"It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University

Jessica Colnago, Summer Devlin*, Maggie Oates, Chelse Swoopes, Lujo Bauer, Lorrie Cranor, Nicolas Christin
Carnegie Mellon University, *University of California, Berkeley
{jcolnago, cswoopes, moates, lbauer, lorrie, nicolasc}@cmu.edu, *devlins@berkeley.edu

ABSTRACT
Despite the additional protection it affords, two-factor authentication (2FA) adoption reportedly remains low. To better understand 2FA adoption and its barriers, we observed the deployment of a 2FA system at Carnegie Mellon University (CMU). We explore user behaviors and opinions around adoption, surrounding a mandatory adoption deadline. Our results show that (a) 2FA adopters found it annoying, but fairly easy to use, and believed it made their accounts more secure; (b) experience with CMU Duo often led to positive perceptions, sometimes translating into 2FA adoption for other accounts; and (c) the differences between users required to adopt 2FA and those who adopted voluntarily are smaller than expected. We also explore the relationship between different usage patterns and perceived usability, and identify user misconceptions, insecure practices, and design issues. We conclude with recommendations for large-scale 2FA deployments to maximize adoption, focusing on implementation design, use of adoption mandates, and strategic messaging.

ACM Classification Keywords
K.6.5 Security and Protection: Authentication; H.5.2 User Interfaces: Evaluation/methodology

Author Keywords
two-factor authentication; adoption; usability

INTRODUCTION
Password breaches, either due to the large number of password database leaks [17] or to increasingly sophisticated (and possibly targeted) phishing attacks, seriously increase the risk of authentication credential compromise. Worse, these risks are further compounded by poor user password hygiene, such as creating easily discoverable passwords or reusing them across multiple accounts [25].

One way to mitigate the harm of password breaches is to couple passwords with another authentication factor. This layered process is known as two-factor authentication (2FA). 2FA is defined as the use of more than one factor from different categories of authentication methods. These categories have been identified as *something you know*, *something you have*, and *something you are* [12]. *Something you know* is knowledge that a user has, for example, a password or answers to security questions. *Something you have* is a device or object such as a paper token (e.g. a list of one-time passwords), a software token (e.g. a cookie or an application-generated token), or a hardware token (e.g. RSA SecurID). Lastly, *something you are* is a biometric (e.g. retina or fingerprint).

While the use of 2FA is not new—Google launched 2FA over five years ago [22] and Automated Teller Machines have used a card (something you have) and a PIN (something you know) for decades—adoption of 2FA for computer systems is not widespread. Recent reports show that less than 10% of Google user accounts use 2FA [23], and in 2016 Dropbox reported 2FA adoption rates of less than 1% of users [14].

Factors behind technology adoption decisions have been explored [26, 27], with a particular focus on the interactions of usability, value, and adoption. However, previous work on transitions to 2FA systems focused on areas where users expect high security, such as in financial applications. As institutions, such as universities have shown increasing interest in adopting 2FA [4, 18, 19, 24], research to understand how 2FA systems are adopted when users place differing values on the security of their accounts becomes even more practically important.

In this paper, we explore the factors behind 2FA adoption decisions by leveraging Carnegie Mellon University (CMU)'s institution-wide switch from a one-factor single-sign-on system to an implementation of a popular 2FA platform, Duo Mobile (Duo) [10]. CMU now requires the use of Duo for anyone who is in the university's payroll system—adoption is optional only for students who do not hold paid university jobs. We explore the behaviors and opinions surrounding 2FA, providing insights into what drives adoption across different types of users (faculty, staff, and students) who may have different perceptions of the value of the added security.

We collected usage and adoption data from CMU's Information Security Office (ISO) and from two large-scale surveys conducted before and after Duo became mandatory for university employees. These surveys explored adoption and usage

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

CHI 2018 April 21–26, 2018, Montreal, QC, Canada

© 2018 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-5620-6/18/04.
DOI: https://doi.org/10.1145/3173574.3174030

patters, sentiment towards 2FA, value perception, and issues experienced with Duo.

Our results show that overall, people who adopted 2FA at CMU found it annoying, but fairly easy to use, and believed it made their accounts more secure. A user's experience with CMU's deployment of Duo often led to positive perceptions of Duo, which sometimes translated into 2FA adoption for other accounts. The likelihood that a user would subsequently adopt 2FA for other accounts was related to their opinions about 2FA ease-of-use and perceived value. While we found some evidence that people who were required to adopt 2FA had more negative perceptions than those who adopted voluntarily, the differences were smaller than expected. We also explored the relationship between usage patterns and perceived usability. Finally, we identified user misconceptions about 2FA, insecure practices that 2FA can help mitigate, and implementation and design issues. We conclude with recommendations for implementing large-scale deployments of 2FA to maximize adoption rates, focusing on smart implementation design, the potential benefits of adoption mandates, and strategic messaging.

RELATED WORK

Fundamental work on technology adoption includes the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). Both theories describe the interactions between information technology *use*, *perceived usefulness*, and *perceived ease-of-use* [8, 27]. UTAUT addresses some of TAM's potential shortcomings with the introduction of other factors including *social influence* (e.g. perceived peer pressure), *voluntariness* and *facilitating conditions* (e.g. perceptions of infrastructural or organizational support) [27]. In a series of studies, perceived usefulness and ease-of-use were correlated with actual use, though the former was a stronger measure than the latter.

Much two-factor authentication research has recognized the need for user-friendly implementations to promote adoption. Technical solutions have allowed for smooth back-end transitions to 2FA implementations that in turn facilitate smooth front-end user transitions [16]. Examination of 2FA factors and schemes have weighed security with user concerns like scalability, general ease-of-use, and ability to recover from failure or factor loss [5, 28]. In response to one such concern, Czeskis et al. developed an opportunistic factor that does not drastically hinder a user in case of failure [7]. Bonneau et al.'s high-level evaluation of alternatives to passwords rated existing two-factor options as more secure but generally less usable than traditional text passwords [5], implying perhaps that other usability factors like social influence or facilitating conditions may be necessary to overcome adoption hurdles.

Apart from these illustrations on balancing usability and security, only a few studies have focused on collecting and assessing perceptions of 2FA in relation to adoption. A better understanding of this balance is crucial to furthering adoption, especially when the *fear* of user resistance, rather than user resistance itself, can inhibit adoption of 2FA systems by an organization. Libicki et al. interviewed representatives from companies that had implemented 2FA and found "little evidence from organizations that their users pushed back against [2FA] adoption—particularly once it became mandatory," but that officials cited worries about user outcry and possible defection to competitors [15]. Grossklags and Weidman explored the transition from an academic institution's token-based 2FA system to a 2FA system that used employee-owned mobile devices, finding that users perceived the mobile device system more negatively than the token-based system, largely due to resentment about being required to use a personal device [29].

