Using Gamification to Improve Information Security Behavior: A Password Strength Experiment

Jacques Ophoff, Frauke Dietz

Using Gamification to Improve Information Security Behavior: A Password Strength Experiment

Jacques Ophoff[0000-0003-0634-5248] and Frauke Dietz

University of Cape Town, Cape Town, South Africa
jacques.ophoff@uct.ac.za, DTZFRA001@myuct.ac.za

Abstract. Information security emphasizes the importance of motivating end users to improve their security behavior towards protecting their private and organizational information assets. Password authentication is widely used as a user authentication method to safeguard information resources from unauthorized access. Despite its prevalence password best practice is not often followed and the use of weak passwords persist. Although password strength feedback mechanisms commonly aim to extrinsically motivate users to improve their password creating behavior, it is not yet clear how other methods, specifically gamification, influences security behavior regarding password creation behavior. The purpose of this study is to examine the effect gamification on user information security behavior, specifically regarding password creation. This study presents results from an online experiment of 232 respondents, who interacted with two different password strength feedback methods, namely a meter feedback method and a gamified feedback method using gamification points. A significant difference between the methods was found when measuring password strength using the number of guesses needed to crack the password, with the points method resulting in stronger passwords. The results of the study reveal that gamified feedback can lead to increased engagement and stronger password creation.

Keywords: Information Security Behavior, Gamification, Authentication, Password Strength Feedback.

1 Introduction

A common approach used to protect user's information assets from unauthorized access, is using user authentication methods [1]. A popular form of authentication that is used in information security is password verification and hence, it is especially important to motivate users to improve their security behavior regarding password creation [2-4]. To motivate users to improve their security behavior regarding password creation, users are often exposed to password strength feedback mechanisms, such as password meters, that commonly extrinsically motivate users to create stronger passwords through fear [4-7]. Considering human motivation, intrinsic motivation is increasingly found to be more effective than extrinsic motivation [8, 9], hence increasing

the interest in investigating the effects of intrinsic motivation on user information security behavior.

Within the context of information security behavior, the effects of gamification on user information security behavior, specifically regarding password creation behavior, are still undiscovered. This study contributes to information security behavior research by investigating this phenomenon. The main objective of this study is to examine the effect of gamified feedback on user information security behavior, specifically regarding password creation. Thus, the primary research question to be addressed in this study is: *How does gamified feedback affect user information security behavior regarding password creation?* This study further aims to investigate an alternative password strength feedback method to existing fear-driven methods (password meter), to potentially motivate users more effectively to create strong passwords. The research question is evaluated using empirical data, which is collected using an online experiment.

The remainder of this paper will proceed as follows. First, the conceptual background relating to information security behavior around password creation and the adopted research model will be presented, along with research propositions for this study. In Section 3, the research design will be discussed in detail. This is followed by the data analysis and discussion of the project findings. Finally, this paper concludes by discussing the limitations of this study, along with opportunities for future research.

2 Literature Review

Password verification is the most commonly used form of authentication in information security [2-4]. Password authentication is a user authentication method that protects valuable information assets and resources within computer-based systems from unauthorized access and violation [10] by "matching the combination of username and password against credentials stored on the server" [3]. Although passwords form an important barrier limiting unauthorized access to information assets, users still engage in poor password practices, such as creating insecure passwords and reusing passwords [2]. Mwagwabi et al. [2] argued that poor password practices amongst users occur because users find it difficult to remember passwords and consider it annoying to have to comply with inconsistent password guidelines. Using weak passwords increases the user's vulnerability to threat, as weak passwords can be cracked without difficulty by easily accessible password cracking software [3, 4]. Given the threats to password security, it is especially important to find ways to improve the security behavior of users by motivating end users to create strong and effective passwords [2-4].

