Proceedings of the Human Factors and Ergonomics Society Annual Meeting
2024, Vol. 68(1) 1374–1379

DOI: 10.1177/10711813241261680
journals.sagepub.com/home/pro
Sage

Context Contributes to Two-Factor Authentication Choices

Fabrizio Chavez[1], Alejandra Fernandez-Reyes[1], and Michael D. Byrne[1]

Abstract

Two-factor authentication (2FA) is a security method for various types of accounts that adds an extra layer of verification. This second layer of verification improves the security of user accounts beyond the regular password. Despite its benefits, the adoption of 2FA has remained low amongst users. A consistent finding in the 2FA literature is that adoption has remained low because users prioritize usability over security benefits when choosing a 2FA method. However, this body of research overlooks the influence of perceived account importance on decisions to adopt 2FA. This study bridges this gap in the literature by offering evidence that, contrary to the current belief in the literature that 2FA adoption is based on perceptions of usability, account context also plays a role in users' choices. This highlights the importance of incorporating users' account importance perceptions in future research that aims to understand users' perceptions of 2FA and in the design of 2FA set-up pages. Furthermore, users' perceptions of 2FA were captured and compared to previous studies that used a similar sample pool (students who are forced to use DUO, a 2FA service). The results show inconsistent findings across studies and reveal that users have a common mental model of 2FA, regardless of the method used. This suggests interfaces can be redesigned to better match user perceptions with the actual needs of various contexts.

Keywords

cybersecurity, two-factor authentication, account context, multilevel, modeling

Background

Accounts, such as those used in personal or work settings, are constantly at a high risk of being compromised. This is due to both external attacks and users' lack of sophisticated or diverse passwords. To create additional security for these accounts, users can use two-factor authentication (2FA). 2FA allows for supplementary verification that can lead to increased protection and reduced risk of harm to accounts. Some 2FA methods include push notifications, short message service (SMS), and one-time passcodes. Although it enhances security, many users continue to choose to opt out of using 2FA. The current literature shows that when people choose a 2FA method they consider usability over security (Colnago et al., 2018).

In our current study, we aimed to determine whether the perceived importance of an account, according to the user, influences their choice of 2FA method. Additionally, users' perceptions of 2FA methods were collected and compared to previous studies that surveyed the same population (university students who had been forced to adopt 2FA). This served as a way to measure if users have adopted erroneous mental models of 2FA and if this varies across sub-populations.

Previous studies have focused on examining users' perceptions and practices regarding 2FA. A study conducted by Marky et al. (2022) found that in terms of online banking services, users who used two-factor authentication on a weekly basis for more than two years preferred to use 2FA versus less experienced participants who preferred to not use it at all. Experienced participants also preferred 2FA methods that they found to be more secure even if they were harder to use. Results showed that participants find security to be an important factor of 2FA but may have misconceptions about the actual security level of some 2FA methods. This impacts the 2FA method that users select for accounts that they prioritize security for (Marky et al., 2022).

Another study focused on how an account's perceived vulnerability to threats and the level of those threats affects their use of 2FA and their belief that it will be helpful against those threats. In the case of this study, results showed that the

[1]Rice University, Houston, TX, USA

Corresponding Author:
Alejandra Fernandez-Reyes, Department of Psychological Sciences, Rice University, 6100 Main St, Houston, TX 77005-1892, USA.
Email: af65@rice.edu

level of the threat and likelihood of their accounts being threatened did not impact the participant's choice to use 2FA. Convenience and efficiency seemed to play a role in why people did not choose to use 2FA. Additionally, people would use 2FA more often if they had more knowledge of potential threats (Holmes & Ophoff, 2019).

De Cristofaro et al. (2014) focused more on the impact of context on 2FA use. The contexts that they observed were personal, financial, and work. In terms of methods of 2FA used, they looked at SMS/email, security tokens, and an app. Results showed that most people used email/SMS for their financial accounts, SMS/email for their personal accounts, and tokens for work. Moreover, this study did not account for personal bias in choices since the experiment had a within-subjects design.

