Empathy as a Response to Frustration in Password Choice

Kovila P.L. Coopamootoo [⋆]

Newcastle University, UK
kovila.coopamootoo@newcastle.ac.uk

Abstract. Previous research often reports that password-based security is frustrating, irritating or annoying, and as a result it often leads to weak password choices. We investigated the impact of empathy as a countermeasure to the anger-related states. We designed an online study with N=194 participants. The experimental group received an empathic message while the control group did not. Participants presented with the empathic message created significantly stronger passwords than those who did not receive the message. Our finding differs from previous research because it shows participants creating stronger passwords with an empathic response to anger arousal. This antidote to frustrated states with regards to password choice provides an initial step towards more supportive and emotionally intelligent security designs.

Keywords: password, security, emotion, user, choice, frustration, anger, empathy

1 Introduction

Frustration is an emotional state resulting from "the occurence of an obstacle that prevent[s] the satisfaction of a need" [3]. Frustration is the most common precursor and often an elicitor of anger [29]. Frustration, annoyance and irritation are emotional states of anger emotion.

User experience of frustration with information security is nowadays well known. For example, Furnell & Thompson discussed security controls that 'annoy', 'frustrate', 'perturb', 'irritate' users as well providing an effort overhead [13]. Stanton et al. observed that users feel weary of being bombarded by warning, feel bothered of being locked out for mistyped passwords, and describing security as 'irritating', 'annoying', and 'frustrating', together with being cumbersome, overwhelming [34] .

With regards to password security, user discontent has been observed when forced to adhere to password policies [17, 21], and annoyance by the shift to

[⋆] Kovila P.L. Coopamootoo, Empathy as a Response to Frustration in Password Choice: Proceedings of AsiaUSEC'20, Financial Cryptography and Data Security 2020 (FC). February 14, 2020 Kota Kinabalu, Sabah, Malaysia Springer, 2020 stricter password policies [27,32]. Passwords chosen following annoyance due to stricter policies were 46% more likely to be guessed [27].

We posit that user frustration and annoyance with password security are here to stay because (1) passwords as a simple method of authentication is both widely used and is easy to implement, and (2) frustration triggered with password security is mainly due to complexity requirements that contributes to strong passwords.

However, security research has yet to respond to the challenges posed by the emotions induced during interaction, as well as their consequences. Meanwhile, the HCI community has proposed lines of research that address the impact of emotions while interacting with computers, such as affective computing [31] and empathic designs [40].

On the user side, individuals have the skills to manage and regulate emotional states and employ coping strategies [14], including passive methods that do not address the emotion themselves such as interacting with the media, consuming food or alcohol, and active methods where people discuss or address their emotions directly as a means of managing them, such as active listening and empathy.

As a way to respond to anger-related states in security, we propose empathy as an affective response and investigate the main RQ "How does empathizing with users impact security behavior, in particular, password choice?" via an online study reported in this paper.

We observe stronger password choices in the empathy condition, with reported anger acting as a positive confounder to password strength. We also report in detail how password characteristics impact emotions, where the odds of inducing a higher level of anger with a unit increase in password length, number of digits and lowercase letters, and password strength, range from 12% to 31%. We therefore offer a first step towards more supportive and emotion-intelligent security designs, as well as provide a deeper understanding of the emotions involved with password choice.

In the rest of the paper, we first present background literature followed with the aim, research questions, procedure and methods of the study, followed by the results and discussion sections. We end the paper with a limitation and a conclusion section.

2 Background

2.1 User Password

Text passwords are created by users as an authentication token that only they know. To combat the inherent and user-induced weaknesses of text passwords, administrators and organisations typically set a series of rules - via a password policy - to which users must adhere when choosing a password. Users develop strategies to cope with password policies. For example, users do not create entirely new passwords, as shown by a study where only 30% of respondents did create an entirely new password when presented with a stronger password requirements [32]. Most users also reuse passwords across sites, where reuse by a student population is 100% [1] and in the general population ranging from 34.6 to 82%) [1, 23]. Users are thought to maintain between 3 (32%) to 5 (24%) distinct passwords only [4]. Another coping strategy involves transformation rules, such as to always pick the same number, or always place a number in the same location in their passwords [32].

Individuals cope with negative emotions via different strategies, where coping is conceptualized as cognitive and behavioral efforts to manage specific external and/or internal demands that are appraised as taxing or exceeding the resources of the person [24]. Two broad classes of coping methods are usually identified, that is either emotion or problem-focused coping. The problem-focused strategy consists of efforts to maintain concentration on the steps needed to fulfill task requirements. Therefore, when individuals remain focused on the task rather than on the damage done by a negative event, they are likely to buffer the adverse effect of negative emotion on their behavior and performance [7].

2.2 Empathy

Baron-Cohen & Wheelwright defined empathy as, 'the drive to identify another person's emotions and thoughts, and to respond to these with an appropriate emotion' (p. 361) [5]. In short, empathy is the ability to feel for someone else. It differs from sympathy. While sympathy refers to an understanding of what another is going through, empathy is an emotional response, that is how someone feels in response to others' situations [19].

Researchers distinguish between dispositional and situational empathy [35]. Dispositional empathy, also known as trait empathy, is the tendency for people to imagine and experience the feelings and experiences of others. In contrast, state or situational empathy, is an immediate response to a specific eliciting situation.

2.3 Frustration Regulation

Computer interaction often has unpleasant side effects including strong, negative emotional states such as frustration, confusion, anxiety, that not only affect the interaction itself, but may also impact productivity, learning, social relationships, and overall well-being. In consequence, computing research have designed meaningful ways to respond to negative emotions such as frustration, thereby supporting users to manage and regulate their emotions. As example, Klein et al. [22] investigated the impact of ignoring emotions, enabling individuals to vent their feelings versus providing an active affect-support agent with components of active listening, empathy and sympathy, where continued interaction resulted with the agent.

3 Aim

We provide the research questions and hypotheses under investigation.

3.1 Impact of Empathy on Password Choice

Empathy has been used as a response to user frustration, or the negative feelings that arise from interacting with computers before [22]. These are in the form of text dialogue and empathic agents that supports emotion regulation of frustration states [18].

We investigate the influence of empathizing with users on password choice via RQ-E "*How does empathizing with users impact password strength?*" We define the hypotheses $H_{E,0}$: "Empathizing with users does not impact password strength'. $H_{E,1}$: "Empathizing with users impacts password strength".

3.2 Impact of Password Characteristics on Emotions

While password security is often thought to involve negative emotions, we are yet to determine the fine-grained details of how password characteristics (such as strength, length and number of characters) evoke anger and other emotions.

We investigate how password characteristics are linked with the extent of emotions induced via RQ-D "*How does password characteristics influence reports of emotions*?" We define the hypotheses $H_{D,0}$: "Password characteristics do not influence reports of emotions". $H_{D,1}$: "Password characteristics influence reports of emotions".

4 Methodology

We designed a between-subject online experiment, where participants were assigned to either of the two conditions, namely the empathy experimental condition or the control condition. We measure password strength as the main dependent variable.

We diligently follow the good practice guidelines for empirical research in security and privacy [8,9,25,30], themselves founded on scientific hallmarks. *First* we replicated validated methods using the standard questionnaires described later in Section 4.5. *Second*, we define research questions and hypotheses at the fore in Section 3 and discuss limitations in Section 6. *Third*, we follow the standard APA Guidelines [2] to report statistical analyses, and we report on effect sizes, assumptions and test constraints.

4.1 Sample Participants

We recruited participants from the Amazon Mechanical Turk (MTurk) crowdsourcing service. MTurk has extensively contributed to user studies before, including that for password research [23]. Passwords created via MTurk in previous studies have been found to be comparable to those of controlled lab studies [27] and in general 70% of study passwords are at least somewhat comparable with real world passwords [12].

With the study lasting on average 20 minutes and no more than 40 minutes, participants were remunerated with $1.5 for their time. This is well within the payment frame for MTurk workers, where $2 per hour has been suggested [16].

The sample $N = 194$ participants consisted of 99 male and 95 female. The mean age = 37.43, $sd = 10.922$. 36.3% of the participants had at least an undergraduate education level, 29.3% graduated from college while 32.3% graduated from high school and 2% either did not graduate from high school or did not attend school. 13.6% of the participants reported a computer science related education background.

We aimed for 50% of the participants to be randomly assigned to the empathy condition and 50% to the control condition. However, 6 participants were excluded due to not fully completing the questionnaires. We consequently ended up with $N = 99$ assigned to the empathy condition and $N = 95$ to the control condition.

4.2 Procedure

The procedure consisted of (1) a pre-task questionnaire for demographics, (2) introduction to the email scenario, (3) either the empathy manipulation or the control (4) a task to enter the chosen password, (5) the password reuse, the brief mood inventory and the empathy quotient questionnaires, Figure 1 depicts the experiment design. We discuss the ecological validity in the Discussion, Section 6.

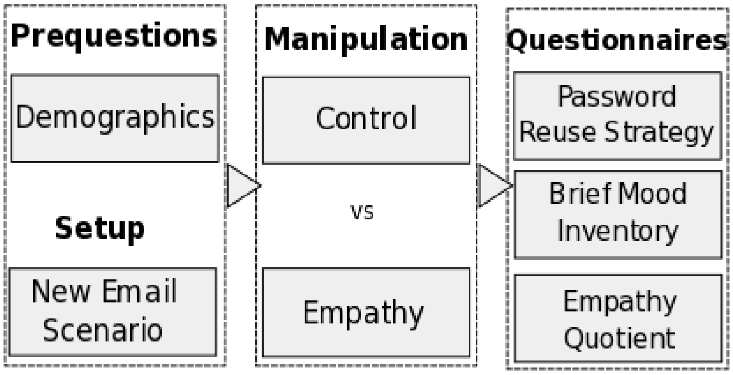

Fig. 1: Experiment design.

4.3 Scenario

Setting: We designed a scenario to choose a password similar to Das et al. [4] where participants were asked to assume they are creating a new account on a new email system where they would also create a password. Instead of asking participants to only think about the password as in Das et al. we adapted the scenario to typing the password into the survey. In particular we ask participants: *"For the following questions, imagine that you are creating a new account on a new email system"*.

Password Policy: Compared to Das et al. who set the new email system to www.bestmail.com with no password policy suggested, our scenario did not focus on a particular email system. We however focused on a password policy suggestion set to the password complexity of mail.google.com, that is, eight or more characters long including digits, uppercase letters and symbols [20]. In both conditions, participants were then presented with the message *"Our questions will focus on the password you choose for this new account, where you can use 8 or more characters with a mix of letters, numbers & symbols for security"*.

We chose GMail's password policy because it is the most widely used email account and we assumed that most participants would have heard of such a password policy before. The GMail password policy suggestion also fits that of other email system requirements, where passwords created following the suggested policy may also comply with policies for shopping and financial websites [4].

Password ReUse: Similar to Das et al.'s study, we query participants about reuse of an existing password. We asked participants to select from three options for reuse strategy. We used the same items as Das et al [4].

4.4 Manipulation

We designed a static text message as the empathy manipulation. The empathy message said *"We empathize with you that choosing a complex password can sometimes feel frustrating, annoying and cumbersome, yet take your time to create your password"*. In contrast, the control message said *"Take your time to create your password"*.

Framing: The empathy message was framed (1) to acknowledge feelings of frustration that specifically arise with password complexity requirements; (2) to clearly empathize with participants about such feelings, rather than ignoring these feelings or blaming participants; (3) to propose a course of action even if participants may be frustrated, thus to avoid them using the empathy message as an excuse or permission to not act.

Cognitive Empathy: An empathetic response to another person's situation or emotional state, can take the form of cognitive empathy (mental perspective taking, understanding of the other) or emotional empathy (vicarious sharing of emotions) [33]. As a first and simple step towards investigating the impact of empathy with regards to security, we chose to employ a cognitive empathy response rather than an emotional one.

Empathic Accuracy: In providing a verbal response to individuals' emotions, it is important to communicate empathy within the context as accurately as possible to avoid negative consequences [10, 19]. As a result, we focused the empathy message to 'complex passwords', as feelings of frustration from strict policies have previously been reported in research [27], rather than leaving it open to *"choosing a password"* or security in general.

Priming: We ensured that both conditions were similarly primed towards security with the same password policy suggestion via the phrase *"for security"*.

4.5 Measurements

Emotion: To measure moods and emotions, previous security and privacy research [15, 28] have employed the short form of the Brief Mood Introspection Scale (BMIS) [6, 26] or PANAS-X [37]. We set the time boundary of the elicitation to "How do you feel right now?" We use the short form of the BMIS, the brief mood inventory (BMI) in this study, including the 8 dimensions, "I feel" ... (a) excited, (b) thoughtful, (c) tired, (d) happy, (e) worn out, (f) sad, (g) angry, and (h) calm. We used *bmi_angry* as elicitation of the anger-related emotional states of frustration, annoyance, or irritation, that have previously been mentioned with respect to security. We added three items as manipulation check for the empathy condition. These were (a) that I am understood, (b) that my condition is received, and (c) that I am cared for. These are to measure participants' receiving of the empathic message. We adapted the 5-point Likert-type items to that used within the 60-item PANAS-X anchored on 1 - "very slightly or not at all", 2 - "a little", 3 - "moderately", 4 - "quite a bit" and 5 - "extremely".

Password Strength: We measured password strength via $\log_{10}$ number of password guesses and an ordinal value from 0 to 4 of password strength via zxcvbn [39]. zxcvbn is a client-side password strength checker developed by Dropbox and is open-sourced. We chose zxcvbn as it employs advanced heuristics [36], and it considers the composition of a password more thoroughly than other checkers, providing a realistic evaluation of the complexity of the password [11].

Empathy: In addition to demographics information, we measured dispositional empathy via the Empathy Quotient (EQ) questionnaire [5]. Dispositional empathy is related to personality trait, and refers to an individual's propensity to empathize with others, that is to give empathy. The EQ has been used across a variety of populations including people with asperger's syndrome. The EQ was designed to be a short, easy to use scale that measures both cognitive and affective components of empathy. It is a 60-item questionnaire with a 4-point Likert items anchored on 1 - "strongly agree", 2 - "slightly agree", 3 - "slightly disagree", and 4 - "strongly disagree". The EQ consists of 40 empathy related items that are scored and summed up and 20 filler items that are not scored.

4.6 Ethics

The study received ethics approval from the institution and followed its ethics guidelines. Although we requested participants' text password, we computed password strength via zxcvbn offline and anonymised and stored participant data on an encrypted hard disk. After computing password strength and characteristics, we remove the actual passwords from the database used for analysis by the research team.

5 Results

We describe the password characteristics across the two conditions in Table 2 and password reuse strategy in Table 3 in the Appendix.

5.1 Manipulation Check

We investigate how participants' responses (1) to feeling understood, (2) that their condition is received and, (3) feeling cared for differs between the two conditions. We observe a significant difference in feeling understood, with $p = .045$, as well as feeling that one's condition is received, with $p = .038$, between the two conditions, with a Mann-Whitney U test.

5.2 Password strength between conditions

We compute an independent samples t-test between the empathy versus control conditions with the zxcvbn $\log_{10}$ guesses as dependent variable. There was a statistically significant difference in password strength between the empathy ($M = 9.349$, $SD = 2.989$) and control ($M = 8.366$, $SD = 2.567$) conditions, $t(192) = 2.451$, $p = .015$, CI$[.191, 1.773]$, effect size $Hedges\ g = .351$, CI$[.067, .635]$ (which is between a small and medium effect).

In addition, we compute a Mann-Whitney test on the ordinal values of zxcvbn password strength score across the two conditions. There was a statistically significant difference in password strength score, where participants in the control condition chose weaker password strength ($Mdn = 2.0$) than participants in the empathy condition ($Mdn = 3.0$), $U = 3959.5$, $z = -1.981$, $p = .048$.

We therefore reject the null hypothesis $\mathsf{H}_{\mathsf{E},0}$ that "Empathizing with users does not impact password strength'.

5.3 Impact of Password Characteristics on Emotions

We investigate how password choice (strength and characteristics) discriminate between reported emotion levels, via RQ-D "*How do password characteristics influence reports of emotions*?" Table 1 summarizes the models' regression coefficients.

We compute ordinal regressions with password strength, password length, number of digits and characters as predictors variable and bmi_angry as target variable. The ordinal regression model with password strength as predictor, was statistically significant with $X^2(194, 1) = 7.307$, $p = .007$. In particular, a one unit increase in password strength was associated with a 14% increase in the odds of reporting a higher level of anger, Wald $X^2(1) = 6.891$, $p = .009$, odds ratio 1.14. The model has a correct classification rate of 64.4%.

However, the proportion of variance in anger level explained by password strength is quite small with pseudo $R^2 = 2.0\%$ (McFadden), 3.7% (Cox & Snell) and 4.3% (Nagelkerke). We reject the null hypothesis $\mathsf{H}_{\mathsf{D},0}$ that "Password characteristics do not influence reports of emotions".

Table 1 shows the regression results for different password characteristic predictors while we provide detailed explanation in the Appendix.

Table 1: Coefficients of the ordinal regressions with password characteristics as predictors and bmi_angry as target variable.

Models	**Predictors**	*B*	**SE**	**Wald** χ^2	**df**	*p*	**Odds Ratio**	**95% CI**	
								LL	UL
1	password strength	.135	0.052	6.891	1	**.009****	**1.14**	1.03	1.27
2	password length	.117	.044	6.947	1	**.008****	**1.12**	1.03	1.23
3	#digits	.269	.099	7.454	1	**.006****	**1.31**	1.08	1.59
	#lower case letters	.134	.046	8.317	1	**.004****	**1.14**	1.04	1.25
	#upper case letters	−.040	.128	.097	1	.755	.96	.75	1.24
	#symbols	.056	.178	.098	1	.754	1.06	.75	1.50

CI refers to the Confidence Interval, LL to the Lower Limit, UL to the Upper Limit.

6 Discussion

Impact of Empathy: The theme of a more supportive and humane alternative to traditional security designs is inline with not making the users the enemy or merely blaming them as the weakest link in security. Our approach contributes to this theme and can ease the burden of compliance.

While we demonstrate a small to medium effect of empathy via the static message, the effect is a positive impact on password choice. This is a first step towards regulating frustrated states during security interaction, and an antidote to user frustration with security. Our research therefore paves the way for empathy to be included as a design choice within security interactions, where affective agents may be further developed. Such agents may detect user emotion in real time and/or engage in a dialogue with users via a text-agent or an embodied agent, as demonstrated previously by Klein et al. [22] and Hone [18].

In addition, by using a static message, we aimed to only validate emotions rather than change them, as observed by the lack of difference in emotions between the conditions.

Ecological Validity: We employed a similar scenario as Das et al. [4] where participants imagine creating a password for an email account. The characteristics of the passwords in Das et al. were compared to leaked datasets. In addition, imagination of a scenario is a valid mood induction protocol [38].

With regards to using an online sample for a password study, Fahl et al found that 70-80% MTurk passwords are at least somewhat comparable to actual user passwords [12] whereas Mazurek et al reported that MTurk passwords are similar in strength to genuine passwords, and have similar characteristics in terms of structure and composition [27]. Our MTurk study passwords were also not disimilar to leaked passwords (CSDNcomp8 and SFcomp8 from [27]).

Limitations: Our manipulation was limited to a simple, static, empathy text message. However, our empathy message design is only a first step towards more supportive (and humane) security systems, where different framing of the stimulus and more interactive versions may further be researched.

Although we did not control participants' emotions at the start of the study, we perceive any incidental emotions would balance out in the two conditions. Also, anger may be one of those emotions that people do not openly acknowledge or know they are feeling. We will therefore complement self-reported emotions in future studies with emotion recognition sensors for comparison and more in-depth evaluation.

7 Conclusion

While previous research have associated frustration with security, in particular in inducing weak security choices, with a simple text empathy stimulus, we were able to demonstrate how anger emotion can act as a positive confounder to password strength, rather than cause weaker passwords. These findings provide a first step towards an antidote to user frustration with cyber security.

We also provide a first study demonstrating in detail how password strength, length and type of characters impact emotional states associated with anger. We show that the odds of inducing higher levels of anger with each unit increase in these password characteristics range from 12% to 31%. This deeper understanding of the emotions involved in password choice can trigger further research into better supporting users to comply to security requirements.

References

1. Alomari, R., Thorpe, J.: On password behaviours and attitudes in different populations. Journal of information security and applications **45**, 79–89 (2019)
2. American Psychological Association (APA): Publication manual. American Psychological Association, 6th revised edn. (2009)
3. Amsel, A.: Frustration theory: Many years later. Psychological bulletin **112**(3), 396 (1992)
4. Anupam Das, Joseph Bonneau, M.C.N.B., Wang, X.: The tangled web of password reuse. In: NDSS. pp. 23–26 (2014)
5. Baron-Cohen, S., Wheelwright, S.: The empathy quotient: an investigation of adults with asperger syndrome or high functioning autism, and normal sex differences. Journal of autism and developmental disorders **34**(2), 163–175 (2004)
6. Baumeister, R., Bratslavsky, E., Muraven, E., Tice, D.: Ego depletion: is the active self a limited resource? Personality and social psychology **74**, 1252–1265 (1998)
7. Carver, C.S.: Cognitive interference and the structure of behavior. Cognitive interference: Theories, methods, and findings pp. 25–45 (1996)

8. Coopamootoo, K.P., Groß, T.: Evidence-based methods for privacy and identity management. In: IFIP Privacy and Identity Management. Facing up to Next Steps. pp. 105–121. Springer (2016)
9. Coopamootoo, K.P., Groß, T.: Cyber security & privacy experiments: A design & reporting toolset. In: Privacy and Identity Management. The Smart World Revolution. Springer (2017), under Publication at IFIP Privacy and Identity Management. The Smart World Revolution
10. Cramer, H., Goddijn, J., Wielinga, B., Evers, V.: Effects of (in) accurate empathy and situational valence on attitudes towards robots. In: 2010 5th ACM/IEEE International Conference on Human-Robot Interaction (HRI). pp. 141–142. IEEE (2010)
11. De Carnavalet, X.D.C., Mannan, M., et al.: From very weak to very strong: Analyzing password-strength meters. In: NDSS. vol. 14, pp. 23–26 (2014)
12. Fahl, S., Harbach, M., Acar, Y., Smith, M.: On the ecological validity of a password study. In: Proceedings of the Ninth Symposium on Usable Privacy and Security. p. 13. ACM (2013)
13. Furnell, S., Thomson, K.L.: Recognising and addressing 'security fatigue'. Computer Fraud & Security **2009**(11), 7–11 (2009)
14. Gross, J.J., Thompson, R.A.: Emotion regulation: Conceptual foundations. (2007)
15. Groß, T., Coopamootoo, K., Al-Jabri, A.: Effect of cognitive depletion on password choice. In: The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016). pp. 55–66. USENIX Association (2016)
16. Hara, K., Adams, A., Milland, K., Savage, S., Callison-Burch, C., Bigham, J.P.: A data-driven analysis of workers' earnings on amazon mechanical turk. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. p. 449. ACM (2018)
17. Herley, C.: So long, and no thanks for the externalities: the rational rejection of security advice by users. In: Proceedings of the 2009 workshop on New security paradigms workshop. pp. 133–144. ACM (2009)
18. Hone, K.: Empathic agents to reduce user frustration: The effects of varying agent characteristics. Interacting with computers **18**(2), 227–245 (2006)
19. Ickes, W.J.: Empathic accuracy. Guilford Press (1997)
20. Inc', G.: Google mail account page (August 2019), https://accounts.google.com/
21. Inglesant, P.G., Sasse, M.A.: The true cost of unusable password policies: password use in the wild. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 383–392. ACM (2010)
22. Klein, J., Moon, Y., Picard, R.W.: This computer responds to user frustration: Theory, design, and results. Interacting with computers **14**(2), 119–140 (2002)
23. Komanduri, S., Shay, R., Kelley, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F., Egelman, S.: Of passwords and people: measuring the effect of password-composition policies. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2595–2604. ACM (2011)
24. Lazarus, R.S., Folkman, S.: Stress. Appraisal, and coping **725** (1984)
25. Maxion, R.: Making experiments dependable. Dependable and Historic Computing pp. 344–357 (2011)
26. Mayer, J.D., Gaschke, Y.N.: The experience and meta-experience of mood. Journal of personality and social psychology **55**(1), 102 (1988)
27. Mazurek, M.L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Kelley, P.G., Shay, R., Ur, B.: Measuring password guessability for an entire university. In: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. pp. 173–186. ACM (2013)

28. Nwadike, U., Groß, T., Coopamootoo, K.P.: Evaluating users' affect states: towards a study on privacy concerns. In: IFIP International Summer School on Privacy and Identity Management. pp. 248–262. Springer (2016)
29. Oatley, K., Duncan, E.: The experience of emotions in everyday life. Cognition & Emotion **8**(4), 369–381 (1994)
30. Peisert, S., Bishop, M.: How to design computer security experiments. In: Fifth World Conference on Information Security Education. pp. 141–148. Springer (2007)
31. Picard, R.W.: Affective computing. MIT press (2000)
32. Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F.: Encountering stronger password requirements: user attitudes and behaviors. In: Proceedings of the Sixth Symposium on Usable Privacy and Security. p. 2. ACM (2010)
33. Smith, A.: Cognitive empathy and emotional empathy in human behavior and evolution. The Psychological Record **56**(1), 3–21 (2006)
34. Stanton, B., Theofanos, M.F., Prettyman, S.S., Furman, S.: Security fatigue. IT Professional **18**(5), 26–32 (2016)
35. Stueber, K.: Empathy. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy. Metaphysics Research Lab, Stanford University, fall 2019 edn. (2019)
36. Ur, B., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., Cranor, L.F., Dixon, H., Emami Naeini, P., Habib, H., et al.: Design and evaluation of a data-driven password meter. In: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. pp. 3775–3786. ACM (2017)
37. Watson, D., Clark, L.A., Tellegen, A.: Development and validation of brief measures of positive and negative affect: the panas scales. Journal of personality and social psychology **54**(6), 1063 (1988)
38. Westermann, R., Spies, K., Stahl, G., Hesse, F.W.: Relative effectiveness and validity of mood induction procedures: A meta-analysis. European Journal of social psychology **26**(4), 557–580 (1996)
39. Wheeler, D.L.: zxcvbn: Low-budget password strength estimation. In: Proc. USENIX Security (2016)
40. Wright, P., McCarthy, J.: Empathy and experience in hci. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 637–646. ACM (2008)

8 Appendix

8.1 Password Characteristics

Table 2: Password Descriptives

Characteristics	**Empathy Condition (N=99)**			**Control Condition (N=95)**		
	mean	median	sd	mean	median	sd
strength	9.35	8.67	3.00	8.37	8.00	2.57
length	11.57	11.00	3.39	10.54	9.00	2.90
# digits	3.04	3.00	1.82	3.00	3.00	1.54
# lwrcase	6.29	6.00	3.89	5.42	5.00	3.33
# uprcase	1.33	1.00	1.25	1.25	1.00	1.39
# symbols	0.90	1.00	0.86	0.86	1.00	0.86

8.2 Password ReUse Strategy

Table 3: Password Choice Strategy (in %)

Strategy	**%**
Reuse an existing password as is	6.7
Modify an existing password	16.0
Create an entirely new password	77.3

8.3 Empathy Quotient

We measured dispositional empathy via the Empathy Quotient (EQ) questionnaire [5]. The sample had a mean EQ of 40.361, $sd = 12.778$.

We do not observe a difference between conditions. However we observe a difference between gender, where women scored a higher dispositional empathy (mean = 42.305, sd = 12.637), EQ, than men (mean = 38.495, sd = 12.697). The difference was statistically significant with the independent samples t-test, with $t(192) = 2.094$, $p = .038$, CI$[.222, 7.399]$, effect size $Hedges\ g = .300$, CI$[.017, .583]$, which is between a small and medium effect.

We compare the mean EQ across the different levels of bmi_anger with an ANOVA. We find a significant difference in EQ across levels of reported anger, where participants with a low EQ expressed more anger, $F(3, 190) = 6.28$, $p <$

.000. The boxplot in Figure 2 depicts the decreasing mean EQ as bmi_anger increases from 1 to 4.

However, we did not find a correlation between EQ and receiving empathy through bmi_understood, bmi_received or bmi_cared-for.

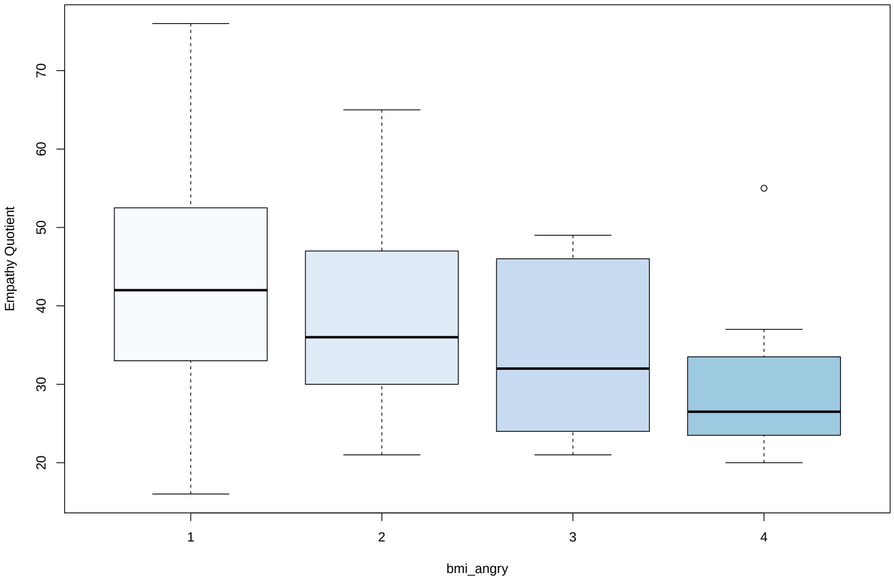

Fig. 2: Plot of Empathy Quotient vs Reported Anger.

8.4 Impact of Password Characteristics on Emotions

Password strength impacts anger reports model assumptions There is no difference in the coefficients between models, with $X^2(2) = 2.324$, $p =$ .313. This means that the proportional odds assumption is satisfied, that is the coefficients that describe the relationship between, the lowest versus all higher levels of bmi_anger are the same as those that describe the relationship between the next lowest level and all higher level. The model goodness of fit assumption was also satisfied via the Pearson Chi-Square statistic with $X^2(443) = 471.605$, $p = .168$.

Password length impacts anger reports We compute an ordinal regression model, with bmi_anger as target variable and password length as predictor. The proportional odds assumption was satisfied with $X^2(2) = 1.523$, $p = .467$, and the model goodness of fit assumption was satisfied via the Pearson Chi-Square statistic with $X^2(47) = 52.562$, $p = .267$.

The model was statistically significant with $X^2(194, 1) = 7.323$, $p = .007$. A one unit increase in password length was associated with a 12% increase in the odds of reporting a higher level of anger, Wald $X^2(1) = 6.947$, $p = .008$, odds ratio 1.12. The model has a correct classification rate of 63.4%. However, The proportion of variance in anger level explained by password strength is quite small with pseudo $R^2 = 2.0\%$ (McFadden), 3.7% (Cox & Snell) and 4.4% (Nagelkerke).

Password components impact anger reports We compute an ordinal regression model, with bmi_anger as target variable and the number of digits, lowercase letters, uppercase letters and symbols as predictors. The proportional odds assumption was satisfied with $X^2(8) = 3.478$, $p = .901$, and the model goodness of fit assumption was satisfied via the Pearson Chi-Square statistic with $X^2(425) = 467.062$, $p = .078$.

The model was statistically significant with $X^2(198, 4) = 12.838$, $p = .012$. A one unit increase in number of digits was associated with a 31% increase in the odds of reporting a higher level of anger, Wald $X^2(1) = 7.454$, $p = .006$, odds ratio 1.31. A one unit increase in number of lowercase letters was associated with an 14% increase in the odds of reporting a higher level of anger, Wald $X^2(1) = 8.317$, $p = .004$, odds ratio 1.14. The model has a correct classification rate of 64.4%. However, The proportion of variance in anger level explained by password strength is quite small with pseudo $R^2 = 3.5\%$ (McFadden), 6.4% (Cox & Snell) and 7.5% (Nagelkerke).

Password strength impacts reports of excitement We compute an ordinal regression model, with bmi_excitement as target variable and password strength as predictor. The proportional odds assumption was satisfied with $X^2(3) = 1.871$, $p = .600$, and the model goodness of fit assumption was satisfied via the Pearson Chi-Square statistic with $X^2(591) = 594.171$, $p = .456$.

The model was statistically significant with $X^2(194, 1) = 4.086$, $p = .043$. A one unit increase in password length was associated with a 9% decrease in the odds of reporting a higher level of excitement, Wald $X^2(1) = 4.000$, $p = .045$, odds ratio .910. However, The proportion of variance in excitement level explained by password strength is quite small with pseudo $R^2 = .07\%$ (McFadden), 2.1% (Cox & Snell) and 2.2% (Nagelkerke).