I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication

Jake Weidman
The Pennsylvania State University
University Park, Pennsylvania
jyw5163@ist.psu.edu

Jens Grossklags
Technical University of Munich
Garching, Germany
jens.grossklags@in.tum.de

ABSTRACT

The continued acceptance of enhanced security technologies in the private sector, such as two-factor authentication, has prompted significant changes of organizational security practices. While past work has focused on understanding how users in consumer settings react to enhanced security measures for banking, email, and more, little work has been done to explore how these technological transitions and applications occur within organizational settings. Moreover, while many corporations have invested significantly to secure their networks for the sake of protecting valuable intellectual property, academic institutions, which also create troves of intellectual property, have fallen behind in this endeavor.

In this paper, we detail a transition from a token-based, two-factor authentication system within an academic institution to an entirely digital system utilizing employee-owned mobile devices. To accomplish this, we first conducted discussions with staff from the Information Security Office to understand the administrative perspective of the transition. Second, our key contribution is the analysis of an in-depth survey to explore the perceived benefits and usability of the novel technological requirements from the employee perspective. In particular, we investigate the implications of the new authentication system based on employee acceptance or opposition to the mandated technological transition, with a specific focus on the utilization of personal devices for workplace authentication.

KEYWORDS

Two-factor authentication, 2FA, Bring-your-own-device, BYOD, Security in organizations, Survey study

1 INTRODUCTION

Two-factor authentication technologies are no longer novel. Many of these tools originally existed for both the corporate and private sector in the form of smartcards, or physical tokens. What initially began in the consumer sector as a tool to further secure banking (e.g., [3, 33, 61]), and in the corporate sectors as a means to secure data [36, 41, 54], two-factor authentication now penetrates many markets including email, ecommerce, and cloud storage, among others. Often met with begrudging acceptance when introduced [10], these physical technologies have dominated the second-factor authentication market for years.

More recently, researchers and technologists took note of the mobile phone boom, and began to transition these physical authentication technologies into the digital realm, thus birthing authenticator apps [4, 29]. Now that technologies such as Google and Microsoft Authenticators exist, large-scale companies have begun adopting them, as they eliminate the need to carry a (now redundant) physical authentication token. In concert with this shift towards mobile authentication, many companies have begun a transition towards technical systems based on Bring Your Own Device (BYOD) [5, 9, 13, 26, 38]. In a standard BYOD system, employees of an organization are expected to provide their own equipment, ranging from smartphones to laptops, and use it to complete their work. While employees may enjoy this ability to use their own devices for work purposes, this trend often actually costs companies more money than if they had purchased devices for their employees [53]. It also often creates security and compliance concerns for corporate policy managers [35, 42].

While a number of published works on 2FA and BYOD exist in the context of personal and corporate technology development, very few researchers have focused on the adoption of (and transition towards) these technologies in the corporate or academic sector. Although not as nationally publicized, academic institutions have increasingly become desirable targets of attackers, with major universities such as Michigan State, Butler, North Dakota, the University of Maryland, The Pennsylvania State University (multiple times), UC Berkeley, and many more, suffering major data breaches over the past three years [21, 28, 31, 34, 37, 40, 49, 56]. In the case of Michigan State, a data breach resulted in the theft of a database containing full names, access IDs, dates of birth, and social security numbers for a large number of current and previous students and employees. Despite there not being any password information in this database, 449 individual user accounts were eventually compromised as a result of this breach [40]. One of Penn State's data breaches involved the theft of 18,000 user names and passwords, though it was unclear from the public reports how many of these accounts were accessed by the attackers [49]. These data breaches provide further evidence of the shortcomings of the so-called standard duality of a user name and password.

Academic institutions, unlike many large-scale corporations, are also often slower to react to data breaches, and likely also more vulnerable to data breaches in the first place, mostly attributed to the historically-grounded openness and collaborative environment between faculty, staff, researchers and students, as well as the fact that faculty and researchers generally have more control over their data than employees do within corporate institutions [51, 58]. Due to the aforementioned attributes of academic environments, securing an academic institution from cyber-attacks becomes not only a

ACSAC 2017, December 4–8, 2017, San Juan, PR, USA

The definitive Version of Record was published in *Proceedings of 2017 Annual Computer Security Applications Conference (ACSAC 2017)*, https://doi.org/10.1145/3134600.3134629.

technical obstacle, but also a social challenge, with a great emphasis needed on the acceptability of advanced security technologies from the perspective of the stakeholders within these institutions.

Despite there being a diverse literature base on the development of two-factor authentication technologies, as well as coverage of technology perception from a private user level, there has been no work, as far as we know, exploring the design, implementation, and reaction of employees within a large academic (or even corporate) institution which adopts a mobile two-factor authentication system utilizing a BYOD framework. In this paper, we seek to fill this literature gap by conducting a study designed to thoroughly understand the rollout of a complex two-factor authentication system utilizing employee's devices. To accomplish this, we worked with the Office of Information Security at the Pennsylvania State University to understand how and why system design choices were planned, as well as how they were implemented. This component of the study was accomplished through a series of discussions with the Assistant Chief Information Security Officer (CISO).

Based on existing literature and the conducted background discussions, we then developed, distributed and analyzed an online survey within the academic organization, which explores concepts of security enhancements, privacy considerations, and usability evaluations of the combined second-factor, BYOD system utilizing a mobile app, DuoMobile. Comparative usability was measured between a previously used token-based two-factor authentication system, as well as the DuoMobile system, with standardized concepts of ease of use, relative advantage, and compatibility. Security concepts and privacy considerations were explored through items including password construction, device security, and general security practices. Although significant research has been conducted regarding the construction of new 2FA systems, as well as research on BYOD concerns, our study is the first that we know of to examine a transition between two 2FA systems and towards a BYOD framework. The main outcome of our work is to explore a system implementation like this from conceptualization to implementation and attempt to understand factors that encourage or discourage employee placation or resentment towards the institution that implements such a change. We also seek to explore any undiscovered issues of BYOD systems, and report on these in a systematic manner to provide guidance for BYOD policies at other academic institutions.

We proceed as follows. In the next section, we introduce relevant literature and begin the formation of central themes for the entire paper. We then discuss our methodology, including our metrics, participant pool, etc. Results of our study are then introduced. Following this, we enter a qualitative discussion covering our results, and formulate general takeaways from the research.

2 BACKGROUND AND RELATED WORK

In this section, we review prior work on two-factor authentication system implementations and designs, as well as how these different systems have been implemented and received across various industry sectors. We then review different literature concerning Bring Your Own Device (BYOD) implications within corporate spaces, and discuss both the merits and security risks of such systems.

2.1 Two-Factor Authentication Technologies

From a technological perspective, two-factor authentication technologies are not a new phenomenon. Originally introduced in its more modern form in 1994 [32], two-factor authentication has primarily been implemented with physical tokens, which usually operate by generating n-digit pins (as shown in Appendix A.1) on the physical token, which can then be entered into a text field on a display after a standard user name and password have been entered. Other authentication methods developed over time have included utilizing audio calls, as well as SMS and email notifications. More recently, new approaches for two-factor authentication solutions have been developed, which are implemented as applications on mobile phones [4, 63]. Popular examples are Google Authenticator, Microsoft Authenticator, and, as is relevant to this study, DuoMobile. Previous work has explored various schemas involving each of these types of authentication methods across multiple technology platforms, with no technologically robust, usable configuration found as of yet to implement an ideal 2FA platform [10].

Originally used by military institutions and corporations, two-factor authentication entered the consumer market primarily as a tool for securing online banking and ATM interactions [19, 22]. Recently, with the aforementioned authenticators, two-factor authentication has become more commonplace on diverse consumer technical systems including banking, email, social networks, and cloud storage spaces [1, 17, 30]. While multiple two-factor authentication methods exist, it remains unclear which method is the most suitable depending on the context and environment [11, 16].

Despite the growing number of services that encourage (or at least permit) second-factor authentication, as well as the larger number of tools to accomplish this security enhancement, two-factor authentication has yet to make a major dent in the consumer marketplace, with only about 6% percent of consumers adopting such technologies [48]. As more institutions implement two-factor authentication utilizing mobile devices and phase out physical tokens, it is conceivable that consumers will adopt such technologies in other contexts, in particular, if they perceive the technology usable and secure.

While there is a robust body of literature concerning two-factor authentication technologies and their effects on factors such as usability and productivity [16, 27, 59, 64, 65], there is less work concerned with the introduction and adoption (consequences) of these security mechanisms in practice, especially within an institutional setting. Some previous work has focused on the introduction and adoption of new 2FA technologies in the private banking sector with customers [33], in which a wide range of usability issues were presented. These included issues such as differing authentication methods across different platforms, or the existence of too many authentication steps. One of the major takeaways of this study was the participant-driven discussion of the, then conceptual, integration of 2FA technologies into mobile phones via SMS (this has now come to pass).