In regard to 2FA set-up processes, currently unpublished work from our lab has shown that participants commit errors when setting up 2FA, despite improvements made to the 2FA setup interface. These results imply that users may have misconceptions about certain 2FA methods.

Most of this body of research fails to take into consideration how different account contexts might impact their choice of 2FA methods. Moreover, we also account for users' varying opinion about which accounts are important.

Method

Participants

A total of 206 (105 female, 85 male, 2 non-binary) Rice University undergraduates completed the survey. The ages of the participants ranged from 18 to 23, with an average of 19. The participants were compensated with credit toward a course requirement. All participants were familiar with DUO since its adoption is required by the university. Respondents that did not complete the survey were removed ($n = 13$) resulting in a total of 193 observations. Respondents were not removed based on the time to complete the survey as they are not deemed to affect marginal results (Greszki et al., 2015).

Materials

The survey was split into three parts. The first part aimed to capture users' perception of account importance based on security and their choice of 2FA method for each account type. For example, the first question asked participants to rank 3 different account types (bank, personal email, social media) based on how important security was to them for each account.

The second part of the survey consisted of capturing users' perceptions and experience with DUO, whose usage is required for all Rice University services. More specifically, this part of the survey asks users about their willingness to adopt DUO if it was not required, the 2FA method they use to authenticate DUO, and about difficulties experienced while using DUO.

The last part of the survey compares users' perceptions of SMS as a 2FA method against Push Notification. This section aims at understanding users' perceptions and misconceptions of these 2FA methods. More specifically, users were asked which of the two 2FA methods they believe to be more secure and why (open ended question). For this analysis, all users who had not used SMS or Push were removed. The survey underwent a pilot test to identify any inconsistencies or unclear questions.

Data Analysis

In the first part of the survey, each participant ranked three different accounts in terms of importance and provided the 2FA method they use for each of these accounts. To analyze this data, which included repeated measures from the participants, a baseline-category multinomial multilevel model was constructed. Observations for the security key 2FA method ("SecKey") were identified as contributing to data sparsity and were removed from this specific analysis. As a result, the outcome variable consisted of the four possible 2FA choices (No 2FA, SMS, Push Notification and Passcode), with account importance (rankings) serving as the predictor.

For our qualitative analyses, all open-ended questions were coded by three researchers separately. Then, the resulting multiple coding schemes were discussed, and a single coding scheme was agreed upon. Additional information, such as which specific accounts users adopt 2FA (Netflix, Instagram, etc) and preferred single-factor authentication method, were also collected but were not used for the present study.

Results

Does Account Importance Vary Across Users?

Analyzing users' ranking of three different accounts, bank, personal email, and social, in terms of security importance, showed that most users considered their bank account to be the most important 95% (184), 63% (121) considered personal email to be the second most important, and 67% (129) considered social media to be the least important (see Figure 1). The results of a chi-square goodness of fit showed that, for each account type, the proportions of account importance rankings significantly differed from a hypothetical equal distribution for bank ($X2(1, 193) = 158.7$, $p < .001$), personal email ($X2\ (2, 193) = 99.24$, $p < .001$), and social media ($X2(2, 193) = 127.4$, $p < .001$). These results indicate that users perceive the importance of various accounts differently. While most users agree that their bank is the most important account in terms of security, their opinion varies more when choosing what their second and third most important accounts are.

