Secure Coding.
Practical steps to defend your web apps.

Copyright SANS Institute

Author Retains Full Rights

This paper is from the SANS Software Security site. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Defending Web Applications Security Essentials (DEV522)"
at http://software-security.sans.orghttp://software-security.sans.org/events/

Impediments to Adoption of Two-factor Authentication by Home End-Users

GIAC GSEC Gold Certification

Author: Preston Ackerman, psackerman@gmail.com
Advisor: Manuel Humberto Santander Pelaez
Accepted: TBD

Template Version September 2014

Abstract

Cyber criminals have proven to be both capable and motivated to profit from compromised personal information. The FBI has reported that victims have suffered over $3 billion in losses through compromise of email accounts alone (IC3 2016). One security measure which has been demonstrated to be effective against many of these attacks is two-factor authentication (2FA). The FBI, the Department of Homeland Security US Computer Emergency Readiness Team (US-CERT), and the internationally recognized security training and awareness organization, the SANS Institute, all strongly recommend the use of two-factor authentication. Nevertheless, adoption rates of 2FA are low.

This study introduced 2FA to a group of millennials as an easily accessible security tool to protect their accounts against takeover by cyber criminals. They were introduced to the purpose of 2FA and provided resources to help begin using it. This paper discusses the factors which influenced the participants' decisions to adopt or not adopt 2FA. The findings of this study will help organizational security awareness programs and 2FA service providers focus their efforts on more persuasive messages and, possibly, enhanced technologies that can improve the use of 2FA services among millennials in the future.

© 2017 The SANS Institute Author retains full rights.

1. Introduction

Cyber crime poses a significant threat to home end-users. In a landmark article chronicling his first-person scorched-earth experience, "How Apple and Amazon Security Flaws Led to My Epic Hacking," tech writer, Mat Honan of WIRED, exposed the danger of account takeover (Honan 2012). In just one hour, his Google account was deleted, his Twitter account was taken over and used for racist and homophobic propaganda, and his Apple ID account was compromised and used to remotely erase all the data on his phone, tablet, and laptop. As Honan concluded following the takeover of these digital accounts, "Password-based security mechanisms – which can be cracked, reset, and socially engineered – no longer suffice in the era of cloud computing" (ibid). Although vendors have since corrected many of the specific flaws Honan exposed, the general threat of account takeover by malicious actors remains prevalent. The consequences of such intrusions can be severe. For example, since the FBI's Internet Crime Complaint Center (IC3) began tracking a specific type of account takeover known as Business Email Compromise (BEC), it has identified over $3 billion in victim losses (IC3 2016). Takeovers can also result in other crimes such as loss of personally identifying information (PII) for use in identity theft, loss of intellectual property, or public exposure of photographs and communications of a personal nature.

Because passwords have long been a primary method of authenticating users to computer systems, attackers have become skilled at circumventing them. The 2016 edition of Verizon's widely- read annual report on data breaches noted 63% of all confirmed data breaches involved weak, default, or stolen passwords (Verizon 2016). Security researchers have followed password trends since the 1990s (Vance 2010), and the patterns observed are discouraging. A 2009 breach of 32 million passwords from RockYou proved to be a boon to security researchers and cyber criminals alike, as the same data which was useful for analyzing user habits from an academic perspective was also effective as a dictionary for password cracking (ibid). Imperva's Amichai Shulman noted that approximately 20% of all users from the breach chose from the same small pool of 5,000 passwords (ibid). The most popular passwords also tended to be the most trivially guessed or cracked, such as "abc123", "iloveyou," and of course "password"

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

(ibid). Choosing simple passwords and using them across multiple web sites, as many users have traditionally done, is a high-risk behavior in today's threat environment.

Home end-users have promising tools available to them to address the age-old security problem of poor password management. For example, dedicated password managers provide users the ability to choose varied and complex passwords across their different accounts, while reducing the burden of remembering passwords to just one which provides access to the tool. These types of applications also improve convenience of username and password input. Although initial setup requires some level of effort based end-user computer self -efficacy, the general ease of use makes password managers rare in the world of security tools, insofar as they tend to save the user time in the long run. Nevertheless, adoption of these technologies is quite low. The study "Best Practices for Workplace Passwords" showed a paltry 14% of users report the use of a password manager for work (Humphries 2015). Although password manager adoption is not the focus of this paper, previous work on this topic, such as "So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications?" (Aurigemma et al. 2017), offers useful insights into end-user security behaviors which this paper seeks to augment.

Because password managers enable users to use long, unique, and complex passwords for every web site and application, they can help protect users against many types of password cracking attacks. Indeed, they are recommended by highly regarded authorities on information security such as the United States Computer Emergency Readiness Team (US-CERT) and the SANS Institute (Huth, Orlando, & Pesante, 2012; Zeltser 2015). However, password managers alone are inadequate to combat the threat of unauthorized account access. Another account protection measure, two-factor authentication (2FA), is also recommended by these same institutions and numerous others such as the FBI (US-CERT 2015, Palmgren 2015, FBI 2015).

While both cyber criminals and security researchers have demonstrated successful attacks against 2FA (Krebs 2009; Konoth 2016), it remains a best practice for reducing or eliminating unauthorized account access (US-CERT 2015). Indeed, Mat Honan admitted it would have prevented his account takeover debacle (Honan 2012). Whereas password

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

managers are designed to help users create and manage strong, unique passwords for each account, the use of 2FA can prevent an attacker from accessing an account even when compromise of the user's credentials has occurred.

