Non-Inclusive Online Security: Older Adults' Experience with Two-Factor Authentication

Sanchari Das
University of Denver
Sanchari.Das@du.edu

Andrew Kim
Indiana University
anykim@indiana.edu

Ben Jelen
Indiana University
bcjelen@indiana.edu

Lesa Huber
Indiana University
lehuber@indiana.edu

L. Jean Camp
Indiana University
ljcamp@indiana.edu

Abstract

Older adults access critical resources online, including bank, retirement, and health insurance accounts. Thus, it is necessary to protect their accounts so they can confidently use these services that are increasingly being moved online. Two-factor authentication (2FA) protects online assets through efficient and robust authentication, but adoption and usability remain a challenge. Our in-depth qualitative research focuses on ten older adults' (≥ 60 years) sustained (non)usage of 2FA for thirty days. Participants' limited adoption of the security keys stemmed from keys' non-inclusive design, lack of tangible benefits, inconsistent instructions, and device dependencies. We propose appropriate assistance, risk communication, registration process changes, and alignment of security-focused requirements to encourage 2FA adoption among older adults and institutions entrusted with their data. We also introduce the concept of 'Security Caregivers,' who can ensure security and digital independence for the aging population.

1. Introduction

By 2030, more than 20% of the US population will be 65 years old or older [1], and by 2050, nearly 17% of the world population will consist of older adults [2]. Additionally, older adults have increased their use of the Internet and everyday digital devices [3]. However, while many digital tools and equipment for older adults are being developed, the rate of adoption is low despite the potential benefits [4]. Additionally, security threats are inherently bundled with those convenience benefits, and older adults are disproportionately targeted [5].

Older adults' risk perception differs significantly from non-older adult populations in digital and physical domains (e.g., [6, 7]). To provide better and more effective solutions, we investigated the usability of hardware security tokens for older adults (≥ 60 years). To understand the challenges they encountered with 2FA tools, we studied their experiences with registering and using a hardware token (Figure 1) by implementing a think-aloud protocol, surveys, and a semi-structured interview. We also captured their ongoing usage experience by conducting a follow-up survey (one month after the original experiment). We particularly examine the following research questions:

Figure 1. Security Key by Yubico that supports U2F and FIDO2

1. What factors contribute to older adults' negative perception/non-adoption of 2FA?
2. What factors could facilitate adoption of 2FA by older adults?

To answer this, we focused on older adults' perceptions of risks related to online identity security, their immediate response to 2FA functionality and usage, 2FA design flaws contributing to non-adoption by older adults, the typical pain points that older adults experience as they try to use 2FA, and the technical expertise/cognitive plasticity older adults might need in using 2FA. Our investigation of 2FA tokens found that non-inclusive design and inadequate risk communication resulted in minimal adoption by our older adult participants.

2. Authentication

Authentication is the verification of identity that proves the right to access an asset or service [8]. Traditionally, authentication has three possible factors: what someone knows, what someone has, and what someone is. These correspond to passwords and personal identification numbers (PINs), physical devices, and biometrics, respectively. Passwords are the most widely used authentication method, though they have been proven to be vulnerable to a wide range of attacks [9, 10]. As a solution, two-factor authentication technologies provide an additional method for identity verification beyond the factor of "what someone knows," (i.e. password) to improve data security [11].

URI: https://hdl.handle.net/10125/71399
978-0-9981331-4-0

3. Related Work

Usability of 2FA has been found to be challenging by many security practitioners and researchers. Das et al., for instance, noted several usability issues with the Yubico Security Key and 2FA in general, where a lack of motivation to use the tools, along with users' confidence in their 'strong' password strategies, were cited as primary reasons for non-adoption [12]. Their study showed that improvement in website design and clarity of instructions significantly improved the user experience of their participants. Here, we summarize similar works.

3.1. User Experience Issues with 2FA

Security tools often have usability and accessibility limitations. These can be exacerbated by a lack of user-friendly terminology or appropriate visual cues [13]. Research has illustrated that misaligned risk perception and usability issues result in negative experiences with 2FA tools and technologies [12, 14, 15, 16, 17]. For example, Braz et al. pointed out that straightforward changes in an interface's design will impact users' overall experience with 2FA [18]. Reynolds et al. studied the Yubico Security Key, focusing on 2FA usability with desktop and web applications. They identified significant user failures in a majority of U2F applications, specifically during the on-boarding (also called enrollment or setup) procedures [19]. Colnago et al. studied the user experience of 2FA among university students and suggested implementation improvements for improving user adoption [20]. In addition to ease of enrollment and usability, researchers have identified how 2FA solutions can impinge self-efficacy and hinder instrumental activities of daily living [21]. These studies have been helpful in understanding the user perspective on 2FA tools; however, they have mostly focused on convenience samples.