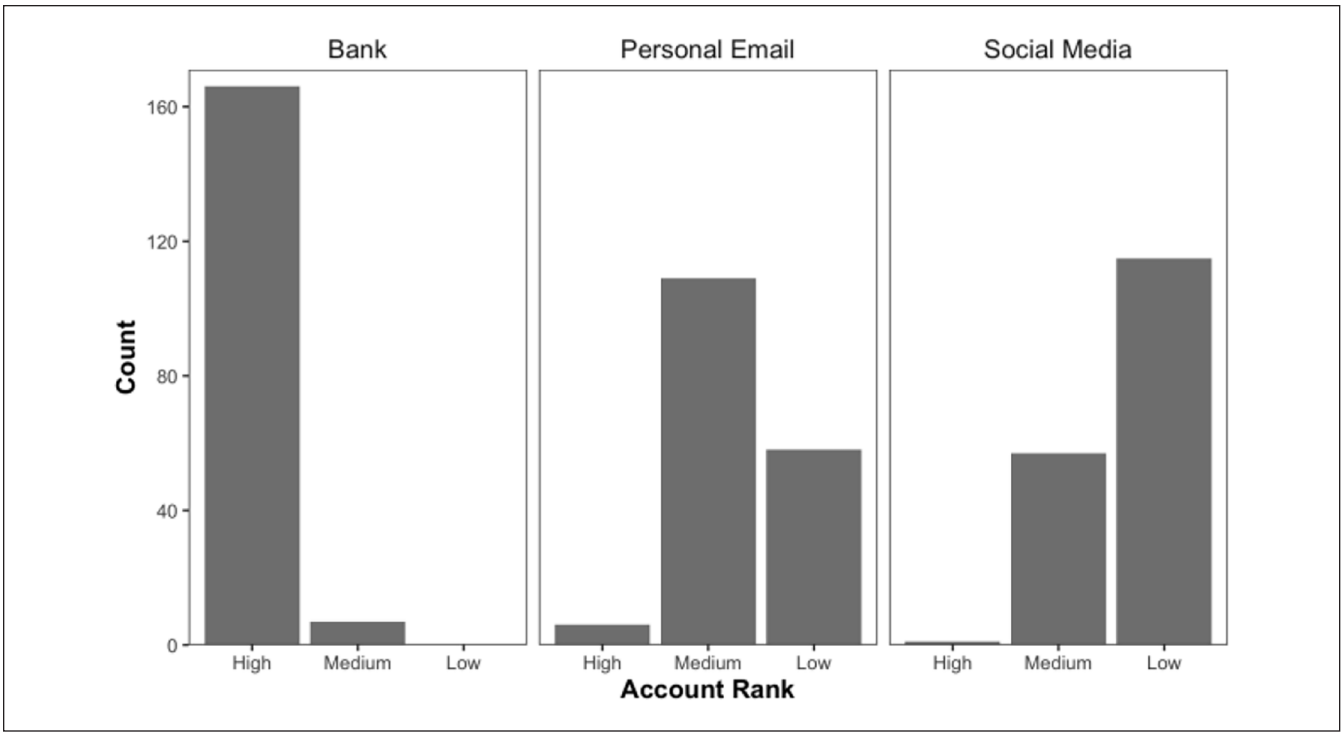

Figure 1. Account ranking based on importance of security.
Note: This graph represents how users ranked each account type, represented by each panel, based on three levels of importance: "High," "Medium," and "Low."

Does 2FA Preference Vary Account Importance?

Given the varying rankings of account importance, users' choice of 2FA method across the three different account types was analyzed, accounting for users' individual differences in how they ranked the three accounts. Figure 2 shows how often each 2FA method was chosen for each account importance.

Comparing No 2FA to Passcode shows a lower odds ratio (OR) of 0.35 for picking Passcode for the highest importance account, with a 95% confidence interval (CI) of [0.22, 0.57], $p < .001$. For the lowest importance account, there was also a lower odds ratio for picking Passcode over No 2FA ($OR = 0.44$, CI = [0.23, 0.87], $p = .02$). This means that for accounts under these categories of importance, users are expected to pick No 2FA over Passcode.

