Until you have something to lose! Loss aversion and two-factor authentication adoption

Ahmad R. Pratama
Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia, and
Firman M. Firmansyah
Technology and Society, Stony Brook University, Stony Brook, New York, USA

Received 18 December 2020
Revised 28 February 2021
Accepted 4 April 2021

Abstract

Purpose – In this study, the authors seek to understand factors that naturally influence users to adopt two-factor authentication (2FA) without even trying to intervene by investigating factors within individuals that may influence their decision to adopt 2FA by themselves.

Design/methodology/approach – A total of 1,852 individuals from all 34 provinces in Indonesia participated in this study by filling out online questionnaires. The authors discussed the results from statistical analysis further through the lens of the loss aversion theory.

Findings – The authors found that loss aversion, represented by higher income that translates to greater potential pain caused by losing things to be the most significant demographic factor behind 2FA adoption. On the contrary, those with a low-income background, even if they have some college degree, are more likely to skip 2FA despite their awareness of this technology. The authors also found that the older generation, particularly females, to be among the most vulnerable groups when it comes to authentication-based cyber threats as they are much less likely to adopt 2FA, or even to be aware of its existence in the first place.

Originality/value – Authentication is one of the most important topics in cybersecurity that is related to human-computer interaction. While 2FA increases the security level of authentication methods, it also requires extra efforts that can translate to some level of inconvenience on the user's end. By identifying the associated factors from the user's ends, a necessary intervention can be made so that more users are willing to jump on the 2FA adopters' train.

Keywords Two-factor authentication, Awareness, Adoption, Loss aversion, Demographics factors, Vulnerable groups

Paper type Research paper

1. Introduction

Authentication is one of the most important topics in computer security, especially the one that is focusing on human–computer interaction. In principle, authentication is a security measure to enforce confidentiality as it allows a device or a system to verify the identity of someone who tries to access some resources within a computer [1], an information system [2] or networks [3]. While the use of passwords as an authentication method has been around since the earliest days of computing, it is still the most common authentication method today

Both authors contributed equally. The authors would like to thank Galih Rahmadi, Muhammad Rifqi Ramadhani, Raja Rizky Riyandhika, Adam Hermawansyah and La Ode Abdul Wahid for their help with data collection.

Declaration of interest: The authors declare that they have neither conflict of interest nor external funding for this study.

Applied Computing and Informatics
Emerald Publishing Limited
e-ISSN: 2210-8327
p-ISSN: 2634-1964
DOI 10.1108/ACI-12-2020-0156

despite the fact that numerous security incidents related to the use of weak passwords [4, 5]. Many have tried to increase the security of password-based authentication method by enforcing users to use only strong passwords that are long and a mix of alphanumeric and special characters (i.e. lowercase letters, uppercase letters, numbers and symbols), but even that seemed to be not enough to prevent many password-related data breaches and other security incidents that have caused huge financial losses [6, 7]. It is partly due to the practice of reusing the same passwords by many [8, 9]. After all, no matter how strong a password is, it is still a single-factor authentication that relies only on "something you know".

A two-factor authentication (2FA), on the other hand, increases the security level of authentication methods by using a different approach. Instead of hardening the one factor (i.e. passwords) used in the authentication process, it adds another factor in the form of "something you have" that is usually a physical item (e.g. a security token, a bank card, a key or a smartphone) or "something you are" that makes use of user biometrics (e.g. fingerprints or irises) on top of the existing password-based authentication method. While adopting 2FA arguably increases security by far, it puts extra efforts that can translate to some level of inconvenience on the user's end, particularly on technical aspects like device remembrance, fragmented login services and authentication timeouts [10]. As such, the adoption rate of 2FA is not that great. For example, a study in 2015 shows that only 6.4% of Google accounts that were part of the data breach a year before had adopted 2FA [11]. Even when some tried to enforce the use of 2FA, it was not always received with open arms by the users [12–14]. Another fact that did not help the cause for 2FA adoption is that some users had a misconception that they would not need to adopt 2FA because of the existence of other security measures such as HTTPS despite the two work differently and are complementary instead of substitutes for each other [15]. Clearly, something needs to be done on this matter. Understanding factors that can help promote 2FA adoption from the user's end is a priority should we want to have more people on board. Some researchers have tried to come up with nonassertive approaches of intervention to help promote 2FA adoptions, either by developing stories [16], video tutorials [17] or even by giving out some incentives in the form of a digital item [18].