3.2. Challenges of IT Adoption

Prior research has investigated the adoption (acceptance and diffusion [22]) of new technologies (or lack thereof) among the general population [23]. Davis described two characteristics of a technical innovation that could predict its adoption among users: perceived ease of use and perceived usefulness [24]. When it comes to technology adoption among older adults, the perceived usability of the tool is particularly critical. Barnard et al. noted that older adults are open to learning new technology when the "learning pains" are not overwhelming and that the social environment the adult is in plays an important role in encouraging or discouraging this learning [25].

3.3. Varied Risk Perception

Users may have differing perceptions of similar online threats; thus, it is critical to study diverse populations [26, 27]. However, a majority of human subject studies in computer security have focused on convenience samples of university students, often in computer science [28]. Research has shown that risk perception for security and privacy is a function of age, technical expertise, and other demographics which are not necessarily represented among computer science students [29, 30]. For example, a 2017 study showed a correlation between security knowledge and security behavior from a study of 898 participants and their security practices [30]. Also, examinations of browser use have illustrated that expertise level is a strong determinant of security usage patterns [29].

3.4. Authentication Security for Older Adults

Supporting older adults' authentication security is a relatively unexplored arena, but human-computer interaction (HCI) security researchers have shown strategies that are effective for older adults. Fisk et al. focused on designing various technologies for older adults, where the learning curve is often greater due to the shift in cognitive ability as people age [31]. Older adults' cognitive capabilities change over time, making some security strengthening methods challenging [32, 33, 34]. Researchers have turned to methods such as graphical passwords to more specifically support them [35, 36]. Nicholson et al. found that younger participants performed better than older adults when using picture-based passwords, but the older adults performed significantly better when the pictures used age-appropriate faces [36]. Another challenge for older adults is that they may be less experienced with online risks, making them potentially more susceptible unless we use age-appropriate risk communication strategies [7, 37]. We sought to better support older adults' online security by studying their use of 2FA. Our study and analysis aids in understanding the everyday online authentication practices of older adults to better develop and design personalized security tools with an under-studied population in mind.

4. Methods

We recruited ten participants through snowball sampling by advertising through flyers and word-of-mouth. The subjects were required to (i) be at least 60 years old, (ii) have a personal mobile phone/tablet/laptop, and (iii) have a personal or work email or social media account. The participants who did not have any experience with computers or digital media of any kind could not participate in the study, since we evaluated the user experience with a hardware-based account authentication tool. Once selected, participants filled out an online pre-survey, where they were asked questions about their computer and security expertise to identify the technology proficiency of the subject pool. The expertise questions were based on previous research by Rajivan et al., who asked questions about user computer and security experiences to a sample of 890 participants [30]. After the pre-survey, an in-person think-aloud protocol was conducted. Every participant was provided with the YubiKey and asked to register the key with their personal Gmail or social media account. We selected the Yubico Security Key, given that it is one of the most widely used and implemented hardware-based security tokens [38]. The hardware token we choose was a Fast IDentity Online (FIDO)[1] Universal 2nd Factor (U2F) Security Key.

We first asked participants to set up the key with their online accounts, including email or social media. Four participants set it up with their Gmail account and one with their work email. Five participants did not have an email account that supported 2FA or did not want to set it up on their email, so they registered it with a social media account. Four of those five participants set it up with Facebook, and one chose Twitter since they did not want to share a required personal phone number with Facebook. During the setup procedure, we implemented the think-aloud protocol [39].

No guidance was given to participants by the interviewer during setup unless help was explicitly requested. All participants were given setup instructions available on the Yubico website[2]. Specific instructions for Google/Facebook/Twitter integration were provided in the application list. The participant who used their work account used the instructions provided by their organization. Every participant was assisted by the researcher (the first author) to provide assistance if needed. After the setup was complete, the researcher asked the participants a series of open-ended questions about their Yubico Security Key usage. We specifically introduced the interview to ensure that participants were aware of the critical functionality and benefits, as well as ensure that they were able to remove the key from their account if desired. Immediately after the interview on the same day, the participants were provided with a short survey to help us 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 walkthrough of how 2FA could be set up and integrated with other online accounts. Thirty days after completing the study, we sent the participants a follow-up survey to ask about their experiences with using or not using the keys with their online accounts. The institution's ethical review board approved the study.

4.1. Analysis and Coding

Similar to the study by Rajivan et al. [30], we calculated and generated the expertise calculation model through factor analysis. We calculated precision scores based on 30 replications done by Das et al. to obtain the computer and security scores [40]. We audio-recorded the interviews and the comments made by the participants during the think-aloud process. All of the recordings were transcribed by researchers and stored in secure locations. We further analyzed the transcripts through thematic coding [41, 42]. Three coders trained in qualitative coding[3] generated the codebook. The codebook consisted of *Halt Points, Confusion Points, and Value Points*.