Comparing Push Notification to No 2FA showed a significant difference between the two for the highest importance account ($OR = 0.27$, CI = [0.16, 0.46], $p < .001$) and for the medium importance account ($OR = 2.44$, CI = [1.31, 4.56], $p = .005$). These results suggest that users are more likely to pick Push Notification over No 2FA for accounts of medium importance, while for accounts of highest importance, the opposite is true.

Comparing SMS to No 2FA shows a statistically significant difference for the lowest importance account ($OR = 0.37$, CI = [0.23, 0.62], $p < .001$), meaning that less users are expected to pick SMS over No 2FA for the least important accounts. The lack of significance for the highest and medium account confirms that one should expect about the same number of users to pick SMS or No 2FA. Overall, these results show that account context impacts 2FA choices.

Perceptions of Duo: Comparison with Previous Studies

First, we removed one participant who reported not using DUO, and seven participants who reported using "touch-id" for DUO even though that is not a valid option. We examined the count of preferred 2FA methods for DUO. A chi-square goodness of fit test was performed to determine whether the proportion of 2FA method choices for DUO (at Rice) was equal to the proportion observed in the BYU DUO study (Dutson et al., 2019). The proportions differed $X2$ (3, 161) = 11.77, $p = .008$. These results show that DUO 2FA method preference varies across this study and the BYU study. These results also differ from those of the CMU study (Colnago et al., 2018) which reported that 4% of their sample used tokens, while none did in the current study, and no users reported using the "call me" option, while 5% of our sample did.

It was also observed that 68% of the users reported that they would not use DUO if it was not required, showing a general dislike for DUO. A chi-square test shows a statistically significant difference between the proportions of these

