Smart Storytelling: Video and Text Risk Communication to Increase MFA Acceptability

Sanchari Das
University of Denver
Email: Sanchari.Das@du.edu

Shrirang Mare
Western Washington University
Email: shri.mare@wwu.edu

L. Jean Camp
Indiana University Bloomington
Email: ljcamp@iu.edu

2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC) | 978-1-7281-4146-6/20/$31.00 ©2020 IEEE | DOI: 10.1109/CIC50333.2020.00027

***Abstract*—Exposure of passwords for authentication and access management is a ubiquitous and constant threat. Yet, reliable solutions, including multi-factor authentication (MFA), face issues with wide-spread adoption. Prior research shows that making MFA mandatory helps with tool adoption but is detrimental to users' mental models and leads to security-avoidance behavior. To explore feasible solutions, we implemented text- and video-based risk communication strategies to evaluate if either mode of risk communication was useful. We sought to explore users' technical biases to further examine the mental models that are associated with safer security habits. Our study of $N = 620$ participants found that users are aware of frequent security attacks, including phishing. We found that text- and video-based communication is often useful when information is aligned with individual actions and their consequences, which can range from benign to catastrophic. Shorter mental-model-aligned video snippets piqued user interest in MFA. On the other hand, detailed risk communication videos or textual descriptions improved users' understanding of MFA and the potential risks of non-usage. Our study indicates that, beyond usability and comprehensive education, risk communication offers the potential to increase MFA adoption.**

***Keywords*—** Authentication, Multi-Factor Authentication, Risk Communication, User Studies

1. Introduction

Passwords are the most common form of authentication. They are also vulnerable to theft through attacks, such as phishing and social engineering. In the third quarter of 2018 alone, email-based credential phishing attacks against corporations quadrupled. To improve password security strength, researchers have suggested increasing the complexity of the passwords by increasing the minimum required length, adding symbols, etc [1], [2]. But many of these recommendations are not feasible, especially from the user perspective [3]. As a solution, multi-factor authentication (MFA) addresses both the human and technical vulnerabilities of single-factor authentication, such as with passwords [4], [5]. MFA uses multiple layers of authentication, which comprises of three main ways to authenticate (commonly called authentication factors): *something one knows* (e.g., passwords), *something one is* (e.g., biometrics [6]), or *something one has* (e.g., physical tokens). MFA is a technically sound and secure authentication strategy [7], but it is questionable whether users find it acceptable and usable to use different MFA tools and technologies [8], [9], [10], [11].

Despite MFA's security benefits, the usability and adoption of MFA remain low, highlighting that merely providing technology is not sufficient for widespread adoption [12]. Thus, the focus of our work is to analyze participants' risk perceptions, address the concerns of MFA users, and identify effective ways to communicate the benefits of MFA while being aligned with users' risk mental models. Our study shows how expertise level can impact the adoption (and thus, effectiveness) of security tools. To help us understand users' perceptions of MFA technology, we surveyed 620 MTurk participants, where we asked participants about their daily passwords and MFA usage. Our research not only revealed that many participants had detailed encounters with MFA but also evaluated the effectiveness of context-driven risk communication on the participants' MFA usage. We specifically addressed the following research questions:

- *RQ1. What are users' risk perceptions of online threats, such as phishing?*
  We note that there is a concern about the non-adoption of MFA. However, there is a lack of research addressing the risk perception-driven mental models of the users. It is critical to understand what users perceive as online threats. To address this, we asked participants questions mainly focusing on cyber threats, such as phishing, to understand the security averse behavior of users. Such a question helped us evaluate whether users can relate to the benefits of adopting MFA or the risk trade-offs of not adopting MFA.
- *RQ2. How does users' computer and security expertise level affect the security practices of users?*
  Expertise plays a critical role in several security-focused behaviors. We wanted to explore whether different levels of computer and security knowledge play a role in users' (non)adoption of security practices, mainly focusing on MFA usage. This evaluation is critical, given that the technical biases of individuals remain under-explored. The addition of the expertise factor helped us address potential biases regarding MFA's widespread (non)adoption.
- *RQ3. How effective are short mental-model specific videos in communicating risk compared to longer generic videos or text?*
  While understanding the risk perception and expertise biases is necessary, we mainly wanted to explore how we can design effective risk communication strategies for users. We wanted to examine how users responded to video communication in comparison to textual forms of communication, which can provide further details about how to communicate MFA benefits effectively. Additionally, we hypothesized that short videos that are aligned with users' mental models are just as effective as the long generic videos. To analyze this, we studied four videos that used

978-1-7281-4146-6/20/$31.00 ©2020 IEEE
DOI 10.1109/CIC50333.2020.00027

different mental models: personal safety, physical space safety, data cleanliness and hygiene, and risk perception (organizational responsibility management and prevention of crimes).

2. Related Work

While multi-factor authentication improves online account security, the adoption of MFA has been low due to the negative user perception towards MFA technologies [13], [14], [15]. Security and usability are both essential for ensuring secure access control [16]. While implementing new tools to enhance security, researchers and practitioners often overlook users' expertise (or lack thereof) in the domain, which leads to knowledge and usage misalignment [17].

