Messaging Campaigns for Motivating Users to Adopt Duo at a University

Elham Al Qahtani
University of North Carolina Charlotte
Department of Software & Information Systems
Charlotte, NC 28223 USA
ealqahta@uncc.edu

Mohamed Shehab
University of North Carolina Charlotte
Department of Software & Information Systems
Charlotte, NC 28223 USA
mshehab@uncc.edu

Abstract

For exploring messaging campaigns that motivate users to adopt a new security behavior and affect their security decisions, we designed different informational videos asking users to adopt Duo Two-Factor Authentication (2FA) on their university account. These videos used five different communication techniques: authoritarian, logic, benefit, personal risk, and enterprise risk. During the first two weeks of the messaging campaigns, our preliminary results showed that the authoritarian video messaging was the highest in motivating users to enable Duo 2FA (20% of university employees enabled Duo 2FA on their university accounts) and the benefit video messaging was the second-most motivating video (17%) in adopting Duo 2FA.

Introduction

Organizations have witnessed data breaches, such as compromised personal information, database password leaks, or phishing attacks [6, 7, 9] that have directed them to apply Two-Factor Authentication (2FA) [3]. Adding 2FA as an extra layer of protection reduces security risks in the organization and prevents unauthorized access to technology. This additional factor can be something users obtain (e.g., a one-time use code provided through text), or something users have, such as a biometric (e.g., fingerprint).

However, the rate of adopting 2FA remains low despite the

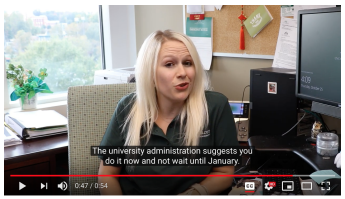

Figure 1: A frame from the authoritarian video content

prevalence of the acceptance of 2FA among security communities. Petsas et al. [8] showed the low rate of adoption for 2FA; based on the results, 6.4% of users enabled the 2FA on their Google accounts. Two studies [1, 2] addressed this challenge using video messages as a powerful motivation to affect users' security decisions for adopting 2FA. Preston [1] found that 31% of participants enabled 2FA within a week after they watched a fear appeal video, and Albayram et al. [2] found in the follow-up study that 27% of participants mentioned they enabled 2FA.

In our study, we designed different video messages (authoritarian, logic, benefit, personal risk, and enterprise risk) that test the effectiveness of different types of messages in videos from Information Technology Services (ITS) at our university, starting from November 26, 2018 to January 31, 2019. Also, we want to better understand the difficulties employees have with adopting Duo Two-Factor Authentication (2FA) in face-to-face information sessions. Our preliminary findings showed that both authoritarian and benefit video messages were effective in raising the adoption rate of Duo 2FA throughout the messaging campaign period.

Methodology

Our university required all university employees to use Duo 2FA service to access their university accounts by the end of January 2019. Therefore, we investigated the effectiveness of the ITS video messages (one example of video messages is shown in Figure 1) and explored the reasons behind users not installing Duo as required by the university. Six groups were included in our study design to investigate the effectiveness of the messaging campaigns as follows.

- Logic group: watched a video that includes the definition of Duo, the purpose of using Duo, due date (January 31, 2019), and motivated cue ("Why wait? It makes sense to do it now") [1]
- Authoritarian group: watched a video that includes the definition of Duo, purpose of using Duo, due date (January 31, 2019), and motivated cue ("The university administration suggests you do it now and not wait until January") [2]
- Benefit group: watched a video that includes the definition of Duo, purpose of using Duo, due date (January 31, 2019), and motivated cue ("The benefit of using Duo is that you will only have to change your password once a year instead of every 90 days...Do not wait till January to enjoy the benefits of improving your security") [3]
- Personal risk group: watched a video that includes the definition of Duo, purpose of using Duo, due date (January 31, 2019), and motivated cue ("If your account is compromised this may provide access to your inbox, and embarrassing emails could be sent to your contacts...Do not wait till January to protect your information") [4]
- Enterprise risk group: watched a video that includes the definition of Duo, the purpose of using Duo, due date (January 31, 2019), and motivated cue ("If your account is compromised, then this sensitive information may be exposed and misused in many different ways. This may affect not only your reputation