Previous work has found differing results on whether users value usability or security more when using 2FA. A survey of online banking users found 2FA approximately as usable as single-factor sign-ons, also citing 2FA as being more secure [3]. On the other hand, a telephone banking study found that users rated 2FA as more secure than single-factor authentication, but also perceived decreased convenience and ease-of-use, and experienced more authentication failures [13]. Another study found a more complex interaction between perceptions of usability, convenience, quality, and security across three different 2FA devices for online banking authentication. Most participants chose their preferred 2FA device based on perceptions of usability rather than security [30]. A small ethnographic study on smart card usage at a U.S. federal research institute reported similar results [20]. De Cristofaro et al. explored 2FA for use with personal accounts, social media accounts, and job-related accounts, finding that 2FA device adoption changes with context. However, usability perceptions were found to be similar across devices and contexts, and were correlated more with user demographics than with context [6].

Both Ackerman [1] and Albayram et al. [2] explored how educational messaging affects 2FA perceptions and adoption, using video experiments with a variety of messaging techniques, such as cybercrime fear appeal, personal fear appeal, or self-efficacy. Both found that exposing participants to messaging about cybersecurity risk was effective. Ackerman also focused on 2FA's ease-of-use, and Albayram et al. found adoption success with videos promoting self-efficacy.

Our work provides a robust contribution to 2FA adoption literature given its scale, heterogeneity of users and contexts, and longitudinal focus. Carnegie Mellon University's variety of systems (e.g. educational, email, financial), user roles (e.g. students vs staff, mandated vs voluntary users), and user experience (new vs experienced 2FA users) allows a deeper assessment of the interactions between individual differences, value of the protected information, user perception, and 2FA adoption. We are among the first to analyze longitudinal data, mapping 2FA adoption over time at an academic institution.

CONTEXT

This study took place at Carnegie Mellon University, a university in the eastern United States, with over 5,000 faculty and staff and approximately 15,000 students. Due to an increasing number of phishing attempts and the positive experience of other universities with 2FA, CMU decided to switch, during the 2016–2017 academic year, from a one-factor authentication system to a two-factor authentication system using Duo. The implementation protected all systems behind the CMU Andrew single sign-on system with an extra layer of security. This included payroll systems, information systems, course-related

systems (e.g. Canvas), physical access systems (through the one-time login required by the CBORD application), and others. While not all university members were required to adopt 2FA, university employees and students who had university jobs had to sign up for 2FA via Duo by April 2017. After a user signed up for Duo, it was activated automatically for all university systems that used the Andrew login page.

The Duo implementation at CMU gives users several options for their second factor: a free hardware token, a Duo app for mobile devices (available for most smart phones, tablets, and smart watches) that generates both a push notification and a one-use token, Yubikey/U2F tokens (although not provided by CMU), and printed codes. While some sensitive CMU systems require Duo authentication at every login attempt, the majority remembers users for 8 hours automatically. A "remember me" option makes 2FA login necessary only once every 30 days for the device or browser on which it is enabled. When a user signs up for Duo, they can choose between always using one method (e.g. automatically receiving a push notification) or always being prompted for their preference. Lastly, users who are not required to adopt Duo can deactivate it after adoption. Unfortunately, we did not obtain data on deactivation rates.

METHODOLOGY

This was an exploratory study to see how people perceived, adopted, and used 2FA. We focused on observations that can guide future deployments and research. In particular, we were interested in user perceptions of 2FA and factors that drive and hinder adoption:

- What is the relationship between mandated use and users' perception of 2FA?
- What is the relationship between users' experiences with Duo and future adoption of 2FA?
- What are the differences between 2FA users' and non-users' perceptions of 2FA?
- What Duo usage aspects relate to users' perception of 2FA?

We were also interested in understanding design and implementation problems, as well as user misconceptions. We obtained data collected by the CMU Information Security Office (ISO) and Computing Services on Duo adoption and usage. The usage data set includes over one million authentication attempts from over 13,000 users, from September 2016 through July 2017, from which 66 were tagged by users as fraudulent login attempts. These data indicate what type of device was used, the outcome, time and date, user IDs (anonymized hashes), role at the university, as well as browser and device details. We also obtained data on Duo adoption rates and Duo-related help-desk tickets.

Furthermore, we ran two online surveys with faculty, staff, and students. The first one (S1) was deployed one to three weeks before the mandatory enrollment date and the second one (S2) three months after the mandatory enrollment date. The surveys were distributed via email by CMU's ISO to a random sample of the CMU population located in the United States. We obtained 1,251 responses for S1 and 796 responses for S2 (each had a response rate of ~13%). Participants were not compensated for their participation. The survey protocol was approved by CMU's IRB.

The first survey focused on better understanding how people perceived Duo and 2FA before being exposed to it or after having used it for only a short time. The second survey followed up on results from S1 to investigate what could cause differences in perception of Duo and explored the effect of time on how people perceive Duo and 2FA. Both surveys had a number of multiple choice, 5-point Likert, and open-ended questions. The median time to complete the surveys was 4.5 minutes for S1 and 10 minutes for S2. S1 asked participants whether they had activated Duo and, if not, how likely they were to activate it; its advantages and disadvantages; past and current 2FA usage; and, their agreement on a 5-point Likert scale with six constructs related to their perceptions of the usability and security of 2FA/Duo:[1]

Security "Activating two-factor authentication makes my account less likely to be compromised."

Tranquility "Activating two-factor authentication means I do not have to worry as much about my account safety."

Fun "I think that two-factor authentication is fun to use."

Easy "I think that two-factor authentication is easy to use."

Difficult "I think that using two-factor authentication is difficult to use."

Annoying "I think that two-factor authentication is annoying to use."

S1 was first deployed to faculty and staff, and two weeks later to students. The student version had extra questions about current Duo usage, as preliminary examination of faculty/staff data showed that many had already adopted it. S2 asked participants whether they had activated Duo and why; if they shared their credentials with third-parties; when they adopted 2FA and if it had been mandatory; their agreement to perception constructs as in S1; their experience with 2FA-related issues; their opinion about whether adding 2FA was a good idea for security; patterns of Duo and general computer use; and 2FA use on other accounts before and after Duo. Both surveys are available as online appendices.

We used ordinal logistic regressions to explore the effects of mandating adoption and experience on sentiment, and logistic regressions to explore the effects of sentiment on future adoption. For these analyses we dropped participants who did not specify one of the main groups for gender and age to simplify interpretation. In S1 we dropped 13 for age and 32 for gender, while in S2 we dropped six for age and five for gender.