2.1. Risk Communication and Mental Models

Another component that researchers have previously explored is risk communication for improving the security behavior of individuals [18], [19]. It has been shown that perception of risk is often lower than what it really is, making users more vulnerable to online threats [20]. This creates a need for understanding user motivation and their mental models when any security tool is designed [21], [22], [23]. Thus, Harbach et al. pointed out the need for learning about user mental models and how risk communication can be utilized as an effective tool for improving users' security hygiene [24]. While studying users' mental models, Wash and Cooper conducted a user study to evaluate whether aligning with user mental models can help them detect malicious emails. Interestingly, they found that the source of these training materials can also impact users' assertiveness and attentiveness towards email threats [25]. Such studies not only show the importance of the source of the content but also point out relevant details about users' behavior if the implementation is aligned with their mental models. These claims are also backed by other studies in the field from Wash and Rader [26], Volkamer, and Renaud [27], and Blythe and Camp [28].

Past research shows that threat avoidance behavior is prevalent among users [29]. For example, Herath et al. showed that users adopted email authentication services when the services addressed their concerns and revealed the benefits of utilizing more secure authentication tools [30]. Thus, risk perception has proven to be a crucial factor in providing a positive influence on users' decision-making [31]. However, the effectiveness of risk communication depends on the medium of communication [32], [33]. Under the specific context of risk communication, Albayram et al. evaluated the visual form of risk communication, where users were motivated through informative and self-sufficient videos [34]. They identified high-priority tasks (e.g. security content to address) and approaches to avoid (e.g. using computer-generated voice) and thus provide improved outcomes for risk communication. Our study expanded their work, as we added another mode of communication via texts. We also tested videos of shorter lengths that align with the mental models of the users. Here, we focus on whether or not mental models specific to different types of risk communication strategies can be effective.

2.2. Multi-Factor Authentication: User Side

Braz et al. pointed out that human factors and graphical user interface (GUI) design impact users' overall experiences with multi-factor authentication [16]. Gunson et al. investigated user perceptions of single-factor and two-factor authentication methods in automated telephone banking [35]. The experiment found that while multi-factor authentication significantly improved security, it resulted in lower user perception of usability. Das et al. studied users' experiences with FIDO U2Fs and revealed that issues with enrollment and verification had caused troubles for users choosing to use the hardware token [36]. Weir et al. conducted experiments in the scenario of phone-based banking and suggested that such additional verification slowed down the banking process [37]. Reynolds et al. studied the YubiKey, focusing on cases of MFA usability in desktop and web applications. They identified major user failures in a majority of U2F applications, especially during the onboarding (setup) procedures [38]. Colnago et al. studied the user experience of MFA in the context of organization-wide deployment, such as universities [39]. They directly collected data from the university's IT office for detailed statistics on MFA usage. They suggested improvements in implementation design and strategic messaging for better user adoption. Cristofaro et al. [40] conducted a survey on MTurk about the adoption and usability of MFA among online users. These studies showed that MFA was perceived as providing higher levels of security, but it was rated as low convenience, low ease-of-use, and more time consuming compared to passwords.

In our research, we explore the usability and acceptability of MFA technologies by analyzing users' attitudes towards new technology while exploring their technological awareness. We do this by expanding on previous research on mental models and risk perception. This study will help the research community in understanding users' pain points with MFA while guiding technology experts through design and architectural recommendations. Additionally, our work reveals how risk communication can be utilized to address users' concerns. Our detailed research on different modes of risk communication provides a context-aware implementation that utilizes several modes of communication to improve security practices.

3. Methods

The purpose of this study was to examine how different risk communication methods affected users' perceptions of multi-factor authentication usage and adoption. We also examined how users associated their online security to the different mental model videos shown, which had themes such as personal safety, physical space safety, data cleanliness and hygiene, and risk perception (organizational responsibility management and prevention of crimes). We expand previous research on video tutorial-based risk communication by adding the comparative analysis of text-based risk communication as well [34]. In this section, we describe our methods and study design in detail.

3.1. Data Collection

Recruitment: We used Amazon's Mechanical Turk (MTurk) [1] platform to recruit participants and surveyed them using Qualtrics [2]. We restricted the survey to Turkers who were currently living in the United States to have some cultural biases control and had a 95% or higher approval rating. We restricted our survey to Turkers who had reading and writing understanding of the English language since our survey was written in English. The videos and text used in the survey were also written and narrated in English.

Demographics of Participants: There were a total of 699 responses, out of which 620 were deemed successful completion

1. https://www.mturk.com/
2. https://www.qualtrics.com/

of the survey. We rejected the other 79 responses, due to incomplete data and/or the attention check question not being answered correctly. Out of the 620 responses, 388 (62.6%) were male, 227 (36.6%) were female, four (0.65%) listed Other as their gender, and one (0.16%) did not wish to specify. Though we would like to have an even split between different genders, this variable was out of our control, given that the survey was advertised in MTurk. The age range categories of the participants spanned from 18 to over 55. 19% were 18–24 years old, 50.1% were 25–34, 20% were 35–44, 5.9% were 45–54, and 4.8% were 55 or above. In terms of expertise, out of the 620 participants, 243 participants were technical experts. Details of the calculation of expertise have been provided later in this section. The majority of the participants had post-secondary education (424) or classified as either 4-year degree college graduates (316), or as having some college (108). The next highest education level was comprised of those with a Masters's or professional degree (133). Only 19 participants out of the 620 reported a language other than English as their native language. The participants took an average of 12.3 minutes to complete the survey (median=11.2 minutes, SD=5.4 minutes). Each user was paid $2.50 for completing the survey. This study was approved by the organization's human research review board.

Survey Design: We conducted a survey-based study to understand users' perceptions of MFA tools and technology. Before the primary questionnaire was given, we asked a pre-screening question once the participant had agreed to participate in the survey to ensure we only collected data from participants who were 18 years or older. After that, we provided a brief video explaining MFA to avoid participants being unaware of MFA in the first place.

