Better Passwords through Prospect Theory

Eryn Ma
Pomona College

Summer Hasama
Pomona College

Eshaan Lumba
Pomona College

Eleanor Birrell
Pomona College

Abstract

User-chosen passwords remain essential to online security, and yet studies have consistently found that people continue to choose weak, insecure passwords. In this work, we investigate whether *prospect theory*, a behavioral economic model of how people evaluate risk, can provide insights into how users choose passwords and whether it can motivate new designs for password selection mechanisms that will nudge users to select stronger passwords. We ran a user study with 577 participants, and we found that an intervention guided by prospect theory—in which the text mentioned specific threats and framed weak passwords as a negative security effect—reduced the number of weak passwords by approximately 25%. The improved password choice appears to be due primarily to the negative framing; conditions with this framing resulted in significantly higher rates of improvement compared to conditions with an interaction that framed strong passwords as an improvement in security or to interactions that used neutral language. These results provide guidance for designing and implementing account registration mechanism that will significantly improve the strength of user-selected passwords, thereby leveraging insights from prospect theory to improve the security of systems that rely on password-based authentication.

1 Introduction

Despite a large body of research into alternate mechanisms for human authentication, user-chosen passwords remain a critical component of security. Many efforts have been made to nudge users towards choosing stronger passwords, including password recipes and password meters, but these efforts have met with limited success. Password recipes are ineffective at enforcing strong password choices [7], password meters are only effective for high-risk accounts [1], and that users continue to select and use weak password. In this work, we investigate whether insights from behavioral economics can provided insights into how users select passwords and whether it can motivate new designs for password selection pages that would nudge users to select stronger passwords.

Prospect theory [2–6] is a behavioral economic model about how people evaluate risks. Developed on the basis of numerous user studies, prospect theory identifies patterns in how humans make decisions that involve risk:

- **Framing effect.** People evaluate outcomes as positive or negative deviations (gains and losses) from a neutral reference point; responses to losses are more extreme than responses to gains.
- **Source-dependence.** In subjective situations, how heavily people weigh particular information depends on the specificity of the information; ambiguous or vague information has less impact on user decisions.
- **Risk Seeking.** People prefer an uncertain large loss over a certain smaller loss.
- **Nonlinear preferences.** Outcomes that are near certainty are treated as certain; changes in probabilities near 0 or 1 can have more impact than equivalent changes in less certain probabilities. The marginal value of both gains and losses also decreases with their size.

In this work, we explore how two of these patterns—framing effect and source-dependence—impact users' choice of passwords, and we explore how these patterns might be leveraged to nudge users towards selecting stronger passwords.

We find an intervention with negative framing results in 20-25% of users improving the strength of their password, significantly higher rate of improvement than interventions

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Vancouver, B.C., Canada.

Condition	Interactive Prompt Language
Neutral-Vague	**Weak/Moderate passwords put your account at risk. Would you like to choose a stronger password?** Yes No
Neutral-Specific	**Weak/Moderate passwords can be guessed or learned by attackers in *x* seconds, which may lead to the loss of personal information, including credit card info, and identity theft. Would you like to choose a stronger password?** Yes No
Negative-Vague	**Weak/Moderate passwords put your account at risk.** Choose a stronger password Ignore potential risks of financial loss and identity theft and create account with current password
Negative-Specific	**Weak/Moderate passwords can be guessed or learned by attackers in *x* seconds, which may lead to the loss of personal information, including credit card info, and identity theft. Would you like to choose a stronger password?** Choose a stronger password Ignore potential risks of financial loss and identity theft and create account with current password
Positive-Vague	**Weak/Moderate passwords put your account at risk.** Chose a stronger password to reduce the risks of financial loss and identity theft Create account with current password
Positive-Specific	**Weak/Moderate passwords can be guessed or learned by attackers in *x* seconds, which may lead to the loss of personal information, including credit card info, and identity theft. Would you like to choose a stronger password?** Chose a stronger password to reduce the risks of financial loss and identity theft Create account with current password

Table 1: Prompts and options used in the interactive prompt that would appear during account creation after a user selected a weak or moderate password. The estimated time to guess the password was computed with the `zxcvbn` password strength estimator.

with positive or neutral framing. Moreover, we found that an intervention that used negative framing and specific language reduced the number of weak passwords selected by 25%. These preliminary results suggest that prospect theory can be a helpful model for understanding how users make security decisions—in particular, how users choose passwords. We believe that insights from prospect theory can form the foundation for designing and implementing mechanisms that improve security by nudging users to make better security decisions.

2 Methodology

We implemented a news aggregation site to serve as our example website; screenshot of our website in shown in Figure 1.

When a user first visited the website, they were asked to create an account with a username and password; a visual password meter categorized their choice of password as strong, moderate, or weak using the `zxcvbn` password strength estimator. Users who selected a weak or moderate password were then presented with an interactive prompt that asked whether they wanted to go back and choose a stronger password; users who opted to go back were allowed to modify their choice of password. Each user was pseudorandomly assigned to one of six conditions corresponding to two independent variables:

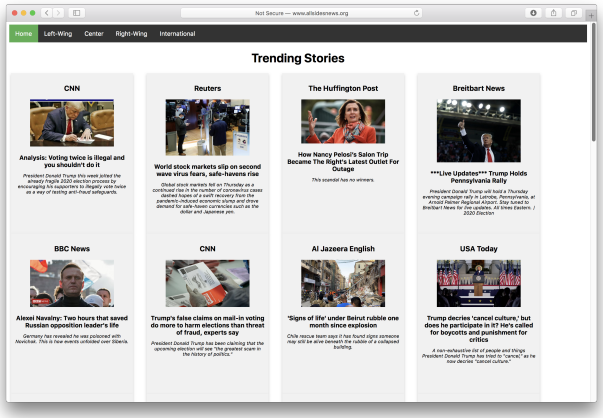

Figure 1: News aggregation site used in user studies.

