"Don't punish all of us": Measuring User Attitudes about Two-Factor Authentication

Jonathan Dutson†, Danny Allen†, Dennis Eggett*, Kent Seamons†
*Computer Science Department†, Department of Statistics**
Brigham Young University
jonathan@isrl.byu.edu, dannyallen@isrl.byu.edu, theegg@stat.byu.edu, seamons@cs.byu.edu

***Abstract*—Two-factor authentication (2FA) defends against password compromise by a remote attacker. We surveyed 4,275 students, faculty, and staff at Brigham Young University to measure user sentiment about Duo 2FA one year after the university adopted it. The results were mixed. A majority of the participants felt more secure using Duo and felt it was easy to use. About half of all participants reported at least one instance of being locked out of their university account because of an inability to authenticate with Duo. We found that students and faculty generally had more negative perceptions of Duo than staff. The survey responses reveal some pain points for Duo users. In response, we offer recommendations that reduce the frequency of 2FA for users. We also suggest UI changes that draw more attention to 2FA methods that do not require WiFi, the "Remember Me" setting, and the help utility.**

***Index Terms*—two-factor authentication, usable security, usability, security**

I. Introduction

Text-based passwords remain the most common form of online user authentication today, despite the tremendous amount of research that demonstrates their security and usability weaknesses [9], [16], [17]. The number of data breaches is increasing rapidly [5], and most data breaches involve weak, compromised, or default passwords [4]. In response to the increasingly apparent problems with passwords, many organizations and individuals have turned to two-factor authentication (2FA) to strengthen existing password security.

2FA requires users to present factors from two different categories of authentication. These categories are *something they know* (such as a password or the answers to a set of security questions), *something they have* (such as a phone or hardware token), and *something they are* (a biometric such as a fingerprint or facial recognition). 2FA protects against remote attackers because attackers are not able to compromise user accounts using passwords alone.

Despite the increased security 2FA brings, voluntary adoption rates remain very low [19]. One of the reasons for low adoption is that many users perceive 2FA methods as difficult to adopt [6], [15]. Improving the usability of 2FA may lead to increased adoption.

Duo Security provides its customers with cloud-based 2FA using a variety of 2FA methods. It provides administrators with a single center for endpoint supervision, policy creation, and user management. Duo manages millions of users with 300 million authentication events every month [1]. More than 300 educational institutions use Duo.

This paper presents a survey of Duo two-factor authentication among 4,275 faculty, students, and staff at Brigham Young University (BYU). The survey was conducted in April 2018, almost a year after BYU adopted Duo during June 2017. A majority of the participants felt more secure using Duo and felt it was easy to use. Many participants were frustrated that they were required to use the system; half of the participants would prefer that BYU not use Duo. One unhappy participant complained that security-conscious users could not opt out—"Don't punish all of us!" Almost half of the survey respondents reported at least one instance of being unable to access their university account when they could not successfully authenticate using Duo. Many of these instances could have been preventable if users better understood the various authentication methods Duo offers.

We make three UI recommendations for Duo based on user feedback. First, the interface should make it clear that there are authentication options that do not require WiFi. Some users assume they cannot login when they have no WiFi. Second, the "Remember Me" option should be more prominent so that users can choose to authenticate with Duo less often from the same device. Third, the help option needs to be more prominent for users that encounter difficulties.

Students and faculty generally had similar perceptions about the poor usability of Duo, while staff typically had much more positive perceptions. Our results confirm findings from a similar overlapping study conducted at CMU [10], and our UI recommendations address issues raised in their study. In addition to being relevant for other institutions that use Duo, our findings provide insights that may improve the usability of other two-factor authentication providers.

II. Related Work

While most prior research measures the usability of a single two-factor authentication system, our work studies perceptions of individuals with multiple 2FA options. This type of study is valuable because many real-world companies that offer two-factor authentication allow users to choose from a variety of second factors. For example, Google allows users to use voice calls, codes sent via text, security keys, verification codes from the Google Authenticator app, or backup codes [2].

The work most directly related to ours is a study of the adoption of Duo in a university setting. Colnago et al. [10]

conducted two large-scale surveys at Carnegie Mellon University (CMU) designed to understand two-factor authentication adoption rates, user sentiments towards 2FA, and problems experienced with Duo. They surveyed CMU students, faculty, and staff before and after Duo became mandatory for university employees. Colnago et al. found that while most individuals who adopted Duo considered 2FA to be annoying, most also considered 2FA to be easy to use and felt safer with 2FA enabled.

A. General perceptions of two-factor authentication usability

Two-factor usability research has produced mixed results. De Cristofaro et al. [11] conducted a Mechanical Turk survey of two-factor authentication users. They found that perceptions about the usability of two-factor authentication correlate with user characteristics (such as age or level of education) rather than the specific second-factor technologies used. Participants found each of the second-factors to be highly usable. The paper suggested that the high usability scores might due to the infrequency with which their users were required to provide their second factor. Many institutions that offer two-factor authentication allow browsers to remember a device indefinitely (by storing a cookie associated with the user login), only requiring a second factor if the device becomes unrecognized (for example, by clearing cookies).

Gunson et al. [13] investigated user perceptions of single-factor and two-factor authentication methods in automated telephone banking. Over 75% of participants rated two-factor authentication as being best for security, while single-factor authentication was ranked best for convenience and ease of use. Most participants expressed an overall preference for single-factor authentication, suggesting that many value convenience and ease of use over security.

B. The usability of specific second-factor systems

Research on Universal Second Factor (U2F) keys (such as the YubiKey) has identified pain points in the set-up process and recommendations to address them. Das et al. [12] recruited students from STEM degree programs to configure a Yubikey Security Key for a Google account. Although the Yubikey is considered one of the most usable hardware 2FA devices, many of the participants struggled with the Yubikey registration process. Most of the paper's recommendations focus on improving the instructions and workflow for individuals trying to register 2FA devices. After some of their recommendations were adopted, Das et al. repeated the study and observed a 33% increase in the number of users who were able to complete the Yubikey registration.