The primary survey questionnaire was split into eight parts. In part 1, we collected necessary demographic information, such as age, gender, educational background, and native language. In parts 2 and 3, we asked ten yes or no questions about tasks they have completed that require computer usage, such as designing a website, registering a domain, using SSH, and configuring a firewall. These questions were developed by previous researchers who performed factor analysis by analyzing a data set of 890 participants [41]. Based on participants' responses to these questions, we computed a technical expertise score for each participant. We utilized these scores to evaluate how users' expertise affected the effectiveness of risk communication through mental model videos. As noted in section 2, expertise can impact the security behavior of an individual. Through these questions, we wanted to capture the technical expertise of individuals to evaluate this correlation.

Part 4 of the survey consisted of questions related to the participants' password behaviors. Through a 5-point Likert scale, we asked questions about how confident participants were that their password would protect their accounts from attacks. We found that only 1.99% of the participants believed that their passwords were not secure enough. On the flip side, 93% of the participants were concerned about their accounts being hacked. These questions helped us answer RQ1 and comprehend the risk perception of the users, especially when it came to authentication and access control. In part 5, we asked questions related to mental models and phishing resilience, where we tried to understand how users aligned and visualized online data security with regards to physical harm, space violation, or financial harm. These questions were derived from a previous study by Garg et al., who explored the nine dimensions of phishing risk [42]. In part 6, we asked participants about their current MFA usage by giving them examples of different websites for which they may be using MFA. These examples included: financial or banking accounts, email, GitHub, Box, accounts at work, other (which had to be specified), and none at all. The questions were focused on the daily MFA usage of the participants and attempted to understand participants' MFA avoidance behavior (if any).

Risk Communication Section: Part 8 of the survey provided risk communication tools, including the videos and texts aligned with mental models of risk perception. The mental models were based on several previous studies by Wash et al. [26], Kang et al. [43], Camp et al. [22], and Sasse [44]. We developed videos of various lengths and with different themes and tested the entire survey through various pilot study protocols with 37 pilot survey takers. Given our analysis, we found that the ten-second videos were most effective in conveying information. This aligns with previous claims on the effectiveness of shorter videos, where videos between seven to ten seconds long are considered to be more effective [45], [46]. Given our pilot studies, we developed four videos with varied lengths. Three of them were shorter videos, with length ranging from 10-13 seconds. The themes were personal safety, physical space safety, cleanliness and hygiene, and risk perception (financial management and crime prevention). The shorter videos were based on mental models of personal safety, physical safety, and data cleanliness and hygiene.

Out of the 620 responses, 125 viewed the personal safety mental model video, 125 viewed the physical space safety video, 122 viewed the data cleanliness and hygiene video, 123 viewed the risk perception (organizational responsibility management and prevention of crimes) video (the lengthier video), and 125 participants viewed the text-based risk communication. Once the risk communication video or text was shown to the participants, we asked open-ended questions about the communication (e.g., what aspects of the video did you like?) and two close-ended questions about the effect of the communication (e.g., did the video/text make you more concerned about your online accounts?) in order to analyze and compare the methods of risk communication. Finally, in the concluding section of the questionnaire, we asked the users multiple questions using a 5-point Likert scale that checked their understanding of MFA after receiving the MFA information through the risk communication methods stated above. With the collected data, we wanted to see how the methods of risk communication impacted MFA adoption as well as how the expertise levels of the users impacted their perceptions of MFA. The survey responses were anonymous. In the following section 4, we will report on the findings of this survey. We will not be reporting on the pilot studies, which were utilized to form a robust study design and protocol.

4. Findings

4.1. Mental Model and Risk Perception (RQ1)

We asked questions about how our participants related online data security with their personal safety, space safety, data cleanliness and hygiene, and others in order to get a sense of their mental model. We found that a large percentage of users either agreed (41%) or somewhat agreed (42%) that their personal computer security was like keeping their physical space secure from theft. Additionally, they agreed (31%) or somewhat agreed (48%) that their personal computer security was like preventing vandalism and petty crimes. The mental model that related personal computer security to practicing good personal hygiene had the lowest percentage for the combined agree and somewhat agree

responses (64%). We also asked questions to gauge user perceptions toward phishing. It was interesting to note that despite the recent increase in phishing attack frequency [47], [48], [49], users believed that they could protect their accounts from any phishing attack and can control the risk (78%). The results clearly show that users had strong confidence in their technical acumen.

4.2. MFA Usage (RQ2)

Through the answers collected with the open-ended questions, we found that the participants expressed many concerns about using MFA. Experts showed greater subversiveness when it came to avoiding MFA. One way experts showed a more considerable increase in avoidance usage behavior was by exclusively using trusted devices to log in to their MFA-enabled online accounts, as one of our expert participants mentioned:

> *"I often avoid triggering the two step authorization by avoiding logging in from different IPs."*

Using trusted devices is a good practice for finding the balance between usability and cumbersome steps of authentication. However, one cannot assume that such devices will always remain secure [50], [51]. Thus, experts should be aware of the security vulnerabilities of using trusted devices to avoid MFA for their authentication.