2FA is one member of a group of closely related technologies which seek to strengthen user authentication by requiring a method of verifying the user's identity in addition to their password. Typically, the additional factor will either be something the user has in his or her possession (e.g. a one-time use code provided via security token, telephone, text, or email), or a biometric characteristic (e.g. fingerprint, voice recognition, or facial recognition). 2FA is one form of multi-factor authentication (MFA), while two-step verification (2SV) technically does not require a second "factor," but requires a code sent through a separate band of communication. The study described in this paper encompasses many online services offering variations of these technologies, with some offering more than one. For example, Paypal supports the use of an SMS code, a software token, or a hardware token. Since this paper covers a variety of providers and implementations, the term 2FA will generally be used to refer to such technology, unless referring to a specific provider's implementation by name (e.g., Google's 2-Step Verification).

Historically, 2FA has primarily been available only to government and other large enterprises. In recent years, however, it has become widely available to home end-users, often at no additional (monetary) cost. Table 1 shows a variety of popular websites which offer users 2FA, encompassing major categories of online activity such as social media; e-commerce and banking; and email, mobile, and cloud computing.

Table 1: Sites Offering 2FA, Categorized by Online Activity

Examples of sites offering 2FA, by category		
Social Media	**E-commerce/Banking**	**Email/Mobile/Cloud**
Facebook Twitter Instagram LinkedIn Google Plus	Chase Citi Bank of America USAA Wells Fargo eBay / PayPal Amazon	Gmail/Google Drive Apple (iCloud) Microsoft (Hotmail, OneDrive) Dropbox Amazon Drive

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

Despite the widespread availability of 2FA and its widespread acceptance as a best practice for preventing account takeover, adoption rates remain low. Providers such as those listed in Table 1 have not provided data on adoption rates. However, one recently published study estimated the percentage of adoption of Google's 2-Step Verification, one of the most mature and robust 2FA implementations, at just 6.4% (Petsas et al. 2015). Other unofficial studies have estimated 2FA adoption across other providers to be in the range of 2%-5% (ibid). In the business context, the previously cited study "Best Practices for Workplace Passwords" showed the use of 2FA to be 17% (Humphries 2015).

While the efforts in this paper focus on home end-users, its findings are relevant in a business context as well. Increasingly, business users' security practices on personal accounts can impact their employers. Trends such as "Bring Your Own Device" (BYOD) and telework serve to move more and more business computing activity outside the bounds of the company's internal network (Aurigemma et al. 2016). Moreover, users often voluntarily provide a treasure trove of information through their social media presence which criminals can use for credential harvesting attacks through phishing.

2. Study of Adoption of 2FA by Millennial End-Users

This research project, in partnership with a private university in the Midwestern United States, conducted a two-phased study of end-users' intentions and adoption rates related to 2FA. This paper uses the data collected in the study to examine the reasons users decide to adopt or not adopt 2FA.

2.1. Research Participants

The study, conducted during late 2016, focused on a key demographic from a security perspective: millennials. The participants were undergraduate students from a private university in the US. This group is valuable to study for several reasons:

- They have a natural affinity for technology and a familiarity with online applications (Junco & Mastrodicasa, 2007) such as those mentioned in Table 1;

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

- A review of available research reveals little which analyzes their behaviors regarding use of 2FA;
- There is a perception they are not security conscious, perhaps stemming from their willingness to post personal information online compared to previous generations (ibid; Anderson & Rainie, 2010; Gross & Acquisti, 2005);
- Because they are likely to enter the workforce within the next few years, their behaviors will impact businesses who employ them in the near-term.

Ninety individuals participated in the study, all of whom reported having at least one account which offered 2FA services. While these students represent an interesting demographic to study, care should be taken not to extend the findings to the general population without further research. Although the participants of this study represent a small convenience sample of millennials available for the purposes of this exploratory research, the findings are consistent with related literature (Aurigemma et al. 2017; Humphries, 2015). Participation in the study was completely voluntarily. The only identifying information collected from users was their email addresses, which were used solely for associating responses between data collection phases. Responses were de-identified before data analysis.

2.2. Mechanics of Study

In the first phase of the study, users viewed a fear appeal video message related to use of 2FA and were given a survey to measure their intent to adopt 2FA services within the next week. One goal of the study was to convince as many users as possible to use 2FA services. The video message incorporated the findings of current behavioral psychology literature regarding the use of fear appeals to motivate protective security behavior. A growing body of information technology research on fear appeal messages state the importance of articulating the threat and providing suggested actions for mitigation (e.g., see Johnston & Warkentin, 2010; Boss et al. 2015). Specifically, this video incorporated the two required components of a successful fear appeal message as argued by Witte et al.: 1) An articulation of the threat magnitude, in a manner which engenders belief the participant could experience the danger on a personal level; and 2) A

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

recommended action which will effectively combat the threat, is within the capabilities of the viewer, and addresses the most common impediments to carrying out the recommended action.

The video, available for viewing at (https://youtu.be/PlIx1uUkcxY), implemented the required components to effective fear appeal by doing the following:

- Providing worldwide cyber crime statistics and threat advisories, including crimes which affect ordinary citizens (e.g., not merely crimes against large businesses, government institutions, or wealthy individuals);
- Providing the recommended solution of 2FA, to include support from reputable authorities such as the FBI and US-CERT;
- Demonstrating real-time implementation of 2FA for a Google account, to show the process is simple enough to be within the capability of most users; this implementation takes about 90 seconds to attempt to address the common excuse of lacking time;
- Directing the viewer to resources on the web to assist with implementation of 2FA services (users received the URLs https://www.turnon2fa.com/ and https://twofactorauth.org/).