Reynolds et al. [20] conducted two YubiKey usability studies to explore differences between two phases of two-factor authentication: setup and daily-use. Many participants in the first study struggled to set up the YubiKey and perceived it as being unusable. However, participants in the second study found the YubiKey to be highly usable in day-to-day usage, and the majority of users preferred U2F-based two-factor authentication to other second-factor authentication methods. The longitudinal results suggest that users perceptions of the usability of two-factor authentication may turn more positive if usability problems in the setup phase can be improved or eliminated.

C. Comparing the usability of different two-factor systems

Other relevant research has been done to compare the usability of different two-factor systems. Bonneau et al. [9] compared the usability, deployability, and security of 35 password replacement schemes. They used eight measurements of usability to analyze how each of the schemes compared with passwords. While they found some password alternatives to be equally or more usable than passwords in a few of the eight measurements, most alternatives were rated overall as being less usable than passwords. Also, none of the systems could compete with the deployability of passwords.

Krol et al. [15] studied the usability of 2FA in online banking. They interviewed 21 individuals that used a variety of second factors, including card readers, hardware passcode generators, text messages, phone calls, and smartphone apps passcode generators. Krol et al. found that participant satisfaction negatively correlates with the use of hardware tokens and the number of credentials required for authentication. Given that their participants consisted of relatively young, well-educated individuals who were already familiar with 2FA and online banking, Krol et al. hypothesized that older or less computer literate groups are put off by the unusability for online banking 2FA.

D. Adoption factors

Ackerman [6] and Albayram et al. [7] have shown that video messaging can be effective at promoting 2FA adoption. Ackerman studied factors that encourage or discourage millennials from adopting two-factor authentication. They showed users a video message which articulated the dangers of cybercrime and recommended two-factor authentication as an action to combat cyber threats. They found that this educational message increased two-factor authentication adoption, with 31% of participants choosing to adopt two-factor authentication services in the week after viewing the video. User perceptions of the threat cybercrime posed to them seemed to have little effect on the user's choice to adopt two-factor authentication. The most common reasons participants gave for non-adoption of two-factor authentication were being too busy or being unconcerned about the threat cybercriminals pose to them. Albayam determined that self-efficacy and risk themes were most effective in influencing adoption because they were interesting, informative, and useful.

III. Duo Background

Duo is a cloud-based two-factor authentication service provider. Their customers include a wide variety of businesses and universities. Users select the authentication method they wish to use as a second factor from Duo's online UI. Duo provides four authentication methods.

1) **Duo Push**— This method pushes a login request notification to a user's phone or tablet. Users review the authentication request and can approve or reject the request with a tap. Duo Push is typically the recommended option, as it is considered more usable than many of the other options, and is resilient to man-in-the-middle attacks. This method requires a user to install the Duo Mobile app on their device, and so is only compatible with smartphones. This method requires an internet connection.
2) **Call Me**— This option calls the user's phone. The user authenticates by pressing any key on their phone or rejects the request by hanging up or ignoring the call. This method requires cell phone service.
3) **Passcode**— Users may authenticate by entering a passcode into the Duo prompt. There are four ways to obtain passcodes:
    a) *Duo Mobile*— The Duo Mobile app uses a time-based one-time password (TOTP) algorithm to generate passcodes. The app does not require an internet connection or mobile service to generate codes.
    b) *SMS*— Duo can send one-time passcodes through SMS messages, requiring cell phone service. Administrators can choose to send up to ten passcodes at a time.
    c) *Hardware token*— Duo supports HMAC-based One-Time Password (HOTP) compatible hardware tokens. These tokens create a hash-based message authentication code (HMAC) using a secret key shared between the hardware token and Duo to generate a series of passwords. Most hardware tokens have a single button that the user presses to advance the counter to the next passcode. Since the online Duo authenticator and the token increment the counter independently, if a user presses the button multiple times without using the passcodes the token may fall out of sync with Duo. If this happens, a Duo administrator must resync the hardware token before it can be used to generate valid passcodes. While a user can add phones, tablets, and U2F tokens, a Duo administrator must add hardware tokens. Duo sells their own hardware tokens, but also supports compatible third-party tokens.
    d) *Provided by administrator*— Duo administrators may provide temporary passcodes (called bypass codes) for specific users. Bypass codes can be set up to expire after a certain time limit, after a specified number of authentications, or to be valid indefinitely.
4) **U2F Security Key**— Duo supports U2F security keys such as the YubiKey or Google's Titan. To authenticate with a U2F key, a user must insert the device into a USB port and tap or press a button on their key. This method requires that users log in with a U2F supported browser (currently only Chrome or Opera).

IV. Methodology

A. Study Design

We created and distributed a 30-question survey designed to identify:

- Threats individuals perceive against their school account
- Sentiment about the efficacy of Duo's threat protection
- Perceptions about the usability of Duo
- Common Duo usability concerns

BYU's institutional review board approved the survey. To be eligible to take the survey, a person had to be 18 or older, a current student, faculty, or staff member, and have Duo enabled for their BYU account.