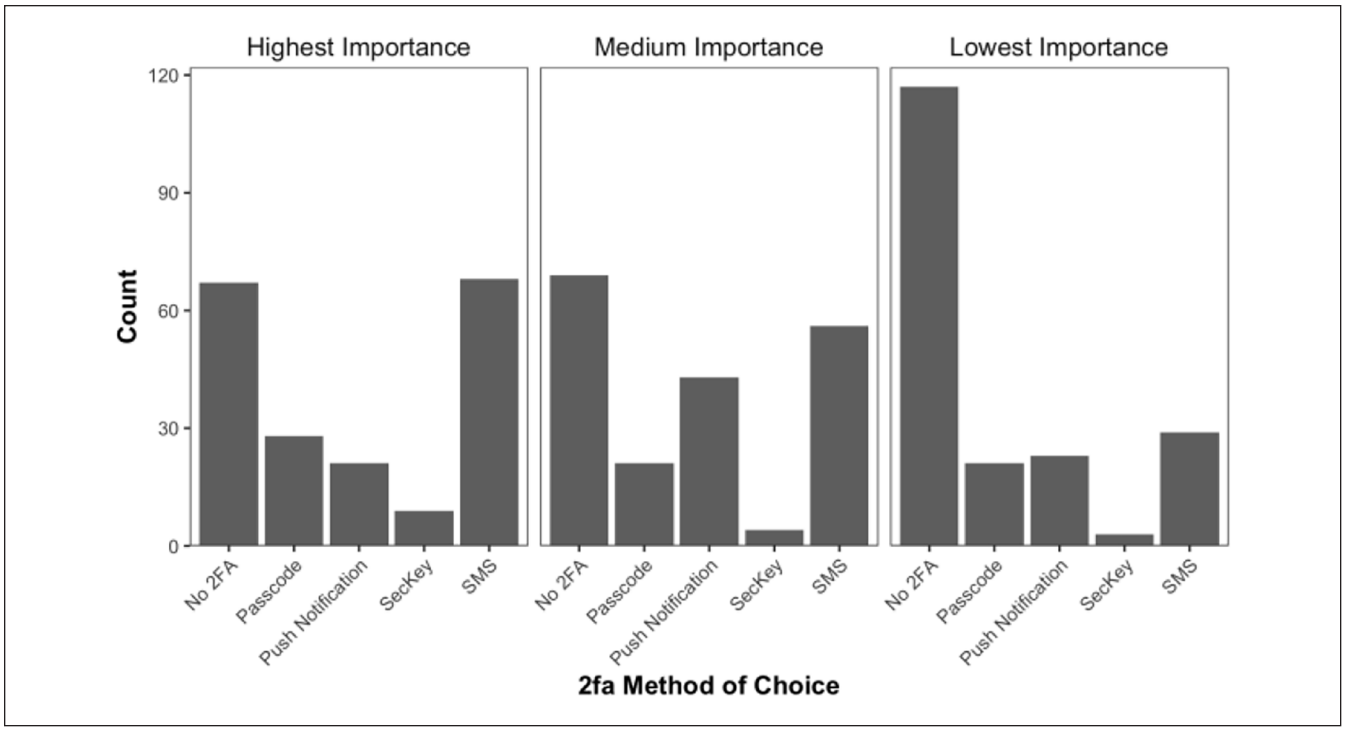

Figure 2. 2FA Method Preference Across Different Account Rankings.
Note: The data was repeated measures, therefore each user provided a preferred 2FA method for each account rank.

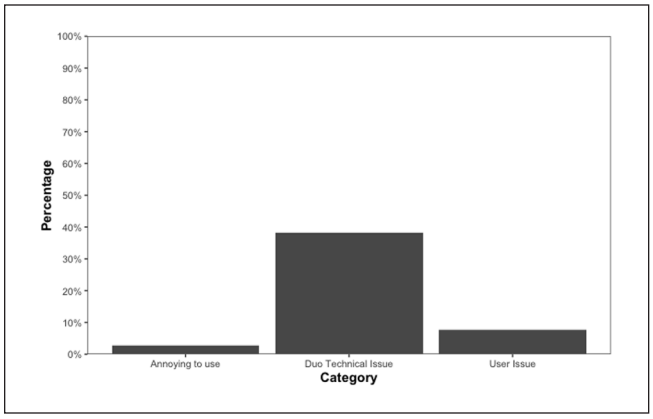

Figure 3. Issues experienced by users while using DUO.

two groups ($X2(1, 183) = 24.5$, $p < .001$). These results differ from those reported in the BYU study, which report that 50% of their users would not use DUO if it was not required. The observed difference in proportions could stem from the composition of the BYU study's sample, which included faculty and other employees constituting 17% of the total. Conducting the same test to examine if a relationship exists between users' willingness to adopt DUO and if they use 2FA for other accounts shows a statistically significant relationship ($X2(1,183) = 5.13$, $p = .02$.). This result is in agreement with the BYU study which reported that users who used 2FA on other accounts were more likely to perceive DUO positively.

Experienced Issues with Duo

Issues that users experienced while using DUO were analyzed to see if they affected willingness to adopt DUO. Surprisingly, most of our users reported *not* having experienced issues with DUO (51%). In general, the rest of the participants reported having experienced technical issues (38%), user-related challenges such as having no service or phone battery (8%), and 3% simply stated that DUO was annoying to use (see Figure 3). A chi-square test of independence was conducted to examine if a relationship exists between users' willingness to adopt DUO and their experienced difficulties. All types of issues were collapsed into a single category to represent that "an issue was experienced." The relationship between these two variables was not significant, $X2(1,183) = 5.13$, $p = .02$. This suggests that the decision to adopt DUO is not influenced by the issues the users have encountered.

Regarding users' suggestions (Figure 4), about half reported that they would not change anything about DUO (46%). This was followed by "speed" (15%), which includes making features faster, increasing expiration time, and the option to remember devices (this already exists though). This comment was also observed in the BYU study. The third most popular suggestion was related to the interface (13%), which includes not requiring an external device, excluding DUO only for Esther (student service portal), and avoiding having to open an app/adding a push notification banner.