For the exploratory analyses of what affects usability, we used Fisher or Chi-Square tests to analyze pairs of nominal variables, such as Duo adoption between users in relation to their use of the HR system and our sample demographics to the university data; and Spearman's rho to report on the relationship between ordinal variables, namely sentiment toward 2FA in relation to usage duration, frequency of use, use of multiple devices, frequencies of issues associated with Duo, and perceived consequences of Duo. For Fisher and Chi-Square tests

[1]We slightly rephrased statements for participants who had never used 2FA before: "makes" was rephrased as "will make."

we report on Cramer's V as their effect size. Cramer's V effect sizes smaller than .15 are considered negligible. We use the Bonferroni correction for multiple hypothesis testing.

We conducted qualitative analyses on open-ended responses using inductive coding to design code books. Two researchers separately coded the data sets. For large data sets (over 300 responses) we performed an iterative coding process with a third of the responses at a time, followed by a final conflict resolution. For small data sets iterations were performed on the entire set. All qualitative coding had substantial to perfect agreement, with the lowest Cohen's Kappa being .731.

LIMITATIONS

Our results are limited by the self-reported nature of surveys and natural selection bias. While we did complement our survey findings with actual usage and adoption data, not all of these findings could be corroborated. Furthermore, we seem to have significantly under sampled non-adopters, possibly as a result of the recruitment text or their belief that they would not be able to contribute to the research as they were not already Duo users. This low number of non-adopters in our sample could lead us to overstate some perspectives, or miss other relevant experiences and opinions.

DEMOGRAPHICS

Our sample was demographically similar to the Carnegie Mellon University population. For both S1 and S2, gender was almost equally distributed (S1. Female: 45%, Male: 52%, Preferred not to answer: 3%, Other: < 1%; S2. Female: 45%, Male: 55%, Other: $< 1\%$) and the gender distribution for students, faculty, and staff are similar to the university-wide population, but with more women for faculty and staff in S1 (S1. Students: $\chi^2(1) = 1.55, p = .213$, Faculty and staff: $\chi^2(1) = 14.4, p < .001$; S2. Students: $\chi^2(1) = 2.75, p = .100$, Faculty and staff: $\chi^2(1) = .491, p = .483$). The largest age group for S1 and S2, aged between 25 and 34 years, represents 23% of the S1 sample, and 22% of the S2 sample. Faculty and staff presented similar opinions and behaviors throughout our analyses and so, we present them as a single group. On the other hand, students generally had different opinions and behaviors from faculty and staff and we thus present the results separately. Whenever there are substantial differences between groups, we report the results separately.

ADOPTION RATES AND USAGE PATTERNS

Figure 1 shows Duo adoption over time. At the mandatory Duo adoption deadline, a significant percentage of faculty and staff had already enrolled (~75%), while only ~20% of students had done so. The overall low adoption rate for students even after three months after the deadline (~50%) is likely because only students on university payroll are required to use Duo.

The first university-wide notification about Duo went out at the end of 2016 through the Computing Service's news feed. This message was sent directly to subscribers and forwarded to department email lists. As shown in Figure 1, this message had little effect on adoption, especially for students. About three months later the Provost sent an email to all students, faculty, and staff about CMU's decision to adopt 2FA and its

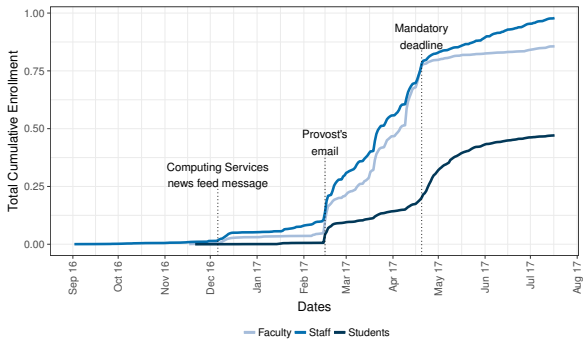

Figure 1. Duo adoption over time by faculty, staff, and students.

importance. This email sparked a large uptick in adoption for faculty and staff, and a moderate one for students.

Previous Use

40% of S1 participants and 39% of S2 participants had previously used 2FA for another account other than for CMU, mainly financial and email accounts. S1 respondents who mentioned prior 2FA use were most likely to have used a system that sent a code via SMS (Faculty and Staff: 52%, Students: 53%), used push notifications (Faculty and Staff: 41%, Students: 43%), software-generated codes (Faculty and Staff: 38%, Students: 41%), or hardware-token-generated codes (Faculty and Staff: 36%, Students: 15%). Faculty and staff were the primary users of hardware tokens.

Duration and Frequency of Use

90% of our S1 sample and 99% of our S2 sample reported having already adopted Duo. Most of the students in our S1 sample reported that they had already been using Duo for at least a month (about a month: 29%; more than a month: 56%).[2] Three months later, at the time of S2, most participants reported that they had been using Duo for at least three months. 45% of students, reported using Duo more than 3 months and 19% more than 6 months. Our analysis of the authentication log data for the entire university population also showed that most users had been using Duo for close to three months at the time of S2 (M: 92 days, Mdn: 86 days).

We asked S2 participants, "How frequently do you have to interact with CMU Duo (e.g. send a push or type in a passcode)?" 47% of participants reported interacting with Duo a few times per month or less, 18% a few times a week, 17% 1 to 2 times a day, and 17% 3 to 5 times a day. The log data from April through July 2017 suggests that survey participants may have under reported their Duo usage. We found that 54% of users averaged more than one login attempt per day, including those who used the "remember me" option. On average, users logged in with Duo twice per day (M: 2.29, Mdn: 2).

Authentication Devices

We asked S1 student participants "What type of devices are you using with CMU Duo?" Most (98%) reported using their smartphone for Duo authentication. We also asked students in

[2]Faculty and staff were not asked about Duo usage in S1.

S1 "Which CMU Duo setup do you use? (Please select all that apply)" and found that the three most used setups were push notification (91%), app-generated passcode (21%), and hard token (4%), with student participants mostly using one (M: 1.13, Mdn: 1). The log data for all users from April through July 2017 exploring logins that used the aforementioned methods shows that push notifications were the most frequently used (89%), followed by app-generated passcode (7%), hardware token (4%), and U2F token and Yubikey (<1%). In addition, the log data for all users and the student subset shows that on average each user uses 1.3 of these methods (Mdn: 1).

WHAT DRIVES AND HINDERS ADOPTION?

Here we describe the main findings related to Duo adoption, focusing on mandated use, previous experience with 2FA, and perceived ease-of-use. Overall, survey respondents found using 2FA annoying but easy to use, and perceived it as improving their account security. Full statistical results and tables summarizing qualitative results are in the online appendix.