The first eight questions collected demographics, which we used to determine whether a person was eligible to take the survey. The next twenty questions focused on the respondents' perceptions about the usability of Duo and on how they typically interacted with the system. These questions included nine questions on a 5-point Likert scale:

1) **Concern about compromise:** I am concerned about my BYU account being compromised.
2) **Concern about cyber-criminals:** It is likely that my BYU account will be a target for cyber-criminals.
3) **Concern about friends and/or acquaintances:** I believe people I know might try to compromise/access my BYU account.
4) **Ease of use:** Duo is easy to use.
5) **Feelings of security:** Duo makes me feel more secure about my BYU account.
6) **Feelings of annoyance:** I feel annoyed when I have to use Duo to log into my BYU account.
7) **Concern about additional time for authentication:** Duo adds an inconvenient amount of additional time to logging into my BYU account.
8) **Glad for Duo:** I am glad that I have Duo enabled for my BYU account.
9) **Would rather not have Duo:** I would prefer if BYU did not use Duo.

Our results section excludes analysis for the "Concern about cyber-criminal" question because participant responses to that question were essentially the same as responses to the "Concern about compromise" question.

We asked questions about how often participants authenticated through Duo, which authentication methods they used most often, whether they had two-factor authentication enabled for another account, and whether they had ever been unable to access their university account because of Duo. We also included two free response questions; the first asked participants to share circumstances in which they were unable to access their account because of an inability to authenticate with Duo, and the second allowed participants to share either positive or negative experiences they had with Duo.

The final two questions allowed participants to choose to enter a drawing for an Amazon gift card. After the study, we randomly selected twenty participants to receive a $15 gift card and one participant to receive a $100 gift card.

After gathering the survey responses, two researchers created a priori codes for the first free response question based on their perspectives of the problem space and an initial, cursory survey of the response set. As the researchers continued with the coding process, codes were either consolidated or made more specific until the use cases they represented effectively partitioned the response set into thematically consistent categories. For example, "no cellular service" and "no WiFi signal" were combined to describe any case where authentication was infeasible due to lack of connectivity. Conversely, "challenge using Duo with a new phone" was distinguished from "difficulty with setting up Duo" to highlight the unique technical struggles associated with the registration of a secondary device. When coding was complete, the refined codebook consisted of the following categories:

1) Device out of battery
2) No cellular or WiFi service
3) Forgot, lost, broke, or left device
4) Challenge using Duo on a new phone
5) Technical issues unrelated to Duo
6) Difficulty with setting up Duo
7) Problems specific to hardware tokens
8) Lack of education about how to use Duo
9) Technical issue related to Duo

Each researcher independently coded every response to the first question, only deliberating with the other to update the codebook. Whenever a respondent reported multiple reasons for being unable to access their account, the researchers assigned multiple codes to that response to cover all failure cases. Finally, a response that did not reasonably fit within any of the categories was classified as "Other" (though this was an infrequent occurrence).

For the second free response question the researchers independently coded for sentiment analysis. Each response was categorized as positive, negative, both positive and negative, or neutral. At the end of the coding process, the two researchers discussed the results for both free response questions and arrived at a consensus for all responses for which they had initially disagreed.

B. Recruitment

We distributed our survey through the official university communications channel (BYU University Communications). They sent an email to all students and another to all full-time and part-time university employees. We distributed the survey near the end of the academic school year to allow new students, faculty, and staff maximum time to experience Duo during the academic year. During the three week survey availability period, we received 4,480 responses. We dropped 205 responses from individuals who were ineligible or who did not complete the survey, leaving 4,275 completed surveys for analysis.

C. Demographics

BYU has a student body of about 33,500 and employs at least 5,000 faculty and staff. Our 4,275 respondents represent an approximate response rate of 11% of the university student, faculty, and staff population. We had a slightly higher response rate from faculty and staff compared with students, but each group had a response rate above 10%.

Because our results are representative of the BYU population, participants were primarily students (3543; 83%) and young adults ages 18-24 years (3091; 72%) and 25-34 years (611; 14%). Slightly more respondents identified as female (2411; 56%) compared to male (1847; 43%), although BYU's female to male ratio skews the other way (52% male to 48% female for student enrollment).

V. Results

The survey questions gathered both qualitative and quantitative. The quantitative data includes demographic data, Likert scale questions measuring user sentiment about the usability of Duo, and questions providing information about the user's typical login experience (e.g., what methods they use as their second factor, whether they have ever been unable to access their account because of the requirement for 2FA). The survey contained two open-ended questions. The first asked users who had ever been unable to access their account because of Duo to explain the circumstances that prevented them from authenticating. The second question allowed users to share their positive or negative experiences with Duo. In this section, we present the results of our quantitative data, insights from the qualitative data, and a discussion of our results in the context of usable two-factor authentication.

A. Quantitative Results

Our quantitative analysis includes percentages, distribution of responses, and ANOVA tests on the Likert scale data. For the ANOVA test, we treat our 8 Likert scale questions as a continuous variable [18], with 1 representing strongly disagree on one end of the scale, and 5 representing strongly agree on the other end. We performed the Bonferroni correction across all variables to counteract the multiple comparisons problem, and performed Tukey's multiple comparison test within each variable to determine how means differed from each other.

1) Usability Perceptions: Figure 1 shows the distribution of agreement for 8 statements related to Duo's usability. The majority of survey participants felt more secure with Duo enabled for their BYU accounts (54.8%) and felt it was easy to use (56.0%). However, respondents generally found Duo to be annoying (86.1%) and felt Duo added an inconvenient amount of time to their login experience (69.2%). Nearly half of the respondents would prefer that the university not use Duo (49.8%). Almost a quarter of respondents were concerned about their BYU accounts being compromised (22.7%), but very few (4.6%) were concerned about compromise by a friend or acquaintance. Nearly half of respondents reported at least one instance of being unable to access their BYU account because of an inability to authenticate with Duo (47.1%).