Additionally, many participants, including experts, expressed frustration with using MFA. One participant commented,

> *"I don't change my use of them [i.e., online accounts that have implemented MFA,] but I definitely find it an obnoxious process to do every time."*

> *"I find it a hassle at times to log in to some services that I have enabled two-factor authentication on because it is constantly asking for it. It makes me not want to log in as much, unless I really need to. If I know the site will only ask for the second step when it detects suspicious behavior, I am fine."*

Finally, both expert and non-expert users showed the avoidance behavior of opting to use their financial institutions' apps in order to avoid MFA once it was made compulsory to use through a web browser. This behavior shows that users will find ways to not use MFA if the risk trade-offs are not communicated properly.

> *"I tend to not log into things I have MFA on but it is because they are sites I don't use on a browser (i.e. I have an app that isn't MFA)"*

4.3. Risk Communication (RQ3)

To understand impact and to predict usage behavior after implementing MFA risk and benefit communications, we performed linear regression on different factors influencing dependent variables. The linear regressions were conducted to examine whether different risk and benefit communication methods had an impact on users' concerns for their online accounts and their understanding of MFA benefits. Furthermore, analysis of shorter versus longer length videos was also performed in the process.

Table 1 shows the coefficients and the standard error for the linear regression, which examines the participants' concerns for their online accounts relative to the risk and benefit communication methods. The dependent variable was users' concerns about not using MFA. The five communication models that we used in the regression were the four video-based communications (personal safety, physical space safety, data cleanliness and hygiene, and risk perception) and text-based communication. We also used gender, age, and expertise levels as independent variables in our analysis. Table 1 also shows the coefficients and standard error for the participants' understanding of the benefits of MFA. In this case, the dependent variable is the perceived benefits of using MFA. A positive correlation in the table suggests an increase in users' security concerns and knowledge of MFA benefits, indicating that they were positively impacted by the risk and benefit communication strategy. A negative coefficient indicates a negative correlation between users' security concerns/understandings of MFA benefits with the different variables. The level of significance where $p < 0.05$ is shown through the standard symbol usage of a star (*).

As mentioned, we used independent variables such as gender, age, and expertise level (experts vs. non-experts) to evaluate whether these variables influenced the participants' concerns for the security of their online accounts and their understanding of the benefits of MFA. Across the three gender types, males ($p = 0.031$) and females ($p = 0.014$) showed statistically significant increases in their concerns for their online accounts. Younger participants had a stronger concern for their online accounts, specifically participants aged between 18 and 24 years old ($p = 0.001$). Lastly, we can conclude that all four expertise groups—technical experts ($p = 1.91e - 13$) and non-experts ($p = 3.03e - 10$)—showed concerns for their online accounts.

We also checked to see if these variables had any significant relation to the participants' understanding of the benefits of MFA. We did not find significance for any of the three gender groups—male ($p = 0.194$), female ($p = 0.181$), and others ($p = 0.180$). Similar to the concerns of online accounts, participants aged between 18 and 24 years ($p = 0.029$) were the only age group to show more of an understanding of the benefits of MFA. None of the participants regardless of their technical prowess showed any significance in regards to understanding the benefits of MFA—experts ($p = 0.942$) and non-experts ($p = 0.852$). With regards to the participants' understanding of the benefits of MFA, we found that data cleanliness and hygiene ($p = 0.000148$) was the most effective short video, with both risk communication through video ($p = 0.021$) and text ($p = 0.00025$) being effective methods of conveying the benefits of MFA.

Personal Safety: Figure 1 shows the distributions of the participants' responses when they were shown a short video relating their online security to personal safety. The participants agreed that the video helped them understand the risk trade-offs of not adopting MFA tools, such as the Yubico security tokens.

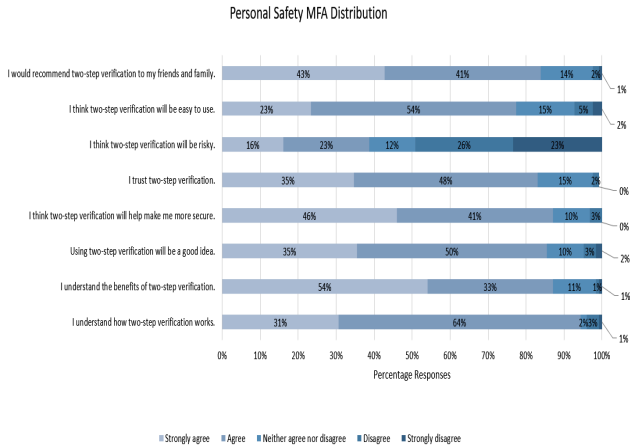

Figure 1: Distributions of participants' responses related to their MFA practices who were shown shorter video related to personal safety.

	Concerns		Benefits	
Variables	Coeff.	Std.Error	Coeff.	Std.Error
Personal Safety	0.222	0.079	0.209	0.0952
Personal Space Safety	0.240*	0.0787	0.231	0.0945
Cleanliness	0.382	0.0780	0.145***	0.0937
Risk Perception	0.120	0.0784	0.183*	0.0942
Text	0.044	0.079	0.221***	0.094
Male	0.518*	0.096	0.688	0.115
Female	0.481*	0.095	0.296	0.114
Other	-0.010	0.016	0.015	0.019
18 - 24 years	0.143**	0.077	0.143*	0.092
25 - 34 years	0.534	0.099	0.511	0.119
35 - 44 years	0.222	0.079	0.230	0.095
45 - 54 years	0.042	0.047	0.080	0.056
55 years or above	0.058	0.042	0.034	0.051
Experts	0.414***	0.095	0.308	0.114
Non Experts	0.925***	0.068	0.741	0.082

TABLE 1: Coefficients for the linear regressions predicting how users visualize the concerns and benefits based on their mental models, type of risk communication, gender, age, and expertise level.

Physical Space Safety: Table 1 shows that the physical space safety video had a significant impact on raising participants' concerns for their online accounts ($p = 0.034$). Figure 2 presents the distribution of the responses to statements by participants who had watched the short video on physical space safety and MFA. Similar to the participants who had viewed the personal safety video, the majority of these participants either Strongly Agreed or Agreed with the supportive statements about two-step verification. Also, the majority of participants did not believe two-step verification to be risky. The percentages for responses to that statement were very similar, but more participants in the personal physical safety group Strongly Disagreed with the statement (30%) compared to those from the personal safety group (23%).

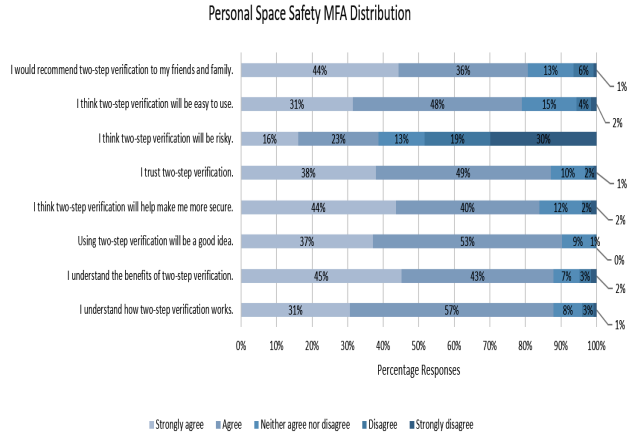

Figure 2: Distributions of participants' responses related to their MFA practices who were shown shorter video related to personal space safety.

Data Cleanliness and Hygiene: Table 1 shows that relating online security to cleanliness and hygiene was an effective form of risk communication to convey the benefits of MFA ($p = 0.000148$). Figure 3 gives the distribution after participants watched the short cleanliness-and-hygiene-themed video. 58% of users thought that MFA would be easy to use, and 45% of participants strongly agreed that they understood the benefits of MFA after watching the video. Furthermore, after watching the video, a high percentage of participants strongly agreed (45%) or agreed (38%) that they understood the benefits of MFA.

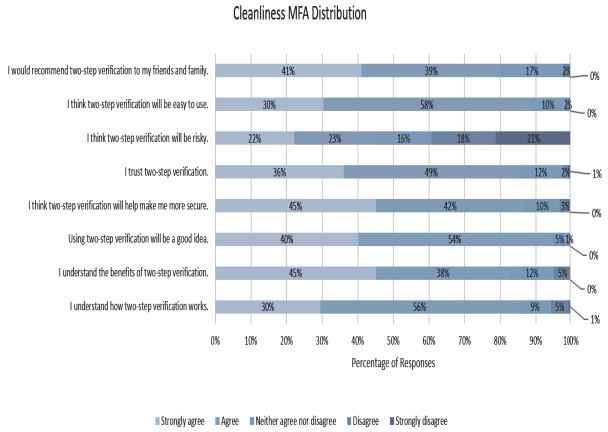

Figure 3: Distributions of participants' responses related to their MFA practices who were shown shorter video related to data cleanliness and hygiene.

Descriptive Communication About MFA Usage: We also utilized a longer video (2 minutes, 06 seconds) to contrast with the first three risk and benefit communication methods. The video was taken from the work of Albayram et al [34]. Table 1 shows that this informative risk perception video proved effective at communicating the benefits of MFA ($p = 0.021$). As shown in Figure 4, this risk and benefit communication method yielded the highest percentage of agreements (87%) with the statement that participants would recommend multi-factor authentication to family and friends, indicating that users found MFA beneficial to those they care about as well as themselves after watching the video. Participants also believed that two-step verification would help them be more secure, as indicated by a 91% agreement after watching this longer video. However, in addition to agreeing with the benefits, the participants did acknowledge that the length of the video could be reduced.

Text: In addition to the video-based risk communications, we also presented some participants with the text-based form of commu-

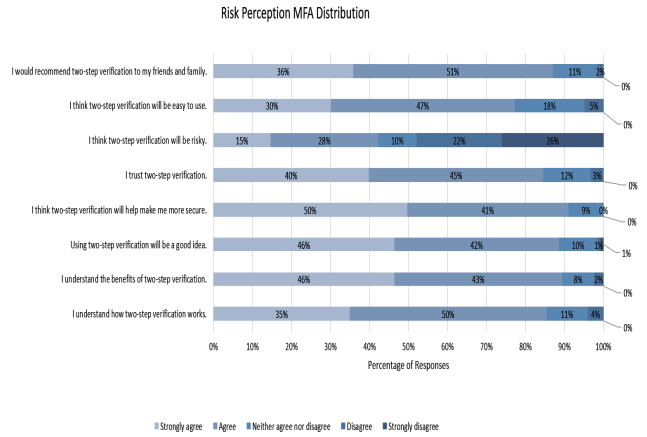

Figure 4: Distributions of participants' responses related to their MFA practices who were shown a longer and informative video that illustrated how MFA works

nication for comparison. The text we used was taken directly from the Yubico website. Table 1 shows that text proved to be an effective form of communication to help users understand the benefits of MFA ($p = 0.00025$). Figure 5 shows that 87% of participants agreed that they understood the benefits of MFA with textual form of communication, and compared to the video-based communications, 79% of participants agreed that they would recommend MFA to a friend or family member. Our results demon-