Immediately following the video, users were surveyed to gauge key factors such as their perceptions of the severity of the threat, their personal perceived vulnerability to the threat, the efficacy of 2FA to protect their accounts from unauthorized access, their self-confidence to implement 2FA on their accounts, and their intention to implement 2FA in the near future. All questions used a 7-point Likert scale, a measurement device used in psychology surveys to assess attitudes, values, and opinions. The scale ranged from (1) strongly disagree to (7) strongly agree.

The second phase of data collection took place one week after participants viewed the video and responded to the initial survey. In the second survey, users reported whether they adopted additional 2FA services along with additional information to ascertain actual adoption, such as the names and total number of accounts protected, as well as 2FA methods used (such as SMS/text, software/hardware token, etc.). Users who

© 2017 The SANS Institute Author retains full rights.

chose not to adopt additional 2FA were prompted to provide the primary rationale behind their decision via an open-ended response question. Subsequently, respondents chose from pre-worded choices for the most common responses anticipated, addressing issues such as threat apathy, time, capability, and self-efficacy.

3. Observations from 2FA Adoption Study

Several interesting observations emerging from the data are detailed below, some expected, but others counterintuitive. This 90-user study of millennials highlights some areas which may merit additional exploration, as well as some information which may inform those intending to influence voluntary user behavior through persuasive messages. Table 2 provides summary data from the study which will facilitate detailed analysis below. Although users responded on a seven-degree scale, for convenience the responses are grouped into three categories on Table 2 (Disagree, Neutral, Agree):

Table 2: Broad Summary of Key Data from 2FA Study

Survey Question	Disagree	Neutral	Agree
It is likely that my online accounts will be targeted for access by cyber-criminals.	36%	22%	42%
2FA services (such as SMS/text, email, Google Authenticator) are an effective solution to protect my online accounts from being accessed by cyber-criminals.	0%	13%	87%
2FA services (such as SMS/text, email, Google Authenticator), are easy to use.	6%	11%	83%
I intend to use 2FA services (such as SMS/text, email, Google Authenticator), to help protect my online accounts within the next week. Adopted 2FA after first week	24% 2%	17% 4%	59% 24%
I intend to use 2FA services...to protect my online accounts from being accessed by cyber criminals sometime in the future. (From second phase participants who did not adopt.)	26%	20%	54%

Preston S. Ackerman,
psackerman@gmail.com

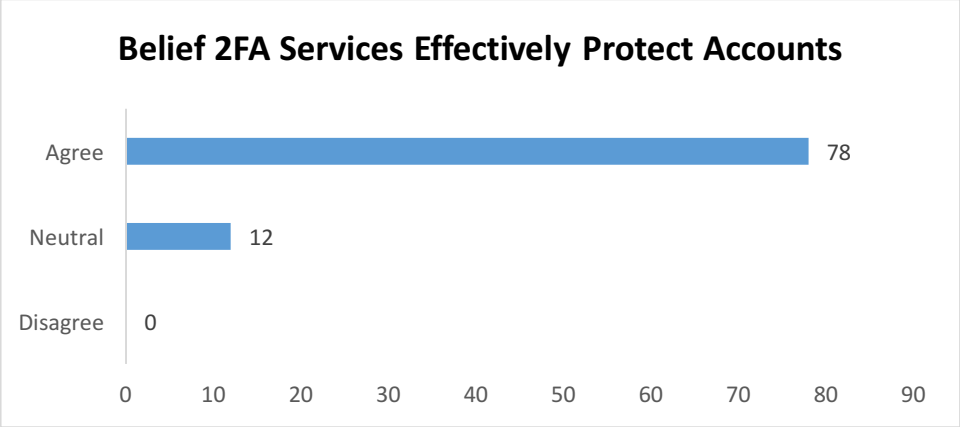
© 2017 The SANS Institute Author retains full rights.

3.1. A Clear Message Resulted in Increased Adoption

One goal of the study was to influence users to improve their security posture through the adoption of additional 2FA services. The data shows that a message which clearly identifies risks on a personal level, provides a mitigating measure, and demonstrates the ease of implementation, did result in a change in behavior for a significant number of users. Of the 90 participants, 28 individuals (31%) chose to adopt additional 2FA services in the week the after exposure to the video message. Getting this percentage of college students to take this non-trivial step to improve their security posture was a major success of this research effort.

Belief in the efficacy of 2FA to protect accounts appeared non-controversial. The large majority of participants (87%) felt that 2FA was an effective solution, and none considered 2FA ineffective (see Figure 1).

Figure 1: Responses to "2FA services (such as SMS/text, email, Google Authenticator) are an effective solution to protect my online accounts from being accessed by cyber criminals."