While the aforementioned studies tried to intervene users in adopting 2FA, this research aimed to step back and explore factors within individuals that may influence their decision to adopt 2FA by themselves. In other words, in this exploratory study, we try to understand factors that naturally influence users to adopt 2FA without even trying to intervene. Our main research question in this paper is: *What internal factors predict 2FA adoption among Internet users?* We are particularly interested in investigating the roles of demographic factors, especially income and educational attainment on 2FA adoption. In doing so, we use the notion of loss aversion [19, 20] as the point of departure. By identifying the associated factors from the user's ends, further research can pick it up to investigate and propose some necessary, more appropriate and cost-effective interventions that can help persuade more users to jump on the train of the 2FA adopters.

2. Literature review

2.1 Loss aversion and cybersecurity behaviors

Loss aversion refers to the condition in which individuals prefer to avoid losses than to acquire the equivalent gains [20]. It is the case due to the disutility curve of losing something is steeper than the utility curve of acquiring it [19] that makes losses loom larger than gains, the pains of losing something more intense than the pleasure of gaining it [21, 22]. Interestingly, this notion also holds true for circumstances where losses are just mere frames. In this respect, there is no actual difference in the expected outcomes, however, individuals still irrationally prefer the situations in which losses can seemingly be avoided. For instance,

in a thought experiment of choosing a program to end a deadly pandemic [23], the majority of participants favored the one that can save 200 out of 600 lives for sure (option 1), over the alternative that has $^{1}/_{3}$ probability to save all and $^{2}/_{3}$ probability not to save all (option 2). Yet, when the choices were framed in the opposite way, the majority favored the one having $^{1}/_{3}$ probability to cause no deaths and $^{2}/_{3}$ probability to cause 600 deaths (option 3), over the alternative that causes 400 deaths for sure (option 4). In the latter case, the participants were willing to take the risk since there was still a hope, though having only a little chance, not to lose lives at all.

On the bright side, loss aversion motivates individuals to engage in behaviors that prevent such losses and thus can be used as a nudge [24]. For example, when good grades were given in the beginning instead of at the end of the semester, students studied harder and performed better to keep their good grades from any deductions should they make errors throughout the semester [25]. In the online context, loss aversion can be utilized to encourage users to be more sensitive to cyberthreats and implement more cybersecurity measures. For instance, in a lab experiment of potential cyberattacks in online shopping, users exhibited more secure behaviors such as using a secure connection, generating a strong password, limiting shared personal information, choosing trusted vendor and logging out after session, when they were notified with a loss-framed message, "*you could lose part of your final endowment*", than with gain-framed messages, "*you could win [the] maximum final endowment*", a priori [26, p. 4]. Indeed, this loss-frame type of message may affect different users in different contexts differently. In online games, it worked effectively in influencing users to change their password should they be future oriented, wanting to keep playing the game in the future, rather than past oriented, embracing memories of playing the game in the past [27].

Considering that loss aversion drives people to play safe, this notion arguably has a stronger effect on those who possess a higher value of endowment than those who do not even have one in the first place. This argument is especially relevant to illuminate the potential roles of income in the 2FA adoption. With income used as a proxy to measure utility of one's endowment [28–30] and the adoption set to be the point of reference, choosing to implement 2FA will protect users against or at least lower the probability of being targets of cybercrimes that can cost them their endowment as past studies highlight [see 6, 7]. This decision however will not give the users further direct incentives other than feeling safer. Choosing not to implement 2FA on the other hand, will increase the probability of being subjects of such crimes while also delivering the same aforementioned incentive. This set of choices then leaves the values of potential losses as the discriminant. In this respect, the higher the income, the more utility the users would give up, the more painful they would feel should such incidents happen. On the contrary, the lower the income, the less utility the users would give up, the less painful they would feel should the same incidents happen. Thus, users would be more likely to adopt 2FA should they have higher income and less likely to adopt it should they have lower income.

2.2 Education levels and cybersecurity behaviors

Having a college degree does help one make substantial gains in critical thinking [31]. It might translate well to users' willingness to accept a slight inconvenience of adopting 2FA in exchange for the peace of mind from getting a better security on their accounts. This argument is in line with the fact that users with higher levels of education tend to be more aware with cyberthreats and cybersecurity than users with lower levels of education [32, 33]. Indeed, attending college does increase the probability to get exposure to cybersecurity-related training and its cutting-edge technology including 2FA [12–14]. On the other hand, many studies have pointed out that higher education is one significant factor behind social inequalities and social mobility, both of which are highly related to income [34–37]. Taking

these findings into account, we expected that higher education would be associated with a higher 2FA adoption rate and that this association would interact with income.