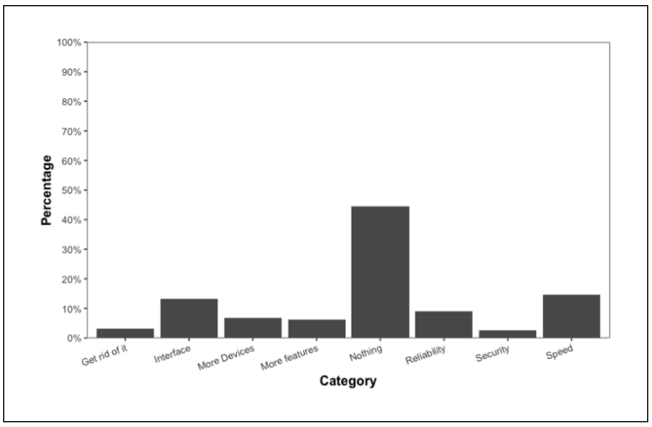

Figure 4. Users' suggestions for duo.

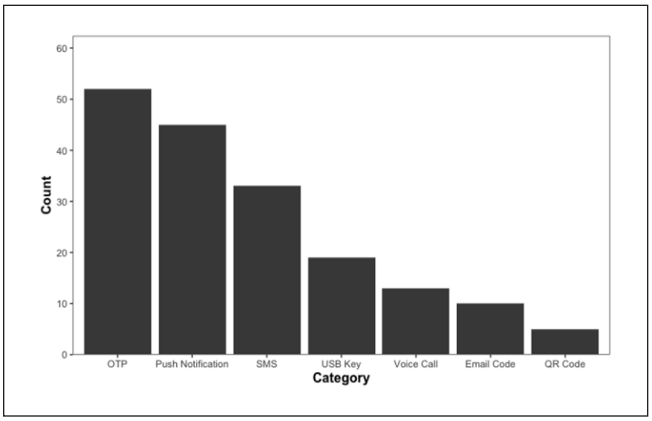

Figure 5. Users' perceptions of which 2FA method is safest.

2FA Method Perceptions/Comparisons

In general, when users had to pick which 2FA method was safest, most picked OTP ("One time password") followed by Push Notification and then SMS (see Figure 5). It was surprising to find that the USB key was not considered to be the safest method, or at least one of the top methods, indicating a general misconception in users' 2FA method mental models regarding security.

Asking users which of the two 2FA methods, Push or SMS, they considered to be safer resulted in twice as many users picking Push Notification (112 for Push vs. 59 for SMS). Surprisingly, when asked why they believed either method was safest, users mostly gave the same reasons. There were two reasons unique to SMS, where one user reported that it was "less error prone" and nine users reported that SMS is safer because it requires more effort to access someone's messages and authenticate ("you must write a code instead of just pressing a button"). There was only one unique reason why users perceived Push to be safer, which was that it "expires faster," as noted by eight users. This means that some users preferred Push because, unlike SMS, the notification expires. This, however, represents a misconception since the validity of SMS codes also expire.

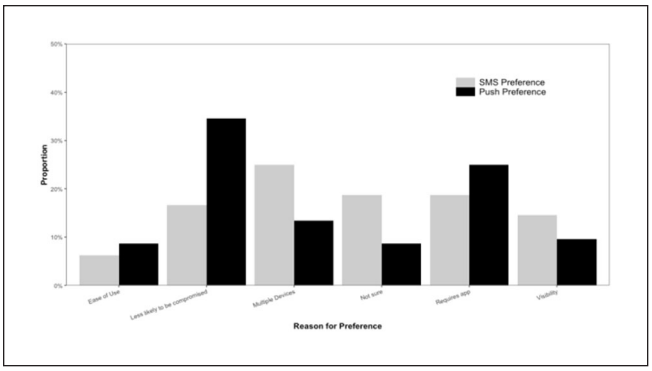

Figure 6. Proportion of comparison of why SMS or push is perceived as safer.

