Use offense to inform defense.
Find flaws before the bad guys do.

A Swipe and a Tap: Does Marketing Easier 2FA Increase Adoption?

GIAC GCIH Gold Certification

Author: Preston S. Ackerman, psackerman@gmail.com
Advisor: Bryan Simon
Accepted: 11/10/2018

Abstract

Data breaches and Internet-enabled fraud remain a costly and troubling issue for businesses and home end-users alike. Two-factor authentication (2FA) has long held promise as one of the most viable solutions that enables ordinary users to implement extraordinary protection. A security industry push for widespread 2FA availability has resulted in the service being offered free of charge on most major platforms; however, user adoption remains low. A previous study (Ackerman, 2017) indicated that awareness videos can influence user behavior by providing a clear message which outlines personal risks, offers a mitigation strategy, and demonstrates the ease of implementing the mitigating measure. Building on that previous work, this study, focused on younger millennials between 21 and 26 years of age, seeks to reveal additional insights by designing experiments around the following key questions: 1) Does including a real-time implementation demonstration increase user adoption? 2) Does marketing the convenient push notification form of 2FA, rather than the popular SMS text method, increase user adoption? To address these questions, a two-phase study exposed groups of users to different video messages advocating use of 2FA. Each phase of the survey collected data measuring self-efficacy, fear, response costs and efficacy, perceived threat vulnerability and severity, and behavioral intent. The second phase also collected survey data regarding actual 2FA adoption. The insights derived from subsequent analysis could be applicable not just to increasing 2FA adoption but to security awareness programs more generally.

1. Introduction

Both business and home internet users continue to suffer the effects of frequent data breaches and frauds, resulting in substantial financial losses. The theft of credentials is at the heart of many of these incidents. The FBI's Internet Crime Complaint Center (IC3) receives over a quarter of a million complaints per year and publishes Public Service Announcements (PSAs) regarding observed trends. All of the IC3 PSAs in Table 1 below cover crime issues which rely in whole or in part on the theft of credentials or the use of previously stolen credentials.

Article Title	Date of Publication
Cyber Actors Increasingly Exploit the Remote Desktop Protocol to Conduct Malicious Activity	September 27, 2018
Cybercriminals Utilize Social Engineering Techniques to Obtain Employee Credentials to Conduct Payroll Diversion	September 18, 2018
Extortionists Increasingly Using Recipients' Personal Information to Intimidate Victims	August 7, 2018
Cyber Actors Use Internet of Things Devices as Proxies for Anonymity and Pursuit of Malicious Cyber Activities	August 2, 2018
Business E-mail Compromise The 12 Billion Dollar Scam	July 12, 2018

Table 1: Selected Articles Published in 2018 by IC3, https://www.ic3.gov/media

The brief list encompasses such major issues as Business Email Compromise (BEC), payroll fraud, extortion, compromise of remote access, and mass compromise of Internet of Things (IoT) devices. Remarkably, the table includes only articles from the third quarter of 2018!

The eleventh installment of the oft-cited Verizon Data Breach Report tells a similar story regarding the importance of credential theft (Widup, Spitler, Hylender, & Bassett, 2018). In an analysis of 1,799 confirmed data breaches, Verizon identified the top hacking activity conducted was "Use of Stolen Credentials" (Widup, Spitler, Hylender, & Bassett, 2018). Many of the other top activities identified are methods often

used in credential compromise (e.g., phishing, brute-force, password dumper, keylogger.) Verizon's report also found that 13% of breaches featured phishing, a common tactic for account takeover, a number which would have been even higher had banking trojan botnets been included. Moreover, Verizon noted that phishing remains the preferred method for social attacks. Actors motivated by both financial gain (59%) and espionage (41%) leveraged phishing frequently. Indeed, 70% of the nation-state sponsored attacks reportedly featured phishing (Widup, Spitler, Hylender, & Bassett, 2018).

Because phishing has been a top attack vector for years, it has also been a fixture in media coverage and security awareness programs. If these awareness programs work, one might ask, "Shouldn't we see some improvement in user behavior regarding phishing?" Fortunately, the Verizon report offers some hopeful evidence that the programs have had some impact. Data from phishing simulations revealed that in a typical organization, 78% of users do not click a single phishing link during a one-year period. Unfortunately, 4% of people still click during any given campaign; however, this is down substantially from the 11% figure Verizon reported during 2014 (Widup, Spitler, Hylender, & Bassett, 2018).

Problems such as poor user password hygeine, credential theft on a mass scale through data breaches, and password cracking have eroded the security of passwords. The situation has become so dismal that many researchers and security companies are looking to develop authentication solutions which do not rely on passwords at all. Famed security consultant and reformed social engineer Frank Abagnale, on whom Leonardo DiCaprio's character in the movie "Catch Me if You Can" was based, humorously quipped "Passwords are for treehouses, not computers!" (Carpenter, 2018). Abagnale's remark was in the context of his endorsing Trusona's password-free authentication system. Until password-free authentication solutions are widely accepted and deployed, Internet users are stuck with securing their accounts to the best of their ability using the existing paradigm.

To this end, two-factor authentication (2FA) is widely regarded by security experts as a viable complement to passwords with which users can enhance their account security. Indeed, Google offers enhanced account protection (of which 2FA is one

component) designed to protect sensitive users such as journalists, activists, business leaders, and political campaign teams, but the protection is free[1] for any who wish to use it ("Google Advanced Protection Program," n.d.). Recent years have seen a push for 2FA availability by security professionals. Subsequently 2FA is now offered free of charge on most major platforms, encompassing such Internet staples as email, cloud storage and services, social media, banking, shopping, mobile devices, and even gaming. Both Fortnite (Epic Games) and World of Warcraft (Blizzard Entertainment) incentivized the use of 2FA for their users by offering a free enhancement to the persona of gamers who enable it (Kuchera, 2018; "Upgrade Your Account Security and Get a Backpack Upgrade - WoW," n.d.).

