Security Mandates are Pervasive: An Inter-School Study on Analyzing User Authentication Behavior

Sanchari Das, Andrew Kim, Shrirang Mare, Joshua Streiff, and L. Jean Camp

Indiana University Bloomington, IN, USA
Email: {sancdas, anykim, smare, jostre, ljcamp}@indiana.edu

***Abstract*—Two-factor authentication (2FA) technologies are designed to increase the security and usability of authentication. Adoption of 2FA hardware devices that generate one-time passwords has proven to be effective as a risk mitigating strategy. Despite 2FA addressing user data security concerns, individuals appear either disinterested or unable to adopt 2FA tools. Many institutions are now mandating 2FA to better secure their network and user data. Some have more rigid requirements than others (e.g., offering only one 2FA method vs. offering multiple 2FA options). To better understand the impact of mandatory 2FA policies, we conducted a study of the usability, adoption, and acceptability of 2FA at three different universities. In our study, using the Yubico FIDO U2F security token, we found that mandating the use of 2FA without complementary risk communication is often inadequate. In our interviews, we found that mandatory 2FA did not necessarily increase security, instead leading to less secure user behavior, such as sharing 2FA tokens, storing credentials for a longer time in public devices, and other security avoidance behaviors.**

***Index Terms*—Authentication, Two factor Authentication, Password, Mandatory Tools, User Studies, Educational Institutes.**

I. Introduction

Passwords are the most common form of authentication. They are also vulnerable to theft with attacks such as phishing and social engineering. In the third quarter of 2018, email-based credential phishing attacks against corporations quadrupled [1], [2]. In a phishing attack, the attacker impersonates a legitimate source in order to steal credentials or install malware onto personal devices [3], [4]. This form of attack can be especially damaging for people who use the same passwords across multiple accounts [5]. And password reuse is common and expected, considering that the average person can reliably recall four truly random passwords [6], [7]. Two-factor authentication is a technically sound and secure authentication strategy, but do users find it acceptable and usable [8]?

There are three main ways to authenticate (commonly called authentication factors): *something you know* (e.g. passwords), *something you are* (e.g. biometrics [9]), or *something you have* (e.g. physical tokens) [10]. Two-factor authentication (2FA) methods use two factors for authentication, i.e., they require users to present two (ideally, different) factors for authentication; for example, a password and a token. Despite the benefits of added security, users still opt out of 2FA [11], and passwords continue to be the primary form of authentication [12], since users either fail to use or gauge the necessity of such tools [13].

Fig. 1. USB-A compatible security key NFC by Yubico

There are multiple 2FA service providers including Duo Security [14], Yubico [15], Authy [16], Google [17], and Microsoft Authenticator [18]. Most of these providers create a mobile phone-dependent mode of authentication, such as a one-time password or a push notification via their authentication-focused application [19]. Despite the focus on making reliable and usable authentication tools, studies have shown that users have negative feelings towards such tools [20] and do not want to integrate them into their daily lives. With this study, we specifically focus on the use of a physical USB hardware token, called Yubico FIDO (fast identifying online) U2F (universal two factor) Security Key (as shown in Figure I). To authenticate to a website using a Yubico security key, also called as YubiKey, a user first enters their username and password, then plugs in the key into their computer, and then presses the main button on the key.

In order to understand user attitudes towards 2FA and usability challenges in using Yubico 2FA, we conducted a user study with students at three different US-based universities. During the setup process, all participants were encouraged to provide verbal feedback and discuss their thought process with the observing researcher. Following setup, we conducted a semi-structured interview and later asked participants to fill out an online post-survey to provide additional insights into their daily usage of 2FA.

We found that participants often failed to completely understand or read the instructions about 2FA, which suggests a need for properly tailored risk and benefits communication as a result. Due to a lack of appropriate notifications or

feedback, participants were often unsure if they had set up the key properly, and they were confused about whether the YubiKey would work for future logins. Furthermore, most of the participants reported not receiving any communication of why their universities were making 2FA mandatory.Many participants described 2FA as an unnecessary chore rather than as a critical security tool or a benefit for the privacy of their accounts.

In this study, we explore why users who are familiar with 2FA do not use it, and how mandatory 2FA policies impact their security perceptions and practices of 2FA. We specifically selected three different institutions for our study to gauge the effectiveness of authentication guidelines and policy changes on 2FA adoption.