Much of the existing literature focuses on user perception of incorporating two-factor technologies into their workflow, often stating that such technologies interrupt normal operating behaviors in a workspace, unless special considerations are given to usability concerns [3, 12, 22]. More recently, conceptual research has been conducted to construct optimal two-factor authentication systems, primarily utilizing mobile devices [39] in terms of system feasibility, and projected usability. In such a system, pre-existing password interfaces are left intact, with the second factor taking place through a third-party service. The ability to maintain these legacy structures allows for rapid deployment of these second factor systems, without the need to entirely re-develop a system backend. Systems built upon this concept have been deployed at several major banks [39], as well as the Pennsylvania State University. This recent 2FA development has seen a great deal of conceptual discussion, but limited work involving implementation; something our study seeks to expand upon via a large-scale institutional setting.

2.2 Bring Your Own Device (BYOD)

As previously mentioned, one recently introduced second-factor authentication approach has been authenticator apps on mobile phones. This has become especially critical for corporations as BYOD implementations have become more widespread [7]. More broadly recognized in the early 2000s, the primary motivation of BYOD is to enable employees of a company to complete their work in an environment that is desirable to them [62], and has become popular as more employees prefer to utilize a device that is inherently personal to them for purposes of work and play [47]. This employee preference has links to various other constructs including personal device self-efficacy (i.e., individuals' beliefs in their ability to complete tasks using their own device) [6, 24], job autonomy (i.e., employees' sense of having a choice in initiating and regulating their work tasks) [23], and device familiarity (i.e., time spent with the device) [66], among others [20].

One of the primary concerns surrounding BYOD within corporate networks is the fact that securing these personal devices is a challenge, and a potential liability to the network owner and anyone else on that network. Concrete threats involving these devices include device theft (and thus, data loss) and malware entering the network through an unsecured device [26, 38, 45]. Other concerns include feelings of resentment towards companies, from the perspective of the user, as security policies enacted by companies may restrict certain functions of a phone, or enable features such as company-initiated "remote wipe" that users may not want [35]. The challenge of BYOD-based systems is to balance employee desires (to use their own device for work-related tasks) and usability concerns (well-designed security mechanisms), as well as continue to provide a level of reasonable security to the corporate network these devices connect to. It is this particular balance that is of interest to us for this study, as the new system introduced at the observed university is designed, in principle, to be an entirely BYOD-based 2FA system, utilizing a second-factor authenticator app installed on these employee-owned devices. In essence, we are studying a system that potentially introduces risks to a network, while simultaneously contributing to security via second-factor authentication.

2.3 2FA Transition Plan

To appropriately frame our study, we worked with the newly minted Office of Information Security at the Pennsylvania State University. Through a series of discussions with the Assistant CISO, we captured motivations for system design and reasoning, with an emphasis on usability and needs to secure the university network. Further conversations focused on deployment procedures that the Office of Information Security crafted, with thorough explanations of deployment rationale. This deployment procedure is discussed in Section 2.4. These meetings took place over a six-month period at critical junctures in the deployment of the new system. For the sake of grounding the reader, we will now detail the configuration of this second-factor authentication system, and contrast it with the previous system as based on discussions with the Assistant CISO.

The original 2FA system at the studied institution was based on the Vasco Digipass Go 6 token [55], which would generate an AES-based code [46] every 60 seconds. An example of this token can be seen in Appendix A.1. When logging in to a system which required authentication, users would be required to provide their standard login credentials, and upon acceptance, enter the generated number from the token to access the desired system.

2.4 Implementation of DuoMobile App

The Pennsylvania State University utilizes a Kerberos single sign-on service [43] which allows authorized users on the network to authenticate to all university services once per session on a per-device basis. Once this session has expired, i.e., all browser windows have been closed, a user wanting to utilize university services would need to re-authenticate via the single sign-on service. Within the original 2FA system for faculty and staff, a physical Vasco token was required as an additional security step before authorizing two critical systems behind the Kerberos sign-on service: an employee scheduling and grading system, and the employee payment portal. Upon accessing one of these systems with a username and password, a user would be required to use their Vasco token, and type in the six-digit code on the device into a textbox in a web browser before the code expired. These tokens did not necessarily have to be accessible to faculty and staff at all times, and many did not carry the token on them; preferring to leave the token in a single safe space, such as a home or work desk drawer.

The implementation of DuoMobile not only introduced a new means of authenticating with a digital second-factor, but also created changes to the Kerberos sign-on service. Instead of only needing to use a token or app to authenticate within one or two critical systems on the campus network, the transition to DuoMobile was also accompanied by a mandated second-factor entry for each authentication into the single sign-on system. This meant that regardless of the authentication method selected, all users of the system would be utilizing their second factor far more often.

2.4.1 DuoMobile Enrollment.

The rollout of this new 2FA service took place over the course of a year. In May 2015, employees were invited for the first time to begin using the service at their own discretion. Employees who did not want to enroll at that time were permitted to continue using their token-based system. Beginning in the fall of 2015, the Office of Information Security began enforcing the DuoMobile rollout on a department-by-department basis. By rolling out the service in this way, the office anticipated to be able to scale the resources required for the service appropriately, as well as limit the number of people who could have issues with the service at any given time. Students and graduate students were not required to enroll in DuoMobile due to administrative concerns about backlash from students who may feel that such an action would be the university infringing upon their own devices. The argument was also presented that students and faculty/staff represent two distinct populations at a university; one group pays money to attend a university, and the other is employed by the university. As students in many cases would not be considered to be employed by, or indebted to, a university, administrators were hesitant to implement this change for all network users.

When it came time for each department to enroll, emails were sent weeks ahead of time in an attempt to encourage employees to enroll well before the deadline. If employees did not enroll early, each department was issued a final cutoff date. After that date, upon attempting to log in, all employees in that department would be directed to the DuoMobile enrollment page, as shown in Appendix A.2, and would be unable to log in to their accounts until they signed up for the service. This enrollment process proceeded periodically, until the final deployment occurred in May of 2016. At that time, all faculty and staff at the university were enrolled in the DuoMobile service if they were not already.

The enrollment procedures consisted of a 3-step process. Step 1 asked new users to select how they would like to enroll in DuoMobile. Advertised options included Mobile Phone (recommended), Tablet, Duo Token (a physical 2FA token), or a Landline. If opting for a mobile phone, users were then presented with a screen, and were required to enter their mobile phone number and what operating system their mobile phone used. If selecting a tablet, users were required to select the operating system of that tablet. Interestingly, and perhaps intentionally less advertised by the transition team, employees and staff were given the option to purchase a standard 2FA token that would be compatible with DuoMobile for a one-time fee of $22. If a DuoMobile Token would ever be misplaced, it would again be the employee's responsibility to purchase an additional unit. It is worth noting that none of our participants opted to purchase a DuoMobile token, though it is possible faculty and staff in areas other than we surveyed may have done so. Finally, if choosing to enroll a landline phone, users were required to provide a phone number and an extension, if applicable.

2.4.2 DuoMobile Use Case Scenarios. Within the newly implemented DuoMobile system (shown in Appendix A.3), the authentication process evolved. Upon logging in to a desired university system using proper credentials on the single sign-on service, users are presented with a screen in their web browser to provide additional authentication. Using this screen, they have 3 options: 1) Use 'Duo Push' to push a responsive notification to their device, 2) Receive an automated phone call to a registered device, and 3) Enter a passcode from a pre-composed list which could be solicited via SMS. These three options were designed to satisfy smartphone and feature phone users alike.

In the recommended 'Duo Push' scenario, users would receive a notification on their phone (or smart watch) informing them that a login attempt is occurring. The user must simply click "Approve" or "Deny" to continue the authentication process. In the event that the user approves the 'push', the response is subsequently received by the web browser, and the user becomes fully authenticated.

If choosing to receive an automated phone call, users are contacted on a registered device, whether it be a landline or smartphone, and are presented with a verbal message. They are then required to press a dial key on the phone after the message has been played to verify that they wish to log in to their account. Lastly, if a user chooses to use a pre-generated passcode, they are directed to either send a SMS containing 10 passcodes to their mobile phone (and then enter the first code, with the 9 others being spares for later), or enter one of their previously generated spare codes. The system was designed to accommodate a wide range of users, including employees who may still use landlines. The service works internationally, and the three authentication methods are designed to create a scenario in which it is highly unlikely an employee would not be able to authenticate in some fashion.