Despite the prevalence of media coverage of breaches and despite the consistent recommendations of security professionals and service providers for users to enable 2FA, user adoption remains low. Providers have historically been reluctant to provide 2FA usage statistics, requiring researchers to resort to more creative means of estimating usage numbers (see, e.g., Petsas et al., 2015; Oberheide, 2015). However, some notable exceptions have emerged. In the case of Google, one of the company's engineers recently estimated 10% of users enable the feature (O'Neill, 2018). Dropbox similarly reported usage statistics in 2016, stating an astonishingly low 1% of its users enable the feature (Heim, 2016). Dropbox further noted it had no documented cases of account compromise for its 2FA-enabled accounts.

1.1. Importance to Information Security Community

Although service providers increasingly appear to encourage their users to enable 2FA and can demonstrate improved outcomes for those who do (Heim, 2016; O'Neill, 2018), providers remain hesitant to mandate the use of 2FA for fear of discouraging customer use due to the inconvenience. So long as this situation remains the status quo, a more secure Internet is dependent on security professionals, service providers, and even

[1] Although the service is free, it does require use of a hardware security key. Even so, with reputable vendors offering compatible keys for under $20, this service is an option for virtually anyone who wishes to use it.

knowledgeable friends/family/acquaintances[2] convincing end-users to enable 2FA voluntarily.

Security Education Training Awareness (SETA) remains a vital part of information security. Implementing a SETA program is one of the Center for Internet Security's Critical Controls (Center for Internet Security, 2018), and programs like SANS Security Awareness offer vast amounts of free and paid resources on information security to the public. Understanding how to best craft and deliver messages to elicit voluntary protective behavior in end-users, including making use of 2FA, is of vital importance to the information security community.

Videos are an important and increasingly popular way to convey security messages. The landing page for Google's aforementioned "Advanced Protection Program" features an explanatory video, as does the popular 2FA information resource turnon2fa.com. Cisco-owned Duo Security, one of the leading providers of 2FA services, hosts numerous informative videos on its products and the advantages of using 2FA, often employing humor to engage its viewers (https://duo.com/resources/videos). Abawajy (2014) demonstrated that information security video messages are more popular than text and game-based delivery combined, and pointed out key advantages:

- Both video and audio learning for participants;
- Self-paced, independent learning and the ability to start and stop as the user's schedule requires;
- The flexibility offered by the ability to watch and re-watch as needed.

Accordingly, in the Ackerman (2017) study, participants viewed a video which recommended adoption of 2FA and provided a real-time demonstration implementing 2FA for a Google account. The users answered survey questions regarding their intent to

[2] In fact, research has shown security messages passed along by friends and family, particularly when given by someone with a computer science or information technology background, to be one of the most common ways users receive security advice (Redmiles, Kross, & Mazurek, 2016).

adopt 2FA. They were surveyed again approximately one week later to assess whether or not users chose to adopt.

The study's key insights included the following:

- Security advocates can influence user behavior by providing a clear message which identifies personal risks, offers a strategy for mitigation, and demonstrates the ease of implementing the mitigating measure;
- Users were not overly responsive to fear appeal in the video message;
- Users who lack self-efficacy (confidence in their ability to carry out an action) to implement 2FA services rarely attempt to adopt 2FA.

Less than two months after Ackerman (2017), another informative study on video messages promoting 2FA was published (Albayram, Hasan Khan, & Fagan, 2017). The Albayram et al. study also employed a two-phase experimental design. Like Ackerman (2017) the study focused on risk and user self-efficacy, but it also included survey questions to address the possible negative consequences of adoption (inconvenience, lost phones, lack of cell service). The study surveyed participants ranging from 19 to 70 years of age. Table 2**Error! Reference source not found.** summarizes key findings which bear mentioning in this discussion:

Users exposed to the self-efficacy and risk themes found the information most useful
Users exposed to longer videos found the messages more useful and interesting
Participants in the 18-25 demographic were more willing to try 2FA than the baseline
Users who viewed both the risk and self-efficacy themes were more willing to try 2FA than those who only viewed the risk theme
There was a significant correlation between willingness to try 2FA and enabling 2FA

Table 2: Selected Insights from (Albayram, Hasan Khan, & Fagan, 2017)

2. New Research on Marketing of 2FA Services

2.1. Millennial Demographic

Researchers, business analysts, and the media have been endlessly fascinated with the market impacts of the behavioral choices of millennials, prompting lists of things millennials are "killing" to spring up all over the Internet (see, e.g., Bryan, 2017; Taylor, 2017; Josuweit, 2017), on outlets ranging from Buzzfeed to Forbes. Common examples include golf, chain restaurants such as Applebee's and Buffalo Wild Wings, cable TV, bar soap, and fabric softener. Mayonnaise was even thrown into the fray recently (Hingston, 2018). Many articles are written in a curmudgeonly tone, seemingly passing judgment on millennials for the impact they have had as a group on various industries. In focusing on millennials and their security behaviors, this study makes no such value judgment. Rather, it simply acknowledges the profound influence millennials have as a demographic, and how they have, in some instances, shown themselves to be markedly different from the preceding generations. As such, the security behaviors of millennials are an important area for researchers to explore.

There is some variance in exactly what birth years are included in the term "millennial". The US Census Bureau designated the millennial demographic as including those born between 1982 and 2000 (US Census Bureau, 2015). The population for this study included college students in their junior year or above, to include some graduate students. The group was at the younger end of the millennial scale, ranging in age from 21 to 26 years old.

Studies have shown there are demonstrable differences in security behaviors between millennials and other generations, both positive and negative. Millennials are considered naturally tech-savvy and comfortable with a wide range of online applications (Junco & Mastrodicasa, 2007). They also post personal information online more readily than previous generations (Anderson & Rainie, 2010; Gross & Acquisti, 2005), sometimes leading to a perception they are not security conscious. A Microsoft threat intelligence presentation at an international cybercrime symposium revealed millennials have the highest click-through rate of all demographics on tech support scams,

accounting for 50% of the fraudulent interactions observed by Microsoft's Digital Crimes Unit (Schrade, 2018).