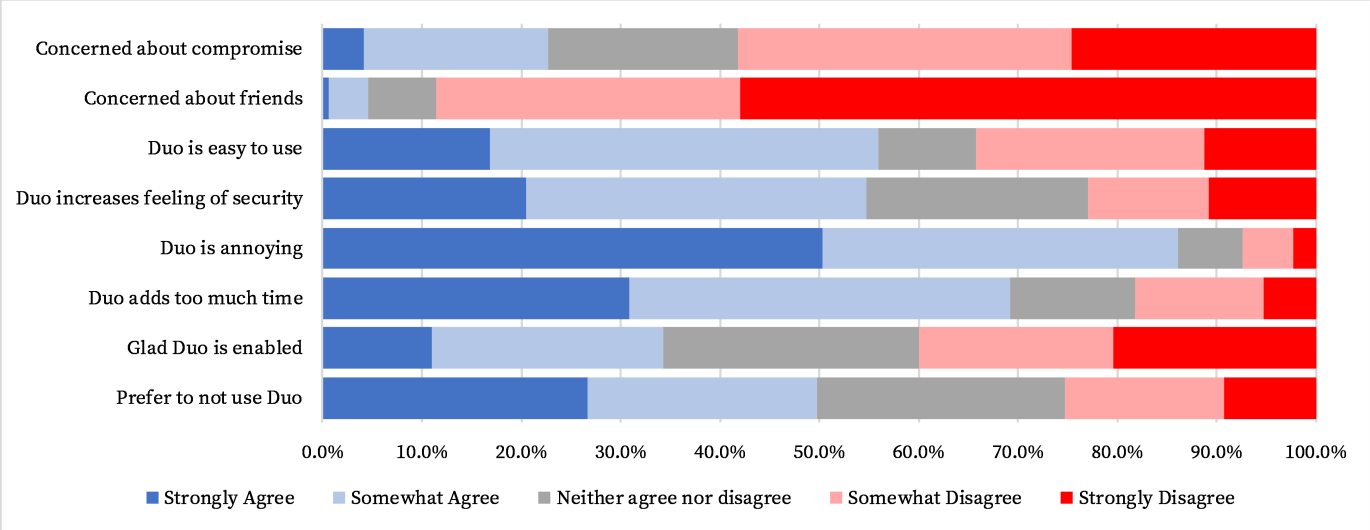

Fig. 1. Distribution of agreement for 8 statements about Duo's usability

TABLE I
TUKEY COMPARISON OF 8 STATEMENTS ABOUT DUO'S USABILITY.

	Student	Faculty	Staff	Other 2FA: Y	Other 2FA: N	Inaccessible: Y	Inaccessible: N
Concerned about compromise	2.3 (0.02)^A	3.1 (0.07)^B	3.3 (0.05)^B	2.8 (0.03)^A	2.3 (0.02)^B	2.3 (0.03)^A	2.5 (0.02)^B
Concerned about friends	1.5 (0.01)^A	1.8 (0.06)^B	1.8 (0.04)^B	1.7 (0.02)^A	1.5 (0.02)^B	1.5 (0.02)^A	1.6 (0.02)^B
Duo is easy to use	3.2 (0.02)^A	3.0 (0.09)^A	3.9 (0.06)^B	3.5 (0.04)^A	3.2 (0.02)^B	2.8 (0.03)^A	3.7 (0.03)^B
Duo increases security	3.3 (0.02)^A	3.5 (0.08)^A	4.1 (0.05)^B	3.8 (0.03)^A	3.3 (0.02)^B	3.1 (0.03)^A	3.7 (0.03)^B
Duo is annoying	4.4 (0.02)^A	4.2 (0.06)^B	3.5 (0.04)^C	4.0 (0.03)^A	4.4 (0.02)^B	4.5 (0.02)^A	4.0 (0.02)^B
Duo adds too much time	3.9 (0.02)^A	3.7 (0.08)^A	3.0 (0.05)^B	3.5 (0.03)^A	3.9 (0.02)^B	4.2 (0.02)^A	3.4 (0.02)^B
Glad Duo is enabled	2.7 (0.02)^A	3.0 (0.08)^B	3.8 (0.05)^C	3.3 (0.04)^A	2.7 (0.02)^B	2.5 (0.03)^A	3.2 (0.03)^B
Prefer not enabled	3.6 (0.02)^A	3.3 (0.08)^B	2.4 (0.05)^C	3.0 (0.04)^A	3.6 (0.02)^B	3.8 (0.03)^A	3.1 (0.03)^B

Note: Means are shown in each column with the corresponding standard errors in parentheses. The superscripts identify which groups have a statistically significant difference between them (i.e., if the groups have a different letter they have a statistically significant difference with $p<0.01$).

Table I shows the mean and standard error for several comparisons. Students, faculty, and staff are compared in the first three columns. "Other 2FA" compares individuals who have 2FA enabled on another account in addition to their university account with those who do not. "Inaccessible" compares individuals who have been unable to access their account because of an inabliity to authenticate with Duo and those who have never had their account inaccessible.

Table 1 shows that users who had 2FA enabled on another account were more likely to view Duo more positively and were more likely to be concerned about their account's security. It also shows that users who have been unable to access their BYU account at least once generally have more negative sentiments towards Duo. Negative events have a stronger influence than positive ones [8], and even if a user is able to use Duo to authenticate without a major issue most of the time, a single negative experience may hurt their sentiment towards the system.

2) Comparing students, faculty, and staff: Figure 2 compares how faculty, students, and staff responded to eight questions related to the usability of Duo[1].

Table I shows that the only categories in which there was no statistically significant difference between faculty and staff were "Concerned about compromise" and "Concerned about friends". In the cases where students, faculty, and staff were all found to be statistically significant, the mean Likert score for faculty is much closer to the mean score for students than to the mean score for staff. In every measure, staff had the most positive perceptions of Duo's usability. Student's had the worst perceptions in every case except for one; slightly more students found Duo to be easy to use than did faculty.