3.2. Users Were Not Overly Responsive to a Threat Message

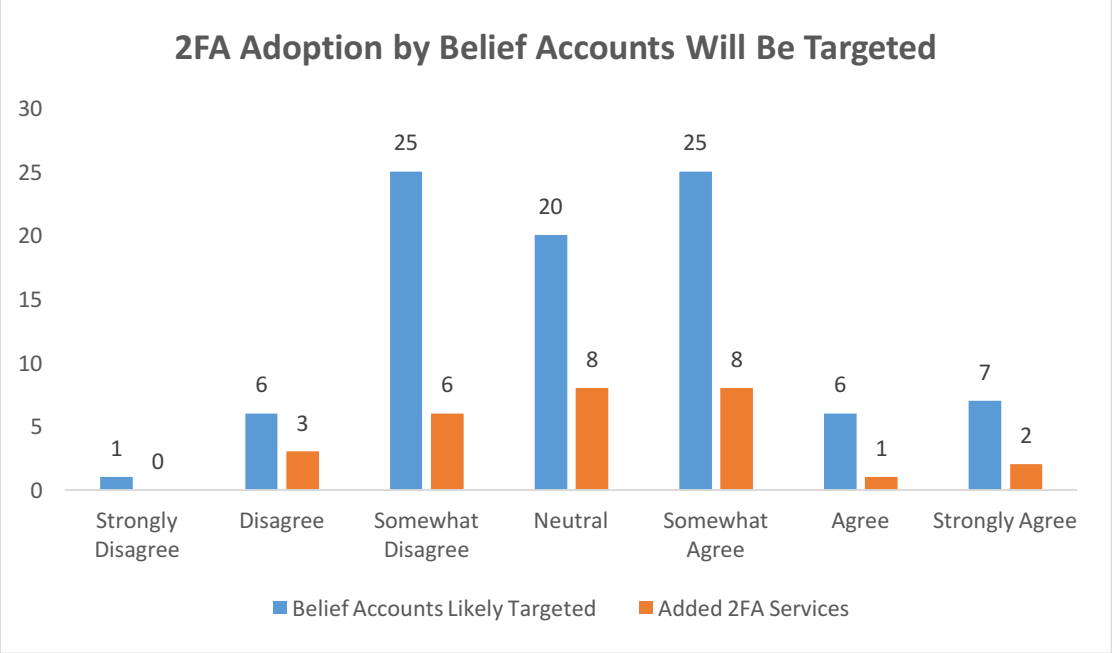
User perceptions of the threat cyber crime poses to them appeared to have little effect on their choice to adopt 2FA services within the first week. Users responded to the statement, “It is likely that my online accounts will be targeted for access by cyber-criminals” using the 7-point Likert scale. The responses were notably clustered to the center of the scale with 78% of the responses in the neutral, somewhat agree, and somewhat disagree categories. When compared to the adoption of 2FA services from the second survey, a counterintuitive finding presents itself: perception of threat severity did not appear to lead to increased adoption of 2FA (see Figure 2). In fact, when accounting

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

for the sample size, the adoption across the threat severity responses tended to track closely with the overall adoption rate of 31%. While Figure 2 shows the full results, combining these results into three categories by separating out neutral and consolidating the varying degrees of agreement and disagreement can be illustrative: Disagree (28%), Neutral (40%), and Agree (29%).

Figure 2: Responses to "It is likely that my online accounts will be targeted for access by cyber-criminals" compared with adoption of additional 2FA services.



While surprising, this data appears consistent with the Gore and Bracken finding that when crafting a fear appeal message, only a moderate amount of threat is necessary to move recipients toward the desired behavior (2005). While the statement of the problem is foundational to the message, the degree of belief in the threat does not appear to be a significant factor for this dataset.

3.3. Users with Stated Intent Tended to Adopt More Often

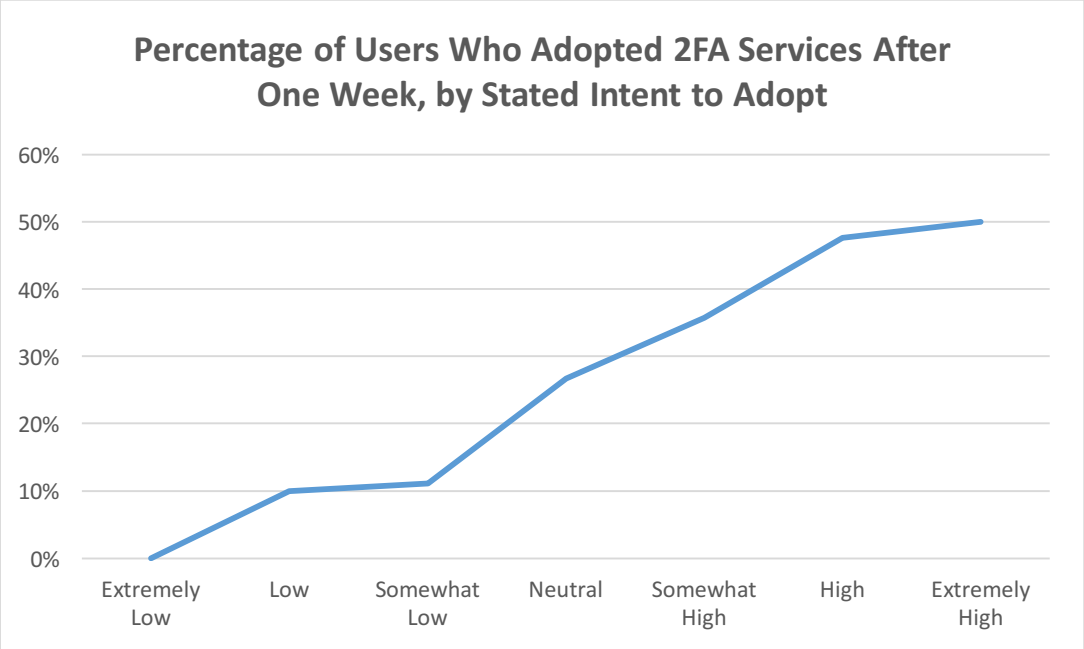
Users who stated an intent to adopt 2FA were more likely to do so than those who did not. After viewing the fear-appeal video, participants responded to the statement, "I intend to use 2FA services (such as SMS/text, email, Google Authenticator), to help protect my online accounts within the next week". Although there is always certain to be a gap between intent to carry out a desired behavior in the future and doing it (only 50%

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

of those users with the highest intent to adopt did so within a week), intent proved to be a significant indicator of 2FA adoption (see Figure 3).