The password hygiene of millennials is generally a bit worse than the baseline, with millennials re-using passwords more often and sharing passwords more often than all other demographics (Pew Research Center, 2017). Over a third of them use four or fewer passwords across all their accounts (TeleSign, 2016). While they tend to be lax about passwords, they are more willing to enable 2FA than their counterparts from other generations (Albayram, Hasan Khan, & Fagan, 2017; IBM Security, 2018), and use biometric authentication mechanisms at a higher rate (IBM Security, 2018).

2.2. Study Objectives

Building upon the Ackerman (2017) study, this work seeks to achieve two objectives related to millennial security behavior choices. Ackerman (2017) used a real-time demonstration of setting up 2FA using SMS for a Google account. On the surface, that certainly seems like useful information to include in the video. The purpose of including it was not so much as a "how-to" – the participants were provided other comprehensive 2FA resources – but rather to show how quick and easy the process is, in hopes of improving user self-efficacy. The Albayram et al. 2017 study featured a similar step-by-step presentation approach, for which it received numerous positive comments from the participants. While users may prefer a real-time or step-by-step approach with setup screenshots, neither study established whether such an approach increases adoption. This study will attempt to do so.

Ackerman (2017) identified prompt-based authentication mechanisms as an area for further research. The previous study selected SMS text-based 2FA for demonstration purposes because daily use of text messaging, either via SMS or other messaging apps, is nearly universal for millennials. Their level of comfort with SMS text messaging made it a good choice for an introductory exposure to 2FA. However, text-based 2FA has its drawbacks. It is the least secure form of 2FA available, such that other security professionals would perhaps question why it was selected at all. After all, it is subject to the well-known vulnerabilities in the SS7 protocol (Brandom, 2017). The answer to that question lies in this study's focus on increasing *voluntary* adoption. Even the use of text-

based 2FA is better than only a password, especially given the lax password habits of the target demographic.

In addition to being more secure than text-based 2FA, prompt-based 2FA is more streamlined. Prompt-based 2FA typically only requires the user to swipe down to reveal the notification and to tap on "Approve" to allow the login[3]. Text-based 2FA typically requires a swipe down to reveal notifications, opening a text message and either memorizing or copying a numeric code (typically six digits), switching back to the appropriate app, and either typing or pasting the temporary code. If the login is from a device other than the phone, the user will not usually have the option of pasting the code[4] and will be required to type it in. Recently some text apps have narrowed this usability gap for text-based 2FA somewhat by including logic that detects 2FA codes the user may wish to copy and including a copy option directly in the notification (see Figure 1). The user then has the extra steps required to paste into the app, typically with a "press and hold" to reveal a context menu followed by a "tap" to paste. Apple's iOS 12 has taken it a step further and will read the text message with the 2FA code and autofill the code into the requesting app (Manalo, 2018).

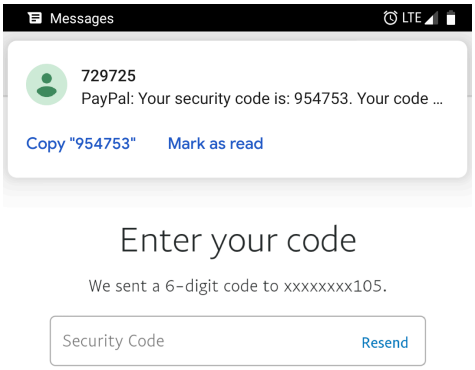

Figure 1: SMS app with logic to copy 2FA code in the notification

[3] There are subtle differences based on factors such as specific provider implementations, mobile OS, whether the phone is locked, etc. For example, some implementations place the box to approve over everything else, such that all that is required is to tap "Approve"! These differences are not important here.

[4] One exception would be if the user has a texting app open on the non-phone device, but surely that is an edge case.

Given the improved security and streamlined usability of prompt-based authentication mechanisms, it presents a promising opportunity to induce more users to adopt 2FA. Carnegie Mellon University (CMU) implemented Duo's 2FA authentication system, and researchers wisely took advantage of the opportunity to analyze the process (Colnago et al., 2018). The CMU implementation did not offer text-based 2FA as an option. With no text-based option, users overwhelmingly selected the push notification option, with it accounting for 91% of the setups and 89% of the overall logins (Colnago et al., 2018). This study seeks to determine if marketing notification-based 2FA's security and ease-of-use can increase adoption.

2.3. Study Design

An Institutional Review Board (IRB) at a small private university in the Midwest United States approved this two-part study conducted with two separate groups of undergraduate students. Data collection took place between February and April 2017. In the first part, each participant viewed a 2FA security message and answered questions regarding their intentions. Table 3**Error! Reference source not found.** below describes the video messages presented to the two groups.

Group	Description of Video Message
Control Group (112 Participants)	Message advocated the use of 2FA, provided links to general 2FA resources, but did not demonstrate setup in real-time (https://youtu.be/ftowWzKqec8).
Intervention Group (117 Participants)	Message advocated the use of 2FA and demonstrated real-time setup of SMS-based 2FA and Google Prompt notification for a Gmail account (https://youtu.be/ItSGEdnXlqk).

Table 3: Video messages presented to study groups

In both surveys, users answered questions regarding their self-efficacy, fear, response costs and efficacy, perceived threat vulnerability and severity, and behavioral intent. These responses used a 7-point scale, with seven indicating the highest self-

efficacy, strongest intent, and so on. Table 4 provides a detailed description of the items collected and the resulting values which form the basis of this study.