Halt Points were noted when a participant got stuck and required the intervention of the researcher. *Confusion Points* occurred when a participant was confused but did not require the researcher's help to move forward. We also noted several *Value Points*, where participants provided direct feedback on the key or its setup process, enabling us to provide actionable recommendations for improved tool design. The coding was implemented with the transcription of the data, which had questions from the interview, the comments made by the participants during the think-aloud process, and observations noted by the primary researcher. Three coders initially took a sample of three interviews and coded them separately. The initial inter-coder reliability (ICR) was 72%. The three coders met and discussed the discrepancies and coded the same set of interviews again to obtain an ICR score of 89% [43]. After that, all researchers coded the interviews. If there was a discrepancy, the code was the one with the majority of votes (two out of three). If every coder coded different codes, all of the points were noted (this did not happen with the current data). Finally, we had another round of discussions to go over the codes. If there was a discrepancy that could not be agreed upon with discussion, the primary researcher made the final call.

4.2. Limitations

We acknowledge that individuals can have different experiences with different types of online accounts, such as email and social media, which cannot be generalized. However, we wanted to provide flexibility to the participants, since online authentication is needed for more than just email accounts, and some may not want 2FA on their email. Additionally, a comparison of different accounts provides us with problem points that

[1] https://www.yubico.com/authentication-standards/fido-u2f/

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

[3] https://www.coursera.org/learn/qualitative-methods

can be addressed at the application level of the YubiKeys to improve digital security.

5. Findings

We analyzed the qualitative data to understand the detailed reasons for participants' non-adoption or negative perception of 2FA. We found that older adults had several underlying reasons for choosing to use or not use 2FA, such as technical expertise, device incompatibility, misaligned mental models, and online accounts not supporting 2FA. In our study, all participants experienced challenges during the installation procedure and required the assistance of the researcher to move forward. Through our analysis, we found that older adults are driven by the tangible benefits that 2FA has to offer, such as increased protection against credential theft. These benefits are often not mentioned by 2FA tool developers or organizations that make 2FA usage mandatory [44].

5.1. Participants' Technical Expertise

Expertise is often a critical factor, especially when we are analyzing users' biases for choosing to adopt (or not adopt) a tool. A majority of the participants (nine out of ten) had no security experience, which was why many participants had security scores of zero. The one participant with some security experience took the least amount of time (14 minutes) to set up the Yubico security key and valued the benefits of using the security tokens. When asked about the purpose of the key, P1 said, *"Prevent anybody else from getting into my computer or accounts."*

Password Practices: To understand users' online data protection and authentication strategies, we focused on the most common method of authentication, i.e. passwords. We analyzed the password usage strategies adopted by the older adult participants, which previous research has shown differ considerably from those of their younger counterparts [45] (shown in Figure 5.1). Even for the participant who had some security experience, their password practices did not adhere to security standards. P1 said, *"...I last changed my password on July 2013..."* (when prompted by Google during the setup procedure).

The participants in our study often chose to write down passwords to remember them. Similar traits have been noted for many users who find it difficult to remember passwords [46, 47]. One of the participants used a password manager but still wrote down their passwords in case they got locked out of their password manager account. P7 mentions, *"...And then password manager, my husband and I share it. (We) write down unique passwords. In case one of us would (have to) navigate when one of us dies..."*

The sharing of credentials between the family members was also a common phenomena we found amongst our participants. As P9 noted, *"Oh, I may as well. Doesn't matter with this laptop. Nobody uses it but me. When I die, my grandkids, my son-in-law will be able to get in easier."*

On the other hand, one participant did acknowledge that writing down passwords is a bad practice, but their reasoning was more related to their fear of losing the paper where the passwords were written rather than any digital security threats. P3 mentions, *"If I wrote down the passwords, there's a good chance I may not remember where it's written. I don't like the invasiveness of biometrics."*

Other participants found other methods of 2FA, such as one-time passwords (OTPs), to be more helpful given their prolonged usage. As P2 notes, *"Security key might make sense to use once I learn how. I have used both verification codes sent by email and text occasionally. I have never used Duo, but I think I have an idea what it is. I have used security question a few times. I generally avoid biometrics."*

Our results confirm that the password habits of older adults do not reflect the habits seen in younger adults [20]. We return to these password habits when we discuss *Security Caregivers* in Section 6.

5.2. Registration Experience

Overall, every participant experienced difficulty while registering the key and took an average of 52 minutes to complete the study. Our pilot study with younger adults yielded results similar to those of Das et al., where participants took around 10-15 minutes using a similar think-aloud protocol to complete the study [12]. Nearly all participants (nine out of ten) acknowledged that registering the key was a complicated process, and P4 noted, *"...I would have given up long ago if I was not registering it with you [The associated researcher]..."*. Two of the participants were extremely disappointed with the experience and came back to the researchers to remove the keys from their account out of fear of being locked out of them. We noted several challenges participants encountered, which included identifying the type of their security token for setup and navigating to their account settings to add the keys.