Figure 3: Responses on User Intent to Use 2FA Services to Help Protect Online Accounts Within the Next Week, Compared with Adoption of Additional 2FA Services (by Percentage).



Participants who stated an intent to adopt were easily the most likely to do so after one week. Again, combining the results is instructive: adoption rate by those with low intent was (9%), neutral (27%), and high (42%). When compared with the previously cited 6.4% estimated adoption of Google's Two-step Verification, users from this sample who viewed the video and stated an intent to adopt 2FA, did so within the first week at a rate 6.5 times that of the general population.

3.4. Intention to Use 2FA in the Future Improved

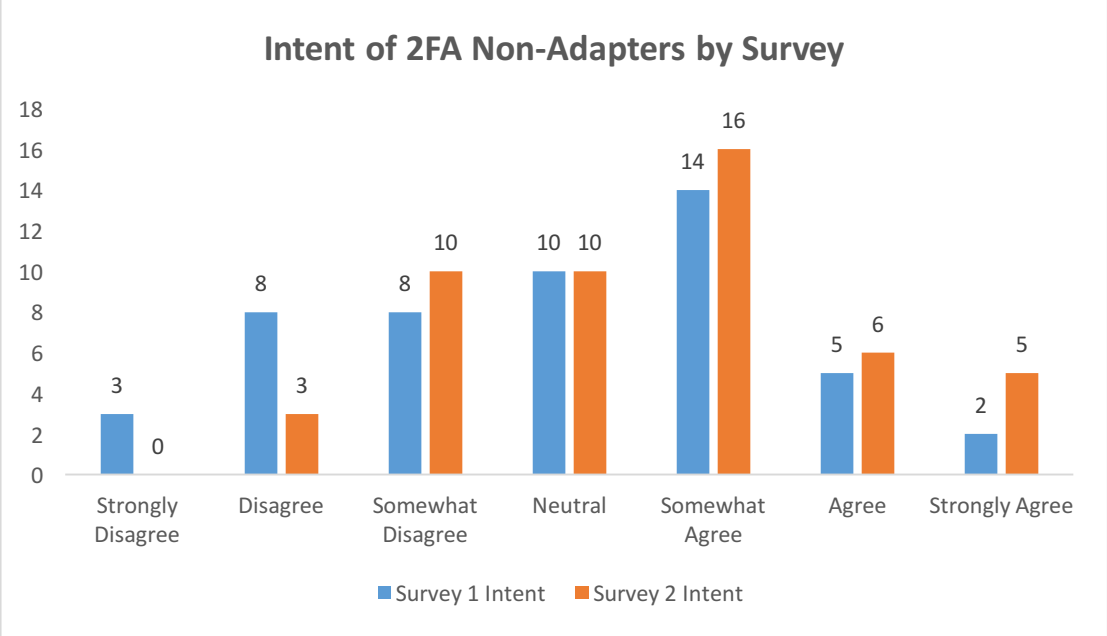
Given the apparent impact of intent on future behavior, it is desirable to try to understand what happened to user intent between the first and second surveys for the users who chose not to adopt 2FA. Did those who intended to use 2FA but failed to do so still intend to use it a week later? What about those who were neutral or did not intend to? Fortunately, in the second survey, users responded to the statement, "I intend to use 2FA services (such as SMS/text, email, Google Authenticator) to protect my online accounts from being accessed by cyber-criminals sometime in the future."

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

The results of this response were another encouraging outcome for this study (see Figure 4). Intent to adopt 2FA not only held steady, but it even showed moderate gains. (Note: A few individual participants showed a decreased intent, but the gains categorically are what is important here for maximum future adoption.) The shift to the right, where intent increases, is apparent in Figure 4. Averaging all participant intent responses (one point for strongly disagree, seven points for strongly agree, yields an average increase in intent of over ½ of a point on the Likert Scale: Survey 1 Intent (3.94 average), Survey 2 Intent (4.54 average).

Figure 4: Comparison of responses to "I intend to use 2FA services (such as SMS/text, email, Google Authenticator), to help protect my online accounts…" Between Surveys for Those Who Did Not Adopt 2FA



The 31% overall adoption rate is not likely the only benefit of the study. The improved behavioral intent in Figure 4 suggests participants are more likely to either adopt 2FA on their own or are at least less averse to adopting it if the opportunity presents itself (for example, when offered the option while opening a new account).