3 METHODOLOGY

To understand the design, implementation, and employee response surrounding a novel two-factor, BYOD system, we conducted an online study designed to elicit beliefs and opinions held by employees at Penn State about two-factor authentication, generally, as well as how they perceived the novel DuoMobile system.

3.1 Online Survey

Our primary instrument, a survey, was distributed following the completion of the DuoMobile roll-out at the university, indicating that at the time of survey deployment, 100% of faculty and staff were utilizing the system (it was not an option to opt-out, and users were enrolled automatically). Utilizing this survey, we were able to simultaneously carry out a high-level, comparative usability evaluation, focused on differences between physical and digital two-factor authentication methods, as well as measure the security and privacy considerations of members of the university with additionally included questions. Technology usability survey studies have been conducted in previous literature [14, 25, 57], and served as a conceptual foundation for the work we wanted to conduct. The survey was quite comprehensive, covering multiple facets of usability, security, and privacy. The specifics of these measurements are detailed in the following section.

3.1.1 Measuring Usability. In the scope of this study, we were presented with a unique opportunity to not only analyze a new two-factor authentication system, but to complete a comparative usability analysis of two technologies as well. In order to capture the relevant data, we first chose to measure perceived ease of use, as developed by Moore et al., as a means to compare, generally, the degree to which the token or DuoMoble system was easy to learn and use [44]. In addition, we sought to capture the relative advantage, or the measure of a degree to which any technological innovation is perceived as being better than its precursor [44, 50], as a means for our participants to make comparisons between DuoMobile and the older token. Finally, we measured compatibility, or the degree to which using either the token or DuoMobile was compatible with, or required change, in our participants' job functions [44]. After consideration, these respective scales were settled on as they allowed us to measure perceptions of each technology (the token and the DuoMobile app) independent of each other, but also in comparison to each other. These scales have been utilized and referenced in a higher number of technology adoption models within institutions since its original in 1991, with Google Scholar indicating over 7000 citations at the time of this writing.

Each of our usability measures were based on pre-developed and validated scales, and are shown in Table 1 [44]. Scales for all items were on a 5-point Likert-Style scale, with a 1 indicating 'Strongly Disagree' and 5 being 'Strongly Agree'.

3.1.2 Measuring Security/Privacy Considerations. As we had previously conducted conversations to understand the decision-making process of the institution in rolling out DuoMobile, we also sought to understand how employees perceived this change across a variety of topics. These included BYOD-specific questions focused on the security of individuals' phones, as well as the security considerations relative to both individuals and the institution. We also worked to understand the general security mindset of the participants, and queried them about their mobile security and privacy habits including: app purchase habits, pin-code/password security, use of two-factor authentication outside of work, and app privacy settings, among others. We will comment on these questions more in Section 4.

3.1.3 Participant Recruitment. Participant recruitment was a multi-step process. Due to the size of the university, it was deemed that reaching out to all faculty and staff members simultaneously across the entire college would be viewed as "spammy", and a misuse of university resources. In coordination with the Assistant CISO, we were permitted to contact individual college and department heads to ask for permission to distribute a link to our survey. These college and department heads, at their discretion, would then either permit us to distribute (or not) our survey materials to their faculty and staff. Upon receiving an email containing a description of the research project and survey from the researchers, potential participants were given the option to follow a link to the survey, hosted on the Qualtrics survey platform. Before completing any part of the survey, all participants were required to review consent documentation and sign an electronic implied consent to participate.

The construction of the survey and survey distribution was designed to protect the identity of the survey-takers, and to not create an environment in which an employee would feel coerced to take part in the study. To accomplish this, we retained control over any data collected, and heads of colleges/departments were not given any access to our data. We also handled all communications directed at participants ourselves, with no intervention by administrators, or college/department heads. Additionally, we did not offer any form of financial or work-based rewards for completing the survey, and rather relied on intrinsic motivation to participate in the survey. Responses collected from our survey-takers were also anonymous, helping to further ensure that no positive or negative organizational consequences could befall a participant for taking part in the survey. Lastly, our study was approved by the Pennsylvania State University's Internal Review Board (IRB), which also considers ethical aspects regarding participation in research studies.

3.2 Participants

To conduct our study, we distributed a survey to a cross-section of the faculty and staff population at the university. Again, this did not include undergraduate or graduate students, though this group may eventually be required to transition to 2FA as well as a means to further strengthen the security of the university network. Professions generally included members of social, natural, and formal sciences, as well as medical professionals. Specifically, this included the colleges of Health & Human Development, Engineering, Nursing, and Earth & Mineral Sciences. These population pools represented departments which permitted us to deploy the survey, and also was an attempt to best represent differing views of participants across a range of professions to make our results more generalizable, as different colleges may have different organizational requirements [60]. An example of this would be that the College of Nursing must abide by further medical (technology) laws and regulations, that would not apply to an individual working out of the College of Engineering, such as HIPAA regulations [8].

Each of the colleges surveyed contained ~200-260 faculty and staff with varying roles including educators, researchers, and support staff. This indicates that our overall target population pool for this study contained ~800-1040 people. A total of 192 individuals took part in the study, which took 26 minutes, on average, to complete. 58 participants were excluded from the final analysis due to failure to complete portions of the survey. Based on this, we estimate that the total response rate for our survey was ~17% optimistically, and ~13% at worst for the overall population. The completion rate for the sub-population that participated in our study was 69.7%. Before removing incomplete survey results (dropouts), completion percentages for the entire population on either end of the response rate spectrum would be 8% higher (~21-25%).

While the high dropout rate (30.3%) could be generally attributed to the length of the survey, we also ran comparative tests between groups to determine whether there were any differences between those who completed the survey and those who did not. Our analysis of the dropout responses revealed that participants who did not finish the survey were less likely to find 2FA technologies to be beneficial (t(86)=-8.635, p<.001), to understand potential security benefits of 2FA technologies (t(87)=-6.741, p<.001), to believe that 2FA technologies make their data more secure (t(89)=-8.174, p<.001), or to believe that 2FA technologies make their workplace more secure (t(97)=-9.378, p<.001). It could be that these participants' predisposition to having negative feelings towards 2FA technologies influenced their decision to withdraw from the survey before completing it. However, we did not find any evidence that the drop-outs would be specifically biased for or against any of the two technologies which we study. Of the 134 who successfully completed the survey, 31 reported as male, with 101 reporting as female. 2 participants reported their gender as 'fluid'. The average age of our participants was 45.7 years (SD=11.6).

4 RESULTS

In the following section, we present results from the survey analysis. We first report on general practices of mobile device usage of the participants, as well as their perceptions about 2FA technologies. We then conduct a usability analysis between the previous, more traditional, security token, and the newly introduced DuoMobile application. Finally, we discuss post-adoption concerns shared by our participants via survey responses, as well as open-ended questions.

4.1 Mobile Device Usage

To begin our analysis, we first sought to understand the breakdown of mobile phone use by the participants; specifically, which operating systems were being used on their devices. We found that 64.5% of the mobile phone users were running a version of Apple's iOS, and 35.5% of the participants were utilizing Android devices. However, we found that the type of mobile phone used did not have any impact on perceived usability, relative advantage, or compatibility.

To continue our analysis, we addressed the issue of determining how many of the participants used the DuoMobile app, as well as what number of participants took alternative means (i.e., SMS codes, phone calls, etc.). It was found that our participants dominantly utilized the DuoMobile app, with only 6 participants (4%) taking an alternative means of authentication within the new DuoMobile system. Of these 6 participants, each of them had opted to use the phone calling system, rather than any other form of authentication. Potentially due to the limited number of non-DuoMobile app users, it was found that there was no interaction between which DuoMobile authentication method was used in regards to perceived usability, relative advantage, or compatibility.

Continuing to refine our understanding of this participant pool, we collected responses about the participants' mobile device security to determine how variations in smartphone use could influence reported usability, relative advantage, and compatibility. Of the participants, it was found that 95.5% of them owned a smartphone. Beyond this, we also measured the enabled (or not disabled) security features on each of these devices. This was critically important, as a phone must be unlocked/authenticated within the local operating system for employees to use the second-factor authentication app. Of the smartphone-owning participants, 74% used some form of authentication on their phone. Thus, 26% of the participants do not use any sort of security lock on their phone, even though they are capable of doing so. A Kruskal-Wallis Test (one-way ANOVA for nonparametric data) was run to determine whether or not a participant using any form of security on their phone would impact any of our outcome measures. It was found that phone security did not interact with any of the outcome measures of perceived usability, relative advantage, or compatibility.