Mandated Use and Usability Perceptions

Because participants would not necessarily know if Duo adoption was mandatory for them before the deadline, as a proxy we asked S1 participants whether they had used CMU's online HR system during the past year. Those who had would likely need to continue using the system going forward, and would have to enroll in Duo. Since the adoption deadline had passed when we administered S2, we asked participants directly if they had been required to adopt Duo. As expected, the vast majority of faculty and staff reported having used the online HR system in the past academic year (92%) while only 61% of students had done so. We found in S1 that those who had used the HR system enabled Duo more frequently than those who had not (92% vs 78%, $\chi^2(1) = 37.4, p < .001, ES = .173$).

Table 1 shows the regression of the binary "Mandatory" status, and binary variables "CMU Duo User" and "Prior 2FA User" on sentiment (5-point Likert). The variables "Student," "Male," and "Age" are control co-variates.[3]

We hypothesized that people would resent being required to use 2FA, affecting how they perceived its usability (i.e. easy, difficult, fun, and annoying). However, as shown in Table 1, for S1 the binary variable that adoption was required ("Mandatory") was not present in any of the best-fit models. For S2, on the other hand, the same variable was statistically significant in all but one of the best-fit models. The largest effect we observed was for agreement with the statement that 2FA is annoying, for which the log-odds were .89 and the odds ratio $e^{.89} = 2.43$. This means, for example, that the chance of participants strongly agreeing with that statement is 2.43 times higher if adoption is mandatory than if it is not. This difference could be a temporal trend, evidence of minor resentment, or a difference in sample groups (e.g. those with more negative opinions decided to respond to S2 to voice them).

[3]Student and male are binary variables. Age ranges from 18 to 85+, with the first group being 18-24, followed by 10-year groupings. Students who were also staff have their opinion represented only as students. Staff and Faculty were grouped together as "non-students."

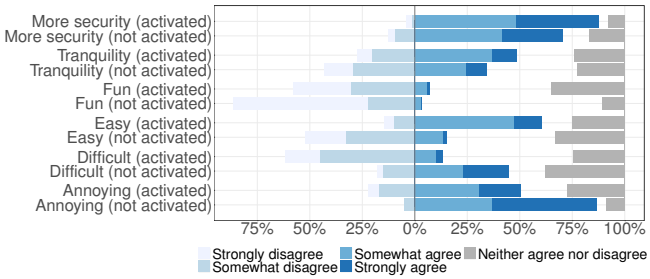

Figure 2. Agreement with sentiment constructs for participants in S1 who had activated Duo and those who had not.

Experience with 2FA and Usability Perceptions

We hypothesized that prior experience with 2FA or use of Duo at CMU would have a positive impact on perceptions about 2FA, and confirmed this. As shown in Table 1, when we compared CMU Duo users with non-users, we found statistically significant differences with strong effect sizes for all usability constructs, and small effects for the security-related constructs. Participants who had activated Duo were more likely to agree that it was easy and fun, and less likely to agree that it was difficult and annoying. Figure 2 shows the distribution of agreement to each statement between those who had activated Duo and those who had not. Furthermore, we found those who reported prior 2FA use were more likely to agree that it was easy, and less likely to agree that it was difficult. These findings suggest that those who have never used 2FA are likely to perceive it as more difficult to use than it actually is.

Preconceived Opinions and Adoption

We asked S1 participants who had not adopted Duo yet how likely they were to adopt and why (open-ended). We received and coded 76 responses, which related predominantly to perceived usefulness and concerns about usability and inconvenience. Seventeen participants did not think their account required the security ("Nothing a CMU student can access on the network is private or important enough to warrant this inane policy"). Twelve participants mentioned the extra time and effort that they believed adoption would incur ("It is a hassle to have 2-factor authentication," "too much trouble"). Ten participants mentioned inconvenience or negative consequences ("It's inconvenient," "if I'm locked out of my room that would be more [hassle] than it's worth"). Six participants mentioned not being able to perform tasks if the second-factor device was not available (forgotten, lost, broken, or uncharged). Finally, five participants reported that hearing about negative experiences led them to not want to adopt it ("I have heard it is a complete hassle and people regret doing it."). Refer to the online appendix for a full list of themes.

What Affects Usability Perception?

In S1 we asked all participants about the disadvantages of using 2FA. From the 2,511 coded responses the two most frequent codes were the extra step/time it would take to log in (13%) and general negative opinions expressing inconvenience (13%). Students who mentioned the extra step/time did so with

Table 1. Ordered log-odds impact of the independent variables on the different sentiment constructs measured in S1 and S2. Dashes are used for the variables that were removed during the BIC stepwise procedure. S2 does not consider "Prior 2FA user" and "CMU Duo user" as the small sample size led to rank deficiency in the regressions. *p<.05; **p<.01; ***p<.005.

	Dependent variable:											
	Security		Tranquility		Fun		Difficult		Easy		Annoying	
	(S1)	(S2)	(S1)	(S2)	(S1)	(S2)	(S1)	(S2)	(S1)	(S2)	(S1)	(S2)
Mandatory	—	−.36	—	−.48*	—	−.75***	—	.72***	—	−.70***	—	.89***
Prior 2FA user	—	NA	.51	NA	.59	NA	−.89*	NA	.77*	NA	—	NA
CMU Duo user	.55**	NA	.32	NA	1.18***	NA	−1.38***	NA	1.45***	NA	−1.36***	NA
Student	−.36*	—	.21	—	−.54***	−.56***	.92***	.98***	−.91***	−.91***	.56***	.72***
Male	.53***	.31*	−.42***	−.32*	—	—	—	—	—	—	−.35***	−.34*
Age	−.07	.08	—	.07	—	—	—	—	—	—	−.19***	−.14*

varying levels of annoyance, from stating it matter-of-factly ("Increased security usually means more work per sign-on") or as a minor issue ("A slightly slower login process, especially on public computers where you can't check 'remember me for 30 days"'), to a more significant complaint ("not easy to sign in an account; and really slow down the speed of opening any new account. For instance, I need to wait about 90 seconds to log into Blackboard after I used 2fa").

The open-ended responses provided insights into the ways different members of the university community used university computing resources, which in turn impacted their perceptions of 2FA. We observed from the S1 open-ended responses that students use multiple devices, including those where cookies are frequently cleared (for example, computers in university computer labs), and experience the most inconvenient consequences, while faculty and staff have to log in more frequently than students. In this section we explore the factors that we expected could have impacted perceptions.

Role: In S1 we observed moderate differences in perceptions based on role, with students finding Duo more annoying and difficult to use than faculty and staff, and less likely to improve their account security. We observed similar results in S2, where "mandatory" and "student" were the most frequently significant predictors of usability, both being conceptually related (i.e. Duo was not mandatory for all students).

Usage Duration: Since S1 participants who were not Duo users perceived it significantly more negatively than those who were, we expected that this positive attitude towards Duo would continue to increase with repeated usage. However, we found borderline statistically significant negative relationships between more security and ease-of-use constructs and the length of time participants reported since enrolling in Duo (security: $r_s(744) = -.100, p = .041$; easy: $r_s(744) = -.102, p = .031$). This shows that after the initial barrier is broken, opinions remain fairly constant with time.