[1] https://www.youtube.com/watch?v=Qk8YO3BMbbY
[2] https://www.youtube.com/watch?v=cIM9WnChGU0
[3] https://www.youtube.com/watch?v=zD2H1dn1gxM
[4] https://www.youtube.com/watch?v=ps-oykvSPUw

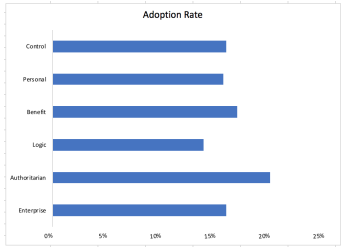

Figure 2: The adoption rate of Duo 2FA for all groups

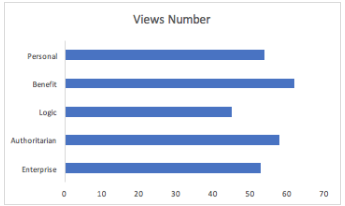

Figure 3: Views number for each group

but also other employees, students, and the university...Do not wait till January to improve the security of your accounts") [5]

- Control group was not shown any video.

The video messages were inspired by the context of selecting a rational choice that influences users' security decisions and users' risk perceptions [2]. Herely [5] mentioned the leading cause of following the recommended security behavior is weighing the costs against the benefits for security actions, which impact the user's security decision (e.g., when a user rejects the security action due to the decision of weighing the cost that is too high and/or the benefit is too low). Also, perceiving the negative risks plays a vital role in users' security decisions. For example, Harbach et al. [4] investigated motivation cues of presenting the user's personal information to alter users' risk perceptions of the possible risks on their data when they are authorizing the android permissions. They found that including these cues altered users' risk perceptions to make the right security decision. Based on the factors of perceived costs, benefits, and risks that affect users' security decisions, we created the motivation cues for each video message in our study.

Our study had two phases that ran from November 26, 2018 to January 31, 2019. The first phase was that ITS sent email messaging campaigns randomly to each group of university employees who had not installed Duo on their accounts. The second phase was face-to-face information sessions, which were conducted before the end of January 2019 and aimed to understand the factors that resulted in employees deciding not to adopt Duo 2FA. ITS sent an email to invite university employees and staff who had not enabled Duo 2FA to attend the information sessions which were 15 minutes long. During the information session, participants were asked to watch a video that was assigned to the same group and to complete a video evaluation survey and to gather their opinions about using Duo. Finally, participants could ask questions regarding using Duo 2FA at the end of the session.

The recruitment was provided by ITS through emails. They recruited 1955 university employees who did not install Duo 2FA previously. ITS randomly assigned 319 of university employees to the authoritarian group, 324 to the logic group, 328 to the benefit group, 312 to the personal group, 353 to the enterprise group, and 319 to the control group. Our study was approved by our university Institutional Review Board (Study #18-0465).

Results

The findings from the first phase of our study indicated the duration of Duo 2FA enrollments and selected device types for the authentication. These results were handled by ITS and taken from the Duo 2FA portal. We found that the adoption rate of Duo 2FA in the authoritarian group from the messaging campaigns (Figure 2) started in the first two weeks was 20%. Also, in the same duration, it was the highest effective video message compared to other groups: 17% of university employees in the benefit group, 16% in both enterprise and control groups, 15.71% in the personal group, and 13.89% in the logic group. Figure 3 represents the number of employees who watched video messages in the beginning of the messaging campaigns.