3.5. Users Not Confident in 2FA Ease of Use Did Not Adopt

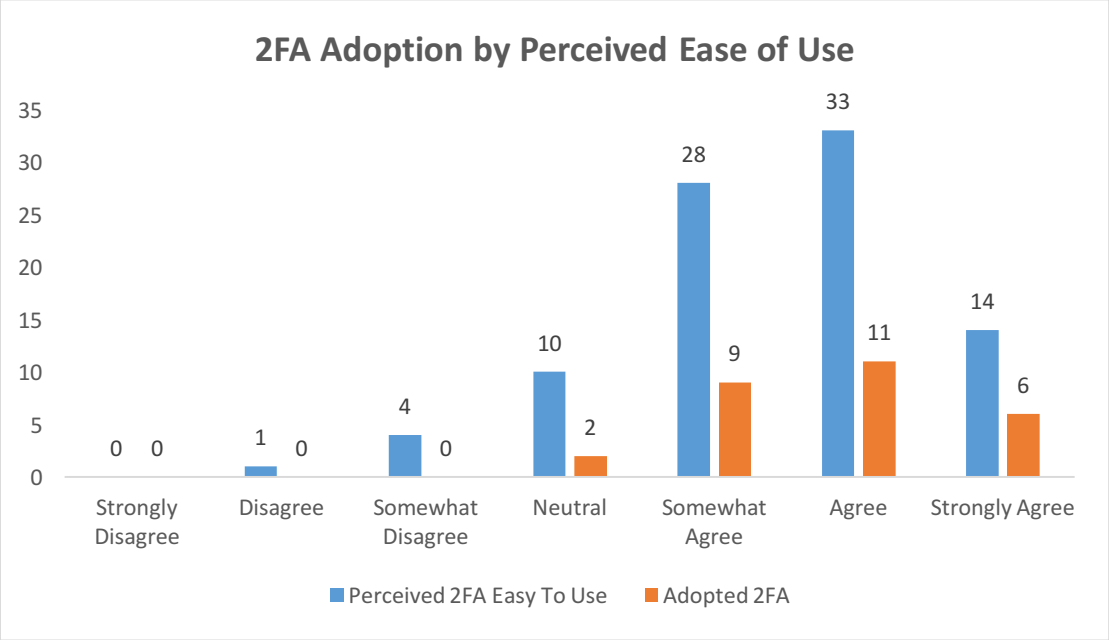
Participants who lacked confidence in their ability to implement 2FA services with ease did not tend to adopt. Participants responded to the statement, "2FA services (such as SMS/text, email, Google Authenticator), are easy to use." Of the 15 who responded

© 2017 The SANS Institute Author retains full rights.

either neutrally or with disagreement, only two users (13%) adopted (see Figure 5). By contrast, 26 out of 75 (35%) of participants who expressed agreement adopted services, with that figure rising to 43% for users who expressed strong agreement.

This lack of confidence in either user self-efficacy or usability of the technology resulted in a decreased intent to adopt from the outset: the average intent to adopt of this population was 4.13, while the average intent to adopt of those who responded with agreement (to any degree) was 4.49. Moreover, although the sample size is small, it appears that those who intended to adopt, despite low self-efficacy, did so at a lower rate than the general population. Of the five members of this group (four agree, one somewhat agree) who had some intention of adopting, only one did so. Figure 3 already demonstrated the importance of intent. This finding demonstrates that user self-efficacy appears to be an important component of intent, and it provides evidence that intent without self-efficacy does not lead to high adoption rates.

Figure 5: Comparison of Responses to "2FA services (such as SMS/text, email, Google Authenticator), are easy to use" with Adoption of 2FA Services



This finding has significant implications when accounting for the fact the study's participants (millennials) are known for their innate grasp of technology. It is not unreasonable for one to speculate other demographics would reflect a lower confidence in

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

their ability to implement 2FA services with ease and a corresponding decrease in the rate of adoption.

3.6. Reasons for Non-Adoption

The 62 study participants who chose not to adopt 2FA services offered their rationale. Participants were asked to explain the main reason they chose not to adopt. They were then asked to select all that apply from a list of potentially common reasons.

Table 3 summarizes user responses regarding non-adoption. Two of the responses are compatible with intent to adopt in the future: being too busy (39 of 62, 63%), and forgetting (10 of 62, 16%). All but two of those who forgot also selected that they were too busy. Lack of time was by far the most common reason for choosing not to adopt.

Table 3: Frequency of Selection of Reasons for Non-adoption

Reasons for Non-Adoption of 2FA Services	
Response (Pre-selected)	**Frequency**
I'm not concerned about the threat of cyber criminals stealing and abusing my online account passwords.	17
I was too busy to do it	39
I don't trust 2FA applications (such as SMS/text, email, Google Authenticator)	3
I'm not really sure how to set up 2FA on my accounts	11
I don't understand how 2FA applications work	5
I was going to, but I forgot	10
Other (Please specify)	3

The second most common reason users declined to set up 2FA was threat apathy, a lack of belief their accounts would be targeted (17 of 62, 16%). With the information provided in the fear appeal message, and news stories such as the Yahoo breach impacting one billion accounts (Goel and Perlroth 2016), this position is becoming increasingly difficult to justify and may indicate user naïveté.

Two of the choices were indicative of user efficacy: being unsure of how to set up 2FA (11 of 62, 18%), and a lack of understanding of how 2FA works (5 of 62, 8%). All but one of those who did not understand how 2FA works also responded that they were unsure how to set up 2FA.

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

A small number of users (3 of 62, 5%) indicated a mistrust of 2FA applications. This response is also indicative of a lack of understanding the technology. It seems illogical to entrust the provider with all information in the user's account, but not trust an enhanced security measure they offer to protect it.

Of the three users who chose "Other," two unique responses worth noting were provided. One user declined services because he or she does not carry a phone at all times. While this position is perhaps not common among millennials, it is valid in that 2FA services would have the substantial additional cost of requiring the user to carry an extra item with them at all times (as is already the case with hardware token implementations). Another user noted he or she had used Google Authenticator previously but uninstalled the app due to storage capacity issues with his or her phone.

The bulk of the open-ended responses were easily identifiable with one of the pre-worded selections, such as the participant was too busy or forgot. Some answers provided new information, however. A couple of users mentioned the inconvenience of the technology, referring not to the initial setup, but rather the day to day use. This inconvenience is an important point: while the use of 2FA is usually not burdensome for the user, it can be in some use cases. For example, SMS and email-based implementations can experience delays in delivery of the one-time use code. SMS-based implementations also may cause issues if a user travels internationally and does not have text service available, or if he or she is simply in an area with poor reception. If a user must change phone numbers, he or she has the added inconvenience of needing to adjust any SMS-based 2FA services. Software-based token implementations can also cause inconvenience when users purchase a new phone.