Seven participants noted they would use the YubiKey to protect their bank account, six for their personal email, five for their shopping account, four for their work email, and six specified some other account. The "Other Accounts" included brokerage and retirement accounts, indicating the financial alignment of risks with their online data security. However, four of the participants thought their work email or personal email were not worth protecting with the security keys. As P5 mentioned, *"Used with brokerage account. Gives me peace of mind that brokerage account cannot be*

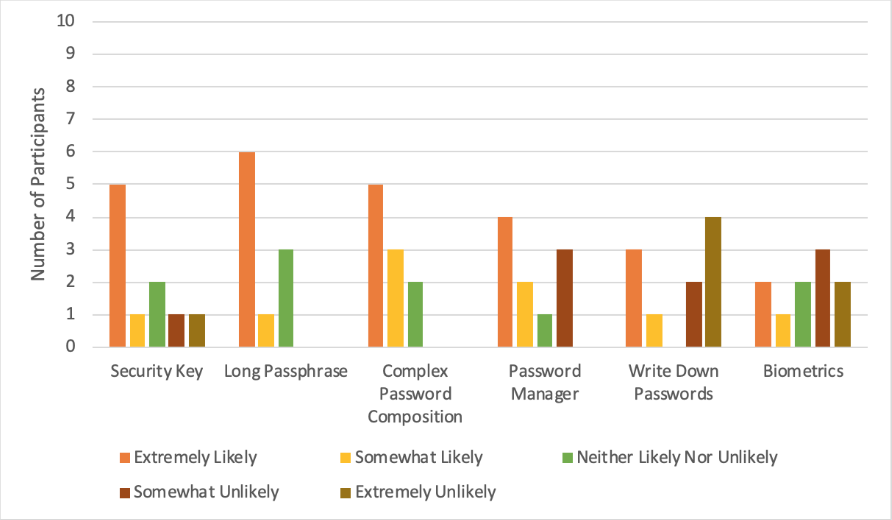

Figure 2. Password strategies adopted by participants. Extremely likely (left) indicates a strong intention to use the particular authentication technique.

accessed without using security key. My other accounts are less important, and they do not appear to have capability to accept security key." Sometimes, though a participant was interested in protecting their financial accounts, the technological limitation prevented the addition of a 2FA to their accounts. As P1 notes: *"...And then it has all my others so I typically log in, lets say to my X[bank name withheld] account by going to my password bank, clicking on X, and it logs me in. I need two-factor to protect my bank [account]."*

Device Compatibility and Form Factor: Most participants only had a tablet or a personal desktop; they did not use a laptop for 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. The participants mentioned that the USB-C port key 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.

Facebook 2FA Issues: In the process of registering the key for two-factor authentication, four participants used 2FA for their Facebook accounts. They chose Facebook because they did not have a Gmail, were worried about getting locked out of their email, or wanted their social media 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 participant refused to provide their phone number to Facebook due to privacy concerns. Another participant, P8, 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[sic] 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..."*

Browser Incompatibility: In addition to server issues from the service's perspective, we also found browser incompatibility issues with the YubiKey. Yubico U2F protocol-enabled keys only work for 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. 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. P9 realized that they were using the wrong browser: *"Would you (thinking aloud and interacting with Yubico) like me to use Chrome? I don't know that. I've got Firefox."*

Hidden and Unclear Instructions: Nine out of ten participants expressed frustration with finding the instructions on how to register the keys. Yubico provides the link to the instruction in the cover of the keys. Additionally, we provided the link to the instructions as well, yet the participants found finding the registration of the tool instructions difficult. Four participants watched the videos on the Yubico website. P7 mentioned that the video was helpful: *"So should I* *watch the video?... So helpful."*

Four participants noted that the keys were useless if they cannot even register them. The instructions seemed verbose to the participants, who wanted a simpler interface where they did not need to go back and forth between instructions and account settings to register the keys. P8 described their reaction: *"Oh my God I hate them (the instructions); they're such a pain in the backside."*

Yubico has designed their website to redirect participants to Google and Facebook instructions based on their preferred platform. The Yubico website also refers to these accounts as "applications," which was an unfamiliar term to the participants. They requested a clear, comprehensive understanding of the process and wished to know what more about what they had to do. In addition, when unexpected errors occurred, they were unable to recover from them on their own and requested further instructions. As P10 notes, they were confused how to use the key in the first place: *"First of all, I'm not quite sure how I use the key. Just be anytime I go to Facebook or while using Facebook I would insert this, or do I need to activate it..."*

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 the account settings, could not find the Facebook account settings in their profile and required the researcher's help. Participants found this frustrating, and they wanted screenshots or app assistance to guide them through the procedure without making them read through the instructions.