As there are newer means of signing in to a phone beyond a passcode, we also tested for alternative approaches. Independent of using a passcode/pin or not, we found that 57.5% of the participants utilized a fingerprint reader on their phone, 28.5% used the ability to draw a pattern to unlock their phone, and 7.2% used form of facial recognition available, meaning that 93.2% of the participants had the ability to access their phones through other approaches beyond a 4 or 6-digit pin. To determine whether or not varying passcode compositions would influence our outcome measures, we ran several Kruskal-Wallis Tests and found that there was no interaction between varying measures of mobile phone security and our outcome measures. That is to say, whether or not a phone was secured with a pincode, pattern, or facial recognition, this did not impact any perceived usability, relative advantage, or compatibility for the DuoMobile app.

As an extension of our analysis of mobile phone practices, we explored whether the participants had a wider range of other connected devices, such as smartwatches, as this creates enhanced interaction possibilities with the DuoMobile app. We recorded that 4.7% of the participants owned and used a smartwatch or related device. Although the number of participants utilizing smartwatches was small, we still conducted a Kruskal-Wallis Test to determine whether or not using a smartwatch regularly would impact perceived usability, relative advantage, or compatibility. No interactions were found.

In addition to phone lock mechanisms, we also surveyed the participants' use of technologies on their phone. We found that 14% of them ran some form of anti-virus software on their devices, while 11% utilized some form of anti-malware software. Despite these relatively low figures for the prevalence of security software, 58.9% of the participants self-reported to have a moderately secure, to very secure mobile device. We also explored the app-related behaviors of the participants to determine whether or not these behaviors might have an impact on our usability results (as DuoMobile primarily functions as a mobile app). Concerning app installations, we found that only 30.5% of our participants regularly downloaded apps on their smartphones. Not surprisingly, we then found that 29.1% of our participants had a great deal of hesitation about installing apps on their mobile devices.

4.2 Preconceived Security Notions

To determine the influence of any preconceived notions towards 2FA that could affect our usability measures, we recorded responses on whether or not participants found 2FA technologies to be beneficial, as well as whether they felt 2FA made personal and institutional data more or less secure. We found that individuals were significantly more likely to claim that they understand the benefits of 2FA, even though they do not actually believe 2FA technologies are beneficial (t(133)=7.77, p<.001). In other words, people claimed that they know using 2FA technologies are useful, just not entirely useful to them. In contrast, we found that our participants were equally likely to believe that 2FA technologies would make their personal data, as well as university data, more secure.

As the introduction of DuoMobile also coincided with a university-wide shift to required 2FA for all internal systems, we also sought to understand employees' opinions on this topic. We found that 57% of the participants believed this newer system to be inconvenient, though we also note that 54.2% of the participants believed this was something the university should be implementing, and requiring.

Similarly, we asked our participants to evaluate how secure they thought the university would be if no form of second-factor authentication would be in use. A combined 44% of the participants felt that the university would be somewhat to very insecure, with 19.4% feeling that the university would be very secure. The remaining 36.6% had moderate opinions on the subject. It does seem likely, based on these results, that many participants understand the value of having a second-factor authentication system, even if they might find it inconvenient at times.

4.3 Comparative Usability, Relative Advantage & Compatibility Results

We first conducted a reliability analysis on each scale item to ensure our results were accurately measuring the desired effects. As shown in Table 1, we found that each of our measures for the token-based, second-factor authentication, as well as for the DuoMobile system, were found to be reliable for analysis (i.e., values for Cronbach’s Alpha are good or excellent).

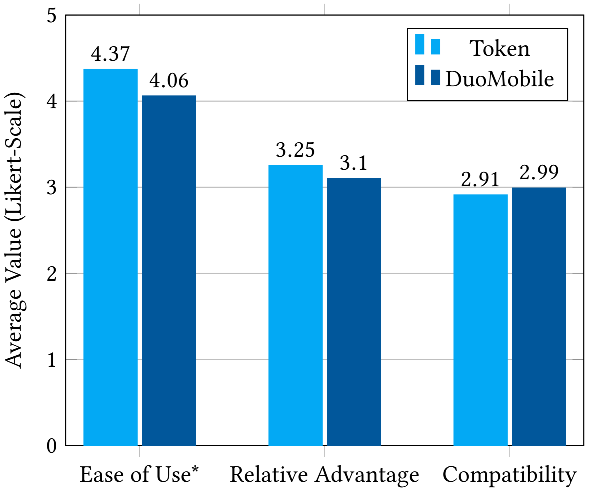


Figure 1: Physical Token compared with DuoMobile. (*Indicates significance)

To begin our investigation of the perceived usability between the traditional token 2FA system and the DuoMobile system, we conducted a comparative analysis of reported ease of use, relative advantage, and compatibility. The results of this analysis are visualized in Figure 1. Perhaps surprisingly, we found that when comparing the perceived ease of use between the physical token and the DuoMobile system, participants consider the token easier to use (t(122)=2.03, p=.04). The same effect direction was also observable for relative advantage between the two systems, but not significant. In contrast, DuoMobile was perceived to be more compatible than the token, that is, the DuoMobile app was found to be more compatible with our participants’ authentication work flows, but (again) not significantly.

To delve deeper into these somewhat unexpected results, we analyzed whether or not time spent being enrolled within the DuoMobile system had any impact on reported ease of use, relative advantage, or compatibility, with the reasoning that those who had been enrolled in DuoMobile for a shorter period of time could perceive the system less favorably. However, it was found that time spent using the DuoMobile system (i.e., our data includes users who had enrolled in January 2015 through May of 2016) had no significant impact on any of our measures.

Continuing with this thread, we also ran an analysis to determine the impact of whether participants enrolled in DuoMobile before their department’s hard deadline, or whether they were forced to enroll on that deadline day. The distribution of enrollment times was normal. There was a statistically significant difference between groups as determined by a one-way ANOVA for measures of *token* ease of use (F(4,103)=2.362, p<.05), DuoMobile relative advantage(F(4,122)=4.826, p<.001), and DuoMobile compatibility (F(4,108)=3.776, p<.05). A Tukey’s post hoc analysis revealed that participants who were forced to enroll on the date of a university-based deadline rather than by choice before the deadline found the token to be significantly easier to use (4.00 ± 1.06, p<.01). Similarly, if forced to enroll in DuoMobile rather than by choice before the deadline, participants found DuoMobile to have less of a relative advantage over the token (2.53 ± 1.01, p<.001), as well as to be less compatible with their workflows (2.46 ± 1.32, p<.05).

Measure (Cronbach’s Alpha)	**Scale Items**
Perceived Ease of Use (.819;.817)	–I believe that it is easy to get a 2FA token to do what I want it to do. –Overall, I believe that a 2FA token is easy to use –Learning to operate a 2FA token was easy for me
Relative Advantage (.847;.844)	–Using the physical 2FA token allowed me to accomplish authentication tasks quickly. –Using the physical 2FA token slowed down my job performance. * –Using the physical 2FA token to authenticate made it harder to do my job. * –Using the physical 2FA token in my job decreased my productivity. * –Using the physical 2FA token enhanced my effectiveness on the job. –I find the physical 2FA token to be useful in my job.
Compatibility (.889;.921)	–Using the 2FA token is compatible with all aspects of my work. –Using the 2FA token fits well with the way I like to work. –Using the 2FA token fits into my work style

Table 1: Comparative Usability Measures for physical 2FA tokens and the DuoMobile app. Items designated as 2FA token can be interchanged for the DuoMobile app. Items denoted with ’*’ indicate reverse scale items. The two reported values for Cronbach’s Alpha are for the token (left), and the DuoMobile app (right).

Beyond comparing the two systems directly, we also sought to explore interactions between our previously measured dependent variables and perceived ease of use, relative advantage, and compatibility to determine what factors may play a role in impacting perceptions regarding adoption of the new DuoMobile system. To begin, we first conducted several analyses on the smartphone usage features that we discussed earlier to determine if any interactions existed to form the basis of a predictive model. By utilizing responses from our mobile device usage data analysis, we ran a multiple regression analysis to determine if any of our measured mobile practices could predict ease of use for DuoMobile. Explicitly, we included phone password complexity, phone containing (or not containing) fingerprint reader, facial recognition, or pattern input, DuoMobile use prior to using it for work, and previous use of another 2FA authenticator within our exploratory model. None of these variables statistically signified predicted ease of use for DuoMobile (F(8,78)=.990, p=.450, r^2=.092). None of the variables added statistical significance to the prediction.