Another user mentioned concern about phone availability, albeit from a different perspective: "Concerned about if my phone dies and I can't get a code to log into my account when I don't have a power cord." Only one participant noted they already have 2FA services enabled for all of their most important accounts. Another user noted, "Gmail already does a good job of protecting me" – an interesting assertion, since Google strongly recommends 2FA to its users on its 2-step verification landing page (https://www.google.com/landing/2step/).

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

4. Discussion, Future Research, and Limitations

The observations from this study raise several questions which may merit further inquiry, either by researchers in academia or commercial enterprises. Some possibilities are outlined in the following sections.

4.1. Opt-In vs. Opt-Out vs. Mandatory

Corporate users often benefit, whether they realize it or not, from security awareness programs and policies surrounding their online behaviors; home end-users have no such awareness programs and policies (Anderson & Agarwal, 2010). While the 31% voluntary adoption rate of users who viewed the fear appeal message is a success, a much higher rate would be desirable. Some service providers, particularly financial institutions, have gradually changed their practices on 2FA. At a minimum, some have implemented a policy of requiring a second factor for any logins from an unrecognized device. This "stealthy" approach to mandating 2FA provides substantial security benefits to the user by automatically requiring attackers attempting to gain access from another system to provide an additional authentication factor. However, a business considering a mandatory implementation would likely benefit from research to answer a variety of questions. Is there a risk to the business? Will users become so frustrated with mandated 2FA that they opt to take their business elsewhere? Does the degree to which that is the case (a user's susceptibility to change providers due to an overly aggressive 2FA implementation they perceive as burdensome) differ across services (e.g. banking, social media accounts, email, cloud storage, mobile)? That is, will a person stick with a bank, perhaps due to the perceived importance of the security or the high response cost of changing (such as closing one account, opening a new account, and changing automatic bill pay setups), but readily choose a different free email provider? Are other costs, such as increased customer support cases, a major impact on providers?

Another option for providers would be to become more aggressive in encouraging the use of 2FA during the signup of new accounts, or even with existing accounts. During the signup process, the user can be prompted to provide another factor and enable 2FA services, with the opportunity to opt out, rather than 2FA services being something a user must seek out after the fact. The decision to improve security may well be analogous to

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

another decision which has been studied extensively by behavioral economists: enrollment in retirement savings plans (e.g., see Madrian and Shea, 2001; Thaler and Benartzi, 2004). Financial literacy and information security are both areas of great importance in people's lives, but ones in which many people are uncomfortable making decisions. As such, both inertia and recommended defaults are of great consequence to ultimate decisions. Participation in retirement plans tends to increase dramatically under systems which feature automatic enrollment, requiring those who do not wish to participate to opt out (Madrian and Shea, 2001). At one Fortune 500 company, the rate of enrollment of new hires went from 37.4% to 85.9% after implementation of an automatic enrollment system (ibid). Given the 2FA intent statistics presented earlier in this paper, it is likely that enrollment in 2FA services would similarly see dramatic gains under an opt-out system. Because users have the freedom to opt out, they would be unlikely to abandon the service provider over this procedural change.

4.2. Improvements in 2FA Usability, Actual and Perceived

As noted above, participants who did not perceive the enhanced authentication procedures as easy to use tended not to adopt. Some recent implementations have included major usability enhancements. Specifically, "Google Prompt" uses a push notification to the user's phone rather than the entry of a one-time use code. This notification replaces the more burdensome code entry with a simple tap on the mobile device to approve the login. Other providers such as Microsoft offer the same functionality. Further research could help determine if this usability improvement could cause more users to be confident in 2FA's ease of use, resulting in a corresponding increase in adoption? Since user perception is important, not merely actual usability, how can these enhancements become known to the masses? Combining these usability improvements with a more aggressive campaign for users to enable the service could potentially present massive gains in participation with few complaints.

4.3. Study Limitations

This study of millennials provides interesting insights as described above. For example, from this sample confidence in 2FA usability appeared to be an important factor in deciding to adopt 2FA services. Further research is necessary to determine if the trends

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

from this sample hold for a larger and more diverse group of millennials, as well as to determine the similarities and differences between millennials and other generations.

5. Conclusions

This study provides value from the perspectives of security advocates and service providers. Security advocates interested in crafting a persuasive message may wish to adjust their tactics slightly based on this data. Specifically, it appears only moderate focus on the threat is appropriate, but persuading recipients the technology is easy to use appears to be critical.

Many service providers have offered 2FA as an enhanced security option, as was demonstrated in Table 1. However, as 2FA has become more prevalent and the technology's usability improves, providers should reevaluate their approach to "marketing" their technology to their user base. The predominant approach has often seemed to be to merely offer 2FA as a service for those who seek it out, but this does little to build awareness among users about its availability or purpose. Public opinions on receptivity to these additional measures are certainly not static, either. Publicity surrounding data breaches has increased in recent years, and likely, with it, an interest in privacy and threat awareness. Moreover, as more businesses adopt 2FA services as a requirement for accessing corporate resources, it is possible for the demonstrably important "ease of use" metrics to shift favorably.

With the overall adoption rate possibly in the 5% range, the opportunity exists for significant improvement. Indeed, participants in this study adopted 2FA services at a 31% rate within one week of viewing of a short video message, and even users who did not adopt reported an increased intent to do so in the future. Results of this study combined with years of research in behavioral psychology offer promising avenues for security practitioners and service providers alike, in the pursuit of improving end-user security postures and a reduction in cyber crime resulting from account takeover.