2.3 Gender and generational gap in cybersecurity behaviors

Past research has revealed that females are less likely than males to implement stronger cybersecurity measures [38]. For instance, in an Australian university, female students tended to use alphabetic or numeric characters only for their email password, which is considerably weaker, while male students tended to use the combination of alphanumeric and symbols, which is considerably stronger [39]. In various organizations and companies in the United States, female employees reported more behaviors that are prone to security threats and cybercrimes such as not using different passwords for different social media accounts, opening email attachments from strangers, sending sensitive personal information via email and clicking unfamiliar short URLs posted on social media sites [40]. This discrepancy is in line with the fact that women are underrepresented in both science, technology, engineering and math (STEM) majors and workforce including cybersecurity [41]. On the other hand, past research has also revealed a generational gap in cybersecurity behaviors. In this respect, elderly people tend to be less knowledgeable with cybersecurity measures and less familiar with possible crimes associated with cyberthreats [32, 33]. In light of those findings in the literature, we expected females and elderly people to be less likely to adopt 2FA. Thus, controlling for both gender and age variables is important in examining how sensitive income and education are in predicting 2FA adoption.

3. Method

3.1 Participants

An online survey was conducted in 2020 as part of a larger study about cybersecurity awareness and behavior in Indonesia. A total of 1910 participants, coming from all 34 provinces of Indonesia and recruited through social media (e.g. WhatsApp, Instagram, Facebook, Twitter), gave their consents and filled out the questionnaire in the study. As this study was aimed at the general public, all Indonesians aged 13 years and older were eligible to participate in this study. The questionnaire was delivered in Indonesian language using Google Forms. We excluded some individuals due to duplicates, incompleteness or missing values within their responses and the final dataset consists of 1852 participants. Table 1 shows a summary of demographic information of participants in the study.

3.2 Measure

3.2.1 2FA adoption. To measure the 2FA adoption, participants were asked whether they use 2FA or not, with three options of answer: "I have no idea what 2FA is", "No" and "Yes". We then categorized participants into three mutually exclusive groups based on their response: (1) not aware of 2FA (I have no idea what 2FA is); (2) skipping 2FA (No) and (3) adopting 2FA (Yes). The reason behind this categorization is that 2FA is not activated by default. Thus, it is highly improbable for someone to adopt 2FA without knowing of its existence in the first place. We did not ask participants to specify further on which applications they implement 2FA if they use one. In other words, it could be anything from their email or social media to banking or other financial services.

3.2.2 Income. We asked participants about their monthly income and categorized them into low-, middle- and high-income categories based on their responses. We used the annual nontaxable income in Indonesia, rounded to the closest million IDR, as the cutoff. Income is used as a proxy to measure potential financial losses that may elicit loss-averse behavior.

Variable	Frequency	%
Gender		
Male	706	38.1
Female	1146	61.9
Age		
13–19 years	293	15.8
20–29 years	1367	73.8
30–49 years	164	8.9
≥ 50 years	28	1.5
Education		
No college degree	1102	59.5
Some college degree	750	40.5
Income		
Low income (less than IDR 1 mil)	716	38.7
Middle income (less than IDR 5 mil)	901	48.6
High income (IDR 5 mil or higher)	235	12.7
Location (Island)		
Sumatra	235	12.7
Java	1128	60.9
Borneo	65	3.5
Sulawesi	260	14.0
Bali and Nusa Tenggara	131	7.1
Papua and the Moluccas	33	1.8

Table 1. Demographic information of all participants (n = 1852)

Higher monthly income means greater values of potential disutility that will be given up should such cyber incidents happen.

3.2.3 Other demographic factors. We asked participants about their educational attainment, to which we categorized them into two groups: those without a college degree and those with some college degree. Higher education is used as a cutoff due to the reasons discussed in the literature review. We also asked participants to indicate their gender and age.

3.3 Data analyses

To explore the extent to which the 2FA adoption rates vary across different demographic factors, we conducted a series of bivariate analyses with chi-square tests. We then used a multinomial logistic regression model to check if the differences as indicated in the descriptive statistics and the bivariate analyses are also statistically significant in a multivariate way. In doing so, we used no awareness of 2FA as the base. Such significant findings thereby should be interpreted as the likelihood of respected factors in predicting being aware of but not adopting 2FA vis a vis with being aware of and adopting 2FA. As explained earlier, we planned to examine the interaction between income and education. All statistical analyses were performed in STATA 15.1.