Issues Using the YubiKey: 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, and they did not understand why the YubiKey was blinking. Participants also experienced confusion when they were asked to provide a name for their key (recall that Yubico expects users to provide a pseudonym for their security tokens). Additionally, participants 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. The issue of orientation is inherently resolved with USB-C YubiKeys because those can be inserted either way. P3 questioned where the key was intended to go: *"Does it go there? I mean it looks thinner than a regular USB..."*

Some of the participants also did not understand when to press the gold button [4] or why the lights were blinking. P2 expressed confusion with this part: *"It's blinking. Okay, so that sounds like it's good. Press – wait a minute if the key is blinking, light press the button or gold disk. What the heck this? You're supposed to press that. Okay and then?"*

5.3. Ongoing Experience

Within 30 days of completing, we distributed a survey to the participants regarding their ongoing experience of the 2FA tokens, which we gave as a token of appreciation to the participants. Nine out of ten participants responded to the follow-up survey distributed a month later. Six had reported continued using of the keys and two of them did not. P1 mentioned: *"It doesn't work with Ubuntu [a distribution of the Linux operating system]. I do still have it and if I log into a public computer, I will probably use it."* P5 used the key for their brokerage account and were particularly happy to see that their online data was protected with an additional layer of security. They mentioned: *"Used with brokerage account. Gives me peace of mind that brokerage account cannot be accessed without using security key."*

One of the participants also met with the researchers and said that they really liked how the keys are easy to use. However, their registration process was hectic, and they noted that if they were unable to install the key, they would return it. This indicates that once the initial hurdles are over, the participants could utilize such security tools, and participants cared about their online data and security; however, inaccessible tools and technologies made that challenging. P10 described their understanding of the device: *"I'm not sure what it does... I assume keep somebody from hacking into my Facebook account... The more authentication required the better. So once I could register the key... from then on I have used that key to get into my Facebook account."* P6 mentioned the lack of Yubico integration with their service providers. Lack of instructions or internal disagreements between the corporations were another difficulty. They wrote: *"I'm not regularly using my Gmail account and haven't been able to get people to give me directions for using the YubiKey. Working on it. How hard it is to use the YubiKey with PeoplePC"* (Note: PeoplePC is another ISP).

6. Discussion and Implications

Through our study of 2FA with older adults, we identified several challenges with supporting older adults' digital independence by strengthening their online account security. The 2FA registration process was particularly challenging for participants, who took an average of 52 minutes to complete the registration process. This is considerably slower than prior work were participants (students) took an average of 10 minutes to complete the task [12, 48]. They all required

[4] This gold button is actually a capacitance sensor which is required by the user to touch when registering with or logging into a U2F site

assistance from the primary researcher to proceed and complete the process.

Our study found several interesting elements that will enable easier and more user-friendly 2FA adoption for older adults. Here, we address the *Halt, Confusion, and Value Points* with recommendations by analyzing the collected qualitative data and the surveys. When the participants required the researchers' assistance to proceed further and were halted completely, we marked it as *Halt Points*. Based on the transcription of the think-aloud protocol, we also found *Confusion Points* – various instances that did not prohibit the users from proceeding further in the registration but created confusion on how to use the keys. These negative experiences are a possibility, and thus, can lead to future rejection of the keys. During our analysis, we also found some interesting *Value Points*, which helped us generate recommendations to enhance the user experience and, in turn, their security behavior. We make the following recommendations to improve the user experience of 2FA and address the security component by studying online risk perspective.

6.1. Appropriate Assistance

Participants did not want to go back and forth with the instructions and were often lost trying to follow them. Appropriate assistance would provide step-by-step instructions integrated with the task at hand, rather than a wall of text one must return to repeatedly to enroll. Colnago et al. described users' positive reception of personalized privacy and security assistance when it comes to their technology devices [49]. Such assistance would help far more users than just older adults, illustrating that designing for everyone has broader benefits for users beyond the participants in our study. Similarly, the integration of password management with the YubiKey is not obvious during enrollment. One significant and immediate benefit of the YubiKey is that it can generate and store passwords. We did not ask our participants to specifically use the password-management feature of the YubiKeys; however, none of the participants inquired about or seemed to be aware of this feature, even though the instructions on the Yubico website mention it. Once researchers performed a walkthrough of the keys, participants confirmed their understanding of the general benefits of using 2FA. They also acknowledged that app-based authentication tools are dependent on having a smartphone readily accessible. Participants mentioned that they could use the keys without worrying about their phones. Thus, providing an additional 2FA tool that is device-independent is beneficial for users. However, the participants would have abandoned enrollment without the research team.

6.2. Communicating Risks

Risk communication, which is critical to encourage effective security practices, was missing [50]. Risk perception is based on people's instincts and the information provided to them; it has a strong role in our decision making process [51, 52]. Thus, for computer security threats, we need to communicate the benefits of 2FA adoption and the risk trade-offs of non-adoption to users. If users cannot perceive the severity of their inaction, they will not be aware of any existing security vulnerabilities that can have adverse consequences [53]. Participants in our study understood in general terms that email can be at risk, but they did not perceive that theirs was, nor did they understand the risk implications of a compromised email account at the beginning of the experiment. Only after researchers explained to participants how emails are used to reset other account passwords, did they understand the technical risk. In addition, participants did not experience or realize the advantages of 2FA.