Frequency of Use and Multiple Devices: S1 participants expressed that they had to log in multiple times during the day, either because it was necessary to log in on multiple websites that required Duo or because they used different devices. In particular, students using campus computers felt extra inconvenience because they were unable to use the "remember me" feature. As one participant put it:

> Before I activated 2fa, I enjoyed using the cluster computers for the lab section of my class. However, using these computers required a login into autolab; which then requires verification with shibboleth; and therefore 2fa. I obviously do not want to "remember for 30 days" on a public computer, but often by the end of day my phone is out of battery. So, I cannot use the cluster computers to do the lab work. Not being able to log into CMU services because I don't have my phone with me (or if my phone is out of battery) is a great inconvenience.

Overall, use of more devices led to more negative opinions. The number of devices a participant used to log in had a statistically significant impact on usability constructs (fun: $r_s(789) = -.144, p < .001$; easy: $r_s(789) = -.140, p = .001$; difficult: $r_s(789) = .173, p < .001$; annoying: $r_s(789) = .174, p < .001$). We did not find statistically significant differences in constructs based on login frequency.

Frequency of Issues Associated with Duo: S1 participants described a number of issues that were associated with Duo use: forgetting one's second factor, having it far away, losing one's phone, having a dead phone battery, having no data connection, and the hard token desynchronizing. We asked S2 participants how frequently these issues occurred. As shown in Figure 3, the device being far was the most frequent issue. The frequency of experiencing these problems had a statistically significant impact on both usability and security constructs, negatively affecting users' perceptions as the frequency of these issues increased, as seen in Table 2.

Perceived Consequences of Duo: S1 participants described a number of negative consequences of using Duo: being locked out of one's office and dorm room, not being able to do homework and participate in class, not having access to email and computer systems, and having one's current task interrupted. Students generally reported experiencing worse consequences, including being locked out of their dorm rooms. CMU students unlock their dorm rooms using their university ID cards or an app called CBORD that runs on mobile devices. One participant described this problem as follows:

> A major problem with duo is that almost all CMU students have ID holders that they stick to the back of their phone. The issue with this is that if you say leave your phone in your room and accidentally lock the door, your

	Forgot df=751	Far df=765	Lost df=736	Battery df=719	WiFi df=731	Desync df=624
Security	−.295	−.332	−.208	−.256	−.218	−.224
Tranquility	−.182	−.230	−.136	−.164	−.120	−.148
Fun	−.305	−.396	−.174	−.309	−.254	−.164
Easy	−.348	−.435	−.187	−.350	−.335	−.253
Difficult	.324	.392	.196	.342	.337	.248
Annoying	.377	.465	.207	.360	.288	.239

Table 2. Spearman's correlation coefficient (r_s) between sentiment constructs and statistically significant frequency of Duo related issues ($p < .001$) with associated degrees of freedom.

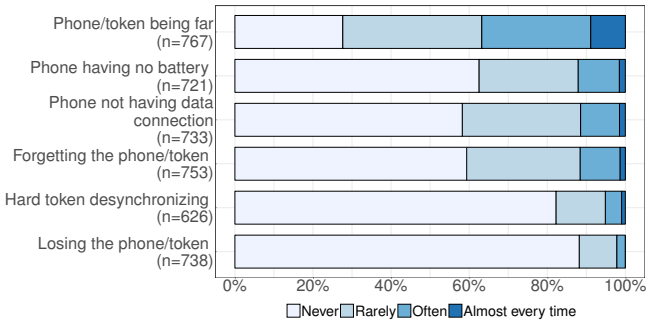

Figure 3. Frequency reported in S2 for each of the issues we identified in S1 and associated response counts. Differences in number of responses reflect N/A responses.

> ID is also in your room. I had this happen to me and whereas before I could sign into another persons phone [using the CBORD app] and get an activation code to open my door; the stupid duo required that I have a code, but the only way I could get the stupid code was [from] my phone, which was in my room!

However, Housing Services clarified that Duo is only required for the initial setup of the CBORD app on students' phones, with Duo being necessary again if the CBORD app needs to be reinstalled (e.g. if the student gets a new phone). Furthermore, only one phone per student is associated with a dorm room. As such, the expressed frustration with Duo related to physical access was likely misplaced and represents a misconception about how the systems work. As 20 S1 participants spontaneously mentioned getting locked out of dorm rooms as a Duo disadvantage, this misconception seems widespread.

As we can see in Figure 4, we asked S2 participants whether they had experienced any of the seven consequences we identified from S1 and to rate how inconvenient they were. We found that participants who experienced at least one of three most frequently reported types of inconveniences (Duo getting in the way of performing a task, accessing a system, or accessing email) generally had more negative opinions about the usability constructs, as seen in Table 3. However, the less frequent but more severe consequences "could not do homework," "could not participate in class," "locked out of my office" and "locked out of my room" were not significant after correcting for multiple hypothesis testing, with the exception of annoying for "locked out of my room" ($r_s(59) = .370, p = .02$).

	No email access df = 330 (42%)	No system access df = 345 (43.6%)	Got in the way of task df = 395 (50%)
Security	−.245	−.277	−.377
Tranquility	$-.185, p = .004$	$-.153, p = .026$	−.220
Fun	−.284	−.311	−.357
Easy	−.320	−.388	−.360
Difficult	.295	.337	.333
Annoying	.338	.434	.392

Table 3. Spearman's correlation coefficient (r_s) between sentiment constructs and statistically significant inconvenience levels of consequences of Duo ($p < .001$, except where indicated). Associated degrees of freedom and frequency are reported for the statistically significant consequences.

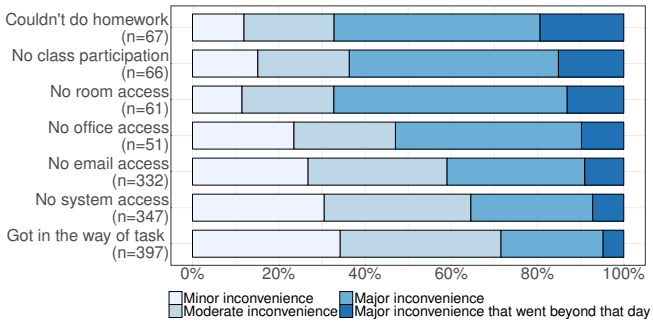

Figure 4. Inconvenience level for each of the negative consequences of Duo and associated S2 response counts.

Past Experiences Influence Future Adoption

We asked S2 participants if they added 2FA to other systems after they started using Duo. We found that 133 participants (17%) had adopted some form of 2FA. The types of second factor most frequently added were SMS-based code (61%), app-based code (47%), and app push (38%).