2.1 Extrinsic and Intrinsic Motivation

Fear appeals, and theories related to fear, including the protection motivation theory and deterrence theory, are extensively used in the field of information security to assist in motivating end users to change their security behavior [11-13]. Fear appeals present end users with persuasive messages that warn the end user of potential threats and recommend security behavior to counteract the threat [11]. Fear appeals refer to persuasive

messages designed to highlight "the seriousness of a threat and a user's ability to cope with it" [4]. Johnston and Warkentin [13] defined fear appeals as messages that aim to encourage individuals to act in a recommended way through the initiation of fear related to a threat.

Fear appeals act as an extrinsic motivator for human behavior, as these propel users externally into choosing stronger passwords. Extrinsic motivation refers to human behavior that is driven by external rewards [14, 15]. Ryan and Deci [15] further pointed out that, if individuals are externally pushed into performing an action, the motivation behind performing that action is extrinsic. When taking human motivation into consideration, intrinsic motivation has sometimes been found to be more effective regarding human motivation than extrinsic incentives [8, 9]. Intrinsic motivation refers to behavior that is driven by personal interest and enjoyment in doing something [14, 15]. The idea of intrinsic motivation is also reflected in the self-determination theory (SDT), which focuses on the degree to which an individual's behavior is self-motivated without external rewards [16].

2.2 Password Meters as Password Strength Feedback Mechanisms

A common existing measure for motivating users to create stronger passwords is the use of password meters as a real-time password strength feedback mechanism to communicate a password's strength visually as the password is typed [4-7]. Feedback mechanisms, also referred to as feedback loops, "provide people with timely information about their actions and opportunities to improve them", hence pushing people towards improved behaviors [6]. Password meters generally appear as a colored bar that changes its color and its length based on the strength of the password entered, and it is often accompanied by a word explicitly representing the strength (e.g., weak, medium or strong) of the password [5]. An example of a password meter, which is displayed during account registration, is depicted in Fig. 1.

The strength and quality of a given password is commonly measured by either enforcing strong password requirements around password length and character set complexity, or by detecting "weak patterns such as common words, repetitions and easy keyboard sequences" [5]. Past studies conducted around the use of password meters concluded that password meters as a password strength feedback mechanism, in general, effectively influence users' security behavior towards choosing stronger passwords [5, 7, 17]. However, Ur et al. [7] observed that password meters with too-strict evaluations had a negative impact on users, resulting in users getting irritated and therefore losing the motivation to satisfy the meter.

Password meters persuade users to create stronger passwords through fear by warning the users that the chosen password is weak or not strong enough. However, it has been found that methods using fear appeal are not necessarily the most effective in achieving security behavior by users [12]. D'Arcy and Herath [12] argued that the increased deterrence through fear appeals does not work for all users. It is, therefore, of increasing interest to research and investigate alternative password feedback mechanisms that will motivate users more effectively to create stronger passwords.

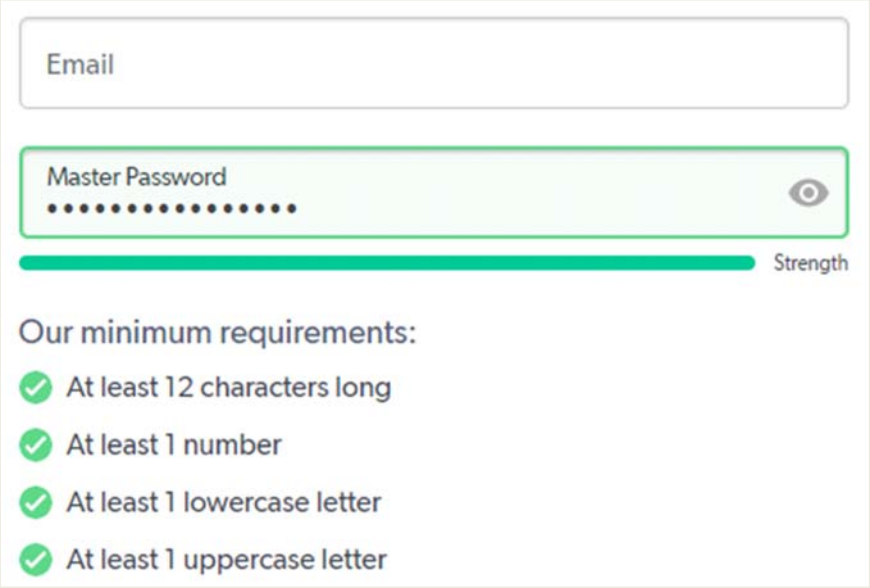

Fig. 1. Password meter example (https://lastpass.com/)