6.3. 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 they could use the safe removal of the device, as with USB flash memory sticks. Also, Finkle et al. shows the importance of confirmation of registration a way of users being aware of the successful completion of the registration operation [54]. Currently, not only is there no positive feedback, there is no indication at all. Most of the participants determined that they were required to log out and log back in again to check if their key was successfully registered. However, even this may be inadequate; after initial enrollment, a machine might be trusted (i.e., not require a 2FA login) either until it is made explicitly untrusted or for some period of time.

6.4. Misalignment of Requirements

The YubiKey is an effective tool for protecting software and network systems that have U2F implementations [55]. However, some of the responsibility for enhancing people's security falls on the shoulders of industry. Study participants showed a strong preference for local Internet Service Providers (ISPs) and the associated emails. Sadly, these smaller, local ISPs have a low rate of U2F/FIDO key integration, so the keys were not usable with their primary email accounts – the accounts most in need of protection. Participants indicated that their main security concerns were their bank and brokerage accounts. P1 noted, they were limited by the technological capability of their financial institution on adding 2FA to protect their account. Similar to how participants used local ISPs, participants also preferred local credit unions for banking. All of the participants associated risks with their financial accounts rather than their other online accounts. Such tools should work with organizations, such as banking institutions, retirement organizations, and others, to enable 2FA.

6.5. Security Caregivers

In our study, older adults trusted the researcher to assist them when they reached Halt Points. Just as older adults need and trust caregivers for assistance with instrumental activities of daily living [21, 56], assistance with evolving tools and processes to assure online security would help them stay secure and maintain their digital independence. We introduce the role of *Security Caregivers* and argue for future work to explore the responsibilities, authorization, and limitations of *Security Caregivers*. We envision *Security Caregivers* to be less available than an IT helpdesk and much less powerful than a person with the power of attorney. A *Security Caregiver* would prioritize the best interests of the older adult, be a recognized member of the caregiving team, and have expertise in digital security.

The specific need for human *Security Caregivers* was found in how participants valued human interaction with the local phone company (see Section 6.4). In addition, *Security Caregivers* would address recovery requirements and provide back-ups, with assistance in password management tools. The range of solutions participants used to manage passwords illustrates that this task places extra cognitive burden on people (Section 5.1) (password creation and recall is not needed with a YubiKey integrated with LastPass[5]). In addition, *Security Caregivers* can address the chronic security weakness of 'security questions', the answers to many of which can be guessed from public information. This would mitigate password loss and provide continuity of access. With currently available technology, this can be implemented with physical ownership of a back-up YubiKey. Recall that a single account can be associated with multiple keys, so this would address concerns about account access loss and recovery. In technical terms, we envision leveraging the integration of password managers on YubiKeys, with two to five keys enrolled as password managers but only the elders' specific hardware recognized by default. That is, if an additional YubiKey is used there is notification sent to the user and possibly other caregivers.

7. Future Work

As an extension of this work, we intend to apply risk communication strategies (graphical and/or textual) to gauge their effectiveness on older adults' risk perceptions. We intend to extend this study through a quantitative research approach. We will try to understand the risk perception of older adults and then test the efficacy of our proposed solutions, including appropriate assistive design, age-friendly instructions, and availability of *Security Caregivers*. Through continued testing of design modifications, easy to understand and regularly updated instructions, hands-on assistance, and risk communication strategies, we aim to ensure that aging adults will have an available toolkit to maintain security, stay online, and stay engaged. Additionally, we want to extend the study into comparing different types of Yubico security tokens to understand the effectiveness of the different models.

8. Conclusion

Older adults face evolving security risks to digital independence through attacks such as phishing, identity theft, and medical fraud [57, 58, 59]. As such, researchers must develop user-friendly, fail-safe security tools to support the aging population. We conducted a think-aloud experiment with ten older adult participants to investigate the usability of the YubiKey and address a gap in research by focusing on older adults' online security. We found numerous challenges to the successful use of 2FA by older adults: (1) they were unable to install it, (2) they did not understand the purpose or process, (3) the security tool did not fit their needs, (4) their place of employment did not support the tool and/or they did not receive 2FA training at work, and (5) there is not currently a service or program that assists with digital security for older adults. We have provided actionable recommendations to address these issues, including improving the form factor, creating age-friendly instructions, informing institutions and organizations serving older adults about the need for 2FA, and providing appropriate assistance to support 2FA installation and use. We introduce the concept of *Security Caregivers* as a way to help older adults with the adoption and use of evolving security tools to ensure digital independence.

Acknowledgement

We would like to thank Joshua Streiff for his help with the data collection. We would also like to acknowledge the Secure and Privacy Research in New-Age Technology (SPRINT) Lab at the University of Denver and the Human and Technical Security (HATS) Lab at Indiana University. This research was sponsored by DHS N66001-12-C-0137, Cisco Research 591000, and Google Privacy & Security Focused Research. Any opinions, findings, and conclusions or recommendations expressed in this material are solely those of the author(s).

[5] `https://www.lastpass.com/`

References

[1] J. Vespa *et al.*, *Demographic Turning Points for the United States: Population Projections for 2020 to 2060*. US Department of Commerce, Economics and Statistics Administration, US , 2018.