We ran an identical analysis for relative advantage in using DuoMobile, and found that a majority of these variables did not statistically signify predicted relative advantage for using DuoMobile (F(8,78)=1.450, p=.190, r^2=.129). We did, however, find that a phone having a fingerprint reader did add statistical significance to the prediction (p<.05).

Finally, we ran a multiple regression analysis based on phone usage for compatibility. Many of the variables did not signify predicted compatibility when using DuoMobile (F(8,78), p=.603, r^2=.077). We did find, however, that prior DuoMobile usage outside of work did add statistical difference to the prediction (p<.05).

Beyond understanding the participants' feelings towards the newly implemented DuoMobile system, we also aimed to explore if we could examine any preconceived notions of 2FA technologies in general, which were normally distributed, and whether these notions impacted favoritism between token-based 2FA systems or the app-based DuoMobile system. To accomplish this, we ran several MANOVAs comparing generalized 2FA measures with perceived ease of use, relative advantage, and compatibility. The 2FA concepts measured were: whether the participants felt 2FA technologies were beneficial, whether participants understood potential benefits of 2FA, if they thought 2FA made their personal data more secure, and if they thought 2FA made their work data more secure.

Through our results, we can first show that 2FA technology being considered beneficial by individuals has a statistically significant, positive effect on the token's relative advantage (F(4,55)=3.281, p=.01), as well as DuoMobile's relative advantage (F(4,55)=3.878, p<.01) and compatibility (F(4,55)=2.647, p<.05). We also found that, for individuals who believe that 2FA keeps their personal data more secure, there is a statistically significant, positive effect on DuoMobile's ease of use (F(4,55)=3.014, p=.02). Finally, we found that for individuals who believe 2FA keeps their work data more secure, there is a statistically significant, positive effect on the token's perceived ease of use (F(4,55)=3.625, p=.01), relative advantage (F(4,55)=3.254, p=.01), and compatibility (F(4,55)=3.863, p<.01). We did not find any statistically significant interactions with the measure seeking to understand if participants felt they understood the potential benefits of 2FA.

4.4 Security & Privacy Post Adoption Concerns

The transition from an institution-owned token device to a personally-owned digital one is not only interesting in terms of usability, but also for security and privacy considerations. To understand potentially shifting concerns in this regard, we surveyed the participants about concerns related to losing their token (or cellphone), as well as any shifting perceived responsibilities about their part in securing an institution. Figure 2 shows the varying concerns for institutional and personal security in the event of a lost device.

As shown in Figure 2, we can observe that concerns caused by any sort of lost second-factor authentication device is only moderate on a 5-point scale (1 indicating No Concern, 5 indicating Very High Concern). In addition, we can first show that when previously using a token, concern for the security of the institution and for the self were not statistically different, (t(132)=1.805, p=.07). However, when using a cell phone, concern for personal security was significantly different than concern for the security of the institution in the event of a lost device (t(132)=-6.576, p<.001).

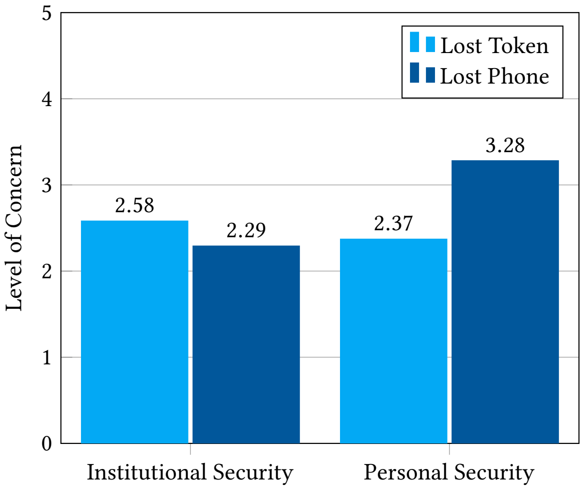


Figure 2: Comparing Concerns about Impact on Personal and Institutional Security in the Event of a Lost Device.

This finding appears intuitive. In the event of the loss (i.e., not targeted theft) of a token, there is typically no discernable way to identify the owner or perhaps even the organization that the token belongs to (unless an individual places extra information on the token itself, such as a name sticker, etc.), thus making it more difficult to initiate a detrimental security incident. However, if a personal phone is lost, personal security immediately becomes more of a concern due to the often sensitive, and personal nature of an individual's data stored on or accessible via a cellphone. In contrast, individuals are only moderately concerned about compromising organizational security if a device of either kind is misplaced.

This is a somewhat interesting contrast, as if an attacker would be able to gain access to a cellphone (beyond the lock screen), they would be able to view information about which institutions or resources any second-factor apps are attached to. Even further, if an attacker would have access to the device during a 'DuoPush' scenario, they would be able to view a logo of the institution, along with the user name attached to the account at that institution (hence the redaction of information in Appendix A.3). This, perhaps, reveals a lack of employee comprehension of possible security risks associated with the loss of a personal device on a university network, or more generalizable, an institutional network.

We also queried the participants about any self-reported perception and behavior changes in their phone usage after adopting the DuoMobile system. Specifically, we asked them if they felt any additional responsibility when using their personal devices to keep the institution secure, and if they had changed any of their phone security habits (such as using a passcode etc.) after adopting DuoMobile. For the latter, only 3 of our participants reported any form of phone security change after adopting DuoMobile. When exploring any perceived added responsibility, 6% of our participants reported a definite perceived increase in the burden of responsibility, 14.9% reported a slight increase, and 11.3% were unsure. The remaining 67.7% reported feeling no more responsibility to keeping their institution secure than before.

Note that the university did not enforce any additional security policies on the phones of employees who installed the DuoMobile app. Unlike many institutions which may enforce some form of passcode requirements, device encryption, or more if an institutional email or other institutional software is added to a mobile phone [52], DuoMobile does not currently mandate any minimum security settings for smartphones, at least at Penn State.

Finally, we asked to which degree participants believed that the physical token and the DuoMobile application were contributing to institutional security. Though there was some variation within the responses, the mean comparisons were exactly even, indicating that our participants felt, collectively, that the physical token and DuoMobile contributed to the security of the institution equally.

5 QUALITATIVE ANALYSIS & DISCUSSION

In this section, we complement our previous findings with qualitative observations derived from open-ended parts of the survey. We also add selected responses from the participants. Implications of this study are discussed throughout.

5.1 2FA System Usability

Although there have been numerous user studies on token-based 2FA systems in the past, our study is the first to our knowledge to conduct a usability study on the often-proposed 2FA authenticator app in an institutional setting. As such, it is somewhat difficult for us to compare our results to previous work, as the varying factors between a token-based system and the DuoMobile app are large. As we have now seen, the transition between a token-based 2FA system and a digital 2FA system (DuoMobile) presents many different usability challenges. As such, previous studies describing usability metrics concerning 2FA tokens may not be as applicable as desired, partially due to fundamental differences in how token systems operate compared to mobile phone-based 2FA apps.

In previous token-based systems, the institutions provided tokens for nearly all employees, and these were maintained by local IT staff in the event of any issue. Due to their simplistic nature, there were not many usability challenges tied to this original authentication method. However, when introducing DuoMobile, the onus of responsibility for second-factor authentication is shifted almost entirely on to the employee. In this new, BYOD-centric authentication system, the employee is responsible for downloading and learning how to use a new app, as well as linking their work profile to this app. This touches a number of usability, privacy and security concerns, both from an app perspective and from a system perspective. This unique interaction of factors makes comparing these two systems directly a challenge.

Prior to examining our outcome measures of ease of use, relative advantage, and compatibility, a deeper analysis exploring the method of enrollment in the DuoMobile system (pre-deadline/early adopters vs. deadline mandated) played a major role in determining how DuoMobile was (negatively) perceived with regards to relative advantage and compatibility. One of the strengths of our study is its ability to explore perceptions not only about a novel technical system introduction, but also conditions within the institution leading up to this adoption. In line with research on technology adoption within organizations [44], it is clear that employee's perception of how voluntary or involuntary a mandated technology adoption is will ultimately have a major impact on how this technology is perceived overall. Universities and organizations should strive to make employees feel as though they are a part of a newer, more secure system rather than make users feel forced and obligated to change their routines, especially when authenticating to a system.

In comparing the factors of ease of use, relative advantage, and compatibility, we found that our participants considered the physical token system easier to use than the new DuoMobile system. However, participants still reported finding the token very inconvenient in terms of compatibility. When comparing ease of use and compatibility, the participants noted that the new DuoMobile system was more compatible with their workflow for authentication. What we note here, and what is, in many ways, a theme of this study, is a dichotomy between finding one system easier to use than the other (token-based), but also realizing and appreciating the benefits of a newer system (DuoMobile).