2.3 Gamification as an Opportunity to Improve Password Security Behavior

Deterding [18] argued that the SDT framework models and explains an individual's gaming motivation and enjoyment very accurately. Over the last five years, gamification has become an emerging trend and has gained increasing popularity within the academic context regarding intrinsically motivating an individual's behavior [19]. Making use of gamification in the security context, specifically regarding authentication, could increase the motivation of users to act more securely [20, 21].

Gamification can be briefly defined as "the use of game design elements in non-game contexts to motivate and increase user activity" [22]. To emphasize the behavioral effects of gamification, an alternative definition of gamification presented by Hamari et al. [19] is acknowledged as "a process of enhancing services with (motivational) affordances to invoke gameful experiences and further behavioral outcomes." Recently, human-computer interaction research has become increasingly interested in the idea of utilizing game design for designing interactive systems for motivation and enjoyment [e.g. 18, 23, 24].

Blohm and Leimeister [25] argued that game design elements can be utilized within processes and services to influence users' motivation, productivity and behavior positively. Game design elements refer to motivational affordances that drive psychological and behavioral outcomes of users [19].

Game design elements consist of game mechanics and game dynamics. Game mechanics are functional components used to gamify processes or applications. Game dynamics, on the other hand, determine the effects of game mechanics on a user's long-

term user experience of the implemented mechanics. These game dynamics correspond to specific user motives that drive specific user behavior [25, 26]. For example, game mechanics such as scoring systems (i.e. gamification points) induce collective dynamics that relate user activities to measurable improvements and thus satisfy the aspiration for achievement. Blohm and Leimeister [25] further argued that, depending on the specific design of a mechanic, a specific mechanic may induce various dynamics and hence may lead to different motives.

Past studies conducted around improving the impact of password meters as a feedback mechanism for password strength, focused solely on variation in scoring algorithms and visual representations of password meters [5, 7, 17]. Shay et al. [27] pointed out that "past research has not looked at the impact of presentation and instructions (beyond password meters), or at ways to help users cope with strict [password] requirements." After conducting literature searches relating to this literature review, it has been found that no research has focused on the use of gamification within the context of password feedback mechanisms. This gap in the literature, therefore, offers an opportunity to research whether password feedback mechanisms that make use of gamification could potentially enhance motivation towards better password choice. Specifically making use of gamification points for password strength feedback is of great interest, as a point system is the game mechanic that can be considered most like the percentage calculation used by the password meter approach. The theoretical proposition in this study therefore is that *the use of gamification points, as opposed to conventional password meters, as a password feedback mechanism will result in users creating stronger passwords.*

3 Methodology

This study used a true experiment, as participants were randomly assigned to treatment groups, namely the experimental group and the control group [28]. More specifically, a Posttest-Only Control-Group Experimental Design was utilized, as the treatment groups were measured only on the posttest provided after the experiment.

The experimental group (Group A) were given a treatment or planned intervention, while the control group (Group B) were not given a treatment. For this study, the experimental group were given a point feedback method as treatment, while the control group were presented with the standard password meter. Both treatment groups were measured on the posttest only, as the study aimed to investigate whether user security behavior differs based on different feedback methods. Treatment groups were not administered a pretest, as the study was not focusing on the change in security behavior before and after a specific treatment.

To add realism to the experiment, the experiment was designed to look like a standard sign-up form to create a new online account. Participants were also presented with pre-experiment instructions that emphasized that participants should fill in the sign-up form as they would in a normal sign-up process for an account that holds sensitive personal information. However, it is acknowledged that participants cannot be forced

to treat the sign-up process in the experiment the same way they would treat a sign-up process in a real-world situation.

