Towards Implementing Inclusive Authentication Technologies for Older Adults

Sanchari Das
Indiana University Bloomington

Andrew Kim
Indiana University Bloomington

Ben Jelen
Indiana University Bloomington

Joshua Streiff
Indiana University Bloomington

L. Jean Camp
Indiana University Bloomington

Lesa Huber
Indiana University Bloomington

Abstract

Two-factor authentication (2FA) provides protection for online accounts through efficient and highly robust access control. Adoption and usability, however, remain challenging for such security tools and technologies. Most current research on 2FA focuses on convenience samples of experts in the technology sector while neglecting non-experts. As older adults increasingly use everyday digital technologies, providing convenient means for them to protect their online data has become extremely crucial. To aid with this, we investigated the user experience of 2FA security tokens with ten older adults ($>$ 60 years) using surveys, semi-structured interviews, and a think-aloud protocol. Their limited adoption of the 2FA security token stems from its non-inclusive design, unclear instructions, lack of tangible benefits, and device dependencies. Hence, we propose design modifications and effective risk communication techniques to encourage 2FA adoption among organizations that are most invested in protecting older adults - such as retirement management funds, banking institutions, and health care organizations.

1 Introduction

Passwords are one of the most prolific methods of online authentication. However, in the wake of common cybersecurity attacks, such as phishing [11], online identity theft [2], and improvements in password cracking techniques [12], passwords have become increasingly vulnerable to both human and technical exploits. In order to reduce the risk of account breaches, two-factor authentication (2FA) is a security measure that can be added to provide an additional layer of identity verification. Despite the additional security benefits of 2FA, it remains relatively underutilized for personal usage. Many studies have shown that the non-adoption of 2FA stems from unclear instructions, lack of tool knowledge, inaccurate risk perception, and user overconfidence with their own security acumen [6, 15]. Das et al. have noted several usability issues with the Yubico Security Key and 2FA in general, where a lack of motivation to use the tools, along with confidence in their 'strong' password strategies, were cited as primary reasons for non-adoption [7]. However, these studies have often used a non-diverse population sample, focusing primarily on student participants.

Technological advancements have led to increased use of the Internet and digital devices by older adults [1]. Previous research has shown differences in risk perception between older adults and other populations [5, 10, 17]. Financial scams in particular are estimated to cause as much as \$36 billion loss [13] for older adults each year. For this reason, we investigated the usability of hardware security tokens for a more diverse and representative population of older adults ($>$ 60 years). To understand the challenges older adults encounter with 2FA tools, we analyzed the end user experience of registering and using the FIDO U2F Security Key (Figure 2) by implementing a think-aloud protocol, surveys, and semi-structured interviews.

Figure 1: YubiKey 5C Nano that fits USB-C computer ports

We investigated the registration of the 2FA security keys, online data risk perceptions of users, and participants' post-installation experiences. Additionally, we asked about other 2FA strategies that the participants adopted (if any). Non-inclusive designs and inadequate risk communication resulted in minimal adoption of authentication tools and technologies within our participant pool. Form factor and device compati-

Who Are You?! Adventures in Authentication (WAY) 2019.
August 11, 2019, Santa Clara, CA, USA.

bility were found to be crucial, as the participants acknowledged that the available security tokens that were compliant with tablets and smartphones have very small form factors, as shown in Figure 1. The larger security keys are device and browser (Google Chrome) dependent. We found that older adults are caught in a negative feedback loop, where lack of adoption prevents availability and vice versa. However, their concerns are straight-forward to overcome through channelized risk communication, clear instructions, proper installation and usage guidance, and usable security tool design, as mentioned in section 4.

Figure 2: Security Key by Yubico that supports U2F and FIDO2

2 Methods

We conducted a qualitative usability study of FIDO U2F Yubico Security Keys (Figure 2) to understand how older adults interact with 2FA security tools. We tested the usage behavior and risk perception of older adults by replicating and extending the study methodology of Das et al.'s work [7]. In that study, we tested the usability of hardware security tokens with university students by conducting surveys and a think-aloud procedure.

2.1 Study Design

We recruited participants through snowball sampling by advertising through flyers and word-of-mouth. The subjects were required to (i) be at least 60 years old, and (ii) have a personal mobile phone/tablet/laptop. Once selected, they filled out an online pre-survey, where they were asked questions about their computer and security expertise in order to identify differences in the technology proficiency of the subject pool. After the pre-survey, an in-person think-aloud protocol was conducted, where a participant was provided with the YubiKey and asked to register the key with their personal Gmail or social media account. During the think-aloud protocol, the participants described their actions while offering real-time explanations about their choices and reasoning.