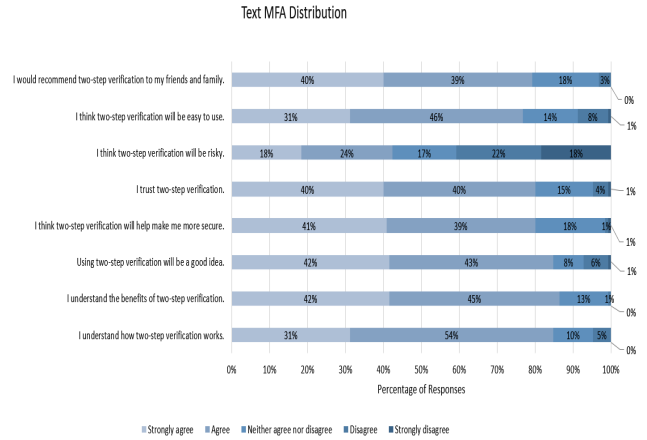

Figure 5: Distributions of participants' responses related to their MFA practices who were shown text-based MFA and its functions.

strate that users, regardless of their technological background, care about their online data. Additionally, our study proves risk and benefit communications to be beneficial in security tool adoption, as long as they resonate with the mental models of the users.

5. Recommendations

Based on our results and risk communication strategies, we propose the following recommendations to enhance security from the user perspective. One of the clear messages we observed through our open-ended questions was that users do not want to go through the additional step of authentication. Thus, to motivate users into adopting an additional step to protect their data, we need to have proper risk communication that is context-aware. Some of the recommendations which emerged from this research are as follows.

5.1. Context-Aware Risk Communication

We often see organizations promoting security tools and strategies such as MFA without any form of motivating the users to use them. Understanding user risk perception and mental models is as crucial as implementing new security tools and technologies. MFA is an effective security tool for protecting digital identity. However, as security researchers and practitioners, we should understand the user's mental models and how users relate data security with real-life incidents to provide solutions accordingly. For example, we implemented the mental models of personal safety, physical space safety, and data cleanliness. One of the techniques has worked when users are motivated to protect organizational data [52], [53]. Such context-aware techniques can be used for motivating the users, as evidenced by this research.

5.2. User Risk Profiling

An extension of the different modes of risk communication strategies could be implemented. Here, based on the user's mental models and usage patterns, we could profile users and provide them with a risk score. Though such approaches may raise privacy concerns, these types of observations are already done by organizations to monitor employees' network usage. We can utilize such scores to create different types of risk communication strategies for users. Such risk scores could result in some false positives and negatives, but periodic reviews and updating of the algorithm code should resolve this problem. We can also use this user profiling to identify more risky users to make them go through targeted user training on MFA, compared to those who have less risky profiles and can have more lenient user training. Effectiveness of user training is often debatable [54], [55], but such user profiling can help with the tediousness of such training.

5.3. Privileged Account Protection

Our data showed that participants unanimously want to protect their financial accounts through MFA, which also resonates with the results of previous studies [56]. Thus, instead of making MFA mandatory for every account, we could create privileged accounts, such as financial accounts, work accounts, etc. that must be protected via MFA. Such implementation aligns with user mental models. However, we have to ensure that even when users do not think accounts, such as gaming profiles in Steam [3], are not essential, they could become essential if they buy anything from the online gaming stores and store their credit card information.

5.4. Seamless On-Premises Integration

This recommendation is primarily focused on workplace usage of MFA. A majority of organizations, both in academia and industry, provide workstations for their employees to conduct work. Organizations that are limited to industrial buildings can provide on-prem MFA, where one of the factors is the physical location of the employees. For example, if the employee logs into the office workstation, they need not provide another factor of authentication, since they are only allowed to use it by entering the office through their organization's ID card. Such a strategy can reduce the burden from the user side and help with seamless integration. However, such strategies should be prohibited from critical tasks where the users can control or modify the data stored directly in the server. IP-based MFA can be used for daily activities, such as communicating over Slack.

3. https://store.steampowered.com/

6. Future Work and Limitations

We conducted a survey-based study. Thus, this is self-reported data, which can be subjective. However, the usage and understanding corroborated other works [4], [36], [39], indicating that our study data is valuable for understanding user perception of MFA. Given the success of proper channeling of information about security tools and risk communication, we aim at finding better means of informing users and motivating them towards better security practices. We also aim to utilize the techniques to test in a larger work setting where MFA is on a critical path. To understand the prolonged effectiveness of the risk communication on the daily usage of MFA, we will further expand this research to conduct a longitudinal study where qualitative analysis would provide a deeper understanding.

7. Conclusion

Online user presence has increased rapidly in the last few years, broadening the user base and leading to an amplified awareness of the need for proper authentication methods. Traditional single-factor authentication, such as textual passwords, has proven to be susceptible to security vulnerabilities such as phishing, brute force attacks, shoulder surfing, identity theft, and others. Through this research, we are focused on mitigating digital risks by exploring authentication technologies like multi-factor authentication that can strengthen authentication processes.

Though MFA tools have improved online security exponentially, users are often reluctant to use such tools or understand their full capacity. To better comprehend user perceptions of MFA technologies, we studied users' mental models through a survey-based analysis. Users related the safety of their personal physical space to their concerns about their online accounts. Users also associated their cleanliness and hygiene with their understanding of the benefits of MFA. Thus, we implemented three risk mental models, including personal safety, physical space safety, and data cleanliness and hygiene. Informative longer videos and textual communications proved to be more effective at teaching users about the benefits of MFA tools and technologies. We propose utilizing risk and benefit communications for better implementation of new MFA tools and technologies aimed at improving security for everyone.