3.1 Sampling

For this study a non-probability convenience sample was selected, consisting of students and staff at a large South African university, as these individuals were readily available and could be reached via email. The sample is believed to be a fair representation of the target population (general users of information systems) – the sample uses several information systems and includes individuals of different ages and genders, who have different levels of technical skills and password creating experience. All individuals in the sample operate within a tertiary institution, which requires them to create passwords for numerous electronic applications, often containing sensitive personal information.

3.2 Data Collection Method

An online experiment, followed by an online questionnaire, was conducted to gather primary data for this research. An email, briefly explaining the purpose of the study and providing a link to the online experiment, was sent out to the individuals in the identified sample. Potential participants were provided only with a brief description of the study (investigation into information security behavior), as informing participants that the study was investigating information security behavior specifically around password strength might have influenced their password-creating behavior. Telling participants about the purpose of the study may lead to demand characteristics, which results in participants interpreting the purpose of the experiment and subconsciously behaving differently to meet their interpretation [29].

The experiment consisted of two different simple account registration interfaces, each representing a different password strength feedback mechanism. One registration interface represented the conventional password meter feedback method (see Fig. 2), while the other registration interface represented a feedback method that used gamification points (see Fig. 3).

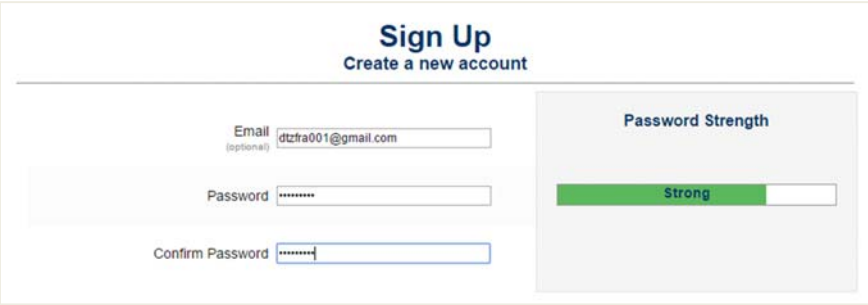

Fig. 2. Registration form with a conventional password strength meter

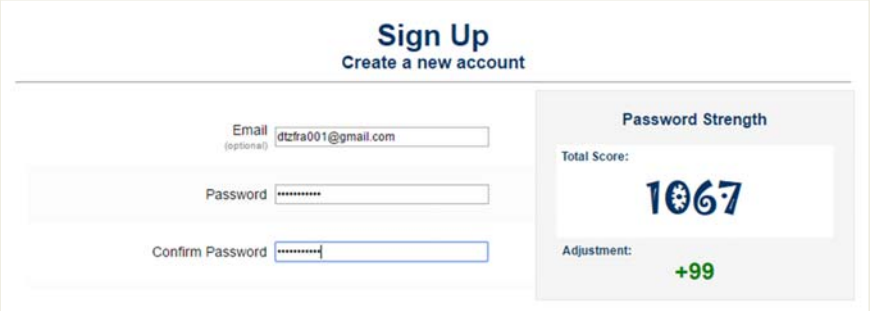

Fig. 3. Registration form with gamification points

Each participant was randomly presented with one of the interfaces and was asked to complete the registration process, which required the user to create a password. Only the password and the confirmation of password were compulsory. These two fields did not have to match to proceed to the questionnaire, however it was recorded whether they matched or not (94% of participants entered matching passwords). The password strength feedback mechanism was updated in real time as a participant entered a password. The real-time calculated password strength score was stored as primary data, avoiding the permanent storage of the actual password created. The password strength was calculated using the zxcvbn library developed by Dropbox. Zxcvbn is a password strength estimator, which recognizes and weighs "several dictionaries (English words, names and surnames, Burnett's 10,000 common passwords), spatial keyboard patterns (QWERTY, Dvorak, and keypad patterns), repeats (aaa), sequences (123, gfedcba), years from 1900 to 2019, and dates (3-13-1997, 13.3.1997, 1331997)" through pattern matching and conservative estimation [30].