Most faculty (62%) reported at least one instance where they were unable to access their account because of Duo, compared to nearly half (49%) of the students and nearly one-third (31%) of the staff. Relatively few students (27%) had 2FA enabled on another account compared to faculty and staff (40% and 47% respectively).

[1]We converted the five-point Likert scale questions into a binary Agree or Do Not Agree variable. Individuals who responded with "Neither agree nor disagree" were considered part of the Do Not Agree group.

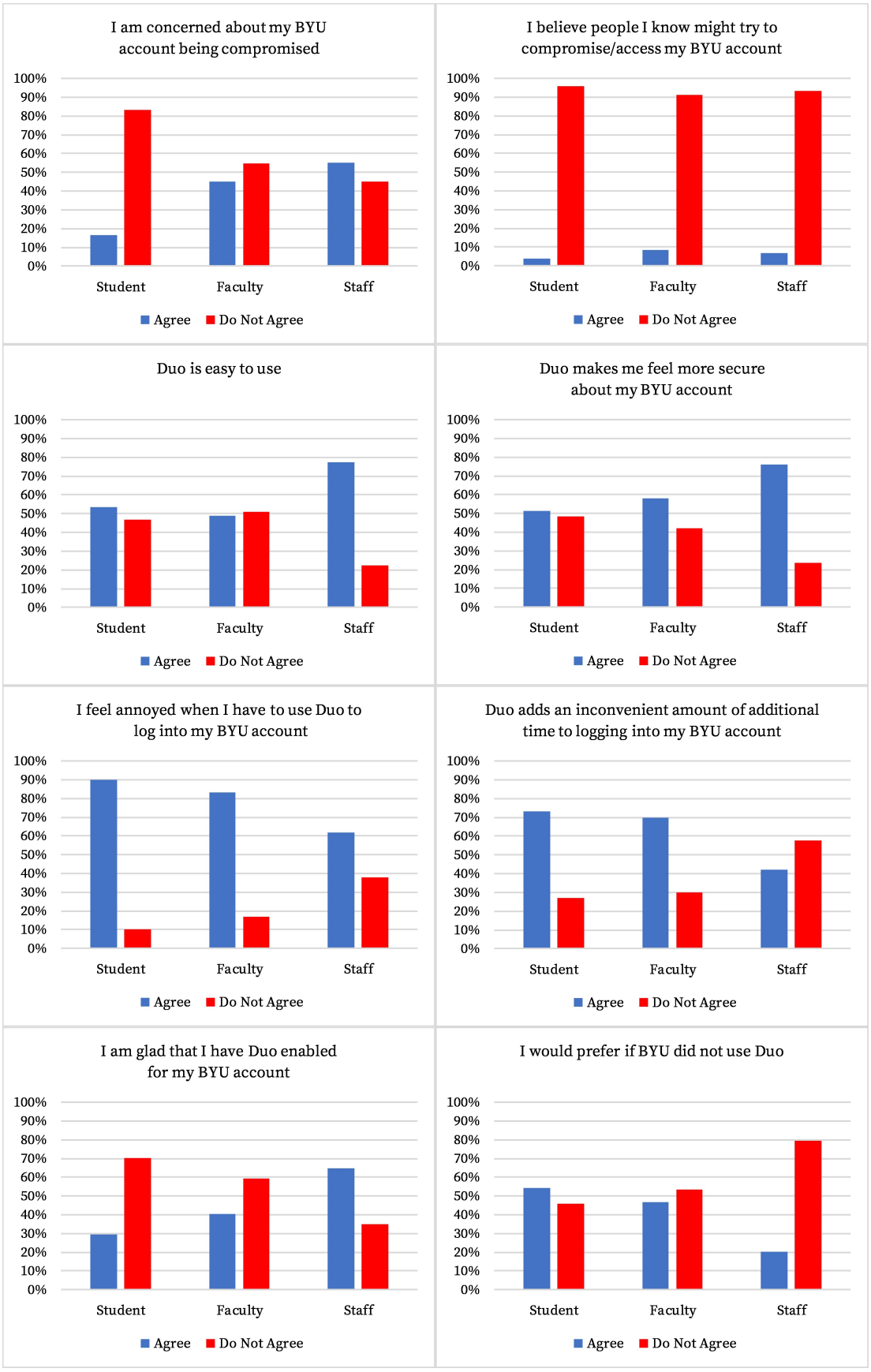

Fig. 2. Comparison of distribution of agreement between students, faculty, and staff

TABLE II
COMPARISON OF DEVICES USED WEEKLY TO ACCESS A BYU ACCOUNT

	Personal Mobile	Personal Computer	Work Computer	Public Computer
Student	85%	94%	37%	27%
Faculty	68%	76%	88%	14%
Staff	64%	62%	88%	1%

3) Duo Authentication methods: Duo Push was the most popular authentication method by far. The vast majority of respondents reported that they always or usually used Duo push to authenticate (81%). The "Call Me" option was the second most common authentication method that participants reported they always or usually used (12%). A smaller percentage relied primarily on passcodes to authenticate (8%), while virtually no one used the U2F token as their primary authentication method[2]. We found no striking differences in the choice of Duo authentication methods between students, faculty, and staff.

4) Device Usage: Although students and faculty opinions about Duo's usability were closer than staff opinions, faculty device usage was closer to staff than it was to students. Table II shows that students use personal computers, public computers, and mobile phones more often than faculty and staff, while faculty and staff use work computers more often than students.

B. Qualitative Results

The survey included 1,806 responses from individuals describing circumstances in which they were unable to access their BYU account because of Duo. These responses were coded into 9 categories by two researchers. Of those 1,806 responses, over half (940; 52%) reported that the incident was due to an inability to access the cell phone they had registered with Duo. This included devices that are lost, stolen, left at home or somewhere else, out of battery, or otherwise inaccessible. Other significant reasons people gave for being unable to authenticate with Duo included technical issues with the Duo app or servers (132; 7%), a lack of cell service or WiFi connectivity (305; 17%), switching to a new phone (150; 8%), and challenges setting up Duo (70; 4%).