Duo Effect

For participants who added 2FA to other accounts (133), we asked whether Duo affected their decision to do so: 34% of participants answered positively. For participants who did not add 2FA to other accounts (663), we asked whether Duo affected their decision not to do so: 16% answered positively. Using only data from the group of participants who reported an effect, we ran a logistic regression of the sentiment constructs, perceived personal and institutional added value, and covariates (gender, age, and role) on the binary decision to adopt future 2FA. We found that the only statistically significant factors that predicted further 2FA adoption from this group were if they found Duo easy to use and perceived the added security to their accounts as valuable.

We identified three main reasons for not adding 2FA to another account after using Duo. Forty-nine participants reported having had general negative experiences with Duo ("Duo increased frustration in my life, something I do my best to avoid."). Twelve participants reported not wanting to be more dependent on their devices ("It handcuffs us to our smartphones even more than we already are"). Nine participants reported not perceiving the usability and security trade-off as net positive for them ("It makes the account more secure, but

for anything that doesn't contain a large amount of personal information I don't think it's worth the hassle.")

We also identified four main reasons that led participants to add 2FA to other accounts after using Duo. Eighteen participants mentioned ease-of-use ("It was much more hassle free than I had initially worried. The fact that it's easy makes me more likely and willing to use it for other services, too."). Eight participants mentioned awareness of 2FA ("Became more aware of the existence of two factor authentication"). Five participants mentioned wanting the same level of protection for personal accounts ("Seemed like my personal account should be at least as secure as my work account."). Five participants reported that the usability and security trade-off were net positive ("previously assumed it would be more of a pain than it was worth. It's not actually that horrible.")

DESIGN AND IMPLEMENTATION PROBLEMS

From the Help Desk tickets and open-ended responses we identified a number of design and implementation problems, both for the Duo platform and CMU's implementation.

Providing Support

As with any computer system made available by the university, Help Desk support is provided via a ticketing system. After the Provost's email and up until three months after the mandatory deadline there was a significant increase in support tickets related to Duo (~10%). In particular in April, the month of the mandatory deadline, Duo-related tickets represented ~24% of all tickets that were processed by the Help Desk. See online appendix for a monthly breakdown of ticket numbers. The majority of the Duo-related tickets were general Duo requests (26%) and installation related requests — 18% hard token requests and 18% requests for help enrolling in Duo. Nevertheless, 9% of the Duo-related tickets were for account lockouts and 14% for other problems with 2FA (e.g. "duo push failed" or "Lost Phone").

Physical Design Problems

One issue participants identified with the hard token's design was "button pressing." They noted that by keeping their devices in their pockets or bags the button used to generate new codes was easily pressed, making the device de-synchronize with the system ("I also have a hard token as a backup, but it de-syncs FAR too easily, rendering it nearly useless" and "getting a fob unlocked after the token has been pushed too many times in my pocket"). When a token gets de-synchronized, its user needs to contact Computing Services so that it can be reset. To avoid this issue, some participants resorted to keeping their device inside the box it came in.

Another issue related to the physical design of the token was that the proper direction to read the codes was not clearly indicated ("Poorly designed token. The block writing comes up as 'duo' in one orientation and 'one' in the other, I have generated pass-codes that can be read in either orientation but only one is correct."). Despite its problems, the hardware token had one of the highest success rates (434 successful log-ins for each failed attempt). This could be because hard-token users, aware of its issues and limitations, are attentive when typing in the code. These issues experienced with the hard token were not frequent, yet they were salient enough to users that these problems were organically brought up in open responses. While they may not actually affect usability for current users, such memorable usability problems can hinder third-party adoption. For example, students from the S1 sample reported that they considered their acquaintances' experiences when deciding to adopt Duo themselves ("I...frankly don't want the hassle as I have heard some people talking about issues that they now have getting into the system.").

Bring Your Own Device (BYOD)

Few S1 participants raised concerns about BYOD: no student mentioned this, and only 2% of the faculty and staff did so ("Because CMU does not provide me with a phone, they should not have the right to require me to have a personal phone, or to install specific software on a personal device."). Similarly, 2% of staff complained about having to install an extra app on their phones. This was also a complaint for ~1% of students. A few participants stated that they did not appreciate having to add a new app to their already cluttered devices ("yet another app to worry about on my phone") and use a 2FA system incompatible with other services ("Does not integrate with my other services (outlook, lastpass, gmail)" and "Every 2fa service I use works with Google Authenticator.").

System Design and Implementation Problems

Push notifications can be unresponsive or slow to arrive and, at times, ill-formed. One participant complained, "Many times the request gets pushed on the phone but does not have the approve option. Sometimes the request does not get pushed to the phone or takes too much time." Furthermore, there was a conflict between features that should increase usability: automatic push notifications and "remember me." Participants who initially configured Duo to send automatic push notifications experienced problems switching to "remember me" mode: "It works fine but to do the Remember Me option you first have to deny the push and then click on the 'remember me' button, which is rather clunky." This design issue could account for survey responses that said the "remember me" check box was "grayed out" or disabled. Similarly, participants identified workflow issues when using mobile devices: "When I am us[ing] my smartphone to open a website that requires login, I don't like to close the navigator to open Duo, and then going back to the navigator." This highlights the importance of considering users' quotidian use when designing 2FA systems, trying to minimize possible sources of inconveniences.

One Size Does Not Fit All

CMU's 2FA implementation was done in an almost monolithic way, but not all systems require the same level of protection and users who use only less-sensitive systems find having to use 2FA an unnecessary burden. S2 participants' perceptions of the value of Duo varied by system: Duo was deemed extremely or very important most of the time for the HR system (73%), course and grade information system (69%), VPN (67%), student information system (66%), Box file sharing system (57%), and the Google Suite (55%). Duo was only deemed important for the CBORD application that can be used

to unlock some doors (e.g. offices and dorms) on campus by 40% of participants overall, and by 32% of student participants. BlueJeans (a video conferencing system) was deemed important by only 22% of participants. BlueJeans was further considered the least important to protect by Duo, with 25% of participants selecting "not important at all."

MISCONCEPTIONS AND INSECURE PRACTICES

Some student participants perceived Duo as a significant hindrance to their daily routine, mentioning dorm room lockouts and CBORD. However, Duo should have little or no impact on students' use of CBORD.This misconception leads to misplaced negative opinion. At best this results in frustrated users, but it can also hinder adoption by users who hear these anecdotes. In this section we present university security and Duo that can affect users' experiences and adoption, and insecure practices that were identified due to Duo.

Should It Remember Me or Not?