The zxcvbn library awards the password strength with a score of 0 (too guessable/very weak), 1 (very guessable/weak), 2 (somewhat guessable/moderate), 3 (safely not guessable/strong) or 4 (strongly not guessable/very strong) [30]. The zxcvbn library was also utilized to calculate additional properties (other than the password score) of a participant's password, including the estimated number of guesses needed to crack the password, the estimated time (in seconds) to crack the password, and the number of milliseconds it took zxcvbn to calculate the password score. These properties were all calculated in real time during password creation and were stored after questionnaire completion. The conventional strength meter (the color and the length of the bar) was populated based on the calculated password score.

For the feedback method that used gamification points, the guesses_log10 password property was used to calculate and update the total point score. The guesses_log10 is the estimated guesses needed to crack a password, expressed as base-10 logarithm [30], thus yielding a user-friendly indication of password strength. For each character that was added or removed from the password during password creation, the difference between the old and new guesses_log10 value was calculated, multiplied by one hundred and displayed as the adjustment, while the total score was adjusted accordingly (see Fig. 4).

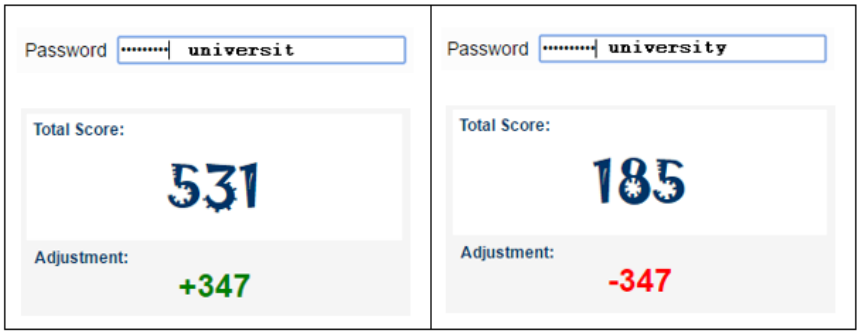

Fig. 4. Password strength points feedback concept

The example in Fig. 4 shows how the password score could be negatively affected by using a dictionary word: going from 'universit' to 'university' decreases the password score by 347 points. Unlike the strength meter, the points feedback method does not have a maximum password strength limit, as the guesses_log10 password property can still increase further even if a password has a strength score of 4 (100%) already. This enabled users to score an infinite amount of points.

Qualtrics, a web-based survey service, was used to host the online experiment, create the online questionnaire, and collect and record the response data in the cloud. Response data refers to data that the respondents provide by participating in the experiment and answering the questionnaire.

4 Data Analysis and Findings

A total of 445 responses were recorded. Of this 232 (52%) were considered valid for analysis due to fully completing the entire experiment. Out of the valid responses, 112 (48%) respondents were presented with the meter feedback method and 120 respondents were presented with the points feedback method.

Most respondents were female (56%). Age groups were divided into seven categories. Most respondents (45%) were 18–24 years old, containing mostly students at UCT. Twenty-one per cent of respondents fell within the 35–44 age group, closely followed by 19% in the age group 25–34 years and 12% in the age group 45–54 years. Only 4% of respondents fell within the age group 55–64 years. Respondents were asked whether they play any form of digital, computer or video games. A large number (59%) of respondents play games, while 41% do not play any form of digital, computer or video games.

4.1 Assessment of the Average Password Strength

Both password strength feedback methods assigned the password strength with a score of 0, 1, 2, 3 or 4 (0 representing very weak and 4 representing very strong). A t-Test for

independent means was performed to test whether there was a significant difference in the average password strength between the two treatment groups, which were independent of one another. The two treatment groups are referred to as being independent, as these groups were unrelated, and each participant was tested only once. IBM SPSS Statistics 25 was used to perform an independent-samples t-Test. The summary results of the t-Test are shown in Table 1.