As a form of sensitivity analysis, we also conducted a two-step logistic regression with the same model to the dataset. In the first step, we used all samples (n = 1,852) to predict user awareness of 2FA. In the second step, we exclude all individuals with no awareness of 2FA to predict user adoption of 2FA among those who are aware of its existence (n = 1,039) using the same model. Furthermore, to check for any problem with the sample bias in our dataset, we also repeated all analyses above with a smaller sample size (n = 429) where we randomly omitted some individuals from the overrepresented groups (i.e. females and young people

aged between 20 and 29 years) in the dataset to give a more balanced distribution that resembles the overall Indonesian population better [42]. The datasets and the STATA code are available as open access supplementary materials in our GitHub repository (https://github.com/ahmadrafie/2fastudy).

4. Results

As shown in Table 2, more participants were aware of the existence of 2FA (66.1%) than those who were not (43.9%). Meanwhile, only two third of those who were aware of its existence decided to adopt it.

As indicated in Table 3, the results show that males had a higher rate of adoption of 2FA compared to females ($\chi^2(1, n = 1{,}852) = 93.66, p < 0.001$), while a higher proportion of females were unaware of 2FA ($\chi^2(1, n = 1{,}852) = 76.84, p < 0.001$). In terms of age, participants in their 30s or 40s had higher rates of 2FA adoption compared to other age groups ($\chi^2(3, n = 1{,}852) = 13.99, p = 0.003$). Whereas most of the older participants in their 50s or 60s were not aware of 2FA ($\chi^2(3, n = 1{,}852) = 10.05, p = 0.018$). There was a higher frequency of participants without a college degree among those who were unaware of 2FA ($\chi^2(1, n = 1{,}852) = 4.50, p = 0.034$) whereas no significant difference was found in educational attainment among those who were adopting 2FA ($\chi^2(1, n = 1{,}852) = 2.86, p > 0.05$). In terms of income, the low-income group had the lowest rates of 2FA awareness ($\chi^2(2, n = 1{,}852) = 19.36, p < 0.001$) while the opposite is true for the high-income group who had the highest rate of 2FA adoption ($\chi^2(2, n = 1{,}852) = 48.35, p < 0.001$).

Table 2. Awareness and adoption of 2FA among all participants

Experience with 2FA	Frequency	%
Not aware of 2FA	813	43.9
Skipping 2FA	397	21.4
Adopting 2FA	642	34.7

Table 3. 2FA awareness and adoption rates in groups of participants

Variable	Not aware of 2FA		Skipping 2FA		Adopting 2FA	
	n	%	*n*	%	*n*	%
Gender						
Male ($n = 706$)	219	31.0	146	20.7	341	48.3
Female ($n = 1146$)	594	51.8	251	21.9	301	26.3
Age						
19 years ($n = 293$)	136	46.4	71	24.2	86	29.4
20–29 years ($n = 1367$)	585	42.8	296	21.7	486	35.6
30–49 years ($n = 164$)	72	43.9	25	15.2	67	40.9
≥50 years ($n = 28$)	20	71.4	5	17.9	3	10.7
Education						
No college degree ($n = 1102$)	506	45.9	231	21.0	365	33.1
Some college degree ($n = 750$)	307	40.9	166	22.1	277	36.9
Income						
Low income (less than IDR 1 mil, $n = 716$)	343	47.9	177	24.7	196	27.4
Middle income (IDR 1–4.99 mil, $n = 901$)	396	44.0	181	20.1	324	36.0
High income (IDR 5 mil or higher, $n = 235$)	74	31.5	39	16.6	122	51.9

Figure 1 presents the 2FA adoption rates viewed through the intersection of income and education level. Compared to their peers of the same category, the majority of low-income participants with no college degree were not aware of 2FA. In contrast, the majority of high-income participants with college degrees were already adopting 2FA. The rates of 2FA awareness and adoption exhibited an upward trend with increasing levels of income. An early indication that loss aversion is at play in the 2FA adoption.