Four participants did not have a Gmail account or did not want to set up 2FA with it, so they were asked to set up the YubiKey with their Facebook account instead. Facebook requires their users to associate their phone number to add security based or app based 2FA. One participant was unwilling to share their phone number with Facebook, so they set up the YubiKey with their Twitter account. Another participant was unable to access their personal Gmail or could not verify their identity from their phone number; thus, they used their work account, which supports security tokens. All participants were given set up instructions available on the Yubico website [1]. Specific instructions for Google/Facebook/Twitter integration were provided in the application list by Yubico.

Each participant was given a FIDO U2F Yubico Security Key, then asked to set up two-factor authentication with their key on their personal Gmail or social media account. During the setup process, participants were told to talk through their decision making with the interviewer. No guidance was given to participants by the interviewer during setup, unless help was specifically requested. All of our participants experienced challenges during the installation procedure and required the assistance of the researcher to move forward. After the setup was completed, the researcher asked the participants a series of open-ended questions about the Yubico Security Key, as outlined by Das et al. [7].

We specifically introduced the interview to the study protocol to ensure that participants were aware of the key functionality and its benefits, as well as ensure that they were able to remove the key from their account (if desired) to ensure that participants were not at risk of getting locked out of their own accounts. Immediately after the interview on the same day, the participants were provided with a short survey to understand their risk-perceptions related to online identity security and their immediate response to 2FA functionality and usage. The 2FA security keys were given to the participants as a token of appreciation for their participation. After the study was complete and before participants left, the primary researcher provided a walk through of how 2FA can be used for everyday life. We audio-recorded the interviews and the setup think-aloud process. All of the recordings were transcribed by researchers and stored in secure locations. Using these transcripts, further qualitative analysis was performed. The study was approved by the institution's ethical review board.

3 Findings and Discussions

We analyzed the qualitative data we collected to understand the detailed reasons for non-adoption or negative perception of 2FA usage in everyday life. For our qualitative analysis, we adopted the methodology of Das et al.'s work [8]. Our pre-screening survey evaluated the computer and security expertise among participants based on Rajivan et al. [14]. Figure 3 shows the computer and security expertise distribution among the participants. The calculation of security and computer expertise scores is shown in Figure 4. The majority of the participants had no experience with computer security, which was why many participants had security scores of 0. For computer knowledge questions, we asked participants

[1] https://www.yubico.com/

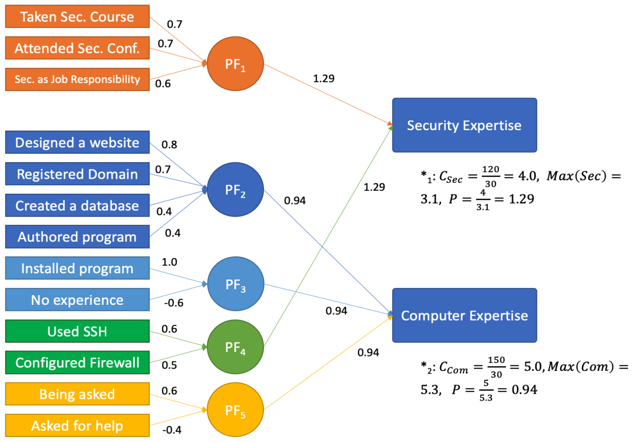

Figure 3: Computer and Security Expertise Score Calculation

about their experience with various technical tasks, such as designing a website or installing a computer program. We performed thematic coding [3, 4], where the pain points of the participants were categorized as Halt Points, Confusion Points, or Value Points. Every participant was assigned a researcher, who observed their behavior while registering the key with their Gmail or social media account. When a participant got stuck and required the intervention of the researcher associated with them, a *Halt Point* was identified. When a participant was confused but did not require the help of the researcher to move forward, a *Confusion Point* was indicated. We also noted several *Value Points*, which enabled us to provide actionable recommendations for improved tool design.

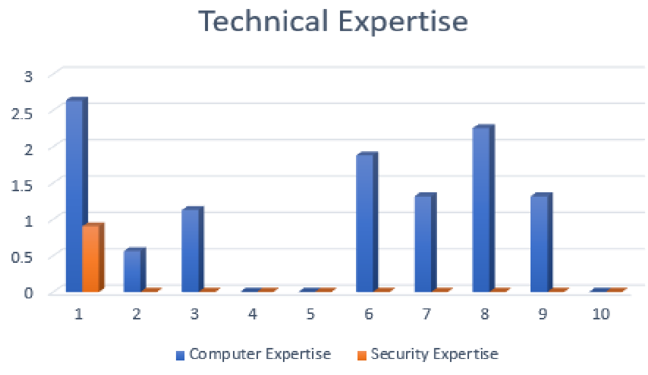

Figure 4: Computer and Security Expertise of the Participants

All of our participants experienced difficulty with registering the keys and took an average of 52 minutes to complete the study. This amount of time was longer compared to students in our pilot studies, who took an average of ten minutes to complete the setup following a similar protocol. Nearly all participants (nine out of ten) acknowledged that registering the keys was a complicated process, as most of the participants noted,