Table 1. Password strength t-Test data summary

Strength calculation	**Score (0-4)**		**guesses_log10**	
Feedback method	**Meter**	**Points**	**Meter**	**Points**
Mean	2.85	2.87	9.19	10.51
Std. Deviation	1.21	1.23	3.69	6.29
Observations	112	120	112	120
Degrees of freedom	230		230	
t statistic	-.115		-1.929	
p value	.461		.010	

The results of the analysis show that, although Group A (points feedback method) did have a slightly higher average password score than Group B (meter feedback method), that score was not significantly different. However, when examining password strength in terms of estimated guesses needed to crack the password (guesses_log10) a significant difference was observed, with Group A having more secure passwords.

In addition to the password score, other properties relating to each feedback method were recorded or calculated. One such property is the time spent on the sign-up form, while another is the time taken to calculate the password score (a higher time indicates a more complex password). Averages scores for these metrics, across all participants, are shown in Table 2.

Table 2. Additional analysis of experiment and passwords

	Meter	**Points**
Average time spent on sign-up form (in seconds)	54.19	72.62
Average time to calculate password score (in milliseconds)	4.84	8.25

Respondents who were presented with the points feedback method, on average, spent more time on the simulated sign-up process than did respondents who were presented with the meter feedback method. This time, also referred to as dwell time, can be seen as a possible proxy measure for engagement [31]. The average time it took zxcvbn to calculate the password score (like the average time to crack a password) was higher for passwords created by respondents who received the points feedback method. This corresponds with the slightly higher average password score attained by respondents who were presented with the points feedback method on the sign-up page.

The findings therefore partially (except for the use of score for calculation of password strength) support the proposition that *the use of gamification points, as opposed*

to conventional password meters, as password feedback mechanism will result in users creating stronger passwords.

4.2 Discussion

Although the difference in password score was not statistically significant, the average password score and averages of other password properties were found to be higher for passwords created with the points feedback method and therefore revealed a slight increase in password strength for passwords created with the gamification feedback method. Interestingly, the findings of this study revealed that, on average, respondents who were presented with the points feedback method spent more time completing the sign-up page than respondents who were presented with the meter feedback method. This could be explained by arguing that the respondents who interacted with the points feedback method might have been more engaged in creating a password, when compared with the respondents, who, on average, spent less time interacting with the meter feedback method.

The findings of this study further revealed that the average time to crack a password was significantly higher for passwords created by respondents who received the points feedback method. This could be explained by the fact that the crack time property of a password can still increase further even if a password has a strength score of 4 already. Since the points feedback method did not visually indicate an upper strength limit (i.e. password score of 4 represented as "very strong"), when compared with the conventional meter feedback method, users may have been encouraged to continue to improve the strength of their password (in terms of crack time) even if their password achieved the highest attainable password score of 4 already.

The implications of the above are twofold. First it shows potential for gamification to enhance user engagement in password creation, possibly resulting in stronger passwords. Second it points to a deficiency in password strength meters in that once a maximum (or good enough) score is reached users likely stop. Switching to a strength indication with no upper bound (e.g. estimated guesses needed to crack a password) would likely result in stronger passwords.

5 Conclusion

Information security is becoming increasingly important owing to increasing globalization and computing complexity and hence, it is becoming more and more important to motivate end users to improve their security behavior towards safeguarding their information assets and resources. This study contributed an alternative password strength feedback method to existing fear-driven methods (password meters), which used gamification points, and further investigated this password strength feedback method using empirical data.

The results of this study revealed that gamification points as a password strength feedback method did not significantly influence users' security behavior more positively than the meter feedback method, as no statistically significant difference

regarding password strength and intrinsic motivation towards better password choice was found between the two password strength feedback methods. However, considering the average password score and averages of other password properties (e.g. the time to crack a password), the findings still revealed a slight increase in password strength for passwords created by respondents who were presented with the points feedback method.