II. Related Work

Previous research offers insights into users' attitudes towards 2FA. In a 2015 study on the adoption rate of 2FA, Petsas et al. [21] analyzed more than 100,000 Google accounts and revealed that 2FA had only been adopted by 6.4% of the studied accounts. As a complement to this quantitative analysis, Das et al. [11] engaged in a qualitative evaluation of the instructions and support available online. That team had participants set up the YubiKey and link it to their personal Gmail account in an in-lab study using a think-aloud protocol. No participants in the first study attempting to follow YubiKey instructions were able to install the security tokens without researcher assistance. After the changes proposed by the researchers were adopted, all participants were able to install it, but many questioned the benefits of the device. This study was limited to students from a single educational institution. To examine users' 2FA practices and perceptions under different types of mandatory policies, we repeated and extended the study at three different universities with different levels and policies of 2FA mandates.

This cross-school investigation was informed by the exploration of authentication modes by Weir et al. in their study of 141 participants who volunteered to use three different forms of security authentication on their accounts [22]. The study gathered quality ratings and preference rankings to determine how the participants perceived the various security tools. The study noted that 2FA usability is often correlated with demographics rather than with the technology or usage context. This provides critical information on user mental models; however, in many studies, age and gender are actually correlated with a hidden variable – expertise. To address this, we included proven measures of expertise in addition to demographics.

An early study in the UK examined the use of 2FA physical tokens, where the customer is required to read off the password during authentication. Gunson et al. examined the preferences of various customers with two different types of authentication techniques [23]. They found that the participants thought that 2FA offered more security than the knowledge-based (password-based) security system. However, participants also reported that 2FA took a long time to complete and was somewhat burdensome to use. In a later similar mixed methods study, Krol et al. also investigated 2FA for online banking in the UK using semi-structured interviews [24]. Many participants reported usability issues with the one-time password (OTP) security token. The researchers' analysis resulted in a list of immediately actionable improvements to address usability challenges for the bank's current 2FA security system. One of these recommendations was to provide information about the benefits of 2FA and the corresponding risk mitigation.

Reynolds et al. conducted a study where they had participants set up the YubiKey with a personal email account [25]. They analyzed usability challenges during the setup process. The results of the study mirrored those of Das et al. [11] in that participants were confused on whether or not they had successfully enrolled in the 2FA service. The study also documented 25 participants' use of the YubiKey over the course of four weeks and found that participants found benefits to using it in their everyday lives. Another study by Fagan et al. reinforced the findings of the three previous studies, and suggested increasing ease of use and including communication about risks and benefits during the roll-out of security tools [26].

Many of the studies described here lead to a similar conclusion that users often perceive 2FA as difficult to set up and a hassle to use. The issues of enrollment are particularly problematic, as one well-known usability challenge in security is that of installation; and installation failures preclude use [27]. This particular study addresses adoption among organizations where the use of 2FA as a security measure is mandated. Like much of the work by Sasse, the results here illustrate the inadequacy of forcing unusable requirements even on quite competent and generally compliant people, e.g. [28]. This reifies previous work on the importance of properly communicating risks or indicating the potential benefits of using 2FA, e.g. [29], [30]. Our results show that requiring security tools without proper justification of the need for such tools can push users to adopt risky security avoidance behavior, such as sharing authentication or using high-risk free online services.

III. Methodology

To extend the work of Das et al. [11], we implemented an identical study in three self-similar populations at three different educational institutions. Our goal was to learn about users' behavior with, and attitudes toward, 2FA. We will refer to these universities as U1, U2, and U3.

A. Participant Recruitment and Ethics

We recruited participants through snowball sampling by advertising the experiment through mailing lists, flyers, word-of-mouth, etc. Similar to Das et al.'s study [11], our participants were required to be at least 18 years old, have a personal Gmail account, have a laptop with the Chrome browser installed, and have a mobile phone. In total, we recruited 33 students: 12 from U1, 10 from U2, and 11 from U3. Since we were targeting students from these three educational institutes, most participant ages ranged between 18-30 years old, with one

TABLE I
DEMOGRAPHIC DETAILS OF OUR PARTICIPANTS RECRUITED FROM THREE DIFFERENT UNIVERSITIES; PARTICIPANTS WERE CATEGORIZED AS EXPERTS AND NON-EXPERTS, WITH SOME EXPERTS HAVING CYBERSECURITY AS THEIR SPECIALIZATION.