Approximately one week after reviewing the video and taking the initial survey regarding their intention to adopt 2FA, the 229 users participated in a second survey. Participants from both groups responded to an identical survey that collected objective data on whether they adopted additional 2FA, the type of 2FA they selected, the platforms on which they chose to enable 2FA, their rationale behind their decision whether to adopt 2FA and their future adoption intentions. Additionally, short in-person interviews were conducted with 20 randomly selected participants (ten from the control group and ten from the intervention group) to discuss the reasons they chose to use or not use 2FA.

Construct	Definition and Item Source(s)	Survey Question/Measurement Item	Item	Mean	Std Dev
Intention to use 2FA	Self-reported intention to use 2FA technologies in the future. Items adapted from Ajzen (1991), Aurigemma & Mattson (2018)	I intend to use 2FA services (such as SMS/text, email, Google Prompt and Authenticator) within the next week.	INT1	4.64	1.44
		I plan to use 2FA services (such as SMS/text, email, Google Prompt and Authenticator) in the next week.	INT2	4.59	1.518
		I predict I will use 2FA services (such as SMS/text, email, Google Prompt and Authenticator) within the next week.	INT3	4.65	1.481
		(INT Totals)		4.626	1.408
Self-efficacy	The perceived ability of the person to carry out the task of using 2FA services. Items adapted from Bandura (1991), Aurigemma & Mattson (2018)	2FA services (such as SMS/text, email, Google Prompt and Authenticator) are easy to use.	SE1	5.66	1.126
		2FA services (such as SMS/text, email, Google Prompt and Authenticator) are convenient to use.	SE2	5.25	1.34
		I am able to use 2FA services (such as SMS/text, email, Google Prompt and Authenticator) without much effort.	SE3	5.39	1.268
		(SE Totals)		5.435	1.089
Response Efficacy	The belief that using 2FA services will work and that using 2FA will be effective in protecting oneself or others. Items adapted from Floyd et al. (2000), Aurigemma & Mattson (2018)	Two-factor Authentication (2FA) services (such as SMS/text, email, Google Prompt and Authenticator) work to protect my online accounts from being stolen and abused by cyber-criminals.	REFF1	5.94	1.176
		2FA services (such as SMS/text, email, Google Prompt and Authenticator) are an effective solution to protect my online accounts from being stolen and abused by cyber-criminals.	REFF2	5.88	1.108
		When using 2FA services (such as SMS/text, email, Google Prompt and Authenticator), online accounts are more likely to be protected from being stolen and abused by cyber-criminals.	REFF3	5.88	1.199

		(REFF Totals)		5.901	1.041
Response Costs	The perceived costs (e.g., monetary, personal, time, effort) associated with using 2FA services. Items adapted from Floyd et al. (2000), Aurigemma & Mattson (2018)	The cost of findng 2FA services (such as SMS/text, email, Google Authenticator) decreases the convenience afforded by the service.	COST1	3.21	1.399
		There is too much work associated with trying to increase the security of my online accounts through the use of 2FA services (such as SMS/text, email, Google Authenticator).	COST2	3.48	1.474
		Using 2FA services (such as SMS/text, email, Google Authenticator), would require considerable investment of effort other than time.	COST3	3.18	1.376
		Using 2FA services (such as SMS/text, email, Google Authenticator), would be time consuming.	COST4	3.63	1.447
		(COST Totals)		3.377	1.164

Table 4: Survey constructs, sources, questions, and values.

3. Study Results

3.1. Actual 2FA Adoption

The adoption rates for the intervention and control groups must be compared to determine if the real-time demonstration of 2FA configuration and use increased adoption. The second survey collected data to determine 2FA adoption rates, both for the university email account as recommended in the message, as well as for other accounts. A Pearson Chi-Square test is applied to the data sets to determine if the increase in adoption of 2FA is a statistically significant increase over the control group. Table 5 shows the results and provides Pearson Chi-Square values for both groups.

	University Email	Other Accounts
Control Group	25/112 (22.3%)	53/112 (47.3%)
Intervention Group	33/117 (28.2%)	56/117 (47.8%)
Pearson Chi-Square, *p* value	$\chi 2 = 1.047$, $p = .306$	$\chi 2 = .0067$, $p = .935$

Table 5: 2FA Adoption Rates for Email and Other Accounts

The differences in adoption rates between the control and intervention groups, both for the university email and for all other accounts, were not statistically significant. Thus, the real-time demonstration did not increase adoption rates. Interestingly, fewer

participants enabled 2FA on their university Gmail account than other services. Although the intervention did not directly increase 2FA adoption rates in the one-week timeframe, it is possible it improved behavioral intent and self-efficacy, two factors which would increase future adoption (Aurigemma & Mattson, 2018; Ackerman, 2017).

3.1.1. Future Intent to Adopt

Participants stated their level of intent to use 2FA services in the next week, summarized in Table 6. The intervention group viewed the video with the real-time demonstration of initial configuration and use of 2FA services, while the control group video did not contain a real-time demo. An independent-samples t-test was conducted to compare future intent to use 2FA services between the intervention and control groups. There was a significant difference [t(227)=2.154, p=.032] for those who watched the real-time demo (mean=4.82, s.d.=1.388) compared to those who watched the video without the real-time demo (mean=4.42, s.d.=1.42). These results indicate video SETA training which highlights 2FA's ease of use and configuration improves a viewer's intent to use 2FA services in the future.

As noted previously, while the real-time 2FA demonstration did not produce a significant increase in 2FA adoption, it did increase future intent to use 2FA. This increase is a positive outcome because increased intent has been shown to later increase a given behavior (Milne, Sheeran, & Orbell, 2006). It is also notable that the future 2FA intention scores for those who actually adopted 2FA (mean=5.17, n=109, s.d.=1.33) are significantly higher than for those who did not (mean=4.13, n=120, s.d.=1.29) [t(227)=5.958, p < 0.001].

Group and Variable	n	Mean	Standard Deviation
Control Group, Behavioral Intent	112	4.42	1.42
Intervention Group, Behavioral Intent	117	4.82	1.388
Adopters, Behavioral Intent	109	5.17	1.33
Non-adopters, Behavioral Intent	120	4.13	1.29

Table 6: Summary of Behavioral Intent Survey Responses

3.1.2. User Self-Efficacy

Because the intervention message provided a full real-time demonstration of implementing 2FA on a Gmail account, it seems plausible the intervention could boost users' confidence in their ability to implement 2FA on their accounts. Participants responded as to whether they believed they could easily implement 2FA services with minimal effort.

An independent-samples t-test was conducted to compare participants' self-efficacy scores based upon whether or not the user viewed the intervention message (which included the real-time demonstration of 2FA configuration and use) or the control video (without a real-time demonstration). There was a significant difference [t(227)=1.964, p=0.051] in the self-efficacy scores for those who viewed the real-time 2FA demo (mean=5.57, s.d.=1.01) compared to those who viewed the video without the real-time demo (mean=5.29, s.d.=1.15).

These results indicate that video SETA training which highlights 2FA's ease of use and configuration improves viewers' confidence in their ability to implement 2FA services. Self-efficacy is a key contributor to one's future intent to perform a security behavior (Aurigemma, 2013), thus improving 2FA-related self-efficacy is expected to improve future 2FA adoption.

3.1.3. Response Costs and Efficacy

One potential benefit of the real-time 2FA video intervention is the opportunity to improve the overall decision calculus of a user evaluating whether or not to take a security action. Two of the primary components of Rational Choice Theory (RCT) are response efficacy and the anticipated costs of a behavior (Simon, 1955). Response efficacy is how good the prescribed action is at achieving its goal. In applying RCT to security behaviors, the more effective a security action is at enhancing information security and the lower the response cost (in time, money, convenience, and so on), the higher the likelihood the user will act (Aurigemma, 2013).

An independent-samples t-test was conducted to compare participants' perceived costs of adopting 2FA, based upon whether or not the user viewed the intervention message (which included the real-time demonstration of 2FA configuration and use) or

the control video (without a real-time demonstration). There was a significant difference [t(227)=1.892, p=0.06] in the response cost scores for those who viewed the real-time 2FA demo (mean=3.235, s.d.=1.24) compared to those who viewed the video without the real-time demo (mean=3.52, s.d.=1.06). These results indicate video SETA training which highlights 2FA's ease of use and configuration reduces the perceived costs and inconvenience of implementing 2FA. A reduction in perceived costs of implementing a security behavior is expected to increase the likelihood of future adoption.

Because the intervention in this study focused on ease of configuration and use of 2FA, the response efficacy scores were expected to be similar between the intervention and control groups. As expected, there was no significant difference in response efficacy between the groups [t(227)=0.701, p=0.454]. Both videos successfully sold participants on the effectiveness of 2FA, as the mean response efficacy for the entire population of the study was 5.901 on a 7-point scale.

3.2. Marketing Google Prompt as Easier and More Secure

The second objective was to assess whether demonstrating user-friendly and secure push-based 2FA offered with Google Prompt would increase user adoption. The intervention video featured a demonstration of Google Prompt, Google's push notification-based 2FA option. As noted previously, the intervention video did not significantly increase overall adoption. However, users stated which form of 2FA they preferred, with responses for the entire study presented in Figure 2.

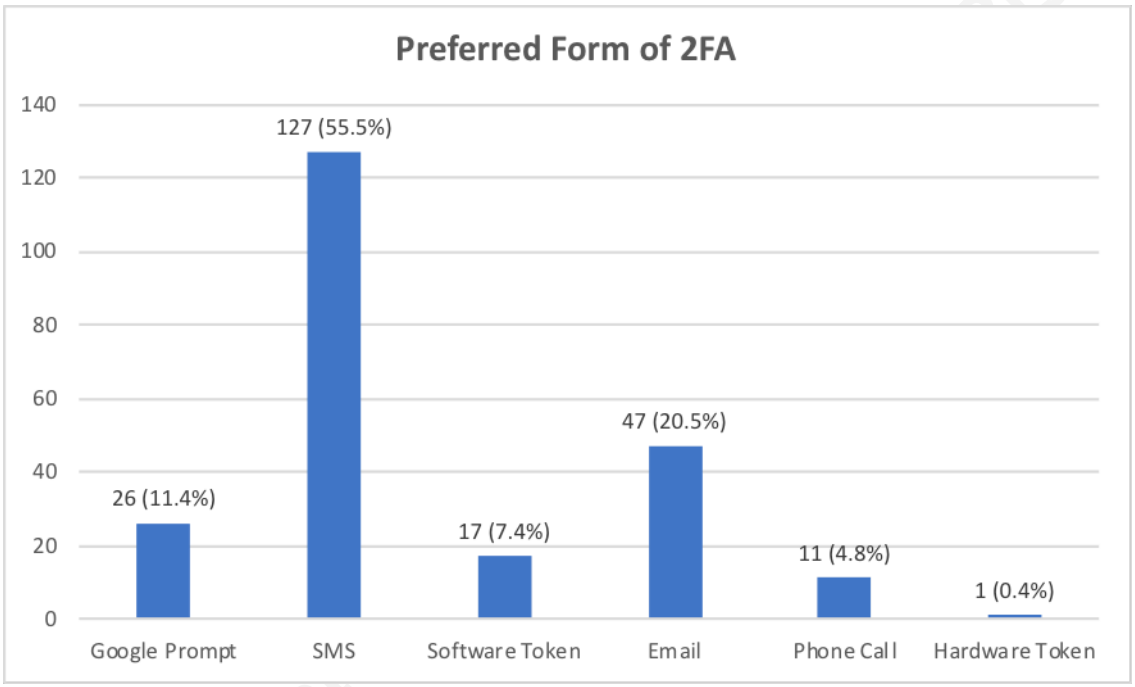

Figure 2: Second Factor Preferences Across Entire Study Population

Push-based notification through Google Prompt was thus the third most popular option. The data appears to show familiarity with the technology used as the second form of authentication is important to users. SMS, email, and phone calls are presumably the three most familiar technologies and are preferred collectively by 81%. Only 19% prefer the less familiar hardware token, software token, and Google Prompt options.

Marketing the push-based 2FA's ease-of-use did not increase voluntary adoption of 2FA. However, for those who did adopt, did it induce more of them to use Google Prompt? Because it is one of the most secure options, shifting more users to Google Prompt would still be a positive outcome. Figure 3 shows the comparison of preferred forms of 2FA comparing the control and intervention groups.

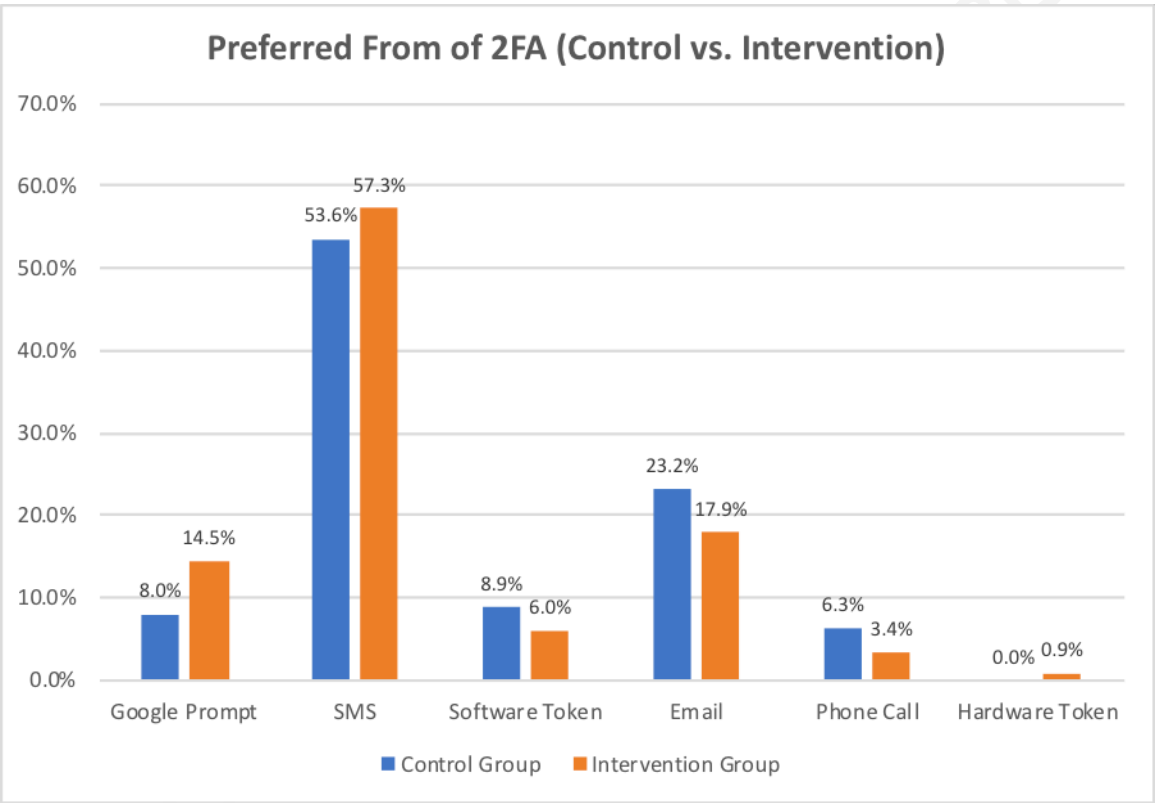

Figure 3: Comparison of Preferred Form of 2FA Across Groups

The intervention message did cause a noticeable shift to Google Prompt, with almost twice as many users stating a preference for it. However, it did not reduce the use of SMS-based 2FA, but rather perhaps contributed to convincing users who may otherwise have implemented software token, email, or phone call 2FA.

One possible contributor to 2FA preference is prior 2FA experience. Table 7 shows the three most popular forms of 2FA, broken down by whether or not the user reported having prior 2FA experience.

Preferred 2FA	Prior 2FA	No Prior 2FA
Google Prompt	14	12
SMS	87	40
Email	11	36

Table 7: Comparison of Preferred 2FA based on previous 2FA experience

Preston S. Ackerman, psackerman@gmail.com

A post hoc test was conducted to explore whether prior 2FA use influenced participants' preferences. A Chi-square test conducted on the results shown in Table 7 revealed a significant difference [Pearson Chi-square=28.374, $p<0.001$, $n=200$] in the preferred choices of 2FA between the two groups for SMS and email, but not for Google Prompt. These results suggest that for this study's sample population, those with prior 2FA experience have a strong preference for SMS-based 2FA, but significantly less interest in using Google prompt or email for the second factor. In contrast, those who had not previously used 2FA also showed little interest in Google Prompt but were approximately equally divided in their preference for SMS or email as the second factor.

These results pose challenges which security professionals must overcome when developing 2FA training. First, those with prior 2FA experience strongly favor SMS as a second factor, despite it being one of the least secure forms of 2FA. Anecdotal evidence from interviews with participants indicated this preference was based on familiarity with SMS as a communication method when compared with the "new" methods such as Google Prompt and hardware or software tokens, even if they are easier, faster, and more secure. Second, users who did not report prior 2FA experience relied less on SMS specifically, but still resisted the more secure second-factor options. Different messaging may be required to convince each of these groups to use stronger forms of 2FA. A one-size-fits-all SETA approach for 2FA may not be effective based on experience levels with the technology.

4. Conclusion

The results of this study provided additional support for Ackerman (2017), strengthening the conclusion that providing users a clear message which identifies risk and suggests mitigating actions within the user's capabilities can increase protective security behavior. Including such detailed information resulted in each video exceeding five minutes (Control Group: 5:13, Intervention Group: 9:34). However, the positive response of 52.8% of the participants implementing 2FA confirms the finding of previous studies that ensuring the videos contain quality information to engage the user is more important than the length of the video message (Albayram, Hasan Khan, & Fagan, 2017).

Preston S. Ackerman, psackerman@gmail.com

Unfortunately, neither use of a real-time demonstration nor marketing the convenient and secure push notification-based 2FA caused a significant increase in voluntary adoption of 2FA. However, that does not necessarily mean neither of those approaches is worthwhile. Users in a previous study spoke highly of including detailed setup instructions (Albayram, Hasan Khan, & Fagan, 2017), and the real-time demo did result in a statistically significant improvement of intent to adopt 2FA in the future. Marketing use of push-based 2FA resulted in the positive outcome of a noticeable but statistically insignificant shift of the users from less convenient and secure forms of 2FA to Google Prompt.

Interviews of survey participants regarding their preference for SMS 2FA brought a couple of reasons to the fore. First, they stated that they are comfortable with SMS and do not like the idea of having to keep track of different forms of 2FA across different services, particularly with something like Google Prompt which only works across Google's services. Second, Google Prompt is built-in to the operating system for Android users, but not for the large market segment of iPhone users, who did not find downloading and configuring another application (a downside for iPhone users which the video explicitly identified) "worth it" compared to simply using SMS. The reluctance to install another application is an example of users factoring response costs into their decision calculus. The user's mobile platform, which this survey did not collect, would be a good data point for future studies into this topic.

A key takeaway from this study is that the inertia of the more venerable technologies as a second form of authentication is a powerful force. SMS being the most popular second factor among the millennial study population was not surprising; however, it is shocking that 20.5% of the users preferred email. Previous experience with 2FA technologies also impacted user behavior, with users who lacked prior 2FA experience showing far more interest in using email than those who had 2FA experience. Corporate deployments should altogether avoid the issue of "convincing" users not to use less secure second factors by requiring a more secure form, as was done at Carnegie Mellon (Colnago et al., 2018). After all, the title of the study from CMU's implementation "It's Not Actually That Horrible" came from a user who found 2FA easier to use than expected.

Preston S. Ackerman, psackerman@gmail.com

Service providers and SETA programs interested in steering, but not mandating, users to select more secure second authentication factors have a challenge in front of them. A tailored approach to the message based on the audience may be beneficial. The message which might resonate most with an individual can depend on a variety of factors, to include generational and cultural differences, previous experiences, and affinity for technology. A possible application of this approach would be to produce awareness training which accounts for these factors and has content to address all of them. The training could then begin with questions assessing key factors such as user experience, and a customized selection of the training content would be provided based on user responses. Further research in this area could make SETA programs both more effective and efficient.

Preston S. Ackerman, psackerman@gmail.com

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Ackerman, P. (2017, February 10). Impediments to Adoption of Two-factor Authentication by Home End-Users. SANS Institute. Retrieved from goo.gl/ZhTQdU

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Albayram, Y., Hasan Khan, M. M., & Fagan, M. (2017). A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA). *International Journal of Human-Computer Interaction*, *33*(11), 927–942. https://doi.org/10.1080/10447318.2017.1306765

Anderson, J. Q., & Rainie, L. (2010). Millennials will make online sharing in networks a lifelong habit. Retrieved January 18, 2017, from http://www.pewinternet.org/2010/07/09/millennials-will-make-online-sharing-in-networks-a-lifelong-habit/

Aurigemma, S. (2013). A Composite Framework for Behavioral Compliance with Information Security Policies. Journal of Organizational and End User Computing, 25(3), 32–51. https://doi.org/10.4018/joeuc.2013070103

Aurigemma, S., & Mattson, T. (2018). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. Computers & Security, 73, 219–234. https://doi.org/10.1016/j.cose.2017.11.001

Bandura, A. (1991). Social cognitive theory of self-regulation. Organizational Behavior and Human Decision Processes, 50(2), 248–287. https://doi.org/10.1016/0749-5978(91)90022-L

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors (SSRN Scholarly Paper No. ID 2607190).

Preston S. Ackerman, psackerman@gmail.com

Rochester, NY: Social Science Research Network. Retrieved from https://papers.ssrn.com/abstract=2607190

Blizzard Entertainment. (2018, January 17). Upgrade Your Account Security and Get a Backpack Upgrade - WoW. Retrieved October 5, 2018, from https://worldofwarcraft.com/en-us/news/21366969/upgrade-your-account-security-and-get-a-backpack-upgrade

Brandom, R. (2017, September 8). This is why you shouldn't use texts for two-factor authentication. Retrieved October 13, 2018, from https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin

Bryan, C. (2017, July 31). RIP: Here are 70 things millennials have killed. Retrieved October 7, 2018, from https://mashable.com/2017/07/31/things-millennials-have-killed/

Carpenter, P. (2018, May 18). "Passwords are for treehouses, not computers!" - Frank Abagnale #kb4con18 [Tweet]. Retrieved from https://twitter.com/PerryCarpenter/status/997483138485030912

Center for Internet Security. (2018, March 19). CIS Control 17: Implement a Security Awareness and Training Program. Retrieved October 5, 2018, from https://www.cisecurity.org/controls/implement-a-security-awareness-and-training-program/

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018). "It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 456:1–456:11). New York, NY, USA: ACM. https://doi.org/10.1145/3173574.3174030

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

Heim, P. (n.d.). An inside look at how we keep customer data safe. Retrieved September 6, 2018, from https://blogs.dropbox.com/business/2016/02/dropbox-customer-data-safety/

Hingston, S. (2018, August 11). How Millennials Killed the Mayonnaise Industry. Retrieved October 7, 2018, from https://www.phillymag.com/articles/2018/08/11/mayonnaise-industry-millennials/

IBM Security. (2018, January 29). IBM Future of Identity Study: Millennials Poised to Disrupt Authentication Landscape. Retrieved October 7, 2018, from https://www-03.ibm.com/press/us/en/pressrelease/53646.wss