> *"...I would have given up long ago if I was not registering it with you (the associated researcher)..."*

3.1 Device Compatibility and Form Factor

Most of the participants in our subject pool only had a tablet or a personal desktop; they did not use a laptop for their online browsing. The YubiKey that we tested does not work with tablets or smartphones. We provided information about other Yubikeys such as near-field communication (NFC)-enabled YubiKeys, as well as security tokens that are compatible with USB-C ports. Our participants mentioned that the USB-C port key (Figure 1) has an extremely small form factor, which would make it difficult for them to use daily. Participants did not initially understand how to use NFC-enabled devices; however, once the process was explained to them, they acknowledged that they would prefer to use those keys if the instructions were better. They could then verify their identity through a wireless connection instead of having to plug a key into a USB port.

3.2 Facebook 2FA Issues

When registering their keys, four participants added 2FA to their Facebook accounts. They chose Facebook because they did not have a Gmail account, were worried about getting locked out of their own account, or wanted their social media account to be secure due to recent data breaches. Facebook recently made it compulsory for users to add their phone number to enable a second factor of authentication. One of the participants refused to provide their phone number to Facebook due to privacy concerns. Another participant tried to receive their verification code, but did not receive anything after repeated attempts due to a Facebook server error. They said:

> *"... I would have given up in the third attempt and returned the key to the seller. I might not be able to login to my own account if Facebook does not allow me to add the key in the first place..."*

3.3 Browser Incompatibility

Yubico U2F protocol-enabled keys only work with Google Chrome version 38 or later or Opera version 40 or later. Five out of the ten participants tried to use other browsers, such as Safari, Mozilla Firefox, and Internet Explorer, where these keys would not work. Thus, they believed that the key was not functioning properly, and the researcher had to guide them to the correct browser. Browser requirements were only mentioned later in the instructions, which confused the participants.

3.4 Hidden and Unclear Instructions

Nine out of ten participants expressed frustration with finding the instructions on how to register the keys. Four of the participants watched the videos on the Yubico website and noted that the keys are useless if they cannot even register them. The instructions seemed verbose to the participants, who wanted a simpler interface where they do not need to go back and forth between instructions and account settings to register the keys. Yubico has changed their website, so that they redirect users to Google or Facebook instructions based on their preferred platform. The Yubico website also refers to these sites as "applications," which was an unfamiliar term to the participants. Participants demanded a clear, comprehensive explanation of the process and wished to know more about what they had to do. In addition, when unexpected errors occurred, they were unable to recover from them, and they requested additional instructions.

3.5 Incorrect Settings

Six out of ten participants went to their device settings or browser settings instead of their account settings, again stemming from unclear instructions. Two of the participants who understood that they needed to go to their account settings could not find the Facebook account settings in their profile and required the help of the researchers to guide them. Participants found this frustrating, and they wanted screenshots or app simulations to guide them through the procedure without making them read through the instructions.

3.6 Issues Plugging in the Key

Participants demonstrated confusion when plugging the Yubico key into the USB ports. The most frequent problem was choosing when to plug in the key, as participants inserted it before it was registered. Users also experienced confusion while naming the security key, which was asked for by Google for Gmail accounts. Older adult users were expected to provide a pseudonym for their security tokens. Additionally, subjects were confused about the correct orientation of the key due to its design, which allows a key to be inserted upside down despite the fact that it must be right-side up in order to function correctly.

4 Implications

Our study found that the FIDO key technology, as implemented with the Yubikey, was a poor match for older adults. It did not cater to their existing technology, and it failed to address their needs and risk perceptions. We encourage confirming registration and clearly communicating the risks of not using 2FA to improve older adults' online security.

4.1 Confirmation of Registration

Adding a page that confirms the registration is a simple design change, but it can be effective in enhancing the user experience. After completing the registration, the participants were not sure whether the registration procedure was complete or not. Due to the key's form factor, they expected that they could use the *Safely Remove Drive* option as they usually do for the USB flash memory sticks. They wanted a clear confirmation, such as a congratulatory message. Most of the participants noted that they would log out and log back in again to check if their key was successfully registered. However, some of the elderly users responded that they would rather not confirm the registration, since they did not want to go through the complicated process again.