The survey also included 1,454 responses to the open-ended question inviting them to share positive or negative feelings about Duo. Most of the responses (997; 69%) were negative. The rest of the responses were divided between positive (253; 17%), both positive and negative (145; 10%), or neutral (59; 4%). In the remainder of this section, we discuss commonly observed sentiments using a selection of representative comments.

1) Lack of understanding about Duo's features: Many individuals are not aware of all of the features Duo offers, and they limit themselves to using less-convenient second factors. Some respondents felt like they did not receive adequate training on Duo when it became required for accessing sensitive information on BYU accounts.

> **P3665:** *"My only concern is that it wasn't explained super well when it first started. I didn't understand the different options for using duo push."*
>
> **P3939:** *"It would have been helpful if someone had explained Duo at the start of the semester."*
>
> **P2826:** *"No one told us how Duo worked, but my parents were needing my tax info, so we went in, set up Duo and got the tax info. My phone had poor service where I was, so my dad used his phone number and it was really messed up. That whole night I was unable to access my account. I spent a week communicating with the IT office to get it fixed. It was so frustrating, even though it was our own fault. We just didn't know what it was or how it worked or why it had to be there."*

Although SMS codes are often one of the most common and convenient second-factors [14] some respondents were not aware that they could receive text codes through Duo.

> **P1107:** *"I didn't know that I could just enable a text message code. If I had known that, I would have done that..."*

Others were unaware of the option to remember their device for 30 days.

> **P4069:** *"I have to login to servers all day long and hate having to go thru Duo at least 20-30 times a day... I never noticed the 'Remember me for 30 days' as I blew past the irritation! Guess I will try it now..."*

Multiple respondents expressed frustration at having to move to a place with cell service or WiFi to authenticate. Only the "Call Me" or "Text me new codes" options require cell service, and only the Duo push option requires Wi-Fi. The Duo Mobile app, which is required for the Duo push option, also includes an HMAC-based One-time Password (HOTP) generator. HOTP codes are generated without Wi-Fi and could save students and professors from running around when Wi-Fi or cell service is poor.

> **P4074:** *"I work in a lab that doesn't always have good WiFi service (and has no cell service). I need to run down the hall to answer any calls from Duo."*
>
> **P3727:** *"It's just frustrating when you are in a classroom with bad wi-fi and it asks for a DuoPush and I have to run frantically down a hallway to get to wifi access before the push expires."*

2) The impact of education on perceptions of usability: Some participants were not aware of core Duo features, such as the option to remember a device.

> **P1107:** *"I hate opening [the Duo] app, and it took me three months before someone pointed out that I could tell the login to remember me for 30 days. Before I found that, it was an incredibly annoying hassle."*

[2]The percentages total more than 100% because some users reported using several methods frequently.

Respondents recognized that being properly trained on how to use Duo impacted their perception of Duo's usability.

> **P3256:** *"I spent time learning the ropes at the beginning, carry passcodes as a backup, and have had no trouble."*
>
> **P3447:** *"I'm not a fan of the system, but I also don't feel like I've been adequately trained."*

3) Lack of concern about account compromise: Many respondents stated that they are not concerned with the consequences of a compromise of their university account.

> **P876:** *"No one I know has had a problem with BYU security before, and even if someone does breach the account, there isn't really an unrepairable issue someone could do. Someone sees my grades, I don't care. Someone try to pay my financial center bills, I pay them immediately anyway. Someone drops or withdraws from a class, I can talk with the university and explain it and continue with my life."*

Other respondents said they would prefer to limit Duo to only sensitive transactions (such as financial transactions or class registration) while allowing access to sites such as Learning Suite (BYU's learning management system) without a second factor.

> **P2801:** *"I understand the point of Duo and think it makes a lot of sense for health information and payroll and stuff. It's just obnoxious when all you want to do is check learning suite from a campus computer."*
>
> **P2960:** *"If someone wants to do my homework for me, go ahead and let them submit it for me. Just put the second authentification on pages like Registrar, or Financial Center."*

4) Misperceptions about how Duo protects: Some of the frustration with Duo stemmed from a misunderstanding about the purpose of Duo in protecting an online account. Many respondents expressed concern that Duo would not protect them if their mobile phone were stolen.

> **P3268:** *"What worries me is that if a person steals your phone, gets in (which supposedly isn't too hard), and accesses your BYU account, can't they do the Duo from the phone as well?"*
>
> **P2171:** *"I don't understand this - So someone can't get into my account from a computer, but if they have my phone they have all that they need to get in. Honestly, I am more concerned about having my phone stolen, it is an easier object to steal. So all a person has to do is take my phone, get the Duo code, and login! I really don't feel like this has made my account safer."*

While it is true that an attacker may be able to use a stolen mobile phone to authenticate with Duo, the attacker would also need to know the individual's username and password to access their university account. Also, smartphones must be unlocked before using them as a second factor for Duo, and most smartphones require a pin, passcode, or biometric to unlock the phone. No respondent acknowledged that a physical second factor protects their account from remote attackers. One respondent suggested that

> **P851:** *"Maybe if students were more educated about why it is important, we would be less annoyed about using it."*

Educating Duo users about how two-factor authentication protects their account could decrease annoyance surrounding the use of 2FA systems.

5) Reliance on cell phones: Many respondents expressed frustration that Duo increased their reliance on cell phones. One staff member was disappointed that they could no longer implement a no-phone policy among their employees.