One explicit expression of this was given by one of the participants who noted the following: "The tokens are inconvenient. I was first resistant to using my personal phone for 2FA, but it was a lot more convenient so I gave in." In many instances within the responses, the participants noted that they ultimately found the DuoMobile authentication to be more convenient than the token, primarily because they seldom had to worry about losing track of their mobile phones, whereas this was a common concern with the tokens. Participants noted this frequently, with most of the comments being summed up by two participants: "It is much easier than the token, since I almost always have my phone with me"; "It is more convenient to use my iPhone than to rummage around in my bag and find my token."

After comparing differences of perceived ease of use, relative advantage, and compatibility between the physical token and the DuoMobile app, we also attempted to establish factors that could impact the positive or negative attributes influencing the perceptions of the newer DuoMobile system. Based on the initial variables we chose to analyze, we found that very few items had an ultimate effect on how DuoMobile was perceived. The exceptions to this were whether a phone had a fingerprint reader feature, and whether the participants had used the DuoMobile app previously. While the latter is fairly obvious, we do believe the fingerprint reader finding is of interest as it ties the ownership of devices with particular features to increased technology acceptance of 2FA.

When discussing how the DuoMobile app operates earlier in the paper, one use case that was not described is how the app operates when an individual's phone is locked. In such a circumstance, an individual is required to first unlock their phone before confirming the DuoMobile request for authentication. As such, the fact that individuals with a fingerprint reader on their phones would find DuoMobile to be more useful, hearkens back to a simplistic GOMS technique; the keystroke-level model [15]. In the event of using DuoMobile when a device is locked, an individual with a fingerprint reader only needs to place their finger on their phone, and then can immediately authenticate. A user without a fingerprint scanner, on the other hand, would have to enter their passcode or other authentication mode (of varying complexity), thus adding additional button presses and time to their authentication task.

5.2 BYOD Concerns

We consider it quite interesting that the token was so highly rated within our scale items compared to DuoMobile, as the DuoMobile system was designed to be highly compatible for various use cases. However, when further investigating comments made via our open-ended questions, we soon encountered a theme applying simultaneously positive and negative attributes towards DuoMobile as a result of the new 2FA system requiring a personal device to operate on. One participant said the following: "I like the fact that there are multiple options: call office phone, call home phone, call cell phone, punch in numbers, I resent the fact that I might be expected to use a personal device to access work functions."

This theme was quite common throughout our responses. We believe that this resentment of BYOD usage for 2FA within institutions caused a certain amount of animosity towards both the administration for enforcing the new app being used, as well as towards the app itself via proxy. For many, this outcry about being required to use personal devices was also accompanied by a desire to be compensated for doing so. As one participant summed up: "A good exemplar of the [institution] expecting more, but not compensating for it." Financial compensation was not the only concern brought up by participants. Others considered the switch to this BYOD system an infringement on the established separation of their personal and work lives: "I prefer to keep work and personal as separate issues so I'm bothered by having to use my personal phone for business purposes." This opinion, which was mentioned by several participants, is in opposition to proponents of BYOD systems, who argue that many people would like to use the same devices for work and play, and would not like a second device [62].

Although it was common for some participants to express negative notions about using their own device for work purposes, not every participant in the study felt this way. As noted by one of our participants: "I have always used my personal phone for business use. DuoMobile is a very, very small part of this. I very frequently respond to university email, make business calls, and may [work on] other work related tasks on my phone." Beyond completing work tasks on phones, other participants felt that this transition to BYOD would be preferred over having a work-issued phone: "I would rather use my personal phone for work than be required to carry two phones - my personal phone and a work phone."

Another prevalent theme found when discussing new issues created by DuoMobile was that of professionalism. This is one aspect of second-factor authentication that we do not believe has been explored previously. Many of our participants reported feelings of lack of perceived professionalism across different circumstances when being required to use their mobile phone to authenticate. As one participant stated: "I don't think it is right to be asked to use my personal expensive device for a work related function daily. I especially don't like getting it out in front of undergraduate students because I think it looks very unprofessional."

Even more troubling, within the institution, some individuals reported not being able to use their mobile phones during work hours, thus making their work difficult to complete at times: "I am not permitted to use my phone on the clinical unit at [location redacted], which prevents me from checking items for students and from students." Based on several comments like these, it is clear that in certain circumstances, BYOD setups can create situations in which an employee would be unable to complete their work within a phone-based 2FA system. Not surprisingly, these few individuals who encountered scenarios in which they could not use DuoMobile at work, or might have trouble using DuoMobile at work had significantly lower perceived ease of use($F(11,120)=1.96$, $p<.05$) and relative advantage ($F(24,106)=1.66$, $p<.05$) for DuoMobile, over the token. Even further, by instituting such a system, an institution can effectively hinder the ability of one of their own employees to complete their work due to conflicting workplace policies.

When exploring these concepts of BYOD within the newly deployed 2FA system, we can see that many factors arise such as convenience (positively), as well as device compensation and professionalism (negatively). While many past studies have focused on technical specifications and security concerns related to BYOD transitions, we have been unable to find any works that elaborate on the day-to-day effects felt at the employee level, post-adoption. These observed side effects are not yet explored and should be flagged as an area for future research.

5.3 Technical Security Concerns

One potentially overlooked consideration by an institution choosing to implement a digital 2FA authentication system is that, in some instances, the second factor becomes nullified. An increasing number of individuals now use their phones as primary work devices. Previously, when using a token, if an individual was completing work on their phone and needed to authenticate themselves into a secured system, they would be required to use their phone and the physical token to authenticate. However, in this new paradigm, the sign-in attempt and second-factor authentication all take place on the same device, without any further authentication being required. One of the participants stated this concern quite succinctly: "Since you can use your cell phone for 2FA, AND you can login to secure pages with it, there really isn't a two factor there.... you can do it all on your phone."

From a system administrator's perspective, this could be viewed as a potential weakness and security concern, in particular, with increasing usage of mobile devices for core work activities. Combining this with the fact that many modern smartphones store usernames and passwords in login fields, and a reported 26% of our participants do not use any sort of passcode lock on their phone, it is conceivable that these devices pose a significant security risk, which would allow an attacker to breach a secured system just by obtaining access to one device. As we predicted such security concerns might arise, we also queried the participants about hypothetical security enforcement policies being added to their devices, as such possible enforcement could be implemented in the future.

Framed by referencing many corporate email systems [2, 18], which enforce strict phone security policies such as a minimum password length, remote wipe features etc., we asked the participants if they believed the university should be allowed to perform a security check on their phones, or even implement corporate security restrictions on their device, similar to the aforementioned corporate email settings. Our participants were almost universally opposed to such policies, with 80% stating that they would be against such a policy, if issued by the university. One participant summed up their feelings about such an implementation: "It is MY PERSONAL device. It does not belong to the University and they did not contribute towards its purchase. I do not feel they can tell me what I must do with my PERSONAL items." Another participant argued that enforcements should be handled at the institutional level, and not on employees' phones: "Security should be tightened from the top level and not branch out to employee levels."

Our participants seemed to be adamant in their stance that additional security requirements added to their devices would be deemed unacceptable. While we had participants willing to argue for both sides for some components of the DuoMobile system, it is apparent that although many are willing to accept the use of a third-party app on their phones for work, these same people are not willing to accept further intervention on their personal devices from the institution.

6 LIMITATIONS

When measuring concepts such as perceived usability, relative advantage, or compatibility, specifically for the DuoMobile app, we recognize that an app is merely a component of an entire smartphone ecosystem. Pre-existing prejudices or usability concerns that the participants may have had towards their mobile phones may have been inadvertently applied to some components of app usability as well. Further, despite there being several ways (beyond the DuoMobile app) for users within this new system to authenticate themselves (SMS codes, phone calls), a large majority of our participants used the DuoMobile app only. As only 6 participants in our study utilized the phone call method to authenticate themselves, we are hesitant to make any strong statements about the impact of various authentication methods within this new 2FA system. Lastly, we note that we can only comment on the results of our surveyed participants, and lack campus-wide data on authentication techniques used by the entire university (token vs. DuoMobile), as this data was not made available to us by the university.

7 CONCLUSION

Using an in-depth survey, as well as discussions with members of an institutional administration, we explored usability and adoption concerns within a new second-factor authentication framework utilizing BYOD. We also examined various factors within this BYOD framework that led to feelings of resentment towards the institution, as well as unforeseen workplace consequences. Our study is the first that we know of to examine a transition between two 2FA systems with a BYOD framework within an institution.