Table 4 presents the multinomial logistic regression, which shows that high income significantly predicts awareness and adoption of 2FA. Also, it interacts with education. Users with no college degree but have a high-income background tend to be aware of and adopt 2FA. In contrast, users with some college degree but have a low-income background tend to skip 2FA despite being aware of it. These significant findings still hold true even after excluding the control variables (i.e. gender and age) from the model (Table 5 in the supplementary materials). The latter of which shows that being female and older is significantly associated with no awareness of 2FA let alone adopting it. The subsequent sensitivity analyses presented in the supplementary materials, both with the two-step simple

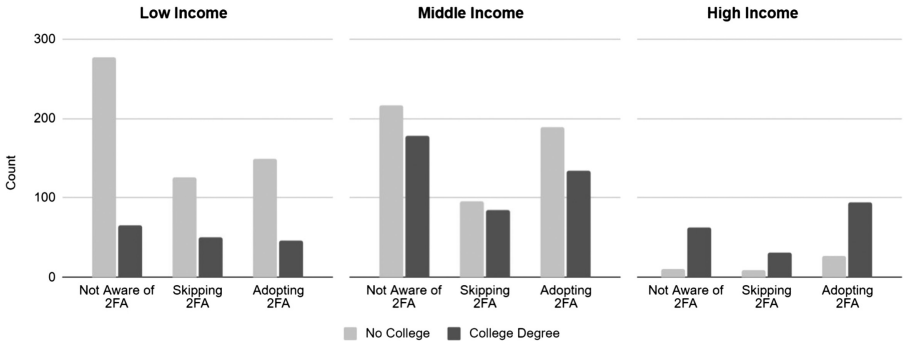

Figure 1.
The 2FA adoption rates based on income and education levels

Variable	Skipping 2FA RR	Skipping 2FA SE	Adopting 2FA RR	Adopting 2FA SE
Gender				
Female	*0.599***	*0.080*	*0.322***	*0.037*
Age	*0.961***	*0.013*	*0.946***	*0.011*
Education and income	1.009	0.165	*1.717***	*0.251*
No college degree, middle income				
No college degree, high income	1.990	0.938	*4.744***	*1.853*
Some college degree, low income	*2.029***	*0.449*	*1.728**	*0.390*
Some college degree, middle income	1.342	0.254	*1.914***	*0.330*
Some college degree, high income	1.532	0.439	*4.317***	*1.019*
Constant	1.484	0.429	3.417***	0.940
Model χ^2		177.84***		
McFadden's Pseudo R^2		0.045		
Count R^2		0.511		
Df		14		
Observation		1,852		

Note(s): Numbers reported are the risk ratio (RR) with the standard errors (SE)
*$p < 0.05$. **$p < 0.01$ ***$p < 0.001$; Reference category: no awareness of 2FA

Table 4.
Multinomial logistic regression estimates of 2FA adoption

logistic regression analysis (Table 6 in the supplementary materials) and with a smaller yet more balanced sample size (Table 7 and Table 8 in the supplementary materials) showed that the results from multinomial logistic regression are robust. The interaction terms between education and income (Figure 2), do play an important role in 2FA adoption.

5. Discussion

Our findings indicate that not only does income play an important role in 2FA adoption with some interactions with education but also that income plays the most important role in the model. Those with a high-income background, with or without a college degree, have the highest probability of adopting 2FA. This finding is consistent with the notion of loss aversion, that motivates individuals to exhibit behaviors to prevent such losses [25] including in the cybersecurity context [26, 27]. In this respect, the higher the income, the more likely people will adopt 2FA despite all the inconvenience that comes with it. People with a high-income background will, thus, suffer the most should security incidents that cause financial loss happen. Meanwhile, users with a low-income background, despite having a college degree, tend to skip 2FA since the expected pain associated with such losses is not as painful as that of those with a higher income. In a more extreme case, some people may not even feel the pain at all considering they have nothing to lose in the first place. Instead, this group of people may perceive 2FA as an extra burden on top of the existing single-factor authentication that usually requires them to memorize passwords. As such, the inconvenience of activating 2FA is much greater than the benefit they can perceive. Thus, it does make sense if these users decide to skip 2FA as they do not see any urgency of adopting it even if they are aware of its existence.

In this study, we control for both gender and age as the past research highlighted their roles in explaining the variations in cybersecurity behaviors [32, 38, 40]. This reveals that our model is robust with respect to the aforementioned factors, and it also helps us identify which demographic groups are the most prone to cyberthreats, especially the authentication-based ones. In this regard, the risk ratios for females showed that they are much more likely to have no awareness of 2FA than males. This finding may be the manifestation of, as past studies assert [41], the low representation of women in STEM majors. Thus, even though they are attending college, women still have lesser opportunity to get exposed to information about 2FA let alone adopting it. Unfortunately, we did not have enough data such as college majors to provide further evidence for this idea.