[2] W. He *et al.*, “An aging world: 2015,” 2016.

[3] M. Anderson and A. Perrin, “Technology use among seniors: Tech adoption climbs among seniors,” 2017.

[4] C. Lee and J. F. Coughlin, “Perspective: Older adults’ adoption of technology: an integrated approach to identifying determinants and barriers,” *Journal of Product Innovation Management*, vol. 32, no. 5, pp. 747–759, 2015.

[5] N. Leiber, “How criminals steal $37 billion a year from america’s elderly,” *Retrieved October*, vol. 9, p. 2018, 2018.

[6] S. L. Willis and K. W. Schaie, “Cognitive training and plasticity: Theoretical perspective and methodological consequences,” *Restorative Neurology and Neuroscience*, vol. 27, no. 5, pp. 375–389, 2009.

[7] V. Garg *et al.*, “Designing risk communication for older adults,” in *Symposium on Usable Privacy and Security*, Citeseer, 2011.

[8] L. O’Gorman, “Comparing passwords, tokens, and biometrics for user authentication,” *Proceedings of the IEEE*, vol. 91, pp. 2021–2040, December 2003.

[9] E. M. Redmiles *et al.*, “You want me to do what? a design study of two-factor authentication messages.,” in *SOUPS*, 2017.

[10] B. Ives *et al.*, “The domino effect of password reuse,” *Communications of the ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[11] A. K. Nag and D. Dasgupta, “An adaptive approach for continuous multi-factor authentication in an identity eco-system,” in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, CISR ’14, (New York, NY, USA), pp. 65–68, ACM, 2014.

[12] S. Das *et al.*, “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.

[13] G. Sauer *et al.*, “Accessible privacy and security: A universally usable human-interaction proof tool,” *Universal Access in the Information Society*, vol. 9, no. 3, pp. 239–248, 2010.

[14] S. Das *et al.*, “Mfa is a waste of time! understanding negative connotation towards mfa applications via user generated content,” in *Proceedings of the Thriteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[15] N. Gunson *et al.*, “User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking,” *Computers & Security*, vol. 30, no. 4, pp. 208–220, 2011.

[16] C. S. Weir *et al.*, “Usable security: User preferences for authentication methods in ebanking and the effects of experience,” *Interacting with Computers*, vol. 22, no. 3, pp. 153–164, 2010.

[17] R. Düzgün *et al.*, “Towards secure and usable authentication for augmented and virtual reality head-mounted displays,” in *Who Are You?! Adventures in Authentication Workshop (WAY), 7. August 2020*, 2020.

[18] C. Braz and J.-M. Robert, “Security and usability: The case of the user authentication methods,” in *Proceedings of the 18th Conference on L’Interaction Homme-Machine*, IHM ’06, (New York, NY, USA), pp. 199–203, ACM, 2006.

[19] J. Reynolds *et al.*, “A tale of two studies: The best and worst of yubikey usability,” in *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 872–888, IEEE, 2018.

[20] J. Colnago *et al.*, ““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*, p. 456, ACM, 2018.

[21] A. H. Quamar *et al.*, “Information communication technology-enabled instrumental activities of daily living: a paradigm shift in functional assessment,” *Disability and Rehabilitation: Assistive Technology*, pp. 1–8, 2019.

[22] M. D. Williams *et al.*, “Contemporary trends and issues in it adoption and diffusion research,” *Journal of Information Technology*, vol. 24, no. 1, pp. 1–10, 2009.

[23] A. Jeyaraj *et al.*, “A review of the predictors, linkages, and biases in it innovation adoption research,” *Journal of information technology*, vol. 21, no. 1, pp. 1–23, 2006.

[24] F. D. Davis, “Perceived usefulness, perceived ease of use, and user acceptance of information technology,” *MIS quarterly*, pp. 319–340, 1989.

[25] Y. Barnard *et al.*, “Learning to use new technologies by older adults: Perceived difficulties, experimentation behaviour and usability,” *Computers in human behavior*, vol. 29, no. 4, pp. 1715–1724, 2013.

[26] V. Garg and J. Camp, “End user perception of online risk under uncertainty,” in *2012 45th Hawaii International Conference on System Sciences*, pp. 3278–3287, IEEE, 2012.

[27] S. Das, *A Risk-reduction-based Incentivization Model for Human-centered Multi-factor Authentication*. PhD thesis, Indiana University, 2020.

[28] S. Das *et al.*, “Evaluating user perception of multi-factor authentication: A systematic review,” in *Proceedings of the Thriteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[29] K. Gallagher *et al.*, “New me: Understanding expert and non-expert perceptions and usage of the tor anonymity network,” in *Thirteenth Symposium on Usable Privacy and Security*, pp. 385–398, USENIX Association, 2017.

[30] P. Rajivan *et al.*, "Factors in an end user security expertise instrument," *Information & Computer Security*, vol. 25, no. 2, pp. 190–205, 2017.