PID	Univ.	Age	Education	Expertise
P1	U1	21-30	Bachelors	Expert (S)
P2	U1	18-20	Current undergraduate student	Expert (S)
P3	U1	18-20	Current undergraduate student	Expert (S)
P4	U1	18-20	Current undergraduate student	None
P5	U1	21-30	Current undergraduate student	Expert
P6	U1	21-30	Current undergraduate student	None
P7	U1	21-30	Bachelors	Expert (S)
P8	U1	21-30	Bachelors	Expert
P9	U1	18-20	Bachelors	None
P10	U1	18-20	Current undergraduate student	None
P11	U1	18-20	Current undergraduate student	None
P12	U2	21-30	Bachelors	None
P13	U2	41-50	Graduate or professional degree	Expert (S)
P14	U2	21-30	Graduate or professional degree	Expert (S)
P15	U2	21-30	Bachelors	Expert (S)
P16	U2	21-30	Bachelors	Expert
P17	U2	21-30	Graduate or professional degree	Expert (S)
P18	U2	21-30	Current graduate student	Expert (S)
P19	U2	21-30	Graduate or professional degree	None
P20	U2	21-30	Current graduate student	Expert (S)
P21	U2	21-30	Current graduate students	Expert
P22	U2	21-30	Current graduate student	None
P23	U2	21-30	Bachelors	None
P24	U3	18-20	Current undergraduate student	Expert
P25	U3	18-20	Current undergraduate student	None
P26	U3	18-20	Current undergraduate student	None
P27	U3	21-30	Current undergraduate student	Expert (S)
P28	U3	18-20	Current undergraduate student	Expert
P29	U3	21-30	Bachelors	Expert (S)
P30	U3	21-30	Current undergraduate student	Expert
P31	U3	21-30	Current undergraduate student	Expert
P32	U3	18-20	Current undergraduate student	None
P33	U3	18-20	Current undergraduate student	Expert

participant over the age of 41. Table I shows the aggregate demographic distribution of the participants, along with their educational background. The study (including the setup procedure, registration survey, and the interview) took on average 15-20 minutes to complete. As a token of appreciation, the participants received a Yubico Security Key. This study was approved by the ethical review board of the universities from which we recruited our participants.

B. Study Design

This study has five components: 1) pre-survey, 2) setup process, 3) interview, 4) post-survey, and 5) follow-up survey.

Participants first took the pre-survey, where they answered questions about their computer and security expertise. Based on their responses, we categorized participants into one of two groups: *expert* (a computer expert or someone with security expertise as a specialization) and *non-expert*. This categorization is based on the expertise scale created by Rajivan et al. [31], using the following thirteen questions.

- Have you taken a security course?
- Have you attended a security conference?
- Is security one of your main job responsibilities?
- Have you designed a website or registered a domain?
- Have you created a database or written a program?
- Have you installed a program?
- Have you used SSH?
- Have you configured a firewall?
- Have you been asked for help by others over computer issues?
- Have you asked others for help over computer issues?

After the pre-survey screening, an in-person think-aloud experiment was conducted, where a participant was provided with a YubiKey and asked to register/set up the key with their personal Gmail account. Specific instructions for Google integration were provided in the application list. During the setup process, participants were instructed to talk through their decision-making with the interviewer. No guidance was given to participants by the interviewer during setup unless assistance was specifically requested. After the setup was completed, the researcher asked the participant a series of open-ended questions such as

1) How would you confirm that your key (YubiKey) is working?
2) If your key was lost or stolen, what would you do?
3) Based on your current understanding of he technology, do you think the same key can be used for a different site, or would you need an additional key?
4) Based on your current understanding, could you add a second key to your account?
5) Do you see any benefits from using the security key? Please explain.
6) Do you expect to continue to use your key after today? Why or why not?
7) How would you remove a key from your account if you decided to?

We specifically conducted the interview at the end of the study to ensure that our participants were aware of the key functionality and its benefits, as well as to ensure that they were able to remove the key from their account if desired. Immediately after the interview, participants were asked to complete an online post-survey in order for us to understand their risk-perceptions related to online identity security, as well as gauge their immediate response to 2FA functionality and usage. Within thirty days of completion of the study, participants were sent a follow-up survey to study their continued usage/non-usage of the 2FA security keys. We audio-recorded the interviews and the think-aloud setup process. All of the recordings were transcribed by researchers and stored in a secure location. During the study, a researcher also took notes how the participant was making progress on the task.