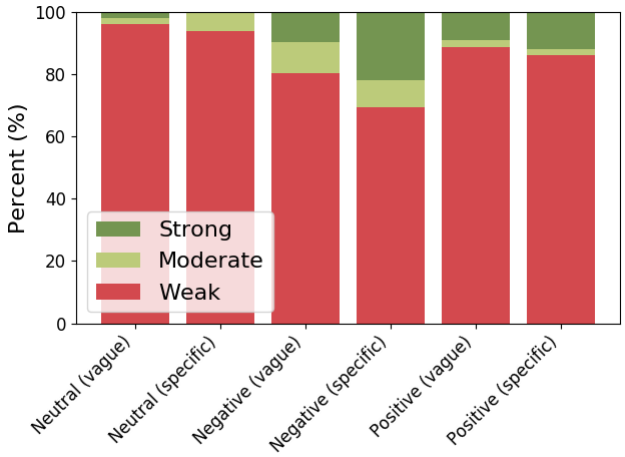

Figure 2: Strength of final password chosen by users who initially chose a weak password.

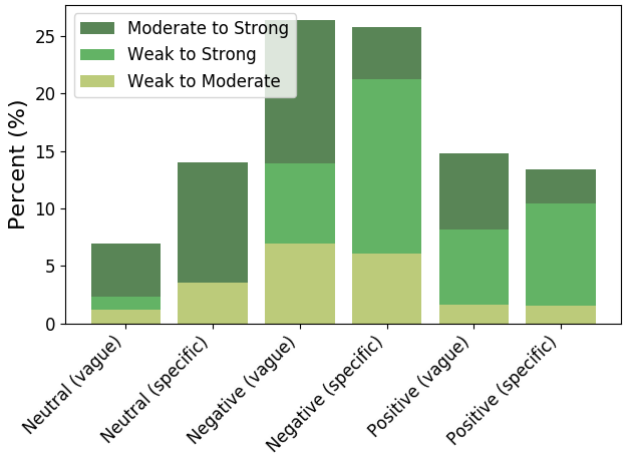

Figure 3: Fraction of users who improved the strength of their password.

framing (neutral, negative, or positive) and source (vague or specific). The language used in the interactive prompt varied depending on which condition the user was assigned; the language used in each condition is given in Table 1.

We ran a user study with 577 participants recruited through Amazon Mechanical Turk. Users were asked to create an account and beta test our website; to avoid collecting any personal information, participants were given a test username and email to use on the site. After completing the task, users filled out a follow-up survey containing questions about their security decisions and their mental models of security, along with demographic information. Recruitment was limited to workers with at least a 95% approval rate and at least 50 accepted HITs who were located in California. Each worker was compensated $1.20 USD for their participation. This study received a waiver from the institutional ethicsreview board (IRB) at our institution.

3 Results

To investigate the effect of individual design factors, we tested whether users who initially selected weak password ultimately improve the strength of their chosen password. We found that the framing of the options had a significant effect the number of users with weak or moderate initial passwords who improved the strength of their password, with negative framing resulting in significantly higher rates of improvement than neutral framing ($p < .001$) or positive framing ($p = .022$). However, source alone did not appear to have a significant impact on whether user went back and selected a stronger password ($p = .611$).

We also tested whether this intervention caused individual users to select stronger passwords. We found that among users assigned to the condition with negative language and specific phrasing, the number of weak passwords selected as a final password was significantly lower than the number of weak passwords selected initially ($p = .049$); the number of weak passwords selected as the final password was also significantly lower when we combined the two negative conditions ($p = .019$). Other conditions showed no significant reduction in the number of weak passwords ultimately selected. These results suggest that insights from prospect theory can be leveraged to nudge users toward selecting strong passwords.

4 Conclusion

Our results suggest that prospect theory can be a helpful model for understanding how users make security decisions—in particular, how users choose passwords. We find that an interaction after users select a preliminary password that frames weak passwords as having a negative impact on security can significantly reduce the number of weak passwords that users ultimately select. We believe that insights from prospect theory can form the foundation for designing and implementing mechanisms that improve security by nudging users to make better security decisions.

References

[1] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. Does my password go up to eleven? the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, page 2379–2388, New York, NY, USA, 2013. Association for Computing Machinery.

[2] Daniel Kahneman and Amos Tversky. Prospect theory: An analysis of decision under risk. *Econometrica*, 47(2):263–292, 1979.

[3] Amos Tversky and Daniel Kahneman. The framing of decisions and the psychology of choice. *science*, 211(4481):453–458, 1981.

[4] Amos Tversky and Daniel Kahneman. The framing of decisions and the evaluation of prospects. In *Studies in Logic and the Foundations of Mathematics*, volume 114, pages 503–520. Elsevier, 1986.

[5] Amos Tversky and Daniel Kahneman. Loss aversion in riskless choice: A reference-dependent model. *The quarterly journal of economics*, 106(4):1039–1061, 1991.

[6] Amos Tversky and Daniel Kahneman. Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and uncertainty*, 5(4):297–323, 1992.

[7] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 162–175, 2010.