This study is limited by the sample and context. The data, therefore, should be interpreted in this context and cannot be generalized to all internet users. Furthermore, this study is limited by the experimental environment, which cannot force respondents to treat the sign-up process as seriously as they would in a real-world situation. This study is also not able to reveal whether password strength was influenced by the password strength feedback method or by other factors (e.g. user's personality, curiosity or password perception). It is acknowledged that potential participants were provided with a brief description of the study ('investigation into information security behavior') which may lead to demand characteristics, resulting in participants interpreting the purpose of the experiment and subconsciously behaving differently to meet their interpretation. We tried to minimize this possibility by not disclosing our focus on password strength and password-creating behavior.

Future research could expand the experiment with questions that investigate whether respondents acknowledged and interacted with the feedback method or not. Password strength should also be investigated further through the consideration and testing of passwords' estimated crack times to determine password strength. The estimated crack time of a password has no upper limit, unlike the strength score of a password, and could serve as a more accurate measure of password strength.

Acknowledgements. This work is based on the research supported wholly / in part by the National Research Foundation of South Africa (Grant Numbers 114838).

References

1. O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE. 91, 2021–2040 (2003). https://doi.org/10.1109/JPROC.2003.819611.
2. Mwagwabi, F., McGill, T., Dixon, M.: Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines. In: 2014 47th Hawaii International Conference on System Sciences. pp. 3188–3197 (2014). https://doi.org/10.1109/HICSS.2014.396.
3. Van Acker, S., Hausknecht, D., Joosen, W., Sabelfeld, A.: Password Meters and Generators on the Web: From Large-Scale Empirical Study to Getting It Right. In: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. pp. 253–262. ACM, New York, NY, USA (2015). https://doi.org/10.1145/2699026.2699118.
4. Vance, A., Eargle, D., Ouimet, K., Straub, D.: Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment. In: 2013 46th Hawaii International Conference on System Sciences. pp. 2988–2997 (2013). https://doi.org/10.1109/HICSS.2013.196.

5. Carnavalet, X. de C. de, Mannan, M.: From Very Weak to Very Strong: Analyzing Password-Strength Meters. In: NDSS (2014). https://doi.org/10.14722/ndss.2014.23268.
6. Kim, T.H.-J., Stuart, H.C., Hsiao, H.-C., Lin, Y.-H., Zhang, L., Dabbish, L., Kiesler, S.: YourPassword: Applying Feedback Loops to Improve Security Behavior of Managing Multiple Passwords. In: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security. pp. 513–518. ACM, New York, NY, USA (2014). https://doi.org/10.1145/2590296.2590345.
7. Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M.L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L.F.: How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. In: Proceedings of the 21st USENIX Conference on Security Symposium. pp. 5–5. USENIX Association, Berkeley, CA, USA (2012).
8. Bénabou, R., Tirole, J.: Intrinsic and Extrinsic Motivation. Rev Econ Stud. 70, 489–520 (2003). https://doi.org/10.1111/1467-937X.00253.
9. Lowry, P., Gaskin, J., Twyman, N., Hammer, B., Roberts, T.: Taking "Fun and Games" Seriously: Proposing the Hedonic-Motivation System Adoption Model (HMSAM). Journal of the Association for Information Systems. 14, (2013).
10. Furnell, S., Bär, N.: Essential Lessons Still Not Learned? Examining the Password Practices of End-Users and Service Providers. In: Marinos, L. and Askoxylakis, I. (eds.) Human Aspects of Information Security, Privacy, and Trust. pp. 217–225. Springer Berlin Heidelberg (2013).
11. Boss, S.R., Galletta, D.F., Benjamin Lowry, P., Moody, G.D., Polak, P.: What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. MIS Quarterly. 39, 837–864 (2015).
12. D'Arcy, J., Herath, T.: A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. Eur J Inf Syst. 20, 643–658 (2011). https://doi.org/10.1057/ejis.2011.23.
13. Johnston, A.C., Warkentin, M.: Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly. 34, 549-A4 (2010).
14. Gagné, M., Deci, E.L.: Self-determination theory and work motivation. Journal of Organizational Behavior. 26, 331–362 (2005). https://doi.org/10.1002/job.322.
15. Ryan, R.M., Deci, E.L.: Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. Contemporary Educational Psychology. 25, 54–67 (2000). https://doi.org/10.1006/ceps.1999.1020.
16. Deci, E.L., Ryan, R.M.: Handbook of self-determination research. University of Rochester Press, Rochester, NY, US (2002).
17. Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., Herley, C.: 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. pp. 2379–2388. ACM, New York, NY, USA (2013). https://doi.org/10.1145/2470654.2481329.
18. Deterding, S.: The Lens of Intrinsic Skill Atoms: A Method for Gameful Design. Human–Computer Interaction. 30, 294–335 (2015). https://doi.org/10.1080/07370024.2014.993471.
19. Hamari, J., Koivisto, J., Sarsa, H.: Does Gamification Work? – A Literature Review of Empirical Studies on Gamification. In: 2014 47th Hawaii International Conference on System Sciences. pp. 3025–3034 (2014). https://doi.org/10.1109/HICSS.2014.377.
20. Kroeze, C., Olivier, M.S.: Gamifying authentication. In: 2012 Information Security for South Africa. pp. 1–8 (2012). https://doi.org/10.1109/ISSA.2012.6320439.