C. Analysis

Our study was specifically designed to understand detailed reasons for users' non-adoption or negative perception of 2FA usage in everyday life. We collected both qualitative data (interview transcripts and research notes) and quantitative data (survey responses) from our study. For our qualitative

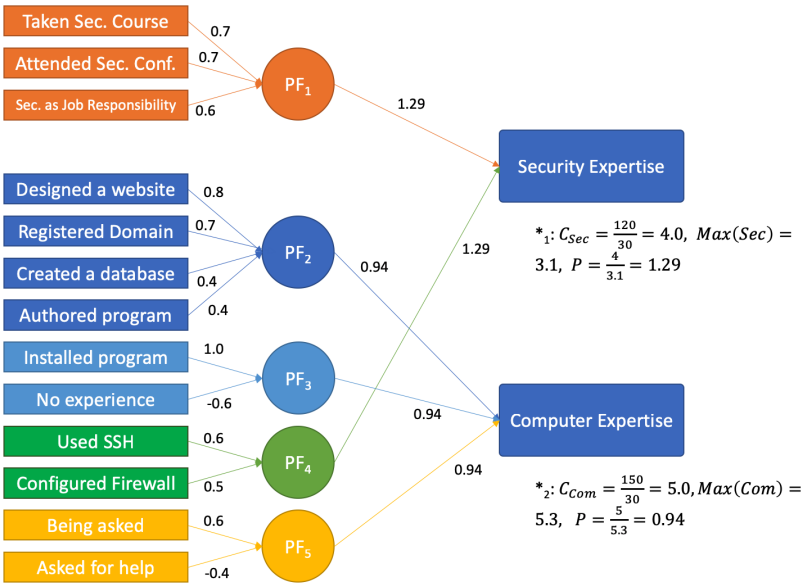

Fig. 2. Methodology for calculating participant expertise

analysis, we adopted the methodology of Das et al.'s work [10] and thematically coded events in the setup process as *halt points*, *confusion points*, or *value points*. When setting up the YubiKey, a *halt point* is when a participant needed/asked for help; a *confusion point* is when a participant was confused, but did not ask for help; and a *value point* is when participants gave feedback that could lead to actionable recommendations for improved tool design.

Using the quantitative data, we calculated participants' respective expertise scores based on the methodology outlined by Rajivan et al. [31] and described here (see Figure 2). Using this metric, we were able to further breakdown participant responses by expertise level to gain more insight into how having a technical background impacts one's attitudes towards 2FA.

IV. Findings

Our study attempted to understand how making security tools and technologies mandatory impacts users' attitudes towards adoption of these tools. We found that, in an attempt to enforce best security practices, two out of the three educational institutions we studied (U2 and U3) required all faculty and students to enable 2FA on their online university account. The other university, U1, made 2FA optional – though it was required for sensitive online accounts, such as payroll and supercomputing clusters. We found that making tools mandatory increased 2FA usage among our participants, since some of them did do not have a choice, but not all participants across the universities were aware of the benefits and correct operation of 2FA tools. And not having enough information about 2FA while going through the cumbersome task of regularly logging in with 2FA led users to have negative views of it. However, as we observed in U3 participants, mandatory 2FA enrollment policies are effective when supplemented with effective risk communication.

A. Password Practices

All participants, regardless of their technological background, expressed concerns with online data theft and wanted to protect their online information.

> P12, non-expert: Passwords are becoming less secure. And there's ways to elongate them or make the characters diverse, to make them harder, but I just think it's a matter of time before we kill the password and the password's gone.

When we asked about their password practices, we found that technical knowledge positively influenced their behavior (as shown in Figure 3). It was also interesting to see that some users did not trust good password practices and expressed concerns with password managers being a single-point-of-failure. Their security concerns were valid, however, their own password practices were more harmful given their usage of the same password for different accounts.

> P6, non-expert: Using a password manager is unlikely because all of my accounts would be at risk if the password manager is vulnerable.

B. Likelihood of Using 2FA

When we asked participants about their 2FA practices, as we expected, most of them mentioned that they limit their 2FA usage to university accounts only, since it is mandatory. Many of the participants did not adopt 2FA for their personal email accounts. On the other hand, they reported using their personal Gmail accounts for multiple interactions with professors or students. This shows a disconnect between the users' expected practices with their university account and their actual practices. When participants were asked whether making 2FA mandatory helps, they mentioned that they waited until the last minute to enroll in 2FA due to the perceived inconvenience. It was surprising to us to learn that even technology experts adopted detrimental usage behavior in order to avoid MFA.

