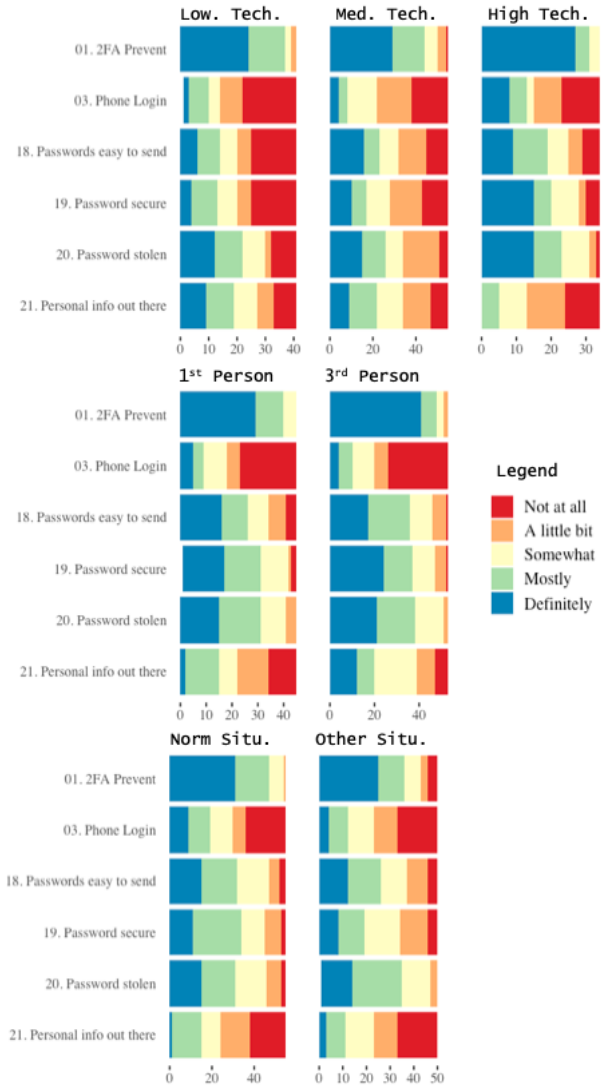

Figure 1: Participants reported the lessons that were in the story. 2FA Prevent being the most important.

[6]https://cran.r-project.org/web/packages/pwr/index.html

across online and in person. We measured willingness to adopt 2FA by asking them to agree from Strongly Disagree (1) to Strongly Agree (5). We asked them if they to rate the statements if they were willing to enable it today, in the near future, or never. For study 1, we varied the stories by modifying the technical language in the stories (See Table 1). We varied them from low, medium and high which translated to 4%, 6%, 10% respectively of the total words in each story. We were interested to see the effect of the technical language on willingness to adopt 2FA. For study 2, we chose to modify the Mat Honan wired article. At face value it seemed to lend credibility that stories are effective but we also were interested if the story could be modified by changing what individuals would identify with. We were also interested in exploring the myriad of different ways to which individuals identify with a story. For this set of stories we thought it would be interesting if we change the perspective of the story from a third person ("Mat Honan") to First Person ("I" or "You"). By doing so we hoped to invoke a greater sense of identification through the immersiveness of the first person perspective. We anticipated that the "I" or "You" condition would elicit greater identification with the main character and as a result would result in a higher willingness to adopt 2FA.

Finally for Study 3, we were aware that the previous two studies had a lot of technical language. We wanted to create a story that had less technical language and used more natural language. Computer Scientists tend to use a fairly heavy technical jargon and often write that way. So we searched through the security blogs and news and selected the John Podesta story. This was adapted from several news stories that recalled the account by the russian government to access 60,000 emails as part of the Hillary Clinton campaign. For this study we investigated another approach of involvement by exploring altering the situations to be what "others" do in a given situation. We compared this modified situation of focusing on what "others like them would do" vs what John did in the normal situation. We anticipated that the "other" situation would invoke greater invovlement than the normal situation in terms of willingness to adopt 2FA.

RESULTS

For each study we were primarily interested in their willingness to adopt two-factor authentication. While the stories varied between the conditions and the subsequent studies, the focal site of 2FA adoption for these stories was Gmail. For study 1, no impact of the technical language manipulation could be detected on the willingness to adopt 2FA. However, for Study 2 we did find differences between the 1st person vs 3rd person (See Table 2) but the results were opposite than what we had predicted and the explained variance was very small for all three regression models. Finally, Study 3 did not show an impact when we changed the situations in the story on the willingness to adopt 2FA. We ran a post-hoc power analysis using the "pwr" package [6] in R and found that with a single coefficient and the expectation that our model should explain about 10% of the overall variance, we should have been able to detect differences given our populations for each study.