In terms of age, the results indicate that people are somewhat less likely to have no awareness of 2FA as they get older. Perhaps, it is because they are more likely to have a higher income than the teenagers or full-time students that made up a big chunk of

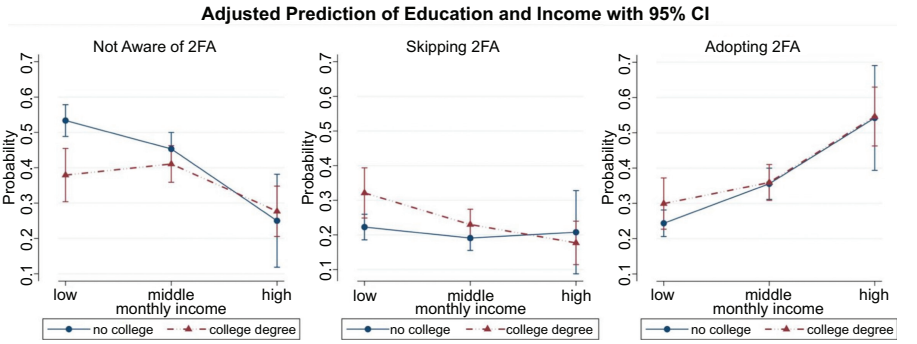

Figure 2.
Probability of having no awareness of 2FA (left), skipping 2FA (center) and adopting 2FA (right) based on the interaction terms between education and income

participants in this study. This idea is in line with the finding that income is the most important variable in the model in predicting 2FA adoption. However, among those who are aware of its existence, people are also less likely to adopt 2FA as they get older. As in the past study, it could be attributed to the existing cybersecurity knowledge divide between the older generations, especially those in their 50s or beyond, and younger generations [33].

6. Conclusion

This study has shown that loss aversion, represented by income as the endowment, is indeed an influential factor behind 2FA adoption. Regardless of their gender, age and education level, those with a high-income background are more likely to be adopting 2FA, whereas those with a low-income background, even if they have a college degree, are more likely to be skipping 2FA despite being aware of its existence. We have also revealed that the older generation tend to be the most vulnerable demographic group from authentication-based cyber threats as they are among the least likely to be aware of the existence of 2FA let alone adopting it to protect their digital accounts. This issue is particularly of greater concern for females compared to males.

6.1 Theoretical and practical implications

The fact that this study used no intervention in examining the 2FA adoption brought with it some important implications for practice. Perhaps developers, employers or other institutions may not need to give neither bigger incentives nor stricter enforcement like past studies documented to promote 2FA adoption [12–14, 18]. As such, it is more likely to happen organically once the users have something to lose and that something's value is higher than the inconvenience associated with adopting 2FA. What needs to be done is remind the users of the value that they will have to give up should such incidents happen as a result of skipping 2FA. In this study, we use income as the proxy to measure the endowment. In other contexts, it may be other things that they value as much as income such as very private/personal information. Moreover, should intervention be utilized, we suggest emphasizing on potential losses of valuable endowments that users may experience by skipping 2FA. Indeed, making 2FA adoption look easy is important [16, 17] and yet, as we found in this study, even those who are more educated and are aware of 2FA existence will still be less likely to activate it until they have something to lose in the first place.

6.2 Limitations and future work

With respect to sample size and sampling method, we argue that the results are considerably adequate for generalization, particularly in the Indonesian context. However, there are some limitations that should be recognized prior to doing so. First, we did not ask participants to specify further which applications that they implement 2FA on. It could be the case that some activate 2FA for more sensitive and risky applications such as internet banking and other financial services, but not for any other applications they deem less sensitive and riskless. We suggest that future studies measure this variability and examine if the effect of loss aversion holds true for all types of applications.

Second, this study is observational by nature. Thereby, even though the results are promising, any causal inference should be proceeded with caution. We also suggest that future studies incorporate college majors or academic disciplines to investigate if the gender gap in 2FA adoption or any other cybersecurity awareness issue is indeed due to low representation of women in STEM majors. As such, we highly recommend that future researchers replicate this study in other countries and examine other endowments. For

example, it would be interesting to examine the difference between given and acquired endowments.

Finally, this study did not consider any nondemographic factors in predicting 2FA adoption. Future research might integrate the findings from this study with some relevant latent independent variables from the literature. For example, protection motivation [43], threat avoidance [44], risk-based decision-making [45] or risky cyber behavior [46] among others. Doing so will arguably help provide a better understanding of why people do or do not adopt 2FA to protect themselves from any authentication-based cybersecurity threats.

References

1. Wood HM. The use of passwords for controlling access to remote computer systems and services. In: AFIPS '77: Proceedings of the June 13-16, 1977, National Computer Conference. ACM; 1977. 27-34.
2. Ahituv N, Lapid Y, Neumann S. Verifying the authentication of an information system user. Comput Secur. 1987; 6(2): 152-7. doi: 10.1016/0167-4048(87)90086-1.
3. Das AK, Sharma P, Chatterjee S, Sing JK. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. J Netw Comput Appl. 2012; 35(5): 1646-56. doi: 10.1016/j.jnca.2012.03.011.
4. Curry M, Marshall B, Correia J, Crossler RE. Infosec process action model (IPAM): targeting insiders' weak password behavior. J Inf Syst. 2019; 33(3): 201-25.
5. Preibusch S, Bonneau J. The password game: negative externalities from weak password practices. In: Alpcan T, Buttyan L, Baras J (Eds). GameSec: International Conference on Decision and Game Theory for Security. Berlin, Germany: Springer; 2010; 6442. 192-207. (Lecture Notes in Computer Science).
6. Riek M, Böhme R. The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. J Cybersecurity. 2018; 4(1): 1-16.
7. Romanosky S. Examining the costs and causes of cyber incidents. J Cybersecurity. 2016; 2(2): 121-35.
8. Han W, Li Z, Ni M, Gu G, Xu W. Shadow attacks based on password reuses: a quantitative empirical analysis. IEEE Trans Dependable Secure Computing. 2018; 15(2): 309-20.
9. Poornachandran P, Nithun M, Pal S, Ashok A, Ajayan A. Password reuse behavior: how massive online data breaches impacts personal data in web. In: Saini HS, Sayal R, Rawat SS (Eds). Proceedings of the third ICICSE, 2015. Hyderabad, Singapore: Springer; 2016. 413. 199-10. (Advances in Intelligent Systems and Computing).
10. Reynolds J, Samarin N, Barnes J, Judd T, Mason J, Bailey M, *et al.* Empirical measurement of systemic 2FA usability. In: Proceedings of the 29th USENIX security symposium. 2020. 127-43.
11. Petsas T, Tsirantonakis G, Athanasopoulos E, Ioannidis S. Two-factor authentication: is the world ready?. In: EuroSec '15: Proceedings of the eighth European workshop on system security. Bordeaux, France: ACM; 2015. 1-7.
12. Abbott J, Patil S. How mandatory second factor affects the authentication user experience. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Honolulu, HI, USA: ACM; 2020. 1-13. doi: 10.1145/3313831.3376457.
13. Colnago J, Devlin S, Oates M, Swoopes C, Bauer L, Cranor L, *et al.* '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. Montréal, QC, Canada: ACM; 2018. 1-11.
14. Dutson J, Allen D, Eggett D, Seamons K. Don't punish all of us: measuring user attitudes about two-factor authentication. In: 2019 IEEE European symposium on security and privacy workshops (EuroS&PW). Stockholm, Sweden: IEEE; 2019. 119-28.