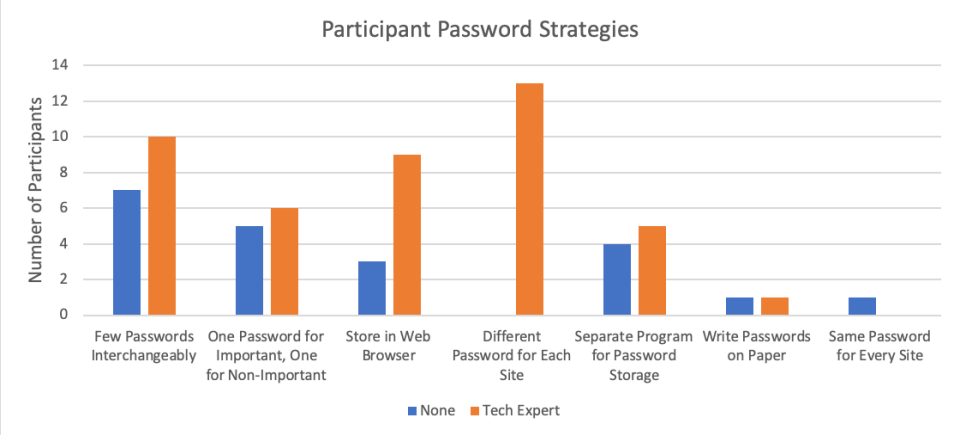

Fig. 3. Password strategies implemented by the participants based on their expertise level.

> P17, expert (s): Because we knew that we do that [enroll 2FA], it's not going to just let us quickly log in from anywhere... I believe that part of the convenience of email and like, Google Drive is that I can copy my or someone's else's passports and if I'm like at a friend's place and then urgently need to like submit something somewhere, thus I use my phone when I need to access something like passport data. I can just copy download it, but 2FA take that possibility [away] if I don't carry my key with me.

However, those from U3, where proper risk communication was done for 2FA integration, mentioned why adopting 2FA is beneficial, and we saw a generally positive attitude towards 2FA.

> P27, expert (s): Well I'm very much for two factor authentication. Given especially with how awful people are with passwords. And how hard it can be to remember them. So, like some mix of two factor authentication with a device or a key like this and like some sort of password manager. I think it's the easiest/best way to make sure that you're being relatively secure with your with your devices given that we have so much information put online now.

Figure 4 shows the usage of different types of 2FA by the participants, where the security tokens emerged as the best possible option for 2FA. However, many participants expressed concerns about different aspects of the Yubico security token.

C. Negative Aspects of the Yubico Security Key

Our study found that students across all of there universities encountered confusion and halting points while setting up a YubiKey with their personal Gmail account. We found that even participants with technical expertise required assistance to set up their YubiKey due to the lack of proper instructions. Participants experienced issues with setting up the keys, such as trying to use an incompatible browser, inserting the key incorrectly, and navigating to the wrong instructions.

> P13, expert (s): Yubico security keys are not compatible with Firefox... I won't use it and I won't use the key... I just believe in Firefox's mission more than Google.

We also found that some participants did not notice that the YubiKey is interactive and did not know to press/touch the button in order to authenticate. One participant (P28, Expert) at U3 noted during setup that the key was "kind of finicky" after they had trouble inserting the key and pressing the button. Another participant (P20, Expert) at U2 attempted to use the Safari web browser, not realizing that the YubiKey only works with the Chrome browser. Due to an operating system upgrade issue, two participants (P10, Non-Expert and P11, Non-Expert at U1) had to install a special YubiKey driver for their Windows machine before they could follow the instructions, leading to a delay in their setup time. Participants across all expertise levels made mistakes, indicating that previous experience with computers and security does not guarantee a successful setup process.

Furthermore, users across various expertise levels often had misconceptions about how the YubiKey operated. For example, one participant (P28) at U3 stated that they were "pretty sure this [the YubiKey] is a Google-specific key" that could only be used with Google-associated accounts; YubiKey can be used with other online services that support it. Another participant (P12, Non-Expert) at U2 believed that losing their YubiKey could potentially lead to the account associated with that key being compromised, "kind of like if you have a debit card that gets lost." We also found knowledge gaps between students of different institutions – particularly between U2 and U3, where U3 participants showed a more positive attitudes towards 2FA due to proper risk communication – even among participants with comparable computer and security expertise scores.