	Adopt 2FA by Story		
	Today	Near Future	Never
(Intercept)	3.53 ***	3.86 ***	4.15 ***
3rd Person	0.42 *	0.29 .	-0.29
Adj R^2	3.59%	2.12%	-0.2%

*Signif. codes: 0 '000' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1*

Table 2: Study 2 - Willingness to Adopt 2FA between 1st and 3rd Person

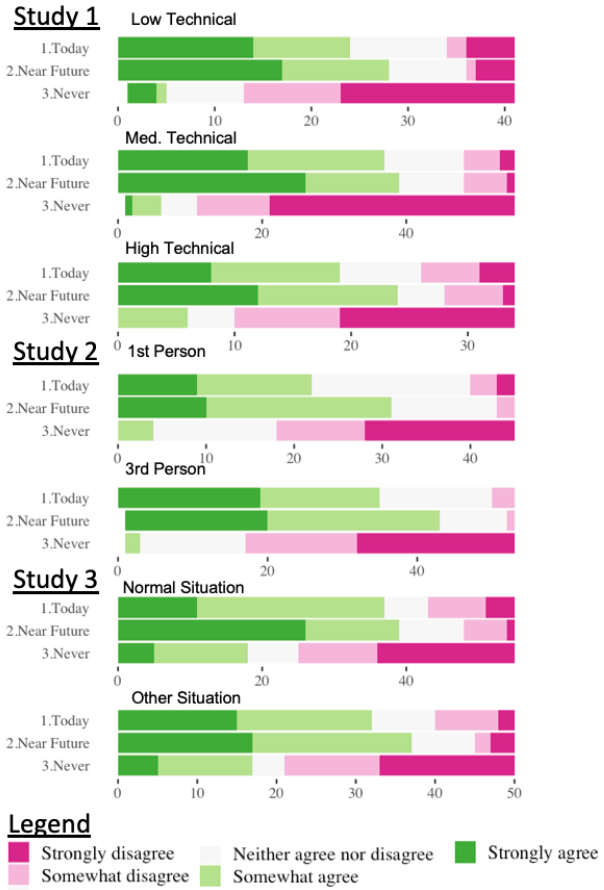

Figure 2: Willingness to Adopt Today, Near Future, Never distributions

DISCUSSION

While the results were not what we expected, we began to look at what the stories meant to the users. We first looked at the lessons that we wanted them to learn about 2FA such as "If hackers get your password, you cant log in without your phone" or "2FA can protect your account(s) from being compromised". Figure 1, shows that across the stories that 2FA can prevent from accounts being compromised but some of the other lessons such as "Your personal information being out there" participants did not report as highly. It is interesting since many of the stories explained that personal information was critical in compromising the accounts. It highlights some of the challenges in training individuals mental models about security. Individuals need to have their own intrinsic motivations for having security practices but individuals also want to know why security events happen. One interesting approach would be to modify the stories and change the focus of the stories from the explicit benefits of Two factor authentication and onto the consequences of having (or not having) 2FA. Some of the stories we tested did do that but that was not their primary focus.

Another interesting point, we examined the means for willingness by story for each study(See Figure 2). As you can see, with all three studies that the willingness to adopt 2FA for "Today" or the "near future" stories was largely from Somewhat Agree to Strongly Agree. The participants also responded with disagreement with the statement that they would never signing up for 2FA. There was some variability between each of the stories but nothing that was statistically significant. What we infer from this is that individuals were reporting that they learned from the story they read. However, we are less sure about why the willingness to adopt was so high for each stories as another alternative explanation is that regardless of conditions, participants understood that we wanted to teach them about the benefits of 2FA. While our stories seem to be effective in encouraging individuals to adopt 2FA, we are less certain as to the mechanisms that individuals found persuasive that would encourage them to adopt.

CONCLUSION

Creating or modifying stories has proven to be no easy task but working with these stories has provided interesting insight into the security decision process of individuals. Across the three studies we found overall that the stories were effective in convincing users to be willing to adopt two-factor authentication. However, we were unable to identify the mechanisms that individuals resonated with. Our future work will continue to explore different mechanisms through stories and then monitor behavioral measures to see if actual adoption of 2FA occurs.

REFERENCES

[1] Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. 2017. A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA). *International Journal of*

Human Computer Interaction 33, 11 (2017), 927–942.

[2] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. 2018. "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA.

[3] Noah J. Goldstein, Robert B. Cialdini, and Vladas Griskevicius. 2008. A Room with a Viewpoint: Using Social Norms to Motivate Environmental Conservation in Hotels. *Journal of Consumer Research* 35, 3 (2008), 472–482.

[4] Eric Grosse and Mayank Upadhyay. 2013. Authentication at Scale. *IEEE Security and Privacy* 11 (2013), 15–22.

[5] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories As Informal Lessons About Security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA.

[6] Elissa M Redmiles, Everest Liu, and Michelle L Mazurek. 2017. You Want Me To Do What? A Design Study of Two-Factor Authentication Messages. In *Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Santa Clara, CA.

[7] Rick Wash and Molly M. Cooper. 2018. Who Provides Phishing Training?: Facts, Stories, and People Like Me. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA.