Exploring How to Overcome Digital Akrasia in Two-Factor Authentication

Early stage paper

Xinhui Zhan
Price College of Business
University of Oklahoma
xzhan@ou.edu

Alexandra Durcikova
Price College of Business
University of Oklahoma
alex@ou.edu

Dennis Galletta
Katz Graduate School of Business
University of Pittsburgh
galletta@pitt.edu

ABSTRACT

This research explores "digital akrasia" in two-factor authentication deployment. To overcome the akrasia, we applied the concept of "nudging" and explored ways to promote the adoption of two-factor authentication. A 2 × 6 factorial experimental design was carried out to explore how six nudging mechanisms and two framings of two-factor authentication influence the employment of two-factor authentication. To obtain statistical power, we narrowed the analysis down to a 2 × 2 factorial design and focused on two extreme nudging mechanisms (i.e., reinforcement and fear). The results revealed an interaction effect between the framing of two-factor authentication and nudging mechanisms. When people are framed for the benefits of two-factor authentication, the reinforcement nudge works better than the fear nudge. In the situation when people were framed with the inconvenience of two-factor authentication, the fear nudge worked better than the reinforcement nudge.

Keywords

Digital akrasia, nudge, two-factor authentication, security decision making

INTRODUCTION

Two-factor authentication (2FA) ——a powerful server-side countermeasure for fighting against password stealing and protecting users and data——is critical to cybersecurity as it directly mitigates the risks associated with weak or compromised passwords (Brooks, 2022). 2FA provides two layers of security. After password and login details, a code will be sent via SMS, email, or a generated number via the 2FA App before the users can access their accounts. When 2FA is activated, an attacker who uses a victim's password needs access to an additional communication channel to receive a one-time-generated token, which must be used following the entry of a password during authentication. Without approval at the second factor, even when a password is hacked, no access to the account or data will be given. A 2019 report from Microsoft concluded that 2FA works, blocking 99.9% of automated attacks (Maynes, 2019). By the end of 2021, Google auto-enrolled 150 million users into using 2FA to access their accounts, which led to a 50% decline in compromised accounts (Li, 2022).

While the use of 2FA has surged in recent years, about 25% of users still choose not to adopt it (Brooks, 2022). Prior study has highlighted that end users believed 2FA made their accounts more secure (Colnago et al., 2018). But why do a quarter of users not employ this powerful, albeit not perfect, defense? One potential explanation for this question is the inability or unwillingness of people to act in their best interest, known as akrasia. Although 2FA is beneficial to the users, they might think operationally about the effort that might be required and thus ignore and choose not to adopt 2FA.

Our research questions focus on users' akrasia in 2FA deployment and explore interventions to overcome the akrasia and prompt the adoption of 2FA.

RQ1. *How does the framing of 2FA (i.e., the benefit of 2FA vs. hassles involved in 2FA) affect users' 2FA deployment?*

RQ2. *How to nudge users into adopting 2FA and thus overcome their akrasia?*

This study aims to address two important research gaps. First, while many studies in information systems security literature find intentions to be an adequate predictor of behavior, the strength of prediction is not as high as one might expect (Jenkins et al., 2021). Prior work has not attempted to explore Akrasia and differentiate it from the intention-behavior gap. We address this gap by differentiating what people believe they should do (normatively) from what people will likely do (predictively) in the context of 2FA. Second, prior information security studies have typically focused on fear appeal as an effective remedy to improve people's information security decision-making (Boss et al., 2015; Johnston et al., 2019; Vance et al., 2022). Our study explores other treatments to "nudge" people toward choices that are in their best interest, including facilitation, confronting, deception, social influence, and reinforcement (Caraban et al., 2019)

Our findings are expected to have important implications for practice. The enrollment rate of 2FA remains low in some industries that handle some of the most sensitive customer data – legal and insurance, with only 20% of employees using 2FA (Mccart, 2022). Our research offers insights into using tailored security nudges to encourage users and employees to adopt 2FA.

THEORETICAL BACKGROUND

Digital Akrasia

The word "Akrasia," Greek for "weakness of will," refers to the inability of people to act in their own best interests (Aagaard, 2019). Aagaard's study reported that the concept has roots as far back as Plato and Aristotle but created the term Digital Akrasia to describe poor habits of smartphone users that are practiced despite the knowledge that those habits are either rude or disruptive to others. Although Aagard's 2019 work in Akrasia addressed behaviors such as ignoring nearby people in favor of focusing on smartphones, he has also focused on other distraction-driven behaviors such as multitasking (Aagaard, 2019), tech addiction (Aagaard, 2021), and technology use while attending class (Aagaard, 2015; Selwyn and Aagaard, 2021),

The concept of Akrasia, well represented in philosophy, religion, and social psychology literature, is that people continually act in ways they know are problematic (Romaioli et al. 2008). Romaioli et al. provided some sample reasons for Akrasia tied to concepts such as gratification, pain avoidance, and expediency. They stated that "it becomes extremely difficult to understand how someone can do something they don't really want to." (p. 180). We find this

seemingly-irrational behavior that appears in our lives so often is an exciting and important area of study.

It is vital to differentiate Akrasia from an intention-behavior gap. While many studies in and out of the information systems literature find intentions to be an adequate predictor of behavior, the strength of prediction is not as high as one might expect. Sheeran's (2002) "meta-analysis of meta-analyses" found that intentions accounted for 28% of actual behavior, indicating that while predicting 28% of the variance in behavior is statistically strong, "72% of the variance has not been explained" (pg. 2). This leads to errors in drawing conclusions about relationships between constructs examined in studies. While Sheeran refers to reasons for the gap and identifies one reason as automatic processes that sometimes occur in people's behavior, there is no reference to Akrasia as another reason.

A deeper look is needed to tease out Akrasia from the intention-behavior gap. Romaioli et al. (2008) and Aagaard (2019) help us differentiate Akrasia by referring to temptation in several of their discussions. Romaioli et al. describe someone wanting to work late at night, intending to stay alert and avoid alcohol, but succumbs to the temptation of a nearby bottle of wine. Aagaard describes students in interviews who strongly criticize their peers for "phubbing" but then proceed to commit that very social behavior: they ignore their nearby friends and instead stare at their digital devices while browsing social media. Aagaard refers to this behavior as unintentional.

This scenario illustrates the key differentiator of the intention-behavior gap: A person might respond that they know that 2FA will improve security and perhaps prevent identity theft or loss of their data. This is the desired behavior. However, when they think operationally about the effort and/or inconvenience that might be required, their intentions might not be consistent with their assessment of the desirability of the action, and there might be a breakdown in their intentions. A common complaint of 2FA is captured in a recent study by describing it as "annoying," which likely led to the fact that even five years after introducing the technology on their platform, "less than 10% of Google user accounts use two-factor authentication" (Colnago et al. 2018, p. 2). Gatlan (2022) reported that Google recently found it necessary to begin automatically enrolling its users, resulting in a 50% reduction in compromised accounts for those who were enrolled.

Therefore, we should differentiate the assessment of the value of an infosec tool (such as the adoption of 2FA) from the intention to use it. Users might value the action but never intend to activate 2FA and subsequently never activate it. In this case, an intention-behavior gap is not the phenomenon of interest but rather the impact of Akrasia. A person answering a question about intentions could reflect on what they would need to do (pull out their mobile phone and confirm their authenticity) potentially every time they initiate an action and then conclude that they do not intend to use 2FA.

In this study, we collected data about subjects' assessment of the value of 2FA as one dependent variable and their likely action (a surrogate for intention) in a particular scenario. The two evaluations were strikingly different, as our results section describes.

Nudge Theory and Relevant Literature

The term "nudging" generally means "gently encouraging someone to do something" (Oxford Dictionary, 2015). Thaler and Sunstein (2008) popularized nudging as a behavioral economics method that aims to "nudge" people toward choices that are in their best interest by restricting their options. For example, when chips are replaced with healthy foods on the counter next to the check-out register, customers are more likely to buy more fruit and fewer chips when both options are still accessible. A nudge is defined as "any aspect of the choice architecture that modifies people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives" (Thaler and Sunstein 2008, pg. 6). Choice architecture is the design of different ways in which choices can be presented to decision-makers (Thaler et al., 2012), such as the different ways to describe the choices, using the "default" option, and changing the order of the choices.

The concept of nudging has also received attention from IS and HCI researchers. They incorporate user interface design elements and define digital nudging as "the use of user-interface design elements to guide people's behavior in digital choice environments" (Schneider et al., 2018). Meske and Potthoff (2017) further expand the definition of digital nudges as a "subtle way of guiding user behavior in digital settings using design, information, and interaction aspects without compromising the individual's freedom of choice."

Nudges have been employed in the security industry to help users make better security decisions. For example, password strength indicators are widely used to influence user behavior to create a more secure password. The effectiveness of password meters in persuading users to create stronger passwords was evaluated by Ur et al. (2017). Nudges have also been used in privacy; Almuhimedi et al. (2019) investigated the impact of nudges on mobile device location disclosure permissions. These studies demonstrate that digital nudging can help users achieve improved security and privacy behavior.

We identified two methods of security nudging in the IS literature: information-based nudging and presentation-based nudging. Information-based nudges provide tailored information to improve users' security awareness and reduce intention to violate security policy (Barlow et al., 2013), reduce cognitive habituation (Anderson et al., 2015; Vance et al., 2018), lead to greater security policy compliance (Johnston et al., 2019, Shepherd and Mejias, 2016) and improved cybersecurity behavior (Chen et al., 2015; Ferreyra et al., 2020; Goel et al., 2017; Hartwig and Reuter, 2021; Hu et al., 2015; Rosoff et al., 2013; Warberg et al., 2019). Table 1 summarizes these studies, providing their context, independent and dependent variables, the primary theory used (if any), and the nudge style.

So far, four papers utilized information-based nudges to prompt users to create a stronger password (Nicholson et al., 2018; Peer et al. 2020; Renaud et al. 2017; Vance et al., 2022). Nicholson et al. (2018) investigated the influence of three nudges on the creation of passwords: monetary incentive, length of the instructions, and using pictures. They discovered that users created longer passwords when provided instructions on creating a lengthy password and when offered a monetary incentive.

Their passwords were more difficult to crack than those passwords created without instructions. Moreover, a nudge that includes a picture that facilitates password strength did not result in longer or more secure passwords. Peer et al. (2020) studied five tips and indicators for password creation. They found that individual decision-making styles influence the nudges' effectiveness. Researchers also examined the framing of information and the inclusion of social proof to support the participant's password strength (Renaud et al., 2017).

General security warnings represent another main application area of security nudges (Vance et al., 2018; Ferreyra et al., 2020). Computers remind their users when detecting suspicious activity, such as the attempt to download a malicious file or to block someone from committing a risky action, such as setting personal information as public on social media. Ferreyra et al. (2020) provided an information-based nudge to communicate the risks associated with online self-disclosure. They found that nudges significantly increase users' perceived severity of privacy threats.

Message framing refers to how the phrasing of the message can influence the choice of one option over another. IS researchers have exploited framing effects when designing security nudges (Anderson and Agarwal, 2010; Barlow et al., 2013). Negative framing increased participants' security concerns if they had low levels of security concerns (Plachkinova and Menard, 2019).

In this study, presentation-based nudges use visual elements or user interface design elements to alter users' behavior. The literature has explored presentation-based security nudges to facilitate cybersecurity decision-making (Chen et al., 2015; Hu et al., 2015), improve password creation (Hartwig and Reuter, 2021; Renaud et al., 2017), and reduce cognitive habituation (Anderson et al., 2015; Anderson et al., 2016; Vance et al., 2018).

Ratings of products and colors (i.e., red and green for positive and negative reviews) were used in an application installation study (Chen et al., 2015). The results show that changes in the interface can have a strong effect on app installation decisions. Hartwig and Reuter (2021) designed a dynamic indicator for the strength of passwords. They found that dynamic radar charts present a moderately effective nudge towards stronger passwords. However, habituation is problematic when users face repeating and monotonous security warnings. Anderson et al. (2015, 2016) designed security nudges with a polymorphic appearance. Using fMRI and mouse cursor tracking, they discovered that polymorphic warnings could significantly reduce habituation than static ones. Similarly, Vance et al. (2022) focused on interactivity and provided "real-time feedback in response to a user's actions" to improve the effectiveness of static and interactive password indicators.

According to the psychology literature, individuals differ based on personality and decision-making styles; these differences may also result in differential responses to behavioral interventions of security decision-making. User security behaviors are expected to be influenced by human factors such as gender, age, education level, personality, and behavioral propensity. Plachkinova and Menard (2019) conducted a study to examine the relationships between initial security concerns, message framing, and security decisions. They found that participants' initial security concerns moderate the effect of framing on security actions. When participants revealed relatively high initial security concerns, the effect of message framing was statistically insignificant.

However, while the use of nudges in security and privacy has traditionally been a "one-size-fits-all" approach, recent research has classified security nudges into six categories: facilitate, confront, deceive, social influence, fear, and reinforce (Caraban et al., 2019). Specifically, the facilitate nudge encourages people to take actions that meet their best interests by diminishing physical or mental effort; the confront nudge attempt to pause mindless behavior by instilling doubts; the deceive nudge deceive people into actions to promote certain action; the social influence nudge urges people to conform to the actions of others; the fear nudge evokes feelings of fear, loss, and uncertainty; and finally the reinforce nudge attempts to get people's attention and reinforce action.

This distinction of nudge type provides the baseline for personalized and tailored security nudges for 2FA deployment. In this study, we designed six types of nudges to promote 2FA deployment and test their effect on users' decision-making.

Author + Year	Context	IV(Nudges)	DV	Primary Theory	Choice architecture of Nudges
Anderson et al., 2015	Security Warning	Polymorphic design of the window	Habituation of the warning	None	Design elements
Anderson et al., 2016	Security Warning	highlighting pre-selected options	Gaze (eye-tracking)	None	Design elements
Barlow et al., 2013	ISP violation	Negative vs positive framing of security training	Intention to violate	Prospect Theory	Text
Chen et al., 2015	Software Downloading	Amount of risk vs the amount of safety	App-installation decisions	Prospect Theory	Both
Ferreyra et al., 2020	Privacy	Cues of privacy risks	Online Self-Disclosure Decisions	None	Text
Goel et al., 2017	Phishing email	Gains and losses	Open or not open the email	Prospect Theory	Text
Hartwig and Reuter, 2021	Password Creation	password strength indicator	short-term effectiveness and users' perception of the nudges	None	Design elements
Hu et al., (2015)	ISP Violations	Choices in the environment	decisions (self-reported intention from scenarios)	Social Cognitive Theory	Design elements
Johnston et al., (2019)	ISP Compliance	Fear appeal rhetoric	Observed compliance behavior	PMT	Text
Nicholson et al., 2018	Password Creation	Instruction (Standard vs. long), Incentive (yes or no)	password length	None	Text
Peer et al., 2020	Password Creation	Five different tips and indicators for password creation	Password Strength	None	Text

Renaud et al., 2017	Password Creation	framing, expectation, social norms, reflection	password strength	None	Both
Rosoff et al., 2013	Software Downloading	Gain- and loss-framed scenarios	Decision	Prospect Theory	Text
Shepherd and Mejias, (2016)	ISP Violations	The remainder of acceptable use policies message	Observed behavior	None	Text
Shropshire et al., 2010	Security technology adoption	Negatively framed messages	Intention to adopt	Prospect Theory	Text
Valecha et al., 2016	Phishing email	Reward-based and risk-based	Response	Prospect Theory	Text
Vance et al., 2018	Security Warning	Pictorial symbols, color, animation	Habituation of the warning	None	Design elements
Vance et al., 2022	Password Creation	Static Fear Appeal vs. Interactive Fear Appeal	Password Strength	None	Both
Warberg et al., 2019	Security technology adoption	set default: opt-in vs opt-out	enroll or not with 'Yes' and 'No' response options	None	Text
Xu and Warkentin, (2020)	General Security Context	Central vs Peripheral Routes	Protection-motivated Behavior	Elaboration Likelihood Model	Not applicable

Table 1. Summary of Literature Review on Security Behavioral Nudges

PROPOSITIONS

In this exploratory study, we focus on studying the following six propositions:

> ***Proposition 1:*** There is a difference in digital Akrasia between novice and experienced 2FA users.
>
> ***Proposition 2:*** There is an effect of types of nudges on 2FA deployment decision-making.
>
> ***Proposition 3:*** There is a difference in digital Akrasia between a positive valence condition (i.e., focusing on the benefits of 2FA) and a negative valence condition (i.e., focusing on the inconvenience of 2FA).
>
> ***Proposition 4:*** There is an interaction between user characteristics and the type of nudge used.
>
> ***Proposition 5:*** There is a gap between intentions and value assessment of 2FA deployment.

METHODOLOGY

To test our propositions, we conducted a 2 x 6 online experiment crossing "scenario" with nudge type. Subjects were told they would be presented with a scenario regarding one of their private online accounts. After the scenario was presented, we showed subjects a pop-up message and asked them to respond to it. Subjects were randomly assigned to a scenario valence (positive impacts of 2FA vs. hassles involved in 2FA). After the scenario was presented, we asked the subject to read the pop-up message at least twice and forced the subject to stay on the nudge page for 10 seconds. Dependent variables were measured on 7-point Likert scales as follows:

> ***DV1 (normative)*** = I should click "Sign me up!" to turn on two-factor authentication.
>
> ***DV2 (predictive)*** = It is likely that I would click "Sign me up!" to turn on two-factor authentication.

Any difference between the normative and predictive DV would be ascribed to Digital Akrasia. After the nudge was presented, subjects were asked to recall the nudge. If they failed, they were disqualified from data collection.

Next, subjects were asked to complete the survey that contained the following constructs: self-control, conformity, big five personality, self-efficacy, attitude towards the color blue (used as a marker variable), and demographic questions. Please see Appendix B for the constructs, items, and their sources.

Data Collection, Sample, and Procedures

We recruited participants using MTurk. We enlisted individuals living in the United States, aged between 18 and 65 years old, who had completed at least 100 tasks on Mturk and maintained at least a 95% approval rating. First, we pre-tested our manipulations. Each valid response was paid $0.50. Second, we paid $1.50 for subjects in the main experiment. For the subject to be paid, s/he must have passed five attention check questions (subjects were alerted to this before consenting to participate in the experiment). A total of 1464 subjects started the survey, of which only 577 passed the attention checks. After further inspection, we removed another 166 responses because the IP address came from the same subnet or an unusual and long response to an open-ended feedback question at the end of the survey (not required) was exactly the same on multiple questionnaires. A net total of 411 valid responses were used to test our propositions. Table 2 provides the sample demographics. Appendix B details the measurement items for existing constructs, including self-control, conformity, self-efficacy, and Big Five.

		Frequency	Percentage
Age	Under 18	2	0.5%
	18-24	20	4.9%
	25-34	264	64.2%
	35-44	56	13.6%
	45-54	33	8.0%
	55-64	28	6.8%
	65+	8	1.9%
Gender	Male	296	72.0%
	Female	112	27.3%
	Other	3	0.7%
Employment	Working full-time	364	88.6%
	Working part-time	34	8.3%
	Unemployed and looking for work	2	0.5%
	A homemaker or stay-at-home parent	2	0.5%
	Student	3	0.7%
Education	High school diploma or GED	43	10.5%
	Some college, but no degree	21	5.1%
	Associates or technical degree	17	4.1%
	Bachelor's degree	275	66.9%
	Graduate or professional degree (MA, MS, MBA, Ph.D., JD, MD, DDS, etc.)	53	12.9%
	Prefer not to say	2	0.4%
2FA Experience	Yes	403	98.1%
	No	6	1.5%
	Not applicable	2	0.5%

Table 2. Sample Demographics (N = 411)

Results

We utilized SPSS to analyze the data. Table 3 shows the reliability values. Cronbach's alpha scores for all constructs were above 0.7. To evaluate the convergent and discriminant validity of the constructs in the questionnaire, confirmative factor analysis (CFA) was carried out. We excluded conformity and all of the Big Five personality measures because they were highly correlated, and the items loaded together. Table 5 shows the results of the confirmatory factor analysis.

	Cronbach's Alpha
Self-control	0.973
Conformity	0.913
Self-efficacy	0.761
Extraversion	0.87
Agreeableness	0.842
Conscientiousness	0.866
Neuroticism	0.897
Openness	0.895

Table 3. Reliability Values

Construct	Mean	SD	1	2	3	4	5	6	7
1. Self-control	4.983	1.377							
2. Conformity	4.953	1.110	-0.016						
3. Self-efficacy	5.500	1.049	-0.033	0.472					
4. Extraversion	4.986	1.308	0.045	0.676	0.462				
5. Agreeableness	5.295	1.080	0.028	0.592	0.623	0.677			
6. Conscientiousness	5.428	1.100	-0.017	0.449	0.685	0.563	0.719		
7. Neuroticism	4.641	1.520	-0.035	0.706	0.258	0.368	0.347	0.179	
8. Openness	5.276	1.054	-0.024	0.564	0.634	0.642	0.731	0.719	0.378

Table 4. Measurement Model Statistics

	Self-Control	Self-Efficacy
Self-Control1	**0.872**	-0.101
Self-Control2	**0.845**	-0.091
Self-Control3	**0.833**	-0.044
Self-Control4	**0.806**	-0.049

Self-Control5	**0.806**	-0.007
Self-Control6	**0.806**	0.018
Self-Control7	**0.849**	-0.066
Self-Control8	**0.824**	-0.036
Self-Control9	**0.83**	-0.024
Self-Control10	**0.826**	-0.055
Self-Control11	**0.826**	-0.084
Self-Control12	**0.854**	-0.025
Self-Control13	**0.802**	-0.039
Self-Control14	**0.819**	-0.145
Self-Control15	**0.787**	0.058
Self-Control16	**0.78**	-0.06
Self-Control17	**0.848**	-0.078
Self-Control18	**0.877**	-0.089
Self-Control19	**0.852**	-0.032
Self-Control20	**0.76**	0.029
Self-Efficacy1	0.318	**0.754**
Self-Efficacy2	0.353	**0.759**
Self-Efficacy3	0.348	**0.77**

Table 5. Results of Factor Analysis

We first conducted a MANOVA of 2 by 6 factorial design to explore our propositions. Table 6 provides the results of the first MANOVA test. The multivariate results indicate that the main effects of valence on both normative DV and predictive DV were not statistically significant. [F = 1.851, df = (1), p = 0.175 for the normative DV, and F = 0.434, df = (1), p = .511 for the predictive DV]. Thus, the positive and negative valence scenarios were not significantly different in their normative DV and predictive DV.

The main effects of a nudge on both normative DV and predictive DV were not statistically significant. [F = 1.313, df = (1), p = 0.260 for normative DV, and F = 0.236, df = (1), p = .946] for predictive DV. Thus, the six nudges were not significantly different in their normative DV and predictive DV.

Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
Valence	Normative DV	4.391	1.000	4.391	1.851	0.175
	Predictive DV	1.178	1.000	1.178	0.434	0.511
Nudge	Normative DV	15.574	5.000	3.115	1.313	0.260
	Predictive DV	3.208	5.000	0.642	0.236	0.946
Valence * Nudge	Normative DV	25.515	5.000	5.103	2.151	0.061
	Predictive DV	29.241	5.000	5.848	2.152	0.061

Table 6. Results of the MANOVA (2X6 factorial design)

We narrowed the study to a 2 x 2 factorial design to examine the effect of a nudge further. We mainly focused on two types of nudges out of the six: reinforcement and fear. A MANOVA was used to compare the means of our normative and predictive dependent variables. Table 7 provides the results of the second MANOVA.

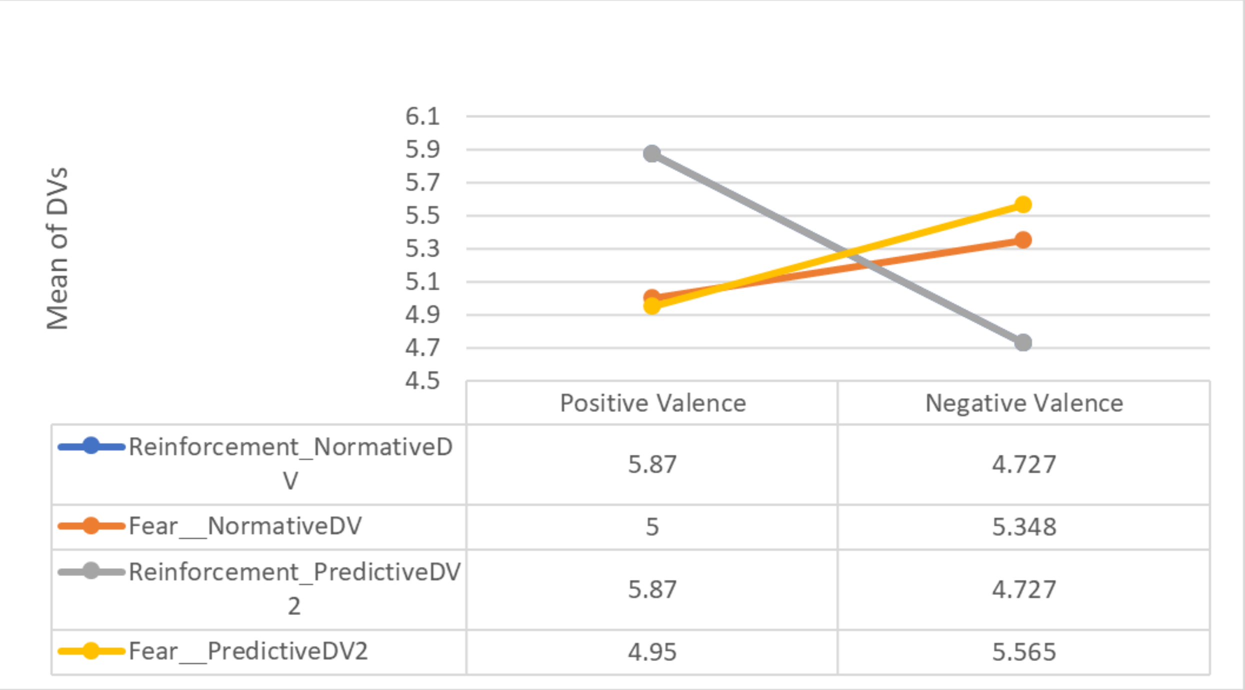
Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
Valence	Normative DV	3.460	1	3.460	1.171	.282
	Predictive DV	1.523	1	1.523	.468	.496
Nudge	Normative DV	.340	1	.340	.115	.735
	Predictive DV	.037	1	.037	.011	.916
Valence * Nudge	Normative DV	12.173	1	12.173	4.120	**.046**
	Predictive DV	16.933	1	16.933	5.199	**.025**

Table 7. Results of the MANOVA (2X2 factorial design)

The multivariate results indicate that the main effects of valence on both normative DV and predictive DV were not statistically significant. [F = 1.171, df = (1), p = 0.282 for the normative DV, and F = 0.468, df = (1), p = .496 for the predictive DV]. Thus, the positive and negative valence scenarios were not significantly different in their normative DV and predictive DV.

The main effects of the type of nudges on both normative DV and predictive DV were not statistically significant. [F = 0.115, df = (1), p = 0.735 for normative DV, and F = 0.011, df = (1), p = .916] for predictive DV. Thus, reinforcement nudge and fear nudge were not significantly different in their normative DV and predictive DV.

However, the interaction effect of types of nudges and scenario valence on the two DVs was statistically significant. F = 4.12, df = (1), p = 0.46 < 0.05 for normative DV, and F = 5.199, df = (1), p = .025 < 0.05 for predictive DV. Thus, the effect of the type of nudge on the dependent variables appears to be contingent on the valence of the nudge. To be more specific, with a positive scenario, the reinforcement nudge led to higher normative beliefs than the fear nudge; however, with the negative valence scenario, the fear nudge led to a higher normative DV than the reinforcement nudge. Similarly, in the positive scenario, the reinforcement nudge led to a higher predictive DV than the fear nudge; however, in the negative scenario, the fear nudge led to a higher predictive DV than the reinforcement nudge. Figure 1 compares the means of the two dependent variables in the 4 conditions.



	Positive Valence	Negative Valence
Reinforcement_NormativeDV	5.87	4.727
Fear__NormativeDV	5	5.348
Reinforcement_PredictiveDV2	5.87	4.727
Fear__PredictiveDV2	4.95	5.565

**Note: the lines of reinforcement for two DVs overlap*.

Figure 1. Means of Normative DV and Predictive DV in the 2 x 2 Factorial Design

DISCUSSION

We employed two "carrot and stick" extremes for two scenarios: one framing the user about the benefits of using 2FA (positive reinforcement) and the other reminding the user about the potential inconvenience of using 2FA.

In our data collection, we tested all six types of nudges, but statistical power suffered when we tested them simultaneously. Informal inspection revealed that their overall differences were not practically significant, and testing revealed that they were not statistically significantly different. We decided to limit our focus to two extreme nudges that were most closely related to the valence of the scenarios: one evoking the negative feeling of not using 2FA to protect the account (i.e., the "fear" nudge), and another facilitating quick action without triggering any negative emotions (i.e., the "reinforcement" nudge). The results revealed that when people are framed for the benefits of 2FA, the reinforcement nudge worked better than the fear nudge. When people were framed with the scenario focusing on the inconvenience of 2FA, the fear nudge worked better than the reinforcement nudge. In sum, the fear nudge was better at combating potential inconveniences in the beginning scenario, and the reinforcement nudge boosted the positive impact presented in the beginning scenario.

CONCLUSION

In this exploratory paper, we used Akrasia as a theoretical background to understand the gap between what people should do and what they are likely to do. At the same time, we explore methods to nudge 2FA deployment. The current study reveals a need for a more in-depth exploration of 2FA.

REFERENCES

Aagaard, J. 2015. "Drawn to Distraction: A Qualitative Study of Off-Task Use of Educational Technology," *Computers & Education* (87), pp. 90-97.

Aagaard, J. 2018. "Multitasking as Distraction: A Conceptual Analysis of Media Multitasking Research," *Theory & Psychology* (29:1), pp. 87-99.

Aagaard, J. 2019. "Digital Akrasia: A Qualitative Study of Phubbing," *Ai & Society* (35:1), pp. 237-244.

Aagaard, J. 2021. "Beyond the Rhetoric of Tech Addiction: Why We Should Be Discussing Tech Habits Instead (and How)," *Phenomenology and the Cognitive Sciences* (20:3), pp. 559-572.

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., and Sleeper, M. 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys (CSUR)* (50:3), pp. 1-41.

Akhawe, D., and Felt, A. P. 2013. "Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness," *USENIX Security Symposium* (13).

Aytes, K., and Connolly, T. 2004. "Computer Security and Risky Computing Practices: A Rational Choice Perspective," *Journal of Organizational and End User Computing (JOEUC)* (16:3), pp. 22-40.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837-864.

Brooks, C. 2022. "Alarming Cyber Statistics for Mid-Year 2022 That You Need to Know," Forbes, June 6. (https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=4dc33a507864, accessed July 1, 2022)

Bruns, H., Kantorowicz-Reznichenko, E., Klement, K., Luistro Jonsson, M., and Rahali, B. 2018. "Can Nudges Be Transparent and yet Effective?" *Journal of Economic Psychology* (65), pp. 41-59.

Bulgurcu, Cavusoglu, and Benbasat. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), p. 523.

Caraban, A., Karapanos, E., Gonçalves, D., and Campos, P. 2019. "23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction," in *Proceedings of the 2019 Chi Conference on Human Factors in Computing Systems*.

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., and 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. 1-11.

Das, S., Kramer, A. D., Dabbish, L. A., and Hong, J. I. 2014. "Increasing Security Sensitivity with Social Proof: A Large-Scale Experimental Confirmation," in *Proceedings of the 2014 Acm Sigsac Conference on Computer and Communications Security*.

Egelman, S., Cranor, L. F., and Hong, J. 2008. "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings," in *Proceedings of the Sigchi Conference on Human Factors in Computing Systems*. ACM, pp. 1065-1074.

Gatlan, Sergiu. 2022 "Google Sees 50% Security Boost for 150m Users after 2FA Enroll." *BleepingComputer*, BleepingComputer, Feb 8.

(https://www.bleepingcomputer.com/news/google/google-sees-50-percent-security-boost-for-150m-users-after-2fa-enroll/, accessed July 2, 2022)

Hansen, P. G., and Jespersen, A. M. 2013. "Nudge and the Manipulation of Choice: A Framework for the Responsible Use of the Nudge Approach to Behaviour Change in Public Policy," *European Journal of Risk Regulation* (4:1), pp. 3-28.

Hartwig, K., and Reuter, C. 2021. "Nudging Users Towards Better Security Decisions in Password Creation Using Whitebox-Based Multidimensional Visualisations," *Behaviour & Information Technology* (41:7), pp. 1357-1380.

Ho, S. Y., and Lim, K. H. 2018. "Nudging Moods to Induce Unplanned Purchases in Imperfect Mobile Personalization Contexts," *MIS Quarterly* (42:3), pp. 757-778.

Jenkins, J. L., Durcikova, A., and Nunamaker, J. F. 2021. "Mitigating the Security Intention-Behavior Gap: The Moderating Role of Required Effort on the Intention-Behavior Relationship," Association for Information Systems.

Jesse, M., and Jannach, D. 2021. "Digital Nudging with Recommender Systems: Survey and Future Directions," *Computers in Human Behavior Reports* (3:100052), p. 100052.

Johnson, E. J., Shu, S. B., Dellaert, B. G. C., Fox, C., Goldstein, D. G., Häubl, G., Larrick, R. P., Payne, J. W., Peters, E., Schkade, D., Wansink, B., and Weber, E. U. 2012. "Beyond Nudges: Tools of a Choice Architecture," *Marketing Letters* (23:2), pp. 487-504.

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113-134.

Kahneman, D., and Tversky, A. 2013. "Prospect Theory: An Analysis of Decision under Risk," in *Handbook of the Fundamentals of Financial Decision Making*. WORLD SCIENTIFIC, pp. 99-127.

Li, Abner. 2022. "Google Auto-Enabled 2SV for over 150m People Leading to 50% Decrease in Compromised Accounts." 9to5*Google*, 9to5Google, Feb 8. (https://9to5google.com/2022/02/08/google-account-2sv/, accessed Sep 5, 2022)

Maddux, J. E., and Rogers, R. W. 1983. "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change," *Journal of Experimental Social Psychology* (19:5), pp. 469-479.

Malkin, N., Mathur, A., Harbach, M., and Egelman, S. 2017. "Personalized Security Messaging: Nudges for Compliance with Browser Warnings," in: *Proceedings 2nd European Workshop on Usable Security*. Internet Society.

McCart, C. 2022. "15+ Two-Factor Authentication Statistics 2020-2022." *Comparitech*, Comparitech, July 19. (https://www.comparitech.com/studies/data-breaches-studies/two-factor-authentication-statistics/, accessed Aug 30, 2022)

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *J Psychol* (91:1), pp. 93-114.

Rogers, R. W. 1983. "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," in *Social Psychophysiology,* J. Cacioppo and Petty (eds.). New York: Guilford Press.

Romaioli, D., Faccio, E., and Salvini, A. 2008. "On Acting against One's Best Judgement: A Social Constructionist Interpretation for the Akrasia Problem," *Journal for the Theory of Social Behaviour* (38:2), pp. 179-192.

Selwyn, N., and Aagaard, J. 2020. "Banning Mobile Phones from Classrooms—an Opportunity to Advance Understandings of Technology Addiction, Distraction and Cyberbullying," *British Journal of Educational Technology* (52:1), pp. 8-19.

Sheeran, P. 2005. "Intention-Behavior Relations: A Conceptual and Empirical Review," in *European Review of Social Psychology*. Chichester, UK: John Wiley & Sons, Ltd, pp. 1-36.

Silic, M., Barlow, J., and Ormond, D. 2015. *Warning! A Comprehensive Model of the Effects of Digital Information Security Warning Messages*.

Story, P. 2021. *Design and Evaluation of Security and Privacy Nudges: From Protection Motivation Theory to Implementation Intentions*.

Sunstein, C. R. 2017. "Nudges That Fail," *Behavioural Public Policy* (1:1), pp. 4-25.

Tversky, A., and Kahneman, D. 1985. "The Framing of Decisions and the Psychology of Choice," in *Environmental Impact Assessment, Technology Assessment, and Risk Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 107-129.

van Bavel, R., Rodríguez-Priego, N., Vila, J., and Briggs, P. 2019. "Using Protection Motivation Theory in the Design of Nudges to Improve Online Security Behavior," *International Journal of Human-Computer Studies* (123), pp. 29-39.

Vance, A., Eargle, D., Ouimet, K., and Straub, D. 2013. "Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment," in: *2013 46th Hawaii International Conference on System Sciences*. IEEE, pp. 2988-2997.

Vishwanath, A. 2015. "Examining the Distinct Antecedents of E-Mail Habits and Its Influence on the Outcomes of a Phishing Attack," *Journal of Computer-Mediated Communication* (20:5), pp. 570-584.

Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., and Sadeh, N. 2014. "A Field Trial of Privacy Nudges for Facebook," in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, pp. 2367-2376.

Warberg, L., Acquisti, A., and Sicker, D. 2019. "Can Privacy Nudges Be Tailored to Individuals' Decision Making and Personality Traits?," in: *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society - WPES'19*. ACM Press, pp. 175-197.

Xu, F., and Warkentin, M. 2020. "Integrating Elaboration Likelihood Model and Herd Theory in Information Security Message Persuasiveness," *Computers & Security* (98:102009), p. 102009.

Zhang, B., and Xu, H. 2016. "Privacy Nudges for Mobile Applications," in: *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM Press, pp. 1676-1690.

Appendix

Appendix A – Scenarios & Nudges

Scenario 1: Positive Valence

Imagine that you have been using a web-based account for several years, both at home and work.

Two-Factor Authentication is a measure for added security, which requires an additional login credential when you log in to the account – beyond just the username and password – to gain account access. That second step of authentication often requires a one-time PIN number that arrives as a text message on your mobile phone.

In fact, a study demonstrates at least an 80% reduction in cyber attacks thanks to two-factor authentication.

One day, when you log in to the account, you see the following information pop up.

Scenario 2: Negative Valence

Imagine that you have been using a web-based account for several years, both at home and work. Also imagine that a month ago, your account was automatically enrolled in a measure for added security - Two-Factor Authentication.

Two-Factor Authentication requires an additional login credential – beyond just the username and password – to gain account access. That second step of authentication often requires a one-time PIN number that arrives as a text message on your mobile phone.

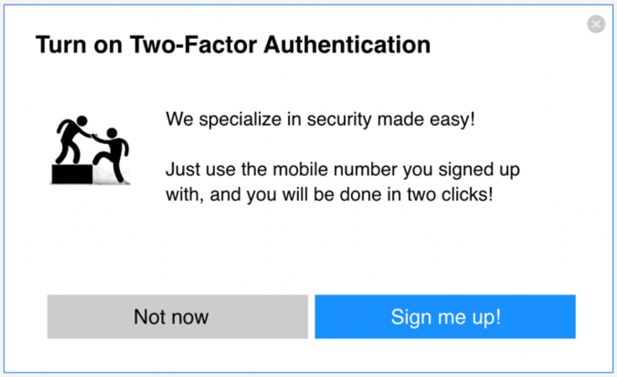
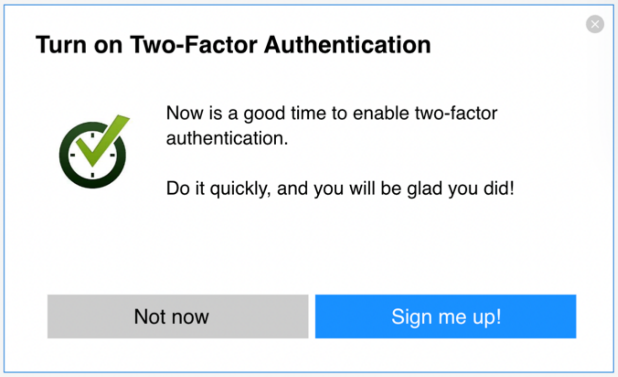
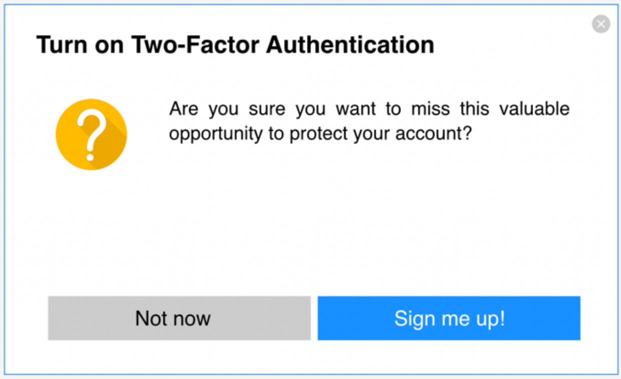
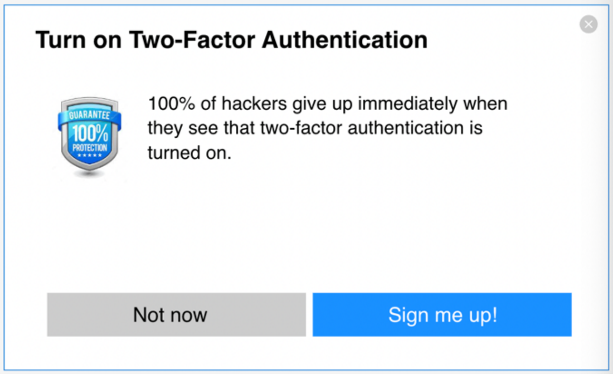
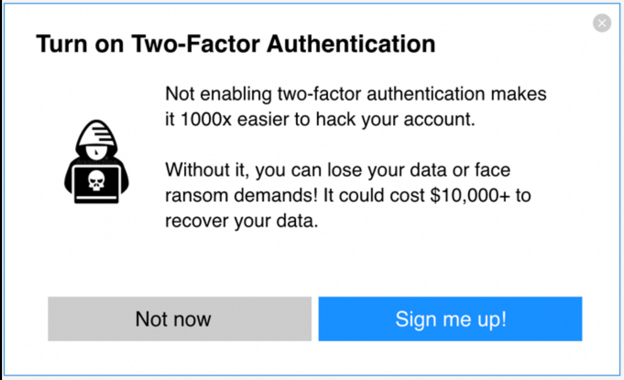
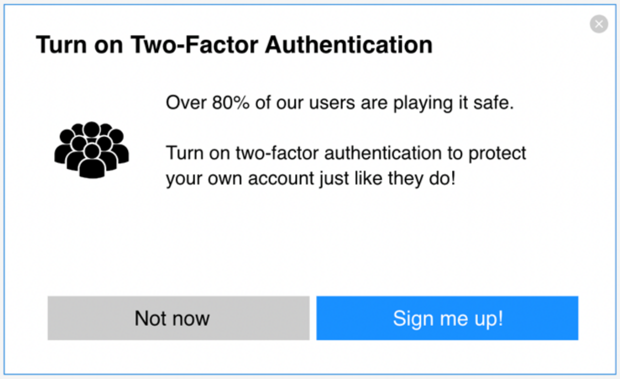
In fact, a study demonstrates at least an **80%** reduction in cyber attacks thanks to two-factor authentication.

However, you might have heard that Two-Factor Authentication could become a hassle because:

- It requires an additional login credential **EVERY TIME** when you log in.
- It causes problems when there is poor or inaccessible cell service, or when your mobile phone battery is dead.

You are considering turning off Two-Factor Authentication. Then you see the following information pop up.

Table A1: Nudges (Pop-up messages)

Facilitation Nudge	Reinforce nudge
 Turn on Two-Factor Authentication We specialize in security made easy! Just use the mobile number you signed up with, and you will be done in two clicks! 	 Turn on Two-Factor Authentication Now is a good time to enable two-factor authentication. Do it quickly, and you will be glad you did!
Confront Nudge	**Deception nudge**
 Turn on Two-Factor Authentication Are you sure you want to miss this valuable opportunity to protect your account? 	 Turn on Two-Factor Authentication 100% of hackers give up immediately when they see that two-factor authentication is turned on.
Fear Nudge	**Social Proof nudge**
 Turn on Two-Factor Authentication Not enabling two-factor authentication makes it 1000x easier to hack your account. Without it, you can lose your data or face ransom demands! It could cost $10,000+ to recover your data. 	 Turn on Two-Factor Authentication Over 80% of our users are playing it safe. Turn on two-factor authentication to protect your own account just like they do!

Appendix B – Instrument

Table B1: Constructs and Items

Construct	Item	Source
Self-efficacy	• I have the necessary knowledge to protect the informational assets. • I have the necessary skills for the organization's security. • I have confidence to achieve the security goals.	Yoo et al. (2020)
Self-control	• I often act on the spur of the moment without stopping to think. • I don't devote much thought and effort to preparing for the future. • I often do whatever brings me pleasure here and now, even at the cost of some distant goal. • I'm more concerned with what happens to me in the short run than in the long run. • I like to test myself every now and then by doing something a little risky. • Sometimes I will take a risk just for the fun of it. • I sometimes find it exciting to do things for which I might get in trouble. • Excitement and adventure are more important to me than security. • I try to look out for myself first, even if it means making things difficult for other people. • I have little sympathy for other people when they are having problems. • If things I do upset people, it's their problem not mine. • I will try to get the things I want even when I know it's causing problems for other people. • I frequently avoid projects that I know will be difficult. • When things get complicated, I tend to quit and withdraw. • The things in life that are easiest to do bring me the most pleasure. • I dislike really hard tasks that stretch my abilities to the limit. • I lose my temper pretty easily. • Often, when I am angry at people, I feel more like hurting them than talking to them about why I am angry. • When I am really angry, other people had better stay away from me. • When I have a serious disagreement with someone, it is usually hard for me to talk calmly about it without getting upset.	Hu et al. (2015)
Big five	I see myself as someone who … • Is outgoing, sociable. (Extraversion) • Is talkative. (Extraversion)	Johnston et al. (2016)

	• Has an assertive personality. (Extraversion) • Generates a lot of enthusiasm. (Extraversion) • Is full of energy. (Extraversion) • Is considerate and kind to almost everyone. (Agreeableness) • Likes to cooperate with others. (Agreeableness) • Is helpful and unselfish with others. (Agreeableness) • Has a forgiving nature. (Agreeableness) • Is generally trusting. (Agreeableness) • Does a thorough job. (Conscientiousness) • Does things efficiently. (Conscientiousness) • Makes plans and follows through with them. (Conscientiousness) • Is a reliable worker. (Conscientiousness) • Perseveres until the task is finished. (Conscientiousness) • Can be moody. (Neuroticism) • Is depressed, blue. (Neuroticism) • Gets nervous easily. (Neuroticism) • Can be tense. (Neuroticism) • Worries a lot. (Neuroticism) • Is inventive (Openness) • Is original, comes up with new ideas. (Openness) • Values artistic, esthetic experiences. (Openness) • Has an active imagination. (Openness) • Likes to reflect, play with ideas. (Openness) • Is sophisticated in art, music, or literature. (Openness) • Is ingenious, a deep thinker. (Openness) • Is curious about many different things. (Openness)	
Conformity	• I often rely on, and act upon, the advice of others. • I would be the last one to change my opinion in a heated argument on a controversial topic. • Generally, I'd rather give in and go along for the sake of peace than struggle to have my way. • I tend to follow family tradition in making political decisions. • Basically, my friends are the ones who decide what we do together. • A charismatic and eloquent speaker can easily influence and change my ideas. • I am more independent than conforming in my ways. • If someone is very persuasive, I tend to change my opinion and go along with them. • I don't give in to others easily. • I tend to rely on others to make an important decision quickly.	Mehrabian, A., & Stefl, C. A. (1995). Basic temperament components of loneliness, shyness, and conformity. Social Behavior and Personality: an international journal, 23(3), 253-263.

	• I prefer to make my own way in life rather than find a group I can follow.	
Marker Variable – Attitude towards the color blue	• Blue is a beautiful color • Blue is a lovely color • Blue is a pleasant color • The color blue is wonderful • Blue is a nice color • I think blue is a pretty color • I like the color blue	Miller, B. K., & Simmering, M. J. (2022). Attitude toward the color blue: An ideal marker variable. *Organizational Research Methods*, 10944281221075361.
MFA Experience	Do you have a work or personal account of some kind (for example, an intranet, a bank account, an email account, or an employee self-service website) that requires a two-factor authentication? • Yes • No • Not sure • Not applicable	

Note: All items were measured on a 7-point Likert scale unless otherwise noted.