[31] A. D. Fisk *et al.*, *Designing for Older Adults: Principles and Creative Human Factors Approaches*. CRC press, 2018.

[32] P. B. Baltes, "The Aging Mind: Potential and Limits," *The Gerontologist*, vol. 33, pp. 580–594, Oct 1993.

[33] F. I. Craik and E. Bialystok, "Cognition through the lifespan: Mechanisms of change," *Trends in Cognitive Sciences*, vol. 10, no. 3, pp. 131 – 138, 2006.

[34] R. Kliegl *et al.*, "Testing-the-Limits and the Study of Adult Age Differences in Cognitive Plasticity of a Mnemonic Skill.," *Developmental Psychology*, vol. 25, no. 2, pp. 247–256, 1989.

[35] N. J. Carter, "Graphical passwords for older computer users," in *Adjunct Proceedings of the 28th Annual ACM Symposium on User Interface Software & Technology*, pp. 29–32, ACM, 2015.

[36] J. Nicholson *et al.*, "Age-related performance issues for pin and face-based authentication systems," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, (New York, NY, USA), pp. 323–332, ACM, 2013.

[37] S. Das *et al.*, "User-centered risk communication for safer browsing," in *Proceedings of the First Asia USEC-Workshop on Usable Security, In Conjunction with the Twenty-Fourth International Conference International Conference on Financial Cryptography and Data Security*, 2020.

[38] F. Reimair *et al.*, "Emulating u2f authenticator devices," in *2016 IEEE Conference on Communications and Network Security (CNS)*, pp. 543–551, IEEE, 2016.

[39] R. Jääskeläinen, "Think-aloud protocol," *Handbook of translation studies*, vol. 1, pp. 371–374, 2010.

[40] S. Das *et al.*, "Mfa is a necessary chore!: Exploring user mental models of multi-factor authentication technologies," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.

[41] R. E. Boyatzis, *Transforming Qualitative Information: Thematic Analysis and Code Development*. sage, 1998.

[42] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[43] K. S. Kurasaki, "Intercoder reliability for validating conclusions drawn from open-ended interview data," *Field methods*, vol. 12, no. 3, pp. 179–194, 2000.

[44] S. Das *et al.*, "Security mandates are pervasive: An inter-school study on analyzing user authentication behavior," in *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, pp. 306–313, IEEE, 2019.

[45] G. A. Grimes *et al.*, "Older adults' knowledge of internet hazards," *Educational Gerontology*, vol. 36, no. 3, pp. 173–192, 2010.

[46] D. S. Carstens *et al.*, "Evaluation of the human impact of password authentication practices on information security," *Informing Science: the International Journal of an Emerging Transdiscipline*, vol. 7, p. 67, 2004.

[47] D. R. Pilar *et al.*, "Passwords usage and human memory limitations: A survey across age and educational background," *PloS one*, vol. 7, no. 12, 2012.

[48] S. Das *et al.*, "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*, pp. 28–39, ACM, 2018.

[49] J. Colnago, Y. Feng, T. Palanivel, S. Pearman, M. Ung, A. Acquisti, L. F. Cranor, and N. Sadeh, "Informing the design of a personalized privacy assistant for the internet of things," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–13, 2020.

[50] S. Motahari *et al.*, "Designing for different levels of social inference risk.," in *SOUPS*, 2009.

[51] P. Slovic and E. Peters, "Risk perception and affect," *Current Directions in Psychological Science*, vol. 15, no. 6, pp. 322–325, 2006.

[52] P. Van Schaik *et al.*, "Risk perceptions of cyber-security and precautionary behaviour," *Computers in Human Behavior*, vol. 75, pp. 547–559, 2017.

[53] N. Davinson and E. Sillence, "It won't happen to me: Promoting secure behaviour among internet users," *Computers in Human Behavior*, vol. 26, no. 6, pp. 1739–1747, 2010.

[54] R. A. Finkel *et al.*, "The suda project: Collaborative web-based translation," in *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers*, pp. 5–pp, IEEE, 1999.

[55] R. Künnemann and G. Steel, "Yubisecure? formal security analysis results for the yubikey and yubihsm," in *International Workshop on Security and Trust Management*, pp. 257–272, Springer, 2012.

[56] L. Huber *et al.*, "Aging in intra-and intergenerational contexts: The family technologist," *Gerontechnology: Research, practice, and principles in the field of technology and aging*, pp. 57–90, 2017.

[57] D. Oliveira *et al.*, "Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 6412–6424, 2017.

[58] S. Das *et al.*, "Towards implementing inclusive authentication technologies for older adults," in *Who Are You?! Adventures in Authentication Workshop*, WAY '19, (Santa Clara, California, USA), pp. 1–5, Aug. 2019.

[59] D. M. Sarno *et al.*, "Which phish is on the hook? phishing vulnerability for older versus younger adults," *Human factors*, vol. 62, no. 5, pp. 704–717, 2020.