Poster: "I Have Nothing to Protect": Understanding the Factors of Adoption of 2FA in Social Media

Yeeun Jo[1], Margie Ruffin[1], Mahnoor Jameel[1], and Camille Cobb[1]

[1]*Computer Science, University of Illinois Urbana-Champaign*
{yeeunjo2, mruffin2, mjameel2, camillec}@illinois.edu

***Abstract*—Understanding the challenges in implementing and improving 2FA for social media platforms is important. To understand the usability and perceptions of 2FA on these platforms, we conducted an interview study where participants conducted tasks of setting up 2FA on a popular social media platform and logging in using this method. We found most users were confident in setting up 2FA as they have learned by setting it up on university accounts and using it to log in daily. We found factors such as self-efficacy, past experience, past behavior, knowledge of costs, and users' awareness of risks and context may influence the adoption of 2FA. Our study result suggests that even with improvements to the usability and effectiveness of 2FA security mechanisms, more things are needed to motivate people to adopt it.**

***Index Terms*—Security Behavior, 2-Factor Authentication, Perception, Usability, Interview Study**

I. Introduction

Social media platforms are vulnerable to security threats such as hacking, phishing, and identity theft [8]. Because of this, popular platforms like Facebook, Instagram, etc., are now offering Two-Factor Authentication (2FA) as an additional security mechanism to secure user accounts [3]. Many people are still hesitant to enable 2FA even though platforms encourage users to be proactive in securing their accounts [2].

A deeper understanding of the true reasons users do not adopt 2FA is essential to increase its acceptance. Users' adoption behavior may be influenced by a number of matters. It might be because people tend to disregard security advice when it is inconvenient or inefficient, such as when setting up a 2FA [4], [7] and assume they are unable to obtain and effectively use information on online protection [9]. It might also not be usable for end users because of poor usability [1], [6]. Only a few studies have concentrated on analyzing users' perception of 2FA as it relates to their adoption of 2FA.

Our study aims to fill the gap by exploring the usability and perception of 2FA in social media platforms, in particular, Instagram. Our goal is to explore how easy it is for a layperson to set up and use 2FA and understand why or why not they may choose to adopt 2FA on their own social media accounts. We answer the following research questions:

- **RQ1**: How do the usability factors related to 2FA influence users' adoption decision of 2FA in social media?
- **RQ2**: How does user perception of 2FA influence their adoption decision of 2FA in social media?
- **RQ3**: What are users' rationality in adopting 2FA in social media?

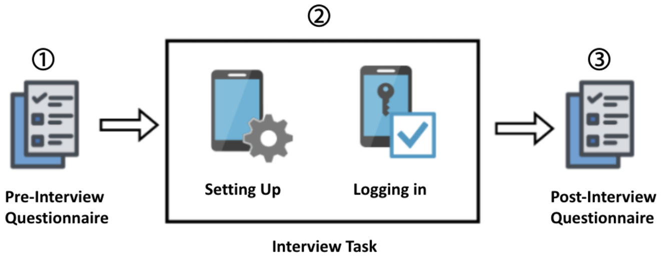

Fig. 1: **Study Methodology**—Our study contains three steps: pre-interview task, interview task. and post-interview task.

We answered these questions with in-person semi-structured interviews (N=6). In this study, we explore measures in the understanding of 2FA in social media. The quantitative (complementary) and qualitative (primary) investigation of those research questions serve as a basis for 1) to better understand how usable everyday people find this security mechanism in Instagram, 2) why they would or would not adopt it themselves, and 3) what would make them change their mind to adopt it in the future or on other platforms. More work is needed to generalize our results to a larger audience and to make our study effective across more platforms. Our research demonstrates the need to raise end users' awareness of the security risks associated with social media platforms, including information exposure and identity theft.

II. Study Method

To answer our research questions listed in Section I, We conduct a within-subject experiment using cognitive walk-through usability testing where participants set-up, use 2FA on a social media platform, and answer questions about the attitude perception, usability, and adoption of 2FA.

A. Pilot Study

The primary purpose of our pilot project is to undertake a small-scale preliminary investigation to discover factors influencing adoption choice and to use the findings to refine and guide the study design for a larger study.

Our pilot study contains three steps: ❶, participants consider 2FA in general and answer two questions about confidence in setting it up and willingness to adopt it. ❷, participants complete a two-step task: Setting up 2FA on Instagram and then logging into the same account with it enabled. ❸, we asked questions regarding participants' understanding of and

Participant	2FA Setup (s)	Login w/ 2FA (s)	Completed?
P1	248	40	Yes
P2	155	27	Yes
P3	201	56	Yes
P4	287	16	Yes
P5	220	15	Yes
P6	77	20	Yes

TABLE I: **Usability Results**—Usability of 2FA in Instagram based on efficiency (the time it took for participants to set up 2FA and use it) and effectiveness (participants' ability to complete the given task).

feelings toward 2FA as well as their confidence and desire to adopt 2FA and gathered demographic information. Figure 1 shows the study process from the participants' perspective.

B. Recruitment and Ethics

This study was reviewed and approved by institutional review board. We recruited participants via word of mouth and by posting flyers around the University between November and December 2022. We recruited 6 participants for the pilot study that were over the age of 18 and had not previously set up 2-Factor Authentication on the social media apps. The survey took a median of 30 minutes to complete, each participant signed written informed consent and was compensated $15.00 for their time.

C. Limitations

Due to our recruitment pool, our study included participants that have more experience in technology, familiar with 2FA, and have experienced setting 2FA in university portal services. Users with low levels of technology literacy may rate usability and self-efficacy components less favorably, which would alter the findings of the study.

D. Data Analysis

In our study, to understand the usability, we measured the number of seconds participants took to set up 2FA using the provided device and a faux Instagram account and measured how long it took for participants to use 2FA (i.e., log into the account with it enabled). We also conducted an inductive thematic analysis [5].

III. Preliminary Results

In this section, we will narrate the preliminary findings of our interview study. We first outline the findings on usability of 2FA in social media and users' perception on 2FA in social media.

A. Quantitative Investigation on Usability of 2FA in Social Media

Effectiveness is defined as being able to complete a specified task using the system. As shown in Table I, the time it took participants to set up 2FA (in seconds) varied. On average, it took them 198 seconds, or about 3 minutes and 30 seconds, to complete the task. We found most users were confident in setting up 2FA as they have learned by setting it up on university accounts and using it to log in daily.

B. Qualitative Investigation on 2FA in Social Media

From the thematic analysis, we identified factors such as self-efficacy, negative past experience, past behavior, knowledge of costs, and users' awareness of risks and context may influence the adoption of 2FA. For instance, participants expressed that low usability will cause low adoption of 2FA for social media. Four participants explained that the high technical barrier for elders will make adopting 2FA difficult: *"Never using it would lead to not knowing. It is difficult, [I] assume getting exposed to a new technology probably would just make it difficult for my mom(P1)."* We also discovered that users are less likely to adopt 2FA when they don't value the information on their accounts. Participants were adamant that they would adopt 2FA in circumstances involving sensitive information. They stated they have nothing to protect on social media, but they also concurred that it will be increasingly vital to protect websites that exchange sensitive data, such as financial or communication details on bank or email accounts.

IV. Outlook

This is an unpublished in-progress work. While still work in progress, our pilot study already provides some first insights. All participants from our study showed end users may be reluctant to implement 2FA systems because they are unaware of the security risk. Moreover, we identified factors which may influence the adoption of 2FA in social media. More work is needed to generalize our results to a larger audience and to make our study effective across more platforms.

References

[1] Muhammad Adnan, Mike Just, Lynne Baillie, and Hilmi Gunes Kayacik. Investigating the work practices of network security professionals. *Information and Computer Security*, 23(3):347–367, 2015.

[2] Jessica Colnago, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, and Nicolas Christin. "it's not actually that horrible" exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–11, 2018.

[3] Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi. On the (in) security of mobile two-factor authentication. In *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18*, pages 365–383. Springer, 2014.

[4] Michael Fagan and Mohammad Maifi Hasan Khan. Why do they do what they do? a study of what motivates users to (not) follow computer security advice. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security*, SOUPS '16, page 59–75, USA, 2016. USENIX Association.

[5] Greg Guest, Kathleen M MacQueen, and Emily E Namey. *Applied thematic analysis*. sage publications, 2011.

[6] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl. "i have no idea what i'm doing" - on the usability of deploying https. *Proceedings of the 26th USENIX Security Symposium*, Aug 2017.

[7] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How i learned to be secure: A census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 666–677, New York, NY, USA, 2016. Association for Computing Machinery.

[8] Tyler Reguly. Save the embarrassment: The value of two-factor authentication on social media.

[9] Nik Thompson, Tanya Jane McGill, and Xuequn Wang. "security begins at home": Determinants of home computer and mobile device security behavior. *Computers Security*, 70:376–391, 2017.