4.2 Communicating the Risks

Risk perception is based on our instincts and the information provided to us; it has a strong role in our decision making process [16]. Thus, for computer security threats, we need to communicate the benefits of 2FA adoption and the risk trade-offs of non-adoption to older adult users. If users cannot perceive the severity of their inaction, they will not be aware of any potential adverse consequences [9].

Our participants did not perceive their email as being at risk, nor did they understand the risk implications of a compromised email account. Only after it was explained to participants how emails are used to reset other account passwords, did the participants understand the technical risk. Still, they did not view themselves as at risk, despite being a common target for criminal activity. In addition, participants did not experience or realize the advantages of 2FA. Older adult users responded that it felt unnecessary to keep track of another authentication factor, since their passwords were already secure enough. Some users indicated that 2FA was useless to them because they used password managers or believed that their data could not be breached. Risk communication, which is critical to encourage effective security practices, was missing.

5 Limitations and Future Work

Studying a representative sample of diverse older adults, rather than a convenience sample of younger adults, is critical to designing effective and acceptable solutions. Older adults are an important population with an increasing online presence. Therefore, it is crucial for us to develop usable security tools to support their needs. Our work addresses the lack of studies focusing on the online security of older adults, particularly regarding their authentication strategies. We explored their 2FA usage and adoption issues and provide actionable recommendations to improve it. We acknowledge that individuals can have different experiences with different types of accounts, such as email and social media, which cannot be generalized. However, a comparison of different accounts provides us with problem points that can be addressed at the application level to improve security for all. As a future extension, we intend to conduct a timeline-based analysis of users' continuous usage/non-usage of the security tokens. We also plan to apply different types of risk communication strategies (graphical and/or textual) to gauge their effectiveness on elderly users' risk perceptions. In future research direction we will subdivide the subject pool by age to provide more granular analysis.

Acknowledgment

This research was supported in part by the National Science Foundation under CNS 1565375, Cisco Research Support, and the Comcast Innovation Fund. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the the US Government, the National Science Foundation, Cisco, Comcast, nor Indiana University. We would like to acknowledge the assistance of Ebuka Egbunam, Kiarra Pratchett, Sabrina Sanchez, and HyeonJung Lee for helping us with the data collection and transcription. We would also like to thank our participants for their valuable data, which helped us in generating the recommendations.

References

[1] Monica Anderson and Andrew Perrin. Technology use among seniors. *Washington, DC: Pew Research Center for Internet & Technology*, 2017.

[2] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web*, pages 551–560. ACM, 2009.

[3] Richard E Boyatzis. *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.

[4] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[5] Jean Camp and Kay Connelly. Beyond consent: privacy in ubiquitous computing (ubicomp). *Digital privacy: Theory, technologies, and practices*, pages 327–343, 2008.

[6] 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*, page 456. ACM, 2018.

[7] Sanchari Das, Andrew Dingman, and L Jean Camp. Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In *2018 International Conference on Financial Cryptography and Data Security (FC)*, 2018.

[8] Sanchari Das, Gianpaolo Russo, Andrew C Dingman, Jayati Dev, Olivia Kenny, and L Jean Camp. A qualitative study on usability and acceptability of yubico security key. In *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*, pages 28–39. ACM, 2018.

[9] Nicola Davinson and Elizabeth Sillence. It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, 26(6):1739–1747, 2010.

[10] Vaibhav Garg, L Jean Camp, Lesa Mae, and Katherine Connelly. Designing risk communication for older adults. In *Symposium on Usable Privacy and Security (SOUPS)*. Citeseer, 2011.

[11] Jason Hong. The state of phishing attacks. *Commun. ACM*, 55(1):74–81, 2012.

[12] Simon Marechal. Advances in password cracking. *Journal in computer virology*, 4(1):73–81, 2008.

[13] Laurie Orlav and True Link Financial. The true link report on elder financial abuse 2015. Technical report.

[14] Prashanth Rajivan, Pablo Moriano, Timothy Kelley, and L Jean Camp. Factors in an end user security expertise instrument. *Information Computer Security*, 25(2):190–205, 2017.

[15] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. A tale of two studies: The best and worst of yubikey usability. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 872–888. IEEE, 2018.

[16] Paul Slovic and Ellen Peters. Risk perception and affect. *Current directions in psychological science*, 15(6):322–325, 2006.

[17] Sherry L Willis and K Warner Schaie. Cognitive training and plasticity: theoretical perspective and methodological consequences. *Restorative neurology and neuroscience*, 27(5):375–389, 2009.