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

References

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Q., 34(3), 613–643.

Anderson, J. Q., & Rainie, L. (2010). Millennials will make online sharing in networks a lifelong habit. Retrieved from http://www.pewinternet.org/2010/07/09/millennials-will-make-online-sharing-in-networks-a-lifelong-habit/

Aurigemma, S., Mattson, T., Leonard, L. (2017). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications? 50th Hawaii International Conference on System Sciences (HICSS) , Computer Society Press.

Aurigemma, S., Leonard, L., Mattson, T. (2016). Exploring the Gap Between Intent and Actual Security Behavior by Evaluating the Use of Password Manager Applications Among Home End-Users. IFIP WG 8.11/11.13 Information Systems Security Research, Santa Fe, NM: Dewald Roode Working Group.

FBI. (2015, October 5). Cyber Tip: Protect Yourself with Two-Factor Authentication. Retrieved November 26, 2016, from https://www.fbi.gov/news/stories/cyber-tip-protect-yourself-with-two-factor-authentication

Gore, T. D., & Bracken, C. C. (2005). Testing the Theoretical Design of a Health Risk Message: Reexamining the Major Tenets of the Extended Parallel Process Model. Health Education & Behavior, 32(1), 27–41. https://doi.org/10.1177/1090198104266901

Goel, Vindu, and Nicole Perlroth. “Yahoo Says 1 Billion User Accounts Were Hacked.” The New York Times, December 14, 2016. http://www.nytimes.com/2016/12/14/technology/yahoo-hack.html.

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (pp. 71–80). New York, NY, USA: ACM. https://doi.org/10.1145/1102199.1102214

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

Honan, M. (2012, August 6). How Apple and Amazon Security Flaws Led to My Epic Hacking. Retrieved November 19, 2016, from https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

Humphries, D. (2015, January 20). Best Practices for Workplace Passwords. Retrieved December 30, 2016, from http://www.softwareadvice.com/security/industryview/password-workplace-report-2015/

Huth, A., Orlando, M., & Pesante, L. (2012). Password Security, Protection, and Management. Retrieved December 30, 2016, from http://aahuth.com/wp-content/uploads/sites/44/2014/02/PasswordMgmt2012-2.pdf

IC3. (2016, June 14). Business E-mail Compromise: The 3.1 Billion Dollar Scam (I-061416-PSA). Retrieved December 30, 2016, from https://www.ic3.gov/media/2016/160614.aspx

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Q., 34(3), 549–566.

Junco, R., & Mastrodicasa, J. (2007). Connecting to the Net.Generation: What Higher Education Professionals Need to Know About Today's Students. Naspa.

Konoth, R. K., van der Veen, V., & Bos, H. (2016). How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication. In Proceedings of the 20th International Conference on Financial Cryptography and Data Security. Retrieved from https://news.asis.io/sites/default/files/24_Konoth_0.pdf

Krebs, Brian. (2009, June 14). Backstage with the Gameover Botnet Hijackers. Retrieved from https://krebsonsecurity.com/2014/06/backstage-with-the-gameover-botnet-hijackers/

Madrian, B. C., & Shea, D. F. (2001). The Power of Suggestion: Inertia in 401(k) Participation and Savings Behavior. The Quarterly Journal of Economics, 116(4), 1149–1187. https://doi.org/10.1162/003355301753265543

Palmgren, K. (2015, September). Two-Step Verification. OUCH! The Monthly Security Awareness Newsletter for Computer Users.

Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015). Two-factor authentication: is the world ready?: Quantifying 2FA adoption. In Proceedings of

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

the Eighth European Workshop on System Security (p. 4). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2751327

Ruiter, R. A. C., Kessels, L. T. E., Peters, G.-J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. International Journal of Psychology, 49(2), 63–70. https://doi.org/10.1002/ijop.12042

Thaler, R. H., & Benartzi, S. (2004). Save More Tomorrow™: Using Behavioral Economics to Increase Employee Saving. Journal of Political Economy, 112(S1), S164–S187. https://doi.org/10.1086/380085

US-CERT. (2015, July 31). Best Practices to Protect You, Your Network, and Your Information. Retrieved November 26, 2016, from https://www.us-cert.gov/ncas/current-activity/2015/07/31/Best-Practices-Protect-You-Your-Network-and-Your-Information

Vance, A. (2010, January 20). Simple Passwords Remain Popular, Despite Risk of Hacking. The New York Times. Retrieved from http://www.nytimes.com/2010/01/21/technology/21password.html

Verizon. (2016). 2016 Data Breach Investigations Report. Retrieved December 30, 2016, from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Witte, K., Meyer, G., & Martell, D. (2001). Effective Health Risk Messages: A Step-By-Step Guide. Sage Publications. Retrieved from https://us.sagepub.com/en-us/nam/effective-health-risk-messages/book10703

Zeltser, L. (2015, October). Password Managers. OUCH! The Monthly Security Awareness Newsletter for Computer Users.

Preston S. Ackerman,
psackerman@gmail.com

© 2017 The SANS Institute Author retains full rights.

Last Updated: June 23rd, 2017

Upcoming SANS App Sec Training

SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Minneapolis DEV534	Minneapolis, MN	Aug 25, 2017 - Aug 28, 2017	Community SANS
Community SANS San Francisco DEV541	San Francisco, CA	Aug 28, 2017 - Aug 31, 2017	Community SANS
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Secure DevOps Summit & Training	Denver, CO	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - DEV522: Defending Web Applications Security Essentials	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced