# Scaring People is Not Enough: An Examination of Fear Appeals within the Context of Promoting Good Password Hygiene

Marc Dupuis
Anna Jennings
marcjd@uw.edu
annajennings1@acm.org
University of Washington
Bothell, Washington, USA

Karen Renaud
University of Strathclyde
Glasgow, United Kingdom
cyber4humans@gmail.com

## ABSTRACT

Fear appeals have been used for thousands of years to scare people into engaging in a specific behavior or omitting an existing one. From religion, public health campaigns, political ads, and most recently, cybersecurity, fear appeals are believed to be effective tools. However, this assumption is often grounded in intuition rather than evidence. We know little about the specific contexts within which fear appeals may or may not work. In this study, we begin to examine various components of a fear appeal within the context of password hygiene. A large-scale randomized controlled experiment was conducted with one control and three treatment groups: (1) fear only; (2) measures needed and the efficacy of such measures, and (3) fear combined with measures needed and the efficacy of such measures. The results suggest that the most effective way to employ a fear appeal within the cybersecurity domain is by ensuring that fear is not used on its own. Instead, it is important that information on the measures needed to address the threat and the efficacy of such measures is used *in combination with* information about the nature of the threat. Since many individuals that enter the information technology profession become the *de facto* security person, it is important for information technology education programs to distill in students the inadequacy of fear, on its own, in motivating secure actions.

## CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; *Systems security*; *Software and application security*; *Security requirements.*

## KEYWORDS

security, privacy, passwords, fear appeals, password best practices

**ACM Reference Format:**

Marc Dupuis, Anna Jennings, and Karen Renaud. 2021. Scaring People is Not Enough: An Examination of Fear Appeals within the Context of Promoting Good Password Hygiene. In *Proceedings of the 22nd Annual Conference on Information Technology Education USB Stick (SIGITE '21), October 6–9, 2021, SnowBird, UT, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn


*SIGITE '21, October 6–9, 2021, SnowBird, UT, USA*

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

## 1 INTRODUCTION

Effective cybersecurity is necessary to protect digital information and systems from a variety of threats. Both individuals and organizations are at risk of having their information or systems compromised, whether from a malicious hacker, disgruntled employee, natural disaster, or hardware failure. However, cybersecurity is not a single process. Effective cybersecurity is a consolidation of processes, people, and technology all working together to protect digital assets.

Authentication is an important part of that process as it facilitates accountability and non-repudiation by validating an end user's identity. In the modern world, authentication usually involves a password: an alphanumeric string used to validate a user before granting access. According to some estimates, password-based authentication is the number one mechanism used to protect user accounts and personal information on web-based services [1].

While passwords have been present since the beginning of the modern computing era, fear appeals have been around even longer. For thousands of years, fear has been used to lead to a change in behavior. Fear appeals have been used by religions, in public health messaging, and cybersecurity, among others [26]. The problem is that the efficacy of fear appeals is taken for granted. It is rare for anyone to consider the fact that there is little solid empirical evidence as to their power in a wide range of contexts. It is important for the deployer to know when, how, where, why, and in what context the use of fear appeals may be most effective, desirable and ethical [11, 32].

While our study uses self-reports of behavioral intentions, we acknowledge the shortcomings associated with only measuring self-reports of behavioral intentions rather than observing or otherwise recording the actual behavior of individuals [29]. Nonetheless, the focus of this study is as a starting point to uncover future avenues for further research rather than as an end point.

In this study, we employ a randomized controlled between-subjects design with three treatment groups to test the efficacy of fear appeals in changing behavioral intentions with respect to three password hygiene target behaviors: 1) password length (10 characters or longer); 2) password reuse (passwords should be different for each website and system one logs into), and 3) password security (passwords should be kept safe and secure so they do not leak).

A large-scale survey (N=799) was used to answer the following research question: *What component(s) of a fear appeal are the most effective in causing a change in behavioral intentions related to password hygiene?* The following four experimental groups were used in this survey: (1) Control (N=202); (2) Fear only (N=201); (3) Measures needed and efficacy of those measures (N=196), and (4) Combined fear with measures needed and efficacy of those measures (N=201). Next, we discuss some of the related research on fear appeals and passwords.

## 2 RELATED RESEARCH

### 2.1 Fear Appeals

Fear is an emotion, and emotions, exert an influence on human behavior [6]. Fear is invoked when a threat exhibits a number of characteristics: it is important to the person, it is negatively valenced, impending, requiring effort to ameliorate with a specified action [26].

Fear is added to behavioral change appeals in the belief that the elicited fear will propel people to take protective action [6, 15]. The fear appeal recipient, it is argued, will carry out the desired recommended action to reduce the fear invoked by the appeal.

Renaud and Dupuis [26] reviewed the use of fear appeals to influence a range of cyber security behaviors. They found that the majority of the studies take a snapshot in time. Participants were presented with a fear appeal and then answered some questions and/or had their subsequent behavior observed. Very few studies returned to the participants after a significant period of time to determine the endurance of the fear appeal affect. None tested the feasibility of the behavior the fear appeal was trying to trigger.

A number of the reviewed studies used fear appeals in the password context [16, 17, 21, 22]. These generally detected a positive effect of the fear appeals, but mostly measured behavioral *intention* via a survey question or self-reported behaviors. The current study measures self-reports of behavior before the treatment (or control) and then behavioral intentions after the treatment (or control) has been completed. Although this study does not address all of the issues raised in Renaud and Dupuis [26], an important contribution of this study is to separate the core components of a fear appeal into two distinct elements, fear and efficacy.

Thus, we examine fear and efficacy treatments separately and combined, and then compare the resulting behavioral intentions with both one another and a control group. By doing so, we address one of the significant issues raised: a lack of examination of the nuances and contexts under which a fear appeal may be most effective.

### 2.2 Passwords

Most users seem to choose a password over other authentication methods likely due to its familiarity and the ubiquity of text entry mechanisms on all devices [31]. What makes a password different than other authentication methods is that it is something a user 'knows'. While some have delineated as many as five authentication classifications [18], the most common three kinds of authentication are: 1) something one knows; 2) something one has, and 3) something one is.

All of these are considered secure enough to protect accounts. Each has their own benefits and downsides, though the reason why most users choose to authenticate with a password is straightforward. Passwords are the most common option provided to users when setting up new accounts, and they are the easiest method of authentication to implement from the development side. When using a password, a user does not need a physical object to authenticate, which is preferred since such an object could be lost or stolen. With a password, a user simply needs to enter a memorized phrase or sequence of characters to authenticate themselves. Even though other authentication methods may be more secure or convenient, passwords remain the dominate form of authentication [1, 27].

Although passwords may be the most popular authentication method, one of their most significant weaknesses is that more than one person can possess the password at the same time [5]. In other forms of authentication (e.g., a fingerprint, token) it is improbable for more than one individual to possess the authentication needed to access the account. With the ease of use of passwords versus other forms of authentication comes a plethora of vulnerabilities. Despite these vulnerabilities, most individuals fail to use a tool known to mitigate many of the vulnerabilities inherent to passwords, such as a password manager [9].

There are generally simple rules related to password format. These rules depend on the program or application being used. Some allow for the use of numerical and special characters, while others only allow for the use of alpha-numeric characters. Frequently, a user will be given a minimum length for their password. For several years, it was 6 characters. Today, users see minimums ranging from eight to 10 characters. This change in the lower limit comes from studies demonstrating that the shorter the password, the weaker it is. Many security experts recommend passwords a minimum of 15-20 characters [5]. Length may be achieved through a variety of approaches, such as combining several unrelated words together or using a password manager to generate one.

The common practice with passwords is using a word or phrase that is easy for the user to remember. However, many system impose complexity requirements on passwords. Having a mix of characters that are upper- and lower-case letters, numbers, and a variety of special characters are elements that add to the complexity of a password. However, such complexity makes it challenging to remember the password, which might lead users to write them down, thus weakening the password. Proponents of the complexity factor may argue that a strong password ends up looking like a cat walked across a keyboard and recorded every key it touched. Nonetheless, there is also ample disagreement related to the emphasis that should be placed on the complexity of the password [25]. Many approaches have been employed to encourage users to create stronger passwords, including varying the type of feedback provided by a password meter [10] or the development of passwords with graphical elements to increase the entropy in a more manageable way cognitively for the end user [12]. However, it is ultimately up to the end user whether or not they will create strong and unique passwords across different systems for which they have credentials.

Third, password reuse is a significant problem. Password reuse occurs when someone uses the same password for more than one account, which has become increasingly prevalent [13]. Such reuse

may often be the result of a compromise a typical user makes with the length and complexity factors previously noted. If a user creates a long and complex password, how can they be expected to not reuse this password but instead repeat the process for every website and system they login to, even if they have success doing it once [4]? The human brain simply cannot do this. Finally, it is important that users keep their passwords safe and secure from others, whether it be from a friend or would-be attackers [30].

# 3 METHODS

## 3.1 Participants

Institutional Review Board (IRB) approval was obtained prior to collecting data from participants in this study. A survey was deployed on the Qualtrics survey platform with recruitment done using Amazon's Mechanical Turk (MTurk). MTurk has been shown to be a reliable and efficient method to recruit research participants, but it is important to employ various quality control measures [8, 28].

In this particular study, we used two automated quality control questions, which would end the survey for the participant if either of the questions were answered incorrectly. An open-ended question toward the end of the survey was also used as a *de facto* quality control question, which helps to detect for automation in the completion of surveys. Additionally, for the video portion of the survey, an embedded timer was used that would not allow the participant to advance the survey until a time consistent with that of the video being shown had elapsed. Finally, MTurk workers were eligible to participate if they had an approval rate of 98% or higher and had successfully completed at least 1,000 prior HITs (human intelligence tasks).

Participants were compensated with $2.50 for their time. 91.2% of participants felt that the compensation provided was either comparable (69.9%) or easier for the money (21.3%) when compared to other projects they had completed on MTurk. The remaining 8.8% felt that more effort was required when compared to other projects.

A total of 811 participants began the survey with 9 participants failing one of the two automated quality control questions and another three participants failed an open-ended question that served as an additional quality check. Thus, 1.5% of participants that began the survey failed quality control measures in place. This resulted in 799 usable responses to the survey that would be used for subsequent analysis.

Slightly over half of our participants identified as male (51.2%) with the remaining participants identifying as female (47.8%), nonbinary or third gender (0.6%), or preferred not to say (0.4%). Most participants identified as White (77.2%), followed by Asian / Pacific Islander (8.4%), Black / African American (8.1%), Hispanic (4.3%), Other / Multi-Racial (1.6%), and Native American / Alaskan Native / Indigenous (0.4%). Slightly less than half (45.1%) of the participants were between the age of 18 and 39 with the remaining participants (54.9%) 40 or older.

As noted earlier, a fear appeal must have information on the nature of the threat, the measures necessary to counter the threat, and the efficacy of those measures. Our interest in this study was to examine differences in intentions related to individuals that were in one of four conditions (a control and three treatment conditions): 1) Control (N=202); 2) Fear only (N=201); 3) Measures needed and efficacy of those measures (N=195), and 4) Combined fear with measures needed and efficacy of those measures (N=201). A between-subjects design with random assignment to one of the four groups was employed.

## 3.2 Materials

Participants were provided with a video to watch commensurate with the group they were randomly assigned to by the Qualtrics survey platform.

*3.2.1 Control group.* A video was developed that had no specific message and included background music that was considered neutral in tone. The video consisted of various short clips of scenery, cars driving, sand in the desert, etc. The length of the video (2:05) was approximately the same length as the videos for treatment groups two and three. It may be found at the following URL: https://youtu.be/E1UViIQRqQU

*3.2.2 Fear only.* For the fear only group, emphasis was placed on communicating the likelihood and severity of passwords being compromised. Information was presented on several different breaches that have occurred and how those breaches may result in further passwords being compromised. Likewise, information was presented on other ways passwords could become compromised, such as making it easy for an attacker to crack a password by using short ones. The length of this video was 2:29. Please see Figure 1. It may be found at the following URL: https://youtu.be/xPu-V7oMXJQ


**Figure 1: Screenshot of Fear Only Video with Examples of Passwords being Compromised Flashing Across the Screen**

*3.2.3 Measures needed and efficacy of those measures.* The efficacy group detailed measures that can be taken to prevent a password from being compromised and the efficacy (i.e., self and response) and costs (i.e., time, energy, effort) associated with those measures. We focused on three specific components of good password hygiene: 1) length (10 characters long or longer); 2) Unique passwords for different websites and systems, and 3) Secure: the password should be kept safe and secure from others. A mnemonic was developed to communicate these measures: P-L-U-S, which meant that passwords should be long, unique, and secure. While there are ample views on what should be communicated to individuals with respect to password hygiene, there remains vast disagreement with the specific components that should be included and why [25].

Ultimately, the three above factors were chosen as they appeared to have the most agreement and the least amount of disagreement among experts.

Using a password manager was the focus of the measures that could be taken. A brief demo was incorporated into this video to show how simple it is to use a password manager and what it is capable of. However, an additional measure was also detailed: combining six or more unrelated words together, including the possibility of making it even more complex by capitalizing some of the characters and/or incorporating special characters into the password. The length of this video was 2:05. Please see Figure 2. It may be found at the following URL: https://youtu.be/Lao1UTO2ogA

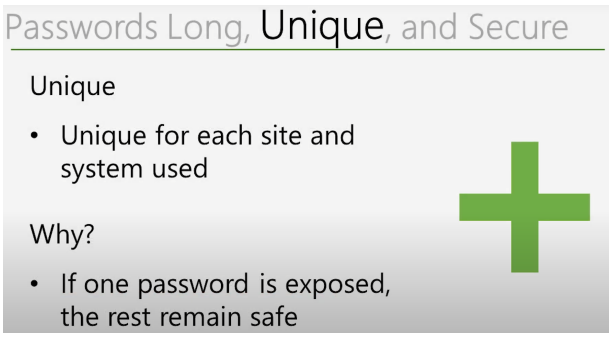


**Figure 2: Screenshot of Efficacy Only Video with Uniqueness of a Password Emphasized and Why**

*3.2.4 Combined fear with measures needed and efficacy of those measures.* The final group combined the messaging from groups two and three by merging the two separate videos into a single video. It began with the fear messaging followed by the efficacy messaging. The length of the combined video was 4:34. It may be found at the following URL: https://youtu.be/VhqfR_ruAjQ

## 4 RESULTS AND ANALYSIS

Analysis was conducted using IBM's Statistical Package for Social Sciences (SPSS) version 19.0. The focus of our analysis was to determine what effect, if any, the different videos that were developed for this study may have had on our participants. Prior to a video being shown to the participants, we asked them how confident they were that they were performing the target behaviors. Next, we discuss the results of this analysis followed by the results of questions related to behavioral intention that were asked after they watched a video.

### 4.1 Pre-Treatment Analyses

A one-way between subjects ANOVA was performed to conduct an a priori analysis of whether there was a statistically significant difference between any of the four experimental groups in this study: 1) Control Group; 2) Fear Only Group; 3) Efficacy Only Group, and 4) Fear and Efficacy Combined Group. There was no significant difference between any of the four groups and the three items (10 characters long or longer; unique, and kept secure) assessed before the treatment was applied. This suggests that any effect found after the treatment was applied is likely the result of the treatment itself.

### 4.2 Post-Treatment Analyses

*4.2.1 Long Passwords (10 characters in length or longer).* A one-way between subjects ANOVA was conducted to compare the effect of various components of a fear appeal on intentions to create a password that is at least 10 characters long or longer in no fear appeal components, fear only, efficacy only, and combined fear and efficacy components conditions. There was a significant effect of fear appeal components on intention to create long passwords for the websites and systems one logs into at the $p<.05$ level for the four conditions [$F(3,795) = 9.601$, $p < .001$]. Post hoc comparisons using the Tukey HSD test indicated that the mean score for the no fear appeal components (M=3.97, SD=1.167) was significantly different than the fear only (M=4.30, SD=0.918), efficacy only (M=4.30, SD=0.808), and combined fear and efficacy components (M=4.45, SD=0.747) conditions. However, the three treatment group conditions did not significantly differ from one another.

Taken together, these results suggest that implementing at least one fear control component (fear only, efficacy only, or a combined fear and efficacy) is more effective in creating behavioral intentions toward individuals creating long passwords compared to the control. Additionally, while the mean for the combined fear and efficacy components was not statistically different when compared to the other two treatment groups, it was higher than both (M=4.45, SD=0.747). This implies that the most effective way to use a fear appeal is to ensure that all components of a fear appeal are employed: information on the threat, including one's susceptibility to it and the level of severity should one become a victim to the threat and information on efficacy, including their ability to take effective measures to combat the threat, the effectiveness of those measures, and the amount of time, energy, and effort involved.

*4.2.2 Unique Passwords.* A one-way between subjects ANOVA was conducted to compare the effect of various components of a fear appeal on intentions to create a password that is unique across different sites and systems in no fear appeal components, fear only, efficacy only, and combined fear and efficacy components conditions. There was not a significant effect of fear appeal components on intention to create unique passwords for the websites and systems one logs into at the $p<.05$ level for the four conditions [$F(3,795)=1.933$, $p=.123$].

*4.2.3 Secure (passwords kept safe and secure from others).* A one-way between subjects ANOVA was conducted to compare the effect of various components of a fear appeal on intentions to keep passwords safe and secure from others in no fear appeal components, fear only, efficacy only, and combined fear and efficacy components conditions. There was a significant effect of fear appeal components on intention to keep one's passwords safe and secure at the $p<.05$ level for the four conditions [$F(3,795) = 2.648$, $p = .048$]. Post hoc comparisons using the Tukey HSD test indicated that the mean score for the no fear appeal components (M=4.61, SD=0.706) was significantly different than the combined fear and efficacy components condition (M=4.77, SD=0.466) conditions. However, no other statistically significant results were observed between the groups.

Taken together, these results suggest that implementing a combined fear and efficacy appeal is more effective than the control in creating behavioral intentions toward individuals keeping their

passwords safe and secure. This is consistent with what we observed with the first targeted behavior, password length.

# 5 DISCUSSION

## 5.1 Implications

This study provides important insight into the use of fear appeals within the cybersecurity domain. It demonstrated that providing messaging on the nature of a threat, what can be done to address the threat, and the efficacy of those measures may help engender behavioral change toward the targeted behavior(s). In this particular study, the use of fear appeal components was effective with respect to causing a difference in behavioral intention toward creating long passwords when compared to the control group. It was also found to be effective for keeping passwords safe and secure when both the fear and efficacy aspects of a fear appeal were employed together.

Thus, for something as simple *and* complicated as passwords, we should not expect a single fear appeal to work equally well for all desired behaviors. By measuring and examining the target behaviors individually, we were able to demonstrate that like many behaviors in life, whether inside or outside of cybersecurity, causing a change in behavior (or behavioral intention) is difficult and complicated.

Our goal may be to improve the cybersecurity hygiene of individuals. However, cybersecurity hygiene itself consists of many different components, including password use. As we delve into password hygiene then, we also see that it consists of many different elements—not all of which can be changed to the same degree and by the same methods.

Additionally, focusing on efficacy alone was not effective by itself for two of the three targeted behaviors. It is likely that the nature of efficacy makes it a complicated factor to address in a two-minute video. Not only do the measures needed to address the threat have to be delineated, but the costs, efficacy of those measures (i.e., response efficacy), and the ability of the individual (i.e., self-efficacy) to enact those measures must also be addressed. As noted earlier, self-efficacy has consistently been shown to be the most effective construct in predicting behavioral intentions and actual behavior. Increasing one's belief in being able to perform a certain task may take time, training, and repeated interventions. This may explain in part why efficacy alone was only effective for creating long passwords and not more effective than fear alone or the combined group. It is also possible that increases in efficacy would be longer lasting than invoking fear, which is a short-term emotion.

## 5.2 Ethical Considerations

In deploying fear in any cybersecurity context, it is important not to ignore ethical considerations. Dupuis and Renaud [11] proposed six ethical principles to guide cybersecurity fear appeal experiments and deployment. These are (1) obtain IRB approval, (2) make the benefits of cybersecurity salient, (3) only use deception if it can be rigorously justified, (4) provide a feasible recommended action (with the implication that feasibility will be verified), (5) calibrate during deployment (with the implication that the option to cease and desist will be considered if undue negative consequences are evident), and (6) debrief targets of fear appeals. If the fear appeal cannot be used within these constraints, deployers should carefully re-consider going ahead with the use of fear appeals.

## 5.3 Limitations

There are several limitations worth noting. First, this was a single survey using a crowd-sourced participant pool. While compensation was considered fair by most, MTurk workers do have an incentive to complete the work as quickly as possible. Thus, some responses and their overall attention may not be optimal for the messaging being delivered.

Second, data was collected for this study via a survey and no other method. Thus, common method bias is a concern [19, 24]. Multiple quality control procedures were implemented to help address this concern. Additionally, the participant population is essentially anonymous to the research team. Thus, while certain elements of the procedures employed and participant pool used help to minimize the likelihood that common method bias was a significant factor in the results obtained, it remains a concern nonetheless.

Third, the data collected comes from a single snapshot in time for our participants. This was not a longitudinal study and we do not know whether the difference in behavioral intentions lasted beyond the completion of the survey. Likewise, we do not know if the behavioral intentions themselves resulted in any actual change in behavior. The measurement of behavioral intentions is inherently flawed and historically has been problematic in the prediction of actual behavior [29]. We do not want to overstate the results and suggest they provide conclusive evidence one way or the other. Instead, they do provide a useful starting point to examine actual behavior in a variety of contexts, especially when fear appeals are employed.

Finally, we do not know if any emotional harm resulted from the fear that was employed. While this study was considered low risk and approved as exempt from a full IRB review, part of the challenge with using fear appeals is the balance between possible efficacy and possible harm that may result for some from being scared into doing something.

# 6 CONCLUSION

In the world of information technology education, it can be easy to focus on the hardware and software systems employed in a typical organizational setting. However, ultimately people use these systems to accomplish tasks deemed important or necessary by other people. Keeping these systems running efficiently without interruption inherently requires that they also be kept safe and secure. Therefore, information technology education cannot and should not divorce itself from either security or human factors of security. The professionals that are being trained in information technology programs will often find themselves tasked with both the security and security training aspects of the profession.

These individuals must take care in ensuring that any security education, training, or awareness (SETA) program that employs fear to provide information on the nature of a threat, must also inform the user how to mitigate the threat and address the efficacy of those measures, including both response and self-efficacy. It is also important to ensure that the action is indeed feasible for that particular user. Given the importance of self-efficacy across

a variety of domains [2, 3, 14, 20], it is important that this issue is not ignored with respect to mitigation efforts.

Beyond the organizational setting, additional efforts are needed in the design of systems, including making security an integral part of the design process [23]. It will also be helpful to focus more energy in providing introductory cybersecurity education to individuals at the undergraduate level in addition to other settings [7]. There is not a single simple solution to the security challenges we face, including those with passwords. However, the use of fear appeals to engender behavioral change is not the panacea it is often made out to be.

## REFERENCES


[1] Mashael AlSabah, Gabriele Oligeri, and Ryan Riley. 2018. Your culture is in your password: An analysis of a demographically-diverse password dataset. *Elsevier* 77, Computers & Security (Aug 2018), 427–441.

[2] Albert Bandura. 1977. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review* 84, 2 (1977), 191–215.

[3] Albert Bandura. 2001. Social cognitive theory: An agentic perspective. *Annual review of psychology* 52, 1 (2001), 1–26.

[4] Joseph Bonneau and Stuart Schechter. 2014. Towards Reliable Storage of 56-bit Secrets in Human Memory. In *Proceedings of the 23rd USENIX Conference on Security Symposium (SEC'14)*. USENIX Association, 607–623. http://dl.acm.org/citation.cfm?id=2671225.2671264

[5] Mark Burnett. 2006. *Perfect Passwords*. Syngress.

[6] James Price Dillard. 1994. Rethinking the study of fear appeals: An emotional perspective. *Communication Theory* 4, 4 (1994), 295–323.

[7] Marc Dupuis. 2017. Cyber Security for Everyone: An Introductory Course for Non-Technical Majors. *Journal of Cybersecurity Education, Research, and Practice* 2017, 1, Article 3 (2017), 17.

[8] Marc Dupuis, Barbara Endicott-Popovsky, and Robert Crossler. 2013. An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud. In *International Conference on Cloud Security Management*.

[9] Marc Dupuis, Tamara Geiger, Marshelle Slayton, and Frances Dewing. 2019. The Use and Non-Use of Cybersecurity Tools Among Consumers: Do They Want Help?. In *Proceedings of The 20th Annual Conference on Information Technology Education (SIGITE '19)*. ACM, 81–86. https://doi.org/10.1145/3349266.3351419

[10] Marc Dupuis and Faisal Khan. 2018. Effects of peer feedback on password strength. In *2018 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 1–9. https://doi.org/10.1109/ECRIME.2018.8376210

[11] Marc Dupuis and Karen Renaud. 2020. Scoping the ethical principles of cybersecurity fear appeals. *Ethics and Information Technology* (2020), 1–20.

[12] Marc J. Dupuis, Jaynie Shorb, James Walker, Fred B. Holt, and Michael McIntosh. 2020. Do You See What I See? The Use of Visual Passwords for Authentication. In *Proceedings of the 21st Annual Conference on Information Technology Education*. ACM, 58–61.

[13] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences* 7, 1 (Mar 2017), 1–20.

[14] Donna L. Floyd, Steven Prentice-Dunn, and Ronald W. Rogers. 2000. A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology* 30, 2 (2000), 407.

[15] Nico H Frijda, Peter Kuipers, and Elisabeth Ter Schure. 1989. Relations among emotion, appraisal, and emotional action readiness. *Journal of Personality and Social Psychology* 57, 2 (1989), 212–228.

[16] Jeffrey L Jenkins, Mark Grimes, Jeffrey Gainer Proudfoot, and Paul Benjamin Lowry. 2014. Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development* 20, 2 (2014), 196–213.

[17] Allen C. Johnston, Merrill Warkentin, and Mikko Siponen. 2015. An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly* 39, 1 (Mar 2015), 113–134.

[18] Kim. 2016. *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning.

[19] Scott B. MacKenzie and Philip M. Podsakoff. 2012. Common method bias in marketing: Causes, mechanisms, and procedural remedies. *Journal of retailing* 88, 4 (2012), 542–555.

[20] James E. Maddux and Ronald W. Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology* 19, 5 (1983), 469–479.

[21] Florence Mwagwabi, Tanya McGill, and Michael Dixon. 2014. Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines. In *47th Hawaii International Conference on System Sciences*. IEEE, 3188–3197. https://doi.org/10.1109/HICSS.2014.396

[22] Florence Mwagwabi, Tanya J. McGill, and Mike Dixon. 2018. Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines. *Communications of the Association for Information Systems* 42, 7 (Feb 2018), 147–182. https://doi.org/10.17705/1CAIS.04207

[23] Jessica Nguyen and Marc Dupuis. 2019. Closing the Feedback Loop Between UX Design, Software Development, Security Engineering, and Operations. In *Proceedings of The 20th Annual Conference on Information Technology Education (SIGITE '19)*. ACM, 93–98. https://doi.org/10.1145/3349266.3351420

[24] Philip M. Podsakoff, Scott B. MacKenzie, Jeong-Yeon Lee, and Nathan P. Podsakoff. 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology* 88, 5 (2003), 879–903.

[25] Suzanne Prior and Karen Renaud. 2020. Age-appropriate password "best practice" ontologies for early educators and parents. *International Journal of Child-Computer Interaction* 23 (2020), 100169.

[26] Karen Renaud and Marc Dupuis. 2019. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop*. 42–56.

[27] Chao Shen, Tianwen Yu, Haodi Xu, Gengshan Yang, and Xiaohong Guan. 2016. User practice in password security: An empirical study of real-life passwords in the wild. *Computers and Security* 61 (Aug 2016), 130–141.

[28] Zachary R. Steelman, Bryan I. Hammer, and Moez Limayem. 2014. Data Collection in the Digital Age: Innovative Alternatives to Student Samples. *MIS Quarterly* 38, 2 (2014), 355–378.

[29] Jiming Wu and Hongwei Du. 2012. Toward a better understanding of behavioral intention and system usage constructs. *European Journal of Information Systems* 21, 6 (Nov 2012), 680–698. https://doi.org/10.1057/ejis.2012.15

[30] J. Yan, A. Blackwell, R. Anderson, and A. Grant. 2004. Password memorability and security: empirical results. *IEEE Security & Privacy Magazine* 2, 5 (2004), 25–31.

[31] Verena Zimmermann and Nina Gerber. 2020. The password is dead, long live the password–A laboratory study on user perceptions of authentication schemes. *International Journal of Human-Computer Studies* 133 (2020), 26–44.

[32] Verena Zimmermann and Karen Renaud. 2021. The nudge puzzle: matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 1 (2021), 1–45.


## A SURVEY QUESTIONS

**Demographics**

(1) What gender do you most closely identify with?
(2) What ethnicity do you primarily identify with?
(3) What is your current age?

**Please indicate the extent to which you agree with each of the following statements (Strongly Disagree - Disagree - Neither Agree nor Disagree - Agree - Strongly Agree):**

(1) I am confident that I currently use long passwords of at least 10 characters for the websites and systems I login to.
(2) I am confident that I currently use unique (i.e., different) passwords for the websites and systems I login to.
(3) I am confident that I currently keep my passwords safe and secure from others.

**Please indicate the extent to which you agree with each of the following statements (Strongly Disagree - Disagree - Neither Agree nor Disagree - Agree - Strongly Agree):**

(1) I intend to use long passwords of at least 10 characters for the websites and systems I login to.
(2) I intend to use unique (i.e., different) passwords for the websites and systems I login to.
(3) I intend to keep my passwords safe and secure from others.