For the remaining categories (see Figure 6), a chi-square goodness of fit test was employed to assess if there was a difference in the distribution of reasons given by users for preferred one method over the other. The results showed that both distributions significantly differed ($X2(5, 171) = 17.2$, $p = .004$). This indicates that, despite mostly giving the same reasons for why SMS or Push was perceived as most secure, the frequency of the reasons varied between these two groups of voters.

Discussion

To conclude, this study emphasizes that users assign varying levels of importance to different types of accounts, leading to varied 2FA method preferences depending on the account context. For example, one would think that a user who prefers SMS, because it has higher perceived usability than other methods, would use SMS for all account contexts. However, as the data shows, when we consider different account contexts, users' preferences change. This highlights the importance of incorporating users' account importance perceptions in future research that aims to understand users' perceptions of 2FA.

It is also possible that certain accounts, like financial accounts, may force users to adopt a 2FA method more often than other accounts. This would mean that users' choices of a 2FA method are more influenced by the requirements imposed on them rather than the account context. If true, this would mean that an interaction exists between account context and reason for adoption. With this in mind, it is also possible that users may not bother to opt out of 2FA when it is a "default" option. Future studies should investigate this potential interaction. This would require a larger sample size as it would increase the complexity, and parameters estimated, of a multilevel model. Researchers should also assess, across different account contexts, users' willingness to adopt 2FA when it is presented as a default security option.

Regarding the inconsistent results across existing studies, it is possible that this is a result of overlooking users' perceived levels of account importance. Additionally, given the existing belief that perceived usability determines the 2FA method to be used, future research should aim to quantify how much account context and perceived usability of a given method affect the choice of a 2FA method. Moreover, the observed decline in 2FA adoption for lower importance accounts raises the question if a threshold at which users decide to not adopt any 2FA method can be quantified.

In terms of users' perceptions, it was surprising to see that, despite the varying preferences for 2FA methods across different account contexts, users still cited the same reasons for believing that SMS or Push notification were the safest, although at different frequencies. This consistency, despite different security method choices, suggests a common mental model of security perception among users, at least for the two most popular methods. This presents an opportunity for interface design improvements that more closely align user perceptions with the actual security needs of different contexts. Specifically, the pros and cons of each 2FA method should be communicated in a manner that aligns with this common mental model as opposed to communicating in general terms of security, which users are less familiar with.

Finally, considering that the reason for 2FA adoption was mostly forced, there may be an opportunity for developing personalized security recommendation systems that consider the types of accounts users are securing in order to provide an adequate level of security while maximizing users' satisfaction.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Lorrie, C., & Christin, N. (2018). It's not actually that horrible: Exploring adoption of two-factor authentication at a university. *(pp*.1–11). https://doi.org/10.1145/3173574.3174030.

De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2014). A comparative usability study of two-factor authentication. Proceedings 2014 Workshop on Usable Security. https://doi.org/10.14722/usec.2014.23025

Dutson, J., Allen, D., Eggett, D., & Seamons, K. (2019). Don't punish all of us: Measuring user attitudes about two-factor authentication. *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp.119–128). https://doi.org/10.1109/EuroSPW.2019.00020

Greszki, R., Meyer, M., & Schoen, H. (2015). Exploring the effects of removing "too fast" responses and respondents from web surveys. *Public Opinion Quarterly*, *79*(2), 471–503. https://doi.org/10.1093/poq/nfu058

Holmes, M., & Ophoff, J. (2019). *Online security behaviour: Factors influencing intention to adopt two-factor authentication*. Academic Conferences International Limited.

Marky, K., Ragozin, K., Chernyshov, G., Matviienko, A., Schmitz, M., Mühlhäuser, M., Eghtebas, C., & Kunze, K. (2022). Nah, it's just annoying!" A deep dive into user perceptions of two-factor authentication. *ACM Transactions on Computer Human Interaction*, *29*, 1–32. https://doi.org/10.1145/3503514