In spite of many participants encountering halting or confusion points during the setup process, many of them expressed that the YubiKey is a better means of security for keeping their accounts safe. One participant noted that the YubiKey does not require an Internet connection to work, unlike a mobile

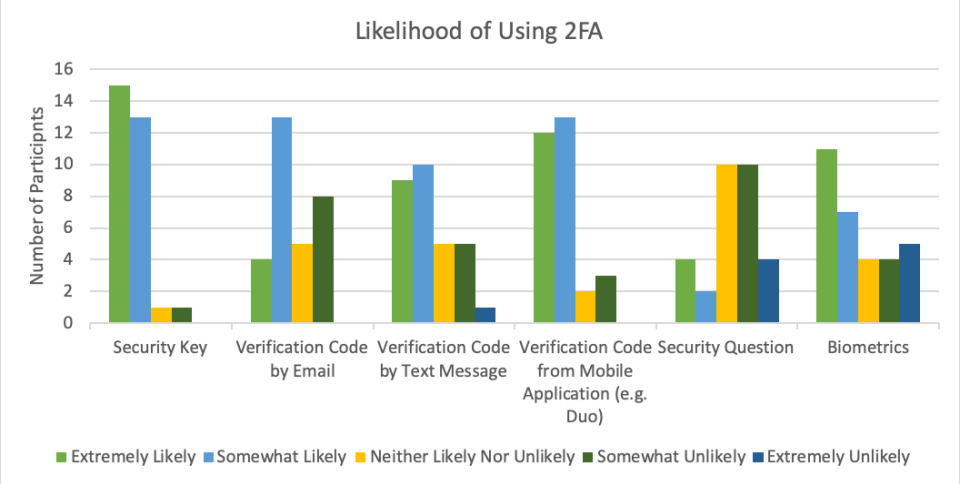

Fig. 4. Participants' likelihood of using various forms of two-factor authentication in addition to passwords.

device, but the key is an addition thing to carry, unlike their mobile phone, which is always with them. When discussing how usability plays a role in their decisions about security tools, participant P13 said they favored tools, like password managers, that are both secure and convenient. As researchers, developers, and designers, we need to develop tools that are secure and convenient to use, or provide a meaningful trade-off between security and usability.

> P31, expert: Security is a priority for me, but [convenience] plays a role in how secure I am willing to be. Writing passwords down is not secure so I avoid it, however, using simple passwords or the same password for multiple sites... is enough for me to do. The password manager seems more secure than this and also convenient so I use a browser based one for those reasons; but just started recently.

V. Discussion

In examining the usability problems with the YubiKey, we found that most of them occur during the setup process. We found that the way security tools are introduced to users is extremely critical regardless of the level of expertise. We also found that mandating security practices can be helpful but risk communication is essential for enabling security behavior, a finding that echoes prior work [30], [6]. We learned that people share authentication and avoid 2FA by using an alternative that does not require 2FA. Perception of benefits, awareness of risk, and the usability of the technology all play a role in securing information.

Participants in U3 were provided an explanation of what 2FA is, when to use it and why, and the setup instructions. However, at U2, participants were not provided with a description of what 2FA is and were only directed to the mandatory process. The lack of information dissemination by universities U1 and U2 may have caused participants to encounter more confusion and halt points throughout the study. The results point to the need for additional information, particularly during enrollment.

On U2's website, the login form has a feature where users can chose to be prompted to authenticate once every 30 days. This reduces the potential inconvenience of having to use 2FA. However, this also reduces the security of the account on the computer/browser where users use that feature. Yet, the linking of the device to the account precludes attackers from using any password should the student be phished or reuse credentials. Students have often reported "remembering" their login on public computers they use on campus to reduce the hassle of going through 2FA every login.

Based on our study, we demonstrate that participants experienced of multitude of challenges with the system during the setup. Some participants did not know that the key could only be set up with the Chrome browser. Other participants did not know that the YubiKey itself was interactive. The instructions should include a brief overview of the device before configuration, so that users would know beforehand how to insert and use the YubiKey. The instructions should also clearly tell the user the correct order of the steps, as some participants completed the setup process out of order. Specific instructions for devices and systems should also be changed, as many of the participants began reading the setup instructions for the wrong devices.

Many participants felt that the instructions were too long, and saw that as a sign of a cumbersome system. This caused many participants to skim through the instructions. As a result, they missed important information that they would need during the setup process. We recommend using visual indicators and timing information, rather than providing it all in one step. Instruction inconsistency is also a critical issue, since setup instructions may not change, even when device interfaces and browsers have.

Many participants were not aware that the YubiKey is capable of supporting more than one account, which raised concerns of having to buy multiple keys to protect their

accounts. Participants stated that they would not want to carry around a YubiKey all the time, as it feels like a hassle. This thinking would be magnified if they felt that they were required to carry around a key for every account they wanted to protect, and this could drive away many potential buyers of the product. The fact that YubiKey supports multiple accounts should be clear in the instructions and overview.