> **P4083:** *"With Duo I cannot reasonably ask employees to leave their phones in their backpacks and still expect that they are going to be able to get to the programs they need to get to without their phones."*

Physical tokens (i.e., hardware passcode generators and U2F keys) are alternatives to phones but are not well advertised.

> **P3684:** *"We were not told about the tokens available in the bookstore originally. One of my colleagues did not have a cellphone nor any desire to get one."*

Some individuals who used the hardware passcode generator complained about the devices failing or getting unsynced. Although BYU adopted Duo over a year ago, knowledge about hardware tokens remains low. The BYU IT website on hardware token information states that users who want to purchase a hardware token can ask about one at BYU's campus store register. When we visited the store and asked about the tokens, most employees we talked with had heard nothing about these tokens. After talking to multiple employees, we found one who knew about the Duo hardware tokens, although none of the employees knew anything about the BYU store selling U2F devices. One survey respondent complained that the BYU store did not carry Yubikey devices. Since then the BYU store has stocked or restocked YubiKeys.

6) Internet filters and safe browsing: Four users attributed difficulties with Duo to their usage of Internet filters.

> **P2087:** *"The Duo log in screen is blocked by certain web filters, which doesn't let me use my BYU account on my phone and iPad. VERY ANNOYING."*

Fifteen users mentioned not being able to log into Duo on Apple devices or browsers. Many attributed this to Apple's safe browsing functionality.

> **P907:** *"When restrictions are enabled on Apple phones, it will block the Duo login, and the page won't load, so I am blocked from my account. I finally worked with OIT, and they helped me add the Duo platform manually, so the phone wouldn't block the website anymore."*

White-listing `https://duo.byu.edu/` solved this for some users, while others simply disabled their web content

restrictions so they could access Duo. Android users did not experience this issue, although five users mentioned having difficulty receiving push notifications on their Android phones.

7) Desires for Duo policy changes: Only certain pages hosted by BYU require Duo, but once an individual enrolls, they are unable to access any page that requires a university login without authenticating with Duo. Multiple survey respondents expressed a desire that Duo protect only sensitive personal information (i.e., the pages where Duo is required to obtain access). In particular, some students expressed a wish that they could access Learning Suite without authenticating with Duo.

> **P2352:** *"I think Duo is a great idea. I would like to see it used ONLY for the financial center portion. I really do not care if someone can hack learning [suite], but I would LOVE to see it involved in everything that has to do with TAX and with FINANCES."*
>
> **P2421:** *"I am glad to have it when I log into things like my financial center, but it feels excessive to have it on Learning Suite."*

Some users felt that 30 days is too short a period for the "Remember Me" option.

> **P3413:** *"The two-factor authentication is not remembered for long enough. Google only requires renewal once on a computer or when you change your password. Every month is kind of annoying especially since checking the "remember me" box doesn't always work."*

VI. Discussion

This section discusses the results, recommends ways to improve 2FA usability, and provides study limitations.

A. Lack of Understanding

Much of the frustration expressed in the free-response subsection of the survey indicates a lack of understanding about how to set up and use Duo. Previous work shows that educational video messages can promote adoption [6] [7]. The challenge is getting users to view them in practice, as the prior work had the users view videos during a lab study.

B. UI Recommendations

The Duo prompt interface at BYU shown in Figure 3 has the basic look and feel of the Duo prompt for all organizations that have adopted Duo. When the link titled "Need help?" on the left side is selected, the blue box along the bottom appears with a message that each organization can customize. At BYU, this message provides the URL of the university's Duo support website and the phone number and email address of the Office of Information Technology. The URL is not a clickable link, and users are not always amenable to making a phone call or sending an email to seek help. Some survey respondents reported feeling rushed to authenticate, which may make them less likely to spend time utilizing these help options.

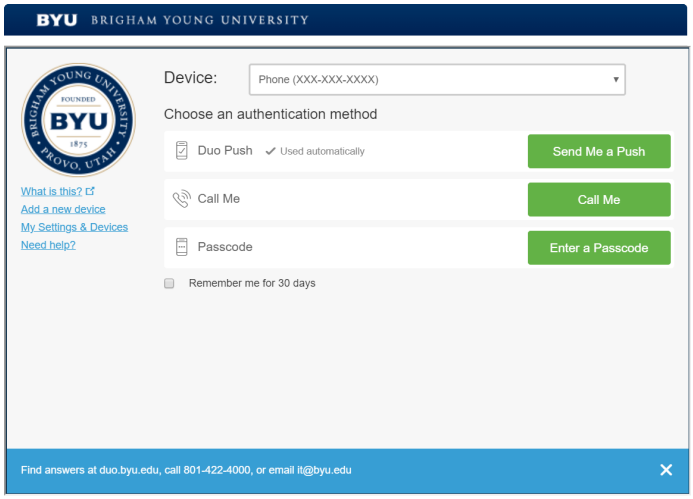

Fig. 3. The Duo prompt after selecting the "Need help?" link

In response to the user feedback we received in the study, we recommend three changes to the Duo UI that may increase usability and improve user sentiment towards Duo.

1) Put an indication next to each authentication option to inform users which methods require Wi-Fi or cell service and which methods do not. Such an indicator would assist users who are unaware of the methods they can use without Wi-Fi or cell service.
2) The "Remember me for 30 days" box should be made larger and more prominent, perhaps moved to be directly beneath "Choose an authentication method." The current design may lead users to push one of the green buttons without noticing the "Remember Me" box.
3) Increasing the conspicuousness of the "Need Help?" link may allow users who are struggling to log in to more easily find the information they need.

Since the Duo prompt has the same basic format for all its clients, our UI recommendations would benefit all Duo clients, not just BYU.