21. Ophoff, J., Janowski, M.: Examining Gamification as a Driver of Individual Information Security Behavior. In: Conference Proceedings of the 2015 Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13. Delaware, USA (2015).
22. Deterding, S., Dixon, D., Khaled, R., Nacke, L.: From Game Design Elements to Gamefulness: Defining "Gamification." In: Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments. pp. 9–15. ACM, New York, NY, USA (2011). https://doi.org/10.1145/2181037.2181040.
23. Jordan, P.W.: Designing Pleasurable Products: An Introduction to the New Human Factors. CRC Press, London (2000).
24. Zhang, P.: Technical Opinion: Motivational Affordances: Reasons for ICT Design and Use. Commun. ACM. 51, 145–147 (2008). https://doi.org/10.1145/1400214.1400244.
25. Blohm, I., Leimeister, J.: Gamification - Design of IT-Based Enhancing Services for Motivational Support and Behavioral Change. Business & Information Systems Engineering. 5, 275–278 (2013).
26. Thiebes, S., Lins, S., Basten, D.: Gamifying Information Systems - A Synthesis of Gamification Mechanics and Dynamics. ECIS 2014 Proceedings. (2014).
27. Shay, R., Bauer, L., Christin, N., Cranor, L.F., Forget, A., Komanduri, S., Mazurek, M.L., Melicher, W., Segreti, S.M., Ur, B.: A Spoonful of Sugar?: The Impact of Guidance and Feedback on Password-Creation Behavior. In: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. pp. 2903–2912. ACM, New York, NY, USA (2015). https://doi.org/10.1145/2702123.2702586.
28. Creswell, J.W.: Research Design: Qualitative, Quantitative and Mixed Methods Approaches. SAGE Publications, Inc, Thousand Oaks (2014).
29. Orne, M.T.: Demand Characteristics and the Concept of Quasi-Controls 1. In: Artifacts in Behavioral Research. Oxford University Press, New York (2009). https://doi.org/10.1093/acprof:oso/9780195385540.003.0005.
30. Wheeler, D.: zxcvbn: realistic password strength estimation, https://blogs.dropbox.com/tech/2012/04/zxcvbn-realistic-password-strength-estimation/, (2012).
31. O'Brien, H.L., Cairns, P., Hall, M.: A practical approach to measuring user engagement with the refined user engagement scale (UES) and new UES short form. International Journal of Human-Computer Studies. 112, 28–39 (2018). https://doi.org/10.1016/j.ijhcs.2018.01.004.