15. Krombholz K, Busse K, Pfeffer K, Smith M, Von Zezschwitz E. 'If HTTPS were secure, I wouldn't need 2FA' - end user and administrator mental models of HTTPS. In: 2019 IEEE Symposium on security and privacy (SP). San Francisco, CA: IEEE; 2019. 246-63.
16. Fennell C, Wash R. Do stories help people adopt two-factor authentication?. In: 15th symposium on usable privacy and security (SOUPS 2019). Santa Clara, CA; 2019.
17. Albayram Y, Khan MMH, Fagan M. A study on designing video tutorials for promoting security features: a case study in the context of two-factor authentication (2FA). Int J Hum Comput Interact. 2017; 33(11): 927-42.
18. Busse K, Amft S, Hecker D, Von Zezschwitz E. 'Get a free item pack with every activation!' Do incentives increase the adoption rates of two-factor authentication?. I-Com. 2020; 18(3): 217-36.
19. Kahneman D, Tversky A. Prospect theory: an analysis of decision under risk. Econometrica. 1979; 47(2): 263-92. Available from: https://www.jstor.org/stable/1914185.
20. Kahneman D, Tversky A. Choices, values, and frames. Am Psychol. 1984; 39(4): 341-50.
21. Tversky A, Kahneman D. Advances in prospect theory: cumulative representation of uncertainty. J Risk Uncertain. 1992; 5: 297-323.
22. Ariely D, Huber J, Wertenbroch K. When do losses loom larger than gains?. J Mark Res. 2005; 42: 134-8.
23. Tversky A, Kahneman D. The framing of decisions and the psychology of choice. Science. 1981; 211: 453-8.
24. Baumeister RF, Bratslavsky E, Finkenauer C, Vohs KD. Bad is stronger than good. Rev Gen Psychol. 2001; 5(4): 323-70.
25. Smith BO, Shrader R, White DR, Wooten J, Dogbey J, Nath S, *et al.* Improving student performance through loss aversion. Scholarsh Teach Learn Psychol. 2019; 5(4): 278-88.
26. Rodríguez-priego N, Van Bavel R, Vila J, Briggs P. Framing effects on online security behavior. Front Psychol. 2020; 11(October): 1-11.
27. Seo BG, Park DH. The effect of message framing on security behavior in online services: focusing on the shift of time orientation via psychological ownership. Comput Human Behav. 2019; 93(January): 357-69. doi: 10.1016/j.chb.2018.12.035.
28. Boyce CJ, Wood AM, Banks J, Clark AE, Brown GDA. Money, well-being, and loss aversion: does an income loss have a greater effect on well-being than an equivalent income gain?. Psychol Sci. 2013; 24(12): 2557-62.
29. Pammi VSC, Ruiz S, Lee S, Noussair CN, Sitaram R. The effect of wealth shocks on loss aversion: behavior and neural correlates. Front Neurosci. 2017; 11(APR): 1-10.
30. Vendrik MCM, Woltjer GB. Happiness and loss aversion: is utility concave or convex in relative income?. J Public Econ. 2007; 91(7-8): 1423-48. doi: 10.1016/j.jpubeco.2007.02.008.
31. Huber CR, Kuncel NR. Does college teach critical thinking? A meta-analysis. Rev Educ Res. 2016; 86(2): 431-68.
32. Fatokun FB, Hamid S, Norman A, Fatokun JO. The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. J Phys Conf Ser. 2019; 1339(1): 0-13.
33. Grimes GA, Hough MG, Mazur E, Signorella ML. Older adults' knowledge of internet hazards. Educ Gerontol. 2010; 36(3): 173-92.
34. DeAngelo L, Franke R. Social mobility and reproduction for whom? College readiness and first-year retention. Am Educ Res J. 2016; 53(6): 1588-625.
35. Haveman R, Smeeding T. The role of higher education in social mobility. Futur Child. 2006; 16(2): 125-50.

36. Torche F. Is a college degree still the great equalizer? Intergenerational mobility across levels of schooling in the United States. Am J Sociol. 2011; 117(3): 763-807.

37. Triventi M. The role of higher education stratification in the reproduction of social inequality in the labor market. Res Soc Stratif Mobil. 2013; 32(1): 45-63. doi: 10.1016/j.rssm.2013.01.003.

38. Gratian M, Bandi S, Cukier M, Dykstra J, Ginther A. Correlating human traits and cyber security behavior intentions. Comput Secur. 2018; 73: 345-58. doi: 10.1016/j.cose.2017.11.015.

39. Bryant K, Campbell J. User behaviours associated with password security and management. Australas J Inf Syst. 2006; 14(1): 81-100.

40. Anwar M, He W, Ash I, Yuan X, Li L, Xu L. Gender difference and employees' cybersecurity behaviors. Comput Human Behav. 2017; 69: 437-43.

41. Mountrouidou X, Vosen D, Kari C, Azhar MQ, Bhatia S, Gagne G, *et al.* Securing the human: a review of literature on broadening diversity in cybersecurity education. In: ITiCSE-WGR '19: proceedings of the working group reports on innovation and technology in computer science education. Aberdeen, Scotland: ACM; 2019. 157-76.

42. Badan Pusat Statistik. Hasil sensus penduduk 2020. Sensus Penduduk 2020. 2020. Available from: https://www.bps.go.id/website/materi_ind/materiBrsInd-20210121151046.pdf.

43. Rogers RW. A protection motivation theory of fear appeals and attitude change1. J Psychol. 1975; 91(1): 93-114.

44. Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J Assoc Inf Syst. 2009; 11(7): 394-413.

45. Kahneman D. Thinking, fast and slow. Farrar, Straus and Giroux; 2011.

46. Hadlington L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon. 2017; 3(7): e00346. doi: 10.1016/j.heliyon.2017.e00346.

Supplementary material
Supplementary materials are available online at: https://github.com/ahmadrafie/2fastudy

Corresponding author
Ahmad R. Pratama can be contacted at: ahmad.rafie@uii.ac.id