C. Balancing Usability and Security

The user study reveals opportunities to reduce the frequency of Duo authentication. However, the tradeoffs in usability and security deserve careful analysis. Some users would prefer that BYU only activate Duo on web pages that involve highly sensitive financial or personal data. Some students did not like BYU requiring 2FA on the learning system for submitting assignments, for instance. Another suggestion is to increase the "Remember Me" period beyond 30 days. The Remembered Devices policy setting in Duo supports up to 365 days [3]. Google and Facebook remember a device indefinitely. Increasing this period may improve Duo's usability for many users.

Duo currently supports only mobile devices (e.g., phones, tablets, hardware tokens) as the second-factor device. Some participants reported logging into their university account from

their phone. In this case, the computing device and second-factor device are the same. This arrangement arguably has less security, but it has the added convenience that a second device is not required. 94% of students (and most faculty and staff) access their BYU account on a personal computer at least once a week. We recommend a Duo authenticator app for personal computers to allow users the option to authenticate from their computer without needing a phone. This convenience could reduce the number of situations where users are unable to access their account, considering that 52% of these situations result from an inability to authenticate with a mobile device.

D. CMU Study

Our results confirm some of the findings from Colnago et al. [10] where participants encountered similar challenges. (1) Some participants are annoyed with 2FA—the differences are minor yet statistically significant. (2) A lack of awareness of the "Remember Me" option. (3) The need for clear, on-screen instructions–we provide specific UI recommendations. (4) A suggestion to consider not requiring 2FA on less-sensitive portions of the web site.

While their study found that the faculty and staff they analyzed "presented similar opinions and behaviors," our study found faculty perceptions to be generally closer to students than to staff. We made several recommendations to reduce how often 2FA occurs. The CMU study also suggests an idea for reducing 2FA authentications for students using campus computers—remember users that have logged into any campus lab computer or from within a subnet.

E. Limitations

Participants were recruited exclusively from the population of students, faculty, and staff at BYU. Our findings may not be as relevant to other populations. Since respondents were self-selected volunteers, our survey has voluntary response bias. Individuals with strong feelings about Duo or two-factor authentication may have been more likely to take the survey. Because we were unaware that BYU offers hardware passcode generators, we did not include a question about the frequency of hardware passcode generator use in the survey. Unfortunately, we do not have data on the specifics of BYU's onboarding process for Duo, which could have provided valuable context to our discussion about the need to improve user awareness and understanding.

VII. Conclusion

This paper presented the results of a large survey of faculty, staff, and students at BYU that use Duo two-factor authentication. A majority of the participants felt more secure using Duo and felt it was easy to use. The survey responses also revealed several pain points for Duo users. In response, we offer recommendations that reduce the frequency of 2FA for Duo users: increase the length of the "Remember Me" option, only use 2FA on the most sensitive portions of the website, and provide an authenticator app on personal computers. These adjustments may have acceptable security tradeoffs given a threat model of a remote attacker. We also suggested UI changes to draw more attention to 2FA methods that do not require WiFi, and making the help option more visible.

Future research can explore whether informational videos can be made available outside the lab in a way that is effective at increasing 2FA adoption and understanding. Another avenue for future research is to explore 2FA with a broader population of users beyond the university setting.

Acknowledgment

The authors thank the anonymous reviewers and our shepherd, Simon Parkin, for their helpful feedback. This material is based in part on work supported by the National Science Foundation under Grant No. CNS-1816929.

References

[1] "About duo." [Online]. Available: https://duo.com/about
[2] "Google 2-step verification," https://www.google.com/landing/2step/#tab=how-it-works, accessed: 2018-11-14.
[3] "Using remembered devices & authorized networks controls." [Online]. Available: https://duo.com/docs/remembered-devices
[4] *2017 Data Breach Investigations Report*, 2017.
[5] *ITRC Data Breach Overview 2005 to 2017*, 2018.
[6] P. Ackerman, "Impediments to adoption of two-factor authentication by home end-users," *SANS Institute InfoSec Reading Room*, Sep 2014.
[7] Y. Albayram, M. M. H. Khan, and M. Fagan, "A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2FA)," *International Journal of HumanComputer Interaction*, vol. 33, no. 11, pp. 927–942, 2017.
[8] R. F. Baumeister, E. Bratslavsky, C. Finkenauer, and K. D. Vohs, "Bad is stronger than good," *Review of General Psychology*, vol. 5, no. 4, 2001.
[9] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, 2012, pp. 553–567.
[10] 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*, 2018.
[11] E. D. Cristofaro, H. Du, J. Freudiger, and G. Norcie, "Two-factor or not two-factor? A comparative usability study of two-factor authentication," *CoRR*, vol. abs/1309.5344, 2013.
[12] 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 *2018 International Conference on Financial Cryptography and Data Security (FC)*, 2018.
[13] 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, pp. 208–220, 2011.
[14] A. Kemshall, "Why mobile two-factor authentication makes sense," *Network Security*, vol. 2011, no. 4, pp. 9–12, 2011.
[15] K. Krol, E. Philippou, E. D. Cristofaro, and M. A. Sasse, ""They brought in the horrible key ring thing!" Analysing the usability of two-factor authentication in UK online banking," *CoRR*, vol. abs/1501.04434, 2015.
[16] N. Kumar, "Password in practice: An usability survey," *Journal of Global Research in Computer Science*, vol. 2, no. 5, p. 107112, 2011.
[17] R. Morris and K. Thompson, "Password security: A case history," *Commun. ACM*, vol. 22, no. 11, pp. 594–597, Nov. 1979.
[18] G. Norman, "Likert scales, levels of measurement and the "laws" of statistics," *Advances in Health Sciences Education*, vol. 15, no. 5, pp. 625–632, Dec 2010.
[19] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, "Two-factor authentication: Is the world ready? quantifying 2FA adoption," in *Eighth European Workshop on System Security (EuroSEC)*, 2015.
[20] 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.