VI. Recommendations

Our research reiterated some of the common findings in earlier studies by Das et al. [11], Colgano et al. [5], Reynolds et al. [25], and others. However, the potential solution of making tools mandatory, while helpful, is inadequate without useful timely information about the risk and benefits, as well as appropriate background information about the security tools.

A. Risk Communication and Convenience

One of the similarities between U2 and U3 was a policy that made it mandatory for both faculty and students of the university to go through two-factor authentication to login to their respective accounts. The key difference between the universities was that U3 communicated why 2FA was required, which was reflected in the participants' perception of it. Many security tools are technologically strong but fail to convey their necessity or the harmful impacts of non-adoption. We need to provide more information to participants through different means that relate to their mental models and stress the importance of such tools. For example, U3's roll-out strategy included a description of why 2FA is needed. This reflects the recommendations by Norcie about Tor: *say why before providing instructions* [27].

B. Easier Navigation

Some participants, who lacked experience with either computers or security, had problems understanding the instructions for the setup of the YubiKey. We cannot follow the *one size fits all* strategy in security because of the different expertise and perceptions of individuals. Thus, providing easier navigation through the setup is recommended. This can be either simulations rather than instructions or pictures for users to follow as another means of showing the process. There could also be a message box that pops up once the setup of the YubiKey is complete, so that the user knows for sure when they have successfully configured the key to their account. It is generally noted in warning science that if you target the average person, then you are missing half the people by design. The basic usability rubric of providing very simple instructions with a quick bypass for more expert users applies here.

C. Regular Updates and Maintenance

An interesting and surprising result is that the instructions are inconsistent. Mandating a tool implies providing usable correct instructions. Both instructions from Yubico and Google were not updated with the changing interface of the accounts. This, of course, confused people who could not register the key and required help from the researchers. Regular updating of instructions is thus critical. Additionally, universities could have completed pilot user testing to find the instructional discrepancies and updated their help guides for users.

D. Clarity of Instructions and Design of Keys

Clear instructions on the form factor and usage of the keys, is required, since many participants were unaware of the interactive nature of the tokens. Another problem with the design of the YubiKey is the fact that users were sometimes unable to determine which direction the key is supposed to face, leading to users inserting the key incorrectly. The keys feel lightweight and fragile, and some participants were scared of breaking the key. Our future research will explore different form factors to address this. Again, one size does not fit all.

E. Incompatible Browser

Some new users of the YubiKey also might not have the necessary browser that is associated with the YubiKey. The YubiKey might attract more buyers if it had a more flexible range of compatible web browsers. As shown by our study, some users may feel as though one web browser has a better message behind it, and some computers may be unable to natively support the Chrome browser.

F. Security Concern

One participant asked whether a hacker would be able to get into the key and take the codes that are inside of the device. The possibility of this happening could be in fact very low, but to give users a peace of mind, this could be tested to ensure that the key does not leak any information if it were to fall into the wrong hands.

G. Provide Users with Options

Many of the participants who had more expertise were generally positive about using biometrics for authentication. One way to improve security is to incorporate a biometric fingerprint scanner into the key's authorization button. This will provide users with more assurance that their accounts are protected.

VII. Conclusion

In order to evaluate the usability and acceptability of the Yubico FIDO U2F Security Key, we had participants set up the key and answer questions about their YubiKey usage before, during, and after the setup process. We sought to determine whether making security tools mandatory helps address usability challenges. We recruited students from three different universities, U1 (2FA was not mandatory), U2 (2FA was mandatory), U3 (2FA was mandatory and effective with proper risk communication). Many of the participants thought that the YubiKey was a good means of keeping their accounts safe and secure, regardless of the universities they belonged to. However, tailored risk and benefits communication helped convince participants that YubiKey adoption is necessary. Technical experts in general were more positive about 2FA adoption, and many of them said that they will continue to use the YubiKey in their everyday lives. Some participants with a

background in cybersecurity had deeply rooted concerns about using the YubiKey on a day-to-day basis.

VIII. Future Work and Limitations

We acknowledge the limitations of a qualitative study and cannot provide a general solution derived from the detailed analysis. However, qualitative studies help find underlying causes of usability challenges that users face, thus generating effective new implementation ideas. As a future work, we want to expand our proposal of risk communication and determine its effectiveness in a larger setting while adding a quantitative component. Our study provides a wealth of information from different organizational settings that informs policies about mandating 2FA, as well as generates hypothesis for future quantitative research. Future research also includes explorations of other organizations to analyze their internal policies regarding the usage of such tools in a naturalistic setting.