After this period, the adoption rate of Duo 2FA increased for all groups until the last day of January 31, 2019. Figure 4 displays the distribution of data for Duo 2FA adoption throughout the messaging campaigns. The authoritarian video had the highest effectiveness in motivating univer-

[5] https://www.youtube.com/watch?v=nMIygQFJzFU

sity employees, and the benefit video was the second-most effective in adopting Duo 2FA on their university accounts compared to other groups during the duration of the massaging campaigns.

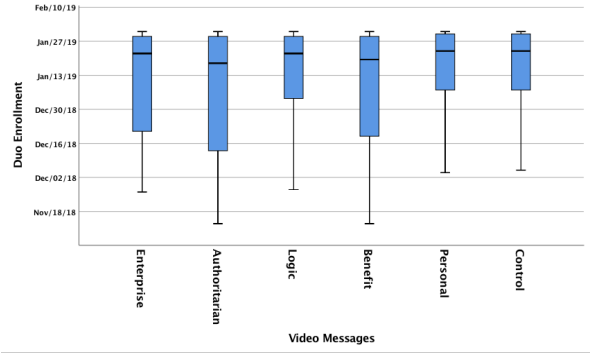

Figure 4: The duration of duo enrollment for all groups

Regarding the device type for Duo authentication, we found that 86.8% of university employees chose mobile devices to authenticate their university accounts, 7.1% chose fob, and 6.1% chose land-line or phone.

The second phase of our study was designed for university employees who have not enabled Duo 2FA to investigate their feedback regarding their 2FA experience and better understand their reasons in a face-to-face information session. We are currently analyzing the participants' feedback. The preliminary results are still being analyzed and we are currently extending the study to solicit feedback from all participants with regards to the effectiveness and engagement of the video messages.

Discussion

We found that both authoritarian and benefit videos were the most effective in motivating university employees to adopt Duo 2FA on their university accounts compared to other groups once the messaging campaigns started.

In the authoritarian group, university employees followed the authority (university administration) suggestion for enabling Duo 2FA on their accounts, and the motivated cue included in this video was: "The university administration suggests you do it now and not wait until January." The authoritarian video message helped university employees to make their security decision effectively compared to other video messages. Regarding the benefit group, university employees valued using Duo 2FA on their accounts because of the benefit, which was changing the password will be once a year instead of every 90 days. Perceiving this benefit affected their decision for adopting Duo 2FA on their university accounts.

Conclusion and Future Work

For testing the effectiveness of different types of ITS messages in videos, we designed different video messages (authoritarian, logic, benefit, personal risk, and enterprise risk) to motivate university employees to enable Duo 2FA on their university accounts. Results showed, during the first two weeks once the messaging campaigns started, that the adoption rate for Duo 2FA in the authoritarian group was the highest compared to other video messages (20% of university employees enabled Duo 2FA). Also, the benefit video message was the second-most motivated video (17% of university employees adopted Duo 2FA). During the remainder of the campaigns, both videos still motivated employees' behaviors. We will examine their perceptions about Duo 2FA and the video evaluation based on the same videos that were assigned in this study.

REFERENCES

1. Preston Ackerman. 2014. Impediments to adoption of two-factor authentication by home end-users. *SANS Institute InfoSec Reading Room* (2014).
2. 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.
3. Josh Davis. 2018. "List of websites and whether or not they support 2FA". twofactorauth.org. (2018). Retrieved May, 2019 from `https://twofactorauth.org/`.
4. Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 2647–2656.
5. Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*. ACM, 133–144.
6. Tracy Kitten. 2012. "LinkedIn: Hashed Passwords Breached". inforisktoday.com. (June 2012). Retrieved May, 2019 from `https://tinyurl.com/y2oqkxyx`.
7. David McCandless. 2019. "World's Biggest Data Breaches Hacks". informationisbeautiful.net. (April 2019). Retrieved May, 2019 from `https://tinyurl.com/ycho2xx4`.
8. Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2015. Two-factor authentication: is the world ready?: quantifying 2FA adoption. In *Proceedings of the eighth european workshop on system security*. ACM, 4.
9. Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. " I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 123–140.