Acknowledgments

We would like to thank Chetan Mehta for his help with data collection and Andrew Kim for his help with the proofreading of the paper. We would also like to acknowledge the Secure and Privacy Research in New-Age Technology (SPRINT) Lab at the University of Denver and the Human and Technical Security (HATS) Lab at Indiana University. This research was sponsored by DHS N66001-12-C-0137, Cisco Research 591000, and Google Privacy & Security Focused Research. Any opinions, findings, and conclusions or recommendations expressed in this material are solely those of the author(s).

References

[1] Y.-Y. Choong, M. Theofanos, and H.-K. Liu, *United States Federal Employees' Password Management Behaviors: A Department of Commerce Case Study*. US Department of Commerce, National Institute of Standards and Technology, 2014.

[2] L. J. Camp, J. Abbott, and S. Chen, "Cpasswords: Leveraging episodic memory and human-centered design for better authentication," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016, pp. 3656–3665.

[3] A. Adams, M. A. Sasse, and P. Lunt, "Making passwords secure and usable," in *People and Computers XII*. Springer, 1997, pp. 1–19.

[4] A. Amin, I. ul Haq, and M. Nazir, "Two factor authentication," *International Journal of Computer Science and Mobile Computing*, 2017.

[5] J.-J. Kim and S.-P. Hong, "A method of risk assessment for multi-factor authentication," *Journal of Information Processing Systems*, vol. 7, no. 1, pp. 187–198, 2011.

[6] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[7] W. N. Owen and E. Shoemaker, "Multi-factor authentication system," May 13 2008, uS Patent 7,373,515.

[8] S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating user perception of multi-factor authentication: A systematic review," *arXiv preprint arXiv:1908.05901*, 2019.

[9] S. Das, A. Kim, S. Mare, J. Streiff, and L. J. Camp, "Security mandates are pervasive: An inter-school study on analyzing user authentication behavior," in *IEEE Humans and Cyber Security Workshop (HACS 2019)*, 2019.

[10] S. Das, A. Kim, B. Jelen, J. Streiff, L. J. Camp, and L. Huber, "Towards implementing inclusive authentication technologies for older adults," *Who Are You*, 2019.

[11] S. Das, B. Wang, A. Kim, and L. J. Camp, "Mfa is a necessary chore! exploring user mental models of multi-factor authentication technologies," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020.

[12] J. S. Lee, H. Park, G. Y. Bang, and J. S. Song, "A password-based authentication by splitting roles of user interface," in *22nd ACM SIGSAC Conference on Computer and Communications Security, CCS 2015*. Association for Computing Machinery, 2015.

[13] K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse, ""They brought in the horrible key ring thing!" analysing the usability of two-factor authentication in UK online banking," *arXiv preprint arXiv:1501.04434*, 2015.

[14] S. Das, G. Russo, A. C. Dingman, J. Dev, O. Kenny, and L. J. Camp, "A qualitative study on usability and acceptability of yubico security key," in *Proceedings of the 7th Workshop on Socio-Technical Aspects in Security and Trust*. ACM, 2018, pp. 28–39.

[15] S. Das, B. Wang, and L. J. Camp, "Mfa is a waste of time! understanding negative connotation towards mfa applications via user generated content," in *Proceedings of the Thriteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[16] C. Braz and J.-M. Robert, "Security and usability: the case of the user authentication methods," in *IHM*, vol. 6, 2006, pp. 199–203.

[17] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0." in *USENIX Security Symposium*, vol. 348, 1999.

[18] M. Harbach, M. Hettig, S. Weber, and M. Smith, "Using personal examples to improve risk communication for security & privacy decisions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 2647–2656.

[19] S. Das, "A risk-reduction-based incentivization model for human-centered multi-factor authentication," Ph.D. dissertation, Indiana University, 2020.

[20] N. D. Weinstein, "Unrealistic optimism about future life events." *Journal of Personality and Social Psychology*, vol. 39, no. 5, p. 806, 1980.

[21] R. West, "The psychology of security," *Communications of the ACM*, vol. 51, no. 4, p. 34, 2008.

[22] L. J. Camp, "Mental models of privacy and security," *IEEE Technology and Society Magazine*, vol. 28, no. 3, pp. 37–46, 2009.

[23] S. Das, J. Abbott, S. Gopavaram, J. Blythe, and L. J. Camp, "User-centered risk communication for safer browsing," in *Proceedings of the First Asia USEC-Workshop on Usable Security, In Conjunction with the Twenty-Fourth International Conference International Conference on Financial Cryptography and Data Security*, 2020.

[24] M. Harbach, S. Fahl, and M. Smith, "Who's afraid of which bad wolf? a survey of it security risk awareness," in *2014 IEEE 27th Computer Security Foundations Symposium*. IEEE, 2014, pp. 97–110.

[25] R. Wash and M. M. Cooper, "Who provides phishing training? facts, stories, and people like me," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–12.

[26] R. Wash and E. Rader, "Influencing mental models of security: A research agenda," in *Proceedings of the 2011 New Security Paradigms Workshop*, 2011, pp. 57–66.

[27] M. Volkamer and K. Renaud, "Mental models–general introduction and review of their application to human-centred security," in *Number Theory and Cryptography*. Springer, 2013, pp. 255–280.