IX. Acknowledgement

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, 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 Dominique Clark and HyeonJung Lee with the transcription of collected data. We would also like to thank our participants for their valuable data, which helped us generate the recommendations.

References

[1] S. Das, D. Kim, T. Kelley, and L. J. Camp, "Grifting in the Digital Age," *PrivacyCon*, 2018.

[2] A. Jentzen, "The Latest in Phishing: First of 2019: Proofpoint US," *Proofpoint*, Jan 2019.

[3] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, "All About Phishing: Exploring User Research Through a Systematic Literature Review," *arXiv preprint arXiv:1908.05897*, 2019.

[4] J. Hong, "The Current State of Phishing Attacks," *Communications of the ACM*, vol. 55, no. 1, Jan. 2012. DOI 10.1145/2063176.2063197

[5] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. 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*. ACM, 2018.

[6] A. Adams and M. A. Sasse, "Users are not the Enemy," *Communications of the ACM*, vol. 42, no. 12, 1999.

[7] A. Newell, H. A. Simon *et al.*, *Human Problem Solving*. Prentice-hall Englewood Cliffs, NJ, 1972, vol. 104, no. 9.

[8] W. N. Owen and E. Shoemaker, "Multi-factor Authentication System," https://patents.google.com/patent/US7373515B2/en, May 13 2008, US Patent 7,373,515.

[9] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: Two-Factor Authentication Featuring Fingerprint Data and Tokenised Random Number," *Pattern Recognition*, vol. 37, no. 11, 2004.

[10] S. Das, G. Russo, A. C. Dingman, J. Dev, O. Kenny, and L. J. 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*. ACM, 2018.

[11] S. Das, A. Dingman, and L. J. Camp, "Why Johnny Doesn't Use Two Factor: a Two-Phase Usability Study of the FIDO U2F Security Key," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, 2018.

[12] S. Ruoti, J. Andersen, and K. E. Seamons, "Strengthening Password-Based Authentication," in *WAY@ SOUPS*, 2016.

[13] S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating User Perception of Multi-Factor Authentication: A Systematic Review," *arXiv preprint arXiv:1908.05901*, 2019.

[14] "Duo Trusted Access." Available online: https://duo.com/

[15] "Yubico | YubiKey Strong Two Factor Authentication." Available online: https://www.yubico.com/

[16] "Authy | Two-factor Authentication (2fa) App & Guides." Available online: https://authy.com/

[17] "Google Authenticator." Available online: https://google-authenticator.com/

[18] "Microsoft Authenticator Securely Access & Manage Your Online Accounts." Available online: https://www.microsoft.com/en-us/account/authenticator

[19] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A Usability Study of Five Two-Factor Authentication Methods," in *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, Aug. 2019. Available online: https://www.usenix.org/conference/soups2019/presentation/reese

[20] S. Das, B. Wang, and L. J. Camp, "MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content," in *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[21] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, "Two-factor Authentication: is the World Ready?: Quantifying 2FA Adoption," in *Proceedings of the Eighth European Workshop on System Security*. ACM, 2015.

[22] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable Security: User Preferences for Authentication Methods in eBanking and the Effects of Experience," *Interacting with Computers*, vol. 22, no. 3, 2009.

[23] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking," *Computers & Security*, vol. 30, no. 4, 2011.

[24] K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse, ""They Brought in the Horrible Key Ring Thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking," *arXiv preprint arXiv:1501.04434*, 2015.

[25] J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti, and K. Seamons, "A Tale of Two Studies: The Best and Worst of YubiKey Usability," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018.

[26] M. Fagan and M. M. H. Khan, "Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice," in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[27] G. Norcie, K. Caine, and L. J. Camp, "Eliminating Stop-Points in the Installation and Use of Anonymity Systems: A Usability Evaluation of the Tor Browser Bundle," in *5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS)*. Citeseer, 2012.

[28] P. G. Inglesant and M. A. Sasse, "The True Cost of Unusable Password Policies: Password Use in the Wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2010.

[29] L. J. Camp, "Beyond Usability: Security Interactions as Risk Perceptions," in *Workshop on Risk Perception in IT Security and Privacy, Newcastle, UK. http://citeseerx. ist. psu. edu/viewdoc/download*, 2013.

[30] V. Garg and L. J. Camp, "Cars, Condoms, and Facebook," in *ISC 2013*. Springer, 2013.

[31] P. Rajivan, P. Moriano, T. Kelley, and L. J. Camp, "Factors in an End User Security Expertise Instrument," *Information & Computer Security*, vol. 25, no. 2, 2017.