From the authentication attempts data we see that "remember me" accounted for 49% of all authentication attempts with no failed attempts. A slight majority of S2 participants used the "remember me" function (55%), with a significant portion not using it for lack of awareness (19%). Some participants chose to not enable it (12%), while others experienced problems trying to enable it (10%). A little over a quarter of users who enabled it had experienced problems (26%): 63 participants stated that it did not remember them for 30 days and 25 participants could not set it up at first. Despite these problems, almost all participants stated that using "remember me" made using Duo more pleasant (95%).

We also noticed in S1 that some participants believed that "remember me" removed the added security from Duo ("Worthless for 30 days for each device being remembered."). We asked S2 participants whether they thought using "remember me" increased, decreased, or left the security level the same. Nearly half the participants (47%) believed that using "remember me" would make the login process more insecure. In response to an open ended follow-up question, 82 responses mentioned the threat model of a physical attack ("I'm not worried about someone remotely getting into my computer. I'm more concerned with someone using my computer while I am away from my desk."). 52 responses mentioned that for 30 days, 2FA would be disabled on the remembered devices.

This shows a mismatch between some users' threat models and the threat targeted by the addition of 2FA: a remote and opportunistic attacker. Enabling the "remember me" functionality vastly improves the user experience and only removes the added security if the attacker gains physical access to a person's computer. Even then, the attacker would need the victim's account credentials, plus any other protection on their devices (e.g. phone with PIN or fingerprint, computer with passwords, etc.). About a quarter of the time participants mentioned physical attacks or rolling back the added 2FA security, but some included this caveat: "I suppose in the event that someone did gain access to my computer while in the midst of a 30-day period, they technically could access the account; that would mean they also had to find my computer password, which is another story...."

Students Share Credentials

Students at CMU often rely on financial guardians to pay their tuition bills. While the university allows students to create a special myPlaidStudent account for financial guardians that gives them access only to the pertinent financial information, some students share their password with financial guardians instead. Open-ended responses to S1 revealed that students who were sharing their password were facing new challenges since they adopted Duo: "My parents have to [pay my tuition bill] for me. But they can't do that when this 2Fa is on," "Also was difficult to allow my parents into my account when I was abroad for spring break because the push/passcode was too slow," and "My parents sometimes want to access my Andrew and they have to go through the trouble of finding a time where I am on my phone so I can provide them with the code."

We asked S2 participants whether they shared their account credentials with others, whether they were experiencing problems, and how they were resolving them. We found that 26% of students (51) reported allowing others to access their account, either using a myPlaidStudent account (16) or sharing account credentials (15). Another 9 students stated that they logged in for the person, so the account was shared, but not the credentials. As a solution to now having Duo, we see that either coordination is required (20) or access is no longer possible (19). Few (3) enrolled the other person's device on the Duo account. One participant, apparently unaware of financial guardian accounts, explained the coordination process as: "They call me and harass me while i'm in class and at work until I have a moment where I can give them the access code which changes every 5 seconds. Extremely infuriating. We nee[d] to give parents their own access."

DISCUSSION

To the best of our knowledge, our study is the first large-scale, longitudinal study of the transition from a single-factor system to a commercially available 2FA system at an academic institution that spanned adoption for both employees and students.

Given that security is generally a secondary goal for most users, and not one on which they want to spend time and effort, users are likely to have an even lower tolerance for security solutions that interrupt their work flow and distract from their primary tasks. Nevertheless, usability problems are very common in security-related software [9, 11, 21]. We observed a number of usability issues that should have been easily identifiable in user testing during the product development cycle. Nonetheless, users in our study reported that 2FA was more usable than anticipated. Some of those with positive experiences even went on to adopt 2FA for other, personal accounts, while some with negative experiences actually actively discouraged others from using 2FA. Drawing from user feedback, we provide the following recommendations for successful 2FA implementation.

(Obviously) Implement It Well

Many of our observations related to 2FA implementation echo recurring suggestions from the HCI community to address

usability issues. At a high level, thoughtful implementation design is crucial to lowering adoption barriers, mitigating negative consequences to users, and preventing unforeseen institutional costs. More specifically, some of the frequently-reported usability problems at CMU came from unanticipated characteristics of common use cases. As a striking example, the "remember me" feature does not work in the campus computer labs (which are very commonly used) because users tend to use different computers each time they visit. One solution worth exploring would be to provide a feature that would remember users if they logged in from any campus computer lab, or from any computer within a particular campus sub-network. The more general lesson here, is that institutions should spend time anticipating and working through how 2FA would work in each of the most common use cases for their organization.

Second, it is worth considering incremental deployment of 2FA, starting from systems where security benefits demonstrably outweigh costs. While such a piecemeal approach may be more expensive to implement, targeting deployment to systems where there is a clear security advantage may reduce the total cost to an organization, and might even help users acquire a positive experience with 2FA systems.

Third, by considering all stages of the implementation, from installation through daily use, one can reduce user annoyance and minimize required support. Providing clear and easily accessible instructions on how to install and use the system will likely lead to fewer requests for help installing the app or reporting difficulties using push notifications. While CMU did provide such materials, they were frequently hard to find or included Duo's own installation guides, which covered more options than those used by CMU. Similarly, clear on-screen instructions about configuration options (for example "remember me") would reduce user frustration. Likewise, by providing users with simple steps to take in order to avoid an account lockout, or how to proceed when lockout occurs, institutions can likely reduce their Help Desk costs.

Despite its problems, the CMU Duo implementation also included features that improved user experience, including mandating adoption only for users of sensitive systems; providing a choice of 2FA factors; and reducing the frequency of Duo authentication through both an 8-hour time-out and the "remember me" option. We expect that the Duo developers could address some of the remaining pain points by fixing reported problems with the hardware token, "remember me" configuration, and push-notification failures.

If Possible, Require Adoption

Institutions should consider the benefits that mandating 2FA can garner, particularly in organizations whose users have less mobility in institutional affiliation. While we found that CMU users required to adopt 2FA had more negative perceptions about it than those who adopted it voluntarily, the effect sizes were small, and many users reported that using 2FA was easier than they had expected. Institutions with security concerns and a captive user base (e.g. employees and students) likely have little to lose by mandating a well-implemented 2FA system.

Convince Your Users (And Keep Convincing Them)

Our results suggest organizations need to dispel negative perceptions and convince those who have not used 2FA that it is valuable and easy to use—especially those that want to encourage voluntary 2FA adoption. We found that past use of 2FA for any service, as well as use of Duo at CMU, were both factors associated with more positive perceptions of 2FA. Our results also suggest that people who have not tried 2FA assume it will be more inconvenient and difficult to use than it actually is. In addition, we found that users who later decided to adopt 2FA for other accounts had higher perceptions of the value of adding another layer of security to their accounts.

Prior work has found educational videos focused on cybersecurity risk, ease-of-use, and self-efficacy to be effective ways of encouraging 2FA adoption [1, 2]. Testimonials that 2FA is "not actually that horrible" and focusing on the positive trade-off between added security and usability may also be worth evaluating. It is also important that these educational materials are easily accessible to reach the target audience.