Josuweit, A. (2017, October 22). 5 Industries Millennials Are "Killing" (And Why). Retrieved October 7, 2018, from https://www.forbes.com/sites/andrewjosuweit/2017/10/22/5-industries-millennials-are-killing-and-why/#6b8a372e44e4

Junco, R., & Mastrodicasa, J. (2007). *Connecting to the Net.Generation: What Higher Education Professionals Need to Know About Today's Students*. Naspa. Retrieved from http://www.sidalc.net/cgi-bin/wxis.exe/?IsisScript=earth.xis&method=post&formato=2&cantidad=1&expresion=mfn=039908

Kuchera, B. (2018, August 24). Epic gives Fortnite players a free emote if they secure their accounts. Retrieved October 5, 2018, from https://www.polygon.com/fortnite/2018/8/24/17777080/fortnite-account-settings-security-two-factor-free-emote

Manalo, A. (2018, September 18). iOS 12 Makes 2FA for Third-Party Apps & Websites Easy with Security Code AutoFill from SMS Texts. Retrieved October 29, 2018, from https://ios.gadgethacks.com/how-to/ios-12-makes-2fa-for-third-party-apps-websites-easy-with-security-code-autofill-from-sms-texts-0185186/

Milne, S., Sheeran, P., & Orbell, S. (2006). Prediction and Intervention in Health- Related Behavior: A Meta- Analytic Review of Protection Motivation Theory. Journal of Applied Social Psychology, 30, 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Oberheide, J. (2015, May 15). Estimating Google's Two-Factor (2SV) Adoption with Pen, Paper, and Poor Math. Retrieved November 19, 2016, from https://duo.com/blog/estimating-googles-two-factor-2sv-adoption

O'Neill, P. H. (2018, January 17). Less than 10 percent of Google users turn on two-factor authentication. Retrieved August 5, 2018, from https://www.cyberscoop.com/two-factor-authentication-google-accounts-enigma-conference/

Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015). Two-factor authentication: is the world ready?: quantifying 2FA adoption. In *Proceedings of the Eighth European Workshop on System Security* (p. 4). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2751327

Pew Research Center. (2017, January 26). Americans, password management and mobile security. Retrieved October 12, 2018, from http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2016). How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16* (pp. 666–677). Vienna, Austria: ACM Press. https://doi.org/10.1145/2976749.2978307

Schrade, M. J. (2018, August). Investigating and Assessing the Impact of Botnets Through Big Data Visualization. Presented at the International Symposium on Cybercrime Response, Seoul, South Korea.

Simon, H. A. (1955). A Behavioral Model of Rational Choice. The Quarterly Journal of Economics, 69(1), 99–118. https://doi.org/10.2307/1884852

Taylor, K. (2017, October 31). "Psychologically scarred" millennials are killing countless industries from napkins to Applebee's — here are the businesses they like the least. Retrieved October 7, 2018, from https://www.businessinsider.com/millennials-are-killing-list-2017-8

TeleSign. (2016, November 16). TeleSign Consumer Account Security Report 2016. Retrieved October 5, 2018, from https://www.telesign.com/wp-

content/uploads/2016/11/TeleSign-Consumer-Account-Security-Report-2016-FINAL.pdf

US Census Bureau. (2015, June 25). Millennials Outnumber Baby Boomers and Are Far More Diverse. Retrieved October 29, 2018, from https://www.census.gov/newsroom/press-releases/2015/cb15-113.html

Widup, S., Spitler, M., Hylender, D., & Bassett, G. (2018). *2018 Verizon Data Breach Investigations Report*.

Last Updated: December 13th, 2018

Upcoming SANS Penetration Testing

Mentor Session AW - SEC542	Oklahoma City, OK	Dec 19, 2018 - Feb 01, 2019	Mentor
SANS Bangalore January 2019	Bangalore, India	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504 - 201901,	Jan 08, 2019 - Feb 14, 2019	vLive
Mentor Session - SEC542	Denver, CO	Jan 10, 2019 - Mar 14, 2019	Mentor
Mentor Session @ Work - SEC560	Louisville, KY	Jan 10, 2019 - Mar 14, 2019	Mentor
SANS Threat Hunting London 2019	London, United Kingdom	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Amsterdam January 2019	Amsterdam, Netherlands	Jan 14, 2019 - Jan 19, 2019	Live Event
Cyber Threat Intelligence Summit & Training 2019	Arlington, VA	Jan 21, 2019 - Jan 28, 2019	Live Event
SANS Miami 2019	Miami, FL	Jan 21, 2019 - Jan 26, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS SEC504 Stuttgart 2019 (In English)	Stuttgart, Germany	Feb 04, 2019 - Feb 09, 2019	Live Event
Community SANS Minneapolis SEC504	Minneapolis, MN	Feb 04, 2019 - Feb 09, 2019	Community SANS
Security East 2019 - SEC542: Web App Penetration Testing and Ethical Hacking	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
Mentor Session - SEC560	Fredericksburg, VA	Feb 06, 2019 - Mar 20, 2019	Mentor
Mentor Session - SEC560	Boca Raton, FL	Feb 07, 2019 - Feb 22, 2019	Mentor
SANS Northern VA Spring- Tysons 2019	Vienna, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS London February 2019	London, United Kingdom	Feb 11, 2019 - Feb 16, 2019	Live Event
Mentor Session: SEC560	Columbia, MD	Feb 16, 2019 - Mar 23, 2019	Mentor
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Zurich February 2019	Zurich, Switzerland	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Riyadh February 2019	Riyadh, Kingdom Of Saudi Arabia	Feb 23, 2019 - Feb 28, 2019	Live Event
Mentor Session - SEC504	Vancouver, BC	Feb 23, 2019 - Mar 23, 2019	Mentor
SANS Brussels February 2019	Brussels, Belgium	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Mentor Session - SEC542	Seattle, WA	Feb 26, 2019 - Apr 02, 2019	Mentor