[28] J. Blythe and L. J. Camp, "Implementing mental models," in *2012 IEEE Symposium on Security and Privacy Workshops*. IEEE, 2012, pp. 86–90.

[29] H. Liang and Y. Xue, "Avoidance of information technology threats: A theoretical perspective," *MIS Quarterly*, pp. 71–90, 2009.

[30] T. Herath, R. Chen, J. Wang, K. Banjara, J. Wilbur, and H. R. Rao, "Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service," *Information Systems Journal*, vol. 24, no. 1, pp. 61–84, 2014.

[31] D.-L. Huang, P.-L. P. Rau, G. Salvendy, F. Gao, and J. Zhou, "Factors affecting perception of information security and their impacts on it adoption and security practices," *International Journal of Human-Computer Studies*, vol. 69, no. 12, pp. 870–883, 2011.

[32] R. Levin, "Uncertainty in risk assessment: contents and modes of communication," Ph.D. dissertation, KTH, 2005.

[33] Y. Albayram, M. M. H. Khan, T. Jensen, and N. Nguyen, ""... better to use a lock screen than to worry about saving a few seconds of time": Effect of fear appeal in the context of smartphone locking behavior," in *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS)*, 2017, pp. 49–63.

[34] Y. Albayram, M. M. H. Khan, and M. Fagan, "A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa)," *International Journal of Human–Computer Interaction*, vol. 33, no. 11, pp. 927–942, 2017.

[35] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computers & Security*, vol. 30, no. 4, pp. 208–220, 2011.

[36] S. Das, A. Dingman, and L. J. Camp, "Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key," in *2018 International Conference on Financial Cryptography and Data Security (FC)*, 2018.

[37] C. S. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in ebanking and the effects of experience," *Interacting with Computers*, vol. 22, no. 3, pp. 153–164, 2010.

[38] J. Reynolds, T. Smith, K. Reese, L. Dickinson, S. Ruoti, and K. Seamons, "A tale of two studies: The best and worst of yubikey usability," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 872–888.

[39] J. Colnago, S. Devlin, M. Oates, C. Swoopes, L. Bauer, L. Cranor, and N. Christin, ""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*. ACM, 2018, p. 456.

[40] E. D. Cristofaro, H. Du, J. Freudiger, and G. Norcie, "Two-factor or not two-factor? A comparative usability study of two-factor authentication," *Computing Research Repository*, vol. abs/1309.5344, 2014.

[41] P. Rajivan, P. Moriano, T. Kelley, and L. J. Camp, "Factors in an end user security expertise instrument," *Information Computer Security*, vol. 25, no. 2, pp. 190–205, 2017.

[42] V. Garg, L. J. Camp, K. Connelly, and L. Lorenzen-Huber, "Risk communication design: Video vs. text," in *Proceedings of the 12th International Conference on Privacy Enhancing Technologies*, ser. PETS'12. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 279–298.

[43] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, ""My data just goes everywhere": User mental models of the internet and implications for privacy and security," in *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS)*, 2015, pp. 39–52.

[44] M. A. Sasse, "Eliciting and describing users' models of computer systems," Ph.D. dissertation, University of Birmingham, 1997.

[45] "Five-second ads try to counter TiVo."

[46] J. 07, "Iab digital video ad effectiveness case study," Jun 2012. [Online]. Available: https://www.iab.com/insights/iab-digital-video-ad-effectiveness-case-study/

[47] T. Moore, R. Clayton, and R. Anderson, "The economics of online crime," *Journal of Economic Perspectives*, vol. 23, no. 3, pp. 3–20, 2009.

[48] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, "All about phishing: Exploring user research through a systematic literature review," *arXiv preprint arXiv:1908.05897*, 2019.

[49] P. Unchit, S. Das, A. Kim, and L. J. Camp, "Quantifying susceptibility to spear phishing in a high school environment using signal detection theory," in *International Symposium on Human Aspects of Information Security and Assurance*. Springer, 2020, pp. 109–120.

[50] N. Ismail, "Should people really trust their 'trusted' devices?" Nov 2017. [Online]. Available: https://www.information-age.com/really-trust-trusted-devices-123469662/

[51] P. A. Loscocco, S. D. Smalley, P. A. Muckelbauer, R. C. Taylor, S. J. Turner, and J. F. Farrell, "The inevitability of failure: The flawed assumption of security in modern computing environments," in *Proceedings of the 21st National Information Systems Security Conference*, vol. 10, 1998, pp. 303–314.

[52] J. M. Haney, M. Theofanos, Y. Acar, and S. S. Prettyman, ""We make it a big deal in the company": Security mindsets in organizations that develop cryptographic products," in *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS)*, 2018, pp. 357–373.

[53] J. M. Blythe, L. Coventry, and L. Little, "Unpacking security policy compliance: The motivators and barriers of employees' security behaviors," in *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, 2015, pp. 103–122.

[54] E. Vaziripour, J. Wu, M. O'Neill, D. Metro, J. Cockrell, T. Moffett, J. Whitehead, N. Bonner, K. Seamons, and D. Zappala, "Action needed! Helping users find and complete the authentication ceremony in signal," in *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS)*, 2018, pp. 47–62.

[55] E. Lastdrager, I. C. Gallardo, P. Hartel, and M. Junger, "How effective is anti-phishing training for children?" in *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS)*, 2017, pp. 229–239.

[56] R. Kumar and G. Gupta, "Forensic authentication of bank checks," in *IFIP International Conference on Digital Forensics*. Springer, 2016, pp. 311–322.