We found that, overall, surveyed individuals found that ease of use was greater for the more traditional token over DuoMobile for second-factor authentication. Conversely, DuoMobile was found to be more compatible with the workflow of the participants. While overall perceptions of the DuoMobile authentication system were not inherently negative, there were several factors that contributed to the system being rated more negatively in terms of ease of use (significantly) and relative advantage (non-significantly) than its traditional token-based counterpart. A number of these concerns were based on BYOD issues of compensation for personal device usage, a feeling of unprofessionalism using a personal device for work in certain contexts, and job restrictions hindering the use of personal devices within work environments. We note that system designers should consider alternative workflows for individuals who have workplace restrictions on personal phone usage. Failure to do so could result in employees being unable to complete their work and growing discord. Additionally, some individuals may place some resentment on an institution if a BYOD policy is implemented without compensation to the employees. This resentment could be amplified if an institution would ever choose to require any additional mandated security features be placed on personal devices (such as password requirements, remote tracking/wiping, etc.), which has been known to occur.

Additionally, we found that how a novel 2FA technology is introduced (mandated vs. perceived as voluntary) has a fairly substantial impact on how that new technology is perceived and accepted in terms of ease of use (of the previous system), and relative advantage and compatibility (of the new system). We note that these concerns have not been discussed in detail before, to the best of our knowledge, in literature related to BYOD. Administrators should strive, to the best of their ability, to encourage independent adoption of institutional technologies, as employees are more likely to positively respond. This could include giving employees more time to adopt a technology on their own, or creating better literature to describe inherent benefits of newly introduced technologies (if there are newly inherent benefits).

Revisiting our findings in support of token use, we still argue that a second-factor authentication system, such as DuoMobile, is a suitable replacement to more traditional, token-based 2FA configurations. While users of such a system may not support such a change initially, they also tend to recognize why such a change is occurring and ultimately support it. Users of a digital 2FA system find that it falls more in-line with their workflow, and have less concerns about misplacing a phone compared to a token.

As second-factor authentication technologies continue to be introduced in the private and corporate sector, the need to better understand user reactions towards these systems becomes more important. In this paper, we showed that while users report aspects that they dislike about 2FA technologies, they also acknowledge the benefits and typically incorporate said technologies into their workflow to further secure themselves, as well as any institution they may work for.

Acknowledgments: We thank the anonymous reviewers and our shepherd, Adam Aviv, for their constructive comments and feedback. The research activities of Jens Grossklags are supported by the German Institute for Trust and Safety on the Internet (DIVSI).

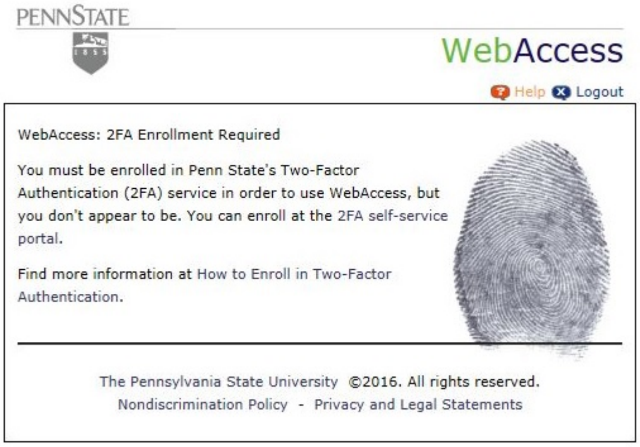
A APPENDIX

A.1 Duo Token

This image below shows a physical two-factor authentication (2FA) token. An individual would carry this device with them, and be asked to enter the randomly generated number displayed on this device, as they would log in to a system. This number typically changes every 30-60 seconds, and is generally based on proprietary algorithms.

A.2 Duo Mandated Enrollment

At the Pennsylvania State University university, if you had not enrolled in DuoMobile by your department's mandated date, upon attempting to log in to any system, this message was shown. You were required to enroll in the system before being given access to any major system.



WebAccess: 2FA Enrollment Required

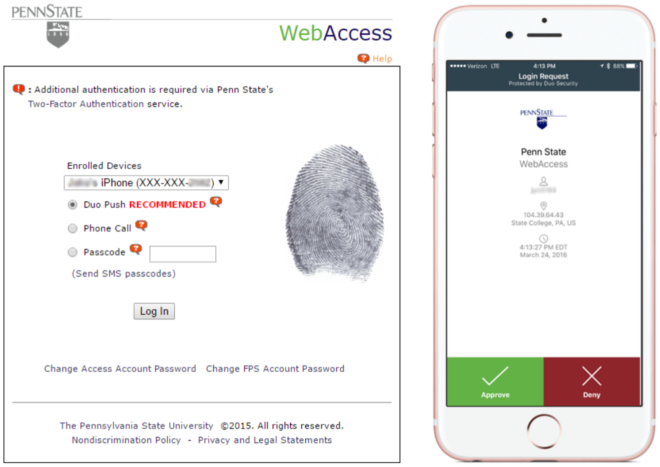
You must be enrolled in Penn State's Two-Factor Authentication (2FA) service in order to use WebAccess, but you don't appear to be. You can enroll at the 2FA self-service portal.

Find more information at How to Enroll in Two-Factor Authentication.

The Pennsylvania State University ©2016. All rights reserved.
Nondiscrimination Policy - Privacy and Legal Statements

A.3 Duo Web Login

This appendix item illustrates the new, 2FA login process at the Pennsylvania State University. After entering standard username/password credentials, users are taken to this page where they can either instantiate a 'Duo Push' to dynamically approve the login, receive an automated phone call from Duo, or use a pre-generated passcode sent via SMS. Upon completing any one of these three actions, the user is authenticated to the network.



: Additional authentication is required via Penn State's Two-Factor Authentication service.

Enrolled Devices
[redacted] iPhone (XXX-XXX-[redacted]) ▾

● Duo Push RECOMMENDED
○ Phone Call
○ Passcode

(Send SMS passcodes)

Log In

Change Access Account Password   Change FPS Account Password

The Pennsylvania State University ©2015. All rights reserved.
Nondiscrimination Policy - Privacy and Legal Statements

REFERENCES

[1] Dave Abraham. 2009. Why 2FA in the cloud? *Network Security* 2009, 9 (2009), 4–5.

[2] Richard Absalom. 2012. International Data Privacy Legislation Review: A Guide for BYOD Policies. *Ovum Consulting, IT006* 234 (2012), 3–5.

[3] Olufemi Adeoye. 2012. Evaluating the performance of two-factor authentication solution in the banking sector. *IJCSI International Journal of Computer Science Issues* 9, 4 (2012), 457–462.

[4] Fadi Aloul, Syed Zahidi, and Wassim El-Hajj. 2009. Two factor authentication using mobile phones. In *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications (AICCSA)*. 641–644.

[5] Rafael Ballagas, Michael Rohs, Jennifer Sheridan, and Jan Borchers. 2004. BYOD: Bring your own device. In *Proceedings of the UBICOMP Workshop on Ubiquitous Display Environments*.

[6] Albert Bandura. 1977. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review* 84, 2 (1977), 191–215.

[7] Manu Bansal. 2013. BYOD: The New Workplace Trend. (2013). http://www.cisco.com/c/en_in/about/knowledge-network/byod-new-workplace-trend.html

[8] David Baumer, Julia Brande Earp, and Fay Cobb Payton. 2000. Privacy of medical records: IT implications of HIPAA. *ACM SIGCAS Computers and Society* 30, 4 (2000), 40–47.

[9] Phil Beckett. 2014. BYOD – Popular and problematic. *Network Security* 2014, 9 (2014), 7–9.

[10] Joseph Bonneau, Cormac Herley, Paul Van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*. 553–567.

[11] Joseph Bonneau, Cormac Herley, Paul van Oorschot, and Frank Stajano. 2015. Passwords and the evolution of imperfect authentication. *Commun. ACM* 58, 7 (2015), 78–87.

[12] Susan Brown, Anne Massey, Mitzi Montoya-Weiss, and James Burkman. 2002. Do I really have to? User acceptance of mandated technology. *European Journal of Information Systems* 11, 4 (2002), 283–295.

[13] Jeffrey Burt. 2011. BYOD trend pressures corporate networks. *eWeek* 28, 14 (Sept. 2011), 30–31.

[14] Fethi Calisir and Ferah Calisir. 2004. The relation of interface usability characteristics, perceived usefulness, and perceived ease of use to end-user satisfaction with enterprise resource planning (ERP) systems. *Computers in Human Behavior* 20, 4 (2004), 505–515.