Furthermore, as users are influenced by others' negative opinions, institutions deploying 2FA should monitor for unanticipated problems and user misconceptions, and address these issues in a timely fashion. If users have bad experiences, word will spread that the system actually is "that horrible."

CONCLUSION

We presented our exploration of Duo 2FA adoption and usage in the heterogeneous context of an American university. Taken as a whole, these results show that even though most users found Duo annoying, they also found it easy to use and, in some cases, easier than they had expected. We see that experience with 2FA and CMU Duo often led to positive perceptions, sometimes translating into 2FA adoption for other accounts and that the differences between those required to adopt 2FA and those who adopted voluntarily were smaller than expected.

We found that experiencing negative consequences, from disrupted tasks to email lockout, or frequent smaller issues with Duo (e.g. not having your phone nearby) led to more negative perceptions, as did behaviors that reduced access to convenience features (e.g. using multiple and public computers hinders the use of the "remember me" option). We identified misconceptions that led to a limited use of this option, insecure practices that 2FA can help identify and mitigate (e.g. credential sharing), and design issues with the Duo platform and CMU's implementation. Our findings led us to identify approaches to help improve user experience and motivate current and future adoption of 2FA. We provided recommendations to those considering 2FA adoption, focusing on implementation design, adoption mandates, and strategic messaging.

ACKNOWLEDGMENTS

We thank the staff of the Information Security Office and Computing Services who helped provide data for this study, distributed our surveys, and answered our questions. In particular Deborah Schill and Mary Ann Blair for their continuous support in providing us with CMU data. We would also like to thank Hana Habib and Vidya Gopalakrishnan for their assistance throughout the project.

REFERENCES

1. Preston Ackerman. 2014. *Impediments to adoption of two-factor authentication by home end-users*. Technical Report. SANS Institute. goo.gl/ZhTQdU
2. Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. 2017. A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2FA). *International Journal of Human-Computer Interaction* 33, 11 (2017).
3. Maha M. Althobaiti and Pam Mayhew. 2014. Security and usability of authenticating process of online banking: User experience study. In *International Carnahan Conference on Security Technology (ICCST)*. IEEE.
4. Ann Bednarz. 2015. After breaches, higher-ed schools adopt two-factor authentication. NetworkWorld. (June 2015). goo.gl/C3MyqE Accessed Sept, 2017.
5. Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. In *IEEE Symposium on Security and Privacy*. IEEE.
6. Emiliano de Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. 2014. A comparative usability study of two-factor authentication. In *Network and Distributed Systems Security Symposium*. Internet Society.
7. Alexei Czeskis, Michael Dietz, Tadayoshi Kohno, Dan Wallach, and Dirk Balfanz. 2012. Strengthening user authentication through opportunistic cryptographic identity assertions. In *ACM conference on computer and communications security (CCS)*. ACM.
8. Fred D. Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly* 13, 3 (1989).
9. Alexander J. DeWitt and Jasna Kuljis. 2006. Aligning usability and security: a usability study of Polaris. In *Symposium on Usable Security and Privacy*. ACM.
10. Duo. 2017. Secure two-factor authentication app. (2017). duo.com Accessed Sept, 2017.
11. Simson Garfinkel and Heather Richter Lipford. 2014. *Usable Security: History, Themes, and Challenges*. Morgan & Claypool.
12. Paul A. Grassie, Michael E. Garcia, and James L. Fenton. 2017. *Digital identity guidelines*. Technical Report. NIST Special Publication 800-63-3.
13. Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. 2011. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers and Security* 30, 4 (2011).
14. Patrick Heim. 2016. An inside look at how we keep customer data safe. Dropbox. (Feb 2016). goo.gl/K6HFqV Accessed Sept, 2017.
15. Martin C. Libicki, Edward Balkovich, Brian A. Jackson, Rena Rudavsky, and Katharine Watkins Webb. 2011. *Influences on the adoption of multifactor authentication*. Technical Report. RAND Corporation. goo.gl/cXLTpz
16. Ziqing Mao, Dinei Florêncio, and Cormac Herley. 2011. Painless migration from passwords to two factor authentication. In *IEEE International Workshop on Information Forensics and Security*. IEEE.
17. David McCandless. 2016. World's biggest data breaches. informationisbeautiful.net. (2016). goo.gl/4w2K3A Accessed Oct, 2016.
18. University of Utah Information Technology. 2016. 2FA: Two-factor authentication required 12/28/16. (December 2016). goo.gl/wu3oQa Accessed Sept, 2017.
19. Karen O'Hara. 2015. Two-factor authentication is a must for all employees. Miami University. (January 2015). goo.gl/1dnVhp Accessed Sept, 2017.
20. Celeste Lyn Paul, Emile Morse, Aiping Zhang, Yee-Yin Choong, and Mary Theofanos. 2011. A field study of user behavior and perceptions in smartcard authentication. *Human-Computer Interaction—INTERACT 2011, Lecture Notes in Computer Science* 6949 (2011).
21. E. Eugene Schultz, Robert W. Proctor, Mei Ching Lien, and Gavriel Salvendy. 2001. Usability and security: An appraisal of usability issues in information security methods. *Computers and Security* 20, 7 (2001).
22. Nishit Shah. 2011. Advanced sign-in security for your Google account. Google Blog. (2011). goo.gl/KmVv7y Accessed Oct, 2016.
23. Iain Thomson. 2018. Who's using 2FA? Sweet FA. Less than 10% of Gmail users enable two-factor authentication. The Register. (2018). goo.gl/HzwQR3 Accessed Jan, 2017.
24. Carnegie Mellon University. 2016. Two-factor authentication (2fa) with Duo now available. (December 2016). goo.gl/mhTt7x Accessed Sept, 2017.
25. Blase Ur, Fumiko Noma, Jonathan Bees, Sean M Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2015. "I added '!' at the end to make it secure": Observing password creation in the lab. In *Symposium On Usable Privacy and Security*. USENIX.
26. Viswanath Venkatesh and Hillol Bala. 2008. Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences* 39, 2 (2008).
27. Viswanath Venkatesh, Michael Morris, Gordon Davis, and Fred Davis. 2003. User acceptance of information technology: Toward a unified view. *MIS Quarterly* 27, 3 (2003).
28. Ding Wang, Qianchen Gu, Haibo Cheng, and Ping Wang. 2016. The request for better measurement: A comparative evaluation of two-factor authentication schemes. In *ACM on Asia conference on computer and communications security (ASIA CCS '16)*. ACM.

29. Jake Weidman and Jens Grossklags. 2017. I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC 2017)*. ACM.

30. Catherine S. Weir, Gary Douglas, Martin Carruthers, and Mervyn Jack. 2009. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers and Security* 28, 1-2 (2009).