[15] Stuart Card, Thomas Moran, and Allen Newell. 1980. The keystroke-level model for user performance time with interactive systems. *Commun. ACM* 23, 7 (1980), 396–410.

[16] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. 2014. A comparative usability study of two-factor authentication. In *Proceedings of the NDSS Workshop on Usable Security (USEC)*.

[17] Ben Dodson, Debangsu Sengupta, Dan Boneh, and Monica Lam. 2010. Secure, consumer-friendly web authentication and payments with a phone. In *Proceedings of the International Conference on Mobile Computing, Applications, and Services (MobiCASE)*. 17–38.

[18] Exchange Online. 2016. Managing devices for Outlook for iOS and Android in Exchange Online. (2016). https://technet.microsoft.com/en-us/library/mt465743(v=exchg.150).aspx

[19] Federal Financial Institutions Examination Council. 2005. Authentication in an internet banking environment. *Financial Institution Letter, FIL-103-2005. Washington, DC: Federal Deposit Insurance Corp. (FDIC)* (Oct. 2005).

[20] Laurie Giddens and John Tripp. 2014. It's my tool, I know how to use it: A theory of the impact of BYOD on device competence and job satisfaction. In *Proceedings of the 20th Americas Conference on Information Systems (AMCIS)*.

[21] Janet Gilmore. 2015. Campus announces data breach. *Berkeley News* (April 2015).

[22] 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 & Security* 30, 4 (2011), 208–220.

[23] Richard Hackman and Greg Oldham. 1980. *Work redesign*. Addison-Wesley.

[24] Michelle Hammond, Nicole Neff, James Farr, Alexander Schwall, and Xinyuan Zhao. 2011. Predictors of individual-level innovation at work: A meta-analysis. *Psychology of Aesthetics, Creativity, and the Arts* 5, 1 (2011), 90–105.

[25] Heather Holden and Roy Rada. 2011. Understanding the influence of perceived usability and technology self-efficacy on teachers' technology acceptance. *Journal of Research on Technology in Education* 43, 4 (2011), 343–367.

[26] Steven Houben, Nicolai Marquardt, Jo Vermeulen, Johannes Schöning, Clemens Klokmose, Harald Reiterer, Henrik Korsgaard, and Mario Schreiner. 2016. Cross-Surface: Challenges and opportunities for 'Bring Your Own Device' in the wild. In *Proceedings of the CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 3366–3372.

[27] Mike Just and David Aspinall. 2012. On the security and usability of dual credential authentication in UK online banking. In *Proceedings of the International Conference for Internet Technology And Secured Transactions (ICITST)*. 259–264.

[28] Leo Kelion. 2016. Students hit by University of Greenwich data breach. *BBC News* (Feb. 2016).

[29] Andy Kemshall. 2011. Why mobile two-factor authentication makes sense. *Network Security* 2011, 4 (2011), 9–12.

[30] Changsu Kim, Wang Tao, Namchul Shin, and Ki-Soo Kim. 2010. An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications* 9, 1 (2010), 84–95.

[31] Michael R. King. 2014. 309,079 UMD social security numbers compromised. *The Diamondback* (Feb. 2014).

[32] Jim Kotanchik. 1994. Kerberos and two-factor authentication. *OSF-DCE Request For Comments: 59.0* (1994).

[33] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and Angela Sasse. 2015. "They brought in the horrible key ring thing!" Analysing the usability of two-factor authentication in UK online banking. In *Proceedings of the NDSS Workshop on Usable Security (USEC)*.

[34] Casey Kuhn. 2014. IU wraps up data breach response effort. *Indiana Public Media* (July 2014).

[35] Max Landman. 2010. Managing smart phone security risks. In *Proceedings of the Information Security Curriculum Development Conference (InfoSecCD)*. 145–155.

[36] Keunwang Lee and Haeseok Oh. 2013. Research on access control method by user authority using two-factor authentication. In *Proceedings of the 1st International Conference on Convergence and its Application (ICCA)*. 172–175.

[37] Emily Longnecker. 2014. Data breach at Butler University exposes personal data of nearly 200,000. (June 2014).

[38] Steve Mansfield-Devine. 2012. Interview: BYOD and the enterprise network. *Computer Fraud & Security* 2012, 4 (2012), 14–17.

[39] Ziqing Mao, Dinei Florencio, and Cormac Herley. 2011. Painless migration from passwords to two factor authentication. In *Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS)*. 1–6.

[40] Michigan State University. 2016. Information on data security incident. (2016).

[41] Ann Miller. 2005. Trends in process control systems security. *IEEE Security & Privacy* 3, 5 (2005), 57–60.

[42] Keith Miller, Jeffrey Voas, and George Hurlburt. 2012. BYOD: Security and privacy considerations. *IT Professional* 14, 5 (2012), 53–55.

[43] Steven Miller, Clifford Neuman, Jeffrey Schiller, and Jermoe Saltzer. 1987. Kerberos authentication and authorization system. In *Project Athena Technical Plan*.

[44] Gary Moore and Izak Benbasat. 1991. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research* 2, 3 (1991), 192–222.

[45] Bill Morrow. 2012. BYOD security challenges: Control and protect your most sensitive data. *Network Security* 2012, 12 (2012), 5–8.

[46] National Institute of Standards and Technology. 2001. Announcing the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197. (Nov. 2001).

[47] Kevin Ortbach, Martin Bode, and Björn Niehaves. 2013. What influences technological individualization? – An analysis of antecedents to IT consumerization behavior. In *Proceedings of the 19th Americas Conference on Information Systems (AMCIS)*.

[48] Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. 2015. Two-factor authentication: Is the world ready?: Quantifying 2FA adoption. In *Proceedings of the Eighth European Workshop on System Security (EuroSec)*.

[49] Reuters. 2015. Penn State says College of Engineering hit by two data breaches. (May 2015).

[50] Everett Rogers. 2010. *Diffusion of innovations*. Simon and Schuster.

[51] Jeffrey Roman. 2014. Add Butler University to breach list. (June 2014).

[52] Manuel Roman, Gregory Buzzard, Shahid Shoaib, Eugene Krivopaltsev, and Michael Diener. 2008. Managing and Enforcing Policies on Mobile Devices. (Aug. 2008). US Patent App. 12/188,936.

[53] Chris Rose. 2013. BYOD: An examination of Bring Your Own Device in business. *Review of Business Information Systems* 17, 2 (2013), 65–69.

[54] Karen Scarfone and Murugiah Souppaya. 2009. Guide to enterprise password management (draft): Recommendations of the National Institute of Standards and Technology. *Gaithersburg, MD: US Dept. of Commerce, Technology Administration, National Institute of Standards and Technology* (2009).

[55] Vasco Data Security. 2010. DIGIPASS GO 6. (2010).

[56] Nick Smith. 2014. North Dakota university system says server hacked. *Bismarck Tribune* (March 2014).

[57] Elizabeth Stephan, Daisy Cheng, and Lauren Young. 2006. A usability survey at the University of Mississippi Libraries for the improvement of the library home page. *The Journal of Academic Librarianship* 32, 1 (2006), 35–51.

[58] Carl Straumsheim. 2015. 'A playground for hackers'. (July 2015).

[59] Dennis Strouble, Gregory Schechtman, and Alan Alsop. 2009. Productivity and usability effects of using a two-factor security system. *Proceedings of the Southern Association for Information Systems Conference (SAIS)* (2009), 196–201.

[60] Heshan Sun and Ping Zhang. 2006. The role of moderating factors in user technology acceptance. *International Journal of Human-Computer Studies* 64, 2 (2006), 53–78.

[61] Karin Svedberg Helgesson. 2011. Public-private partners against crime: Governance, surveillance and the limits of corporate accountability. *Surveillance & Society* 8, 4 (2011), 471–484.

[62] Gordon Thomson. 2012. BYOD: Enabling the chaos. *Network Security* 2012, 2 (2012), 5–8.

[63] Do van Thanh, Ivar Jorstad, Tore Jonvik, and Do van Thuan. 2009. Strong authentication with mobile phone as security token. In *Proceedings of the IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS)*. 777–782.

[64] Catherine Weir, Gary Douglas, Martin Carruthers, and Mervyn Jack. 2009. User perceptions of security, convenience and usability for eBanking authentication tokens. *Computers & Security* 28, 1 (2009), 47–62.

[65] Catherine Weir, Gary Douglas, Tim Richardson, and Mervyn Jack. 2010. Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers* 22, 3 (2010), 153–164.

[66] Robert Wood and Albert Bandura. 1989. Social cognitive theory of organizational management. *Academy of Management Review* 14, 3 (1989), 361–384.