**Research proposal transcript**

**Title of Research:** Using gender specific Human Factors for password meter designs to improve women’s password strength

University of Essex Online: Research Methods and Professional Practice September 2022

Agne Angelides

Student ID: 12688066

**Table of contents**

[Introduction 2](#_Toc119251428)

[Significance, Contribution to the discipline and Research Problem 4](#_Toc119251429)

[Research project aims and objectives 5](#_Toc119251430)

[Research question(s) 6](#_Toc119251431)

[Research methodology 6](#_Toc119251432)

[Ethical considerations and risk assessment 8](#_Toc119251433)

[Description of artefact(s) that will be created 8](#_Toc119251434)

[Timeline of the proposed activities 9](#_Toc119251435)

[References 10](#_Toc119251436)

# **Introduction**

“Human is the weakest link” has become the daily mantra of the cyber security specialists over the years and it can often be seen quoted in popular media content as well as the research related work; a quick Google search returns over 2000 results using this exact phrase. Whilst there has been an increase in the research on how the Human Factors impact the cyber security, the multidisciplinary approach to resolving the cyber security issues is still somewhat lagging, especially in terms of whether the gender has any impact on the overall person’s security practices and whether the technology should be designed with this in consideration.

Although there is a lack of research on whether the gender specific policies and user interface designs could improve one’s security hygiene, the relationship between the gender and the security has been explored a little. Women between the age of 40 and 49 have been found to fall for the cybercrimes more often than other age group and gender combinations (Gratian et al, 2018) and they appear to be less dedicated in keeping the devices up to date (Gratian et al, 2018). Moreover, women have been shown to use weaker passwords (Gratian et al, 2018; Juozapavičius, 2022) with men’s passwords having been found to be twice as strong as women’s (Juozapavičius, 2022). The passwords used by women usually contain personally significant and meaningful information with 30% of women using their family member names, pet names and personal dates (Grigas, 2021) making it easy to crack with brute force attacks.

The relationship between the security hygiene and the gender, however, is not quite conclusive. Both men and women have been shown to use similar data access control settings on their smartphones (Clausnitzer, 2021), although, the figures do not say how many of these settings were the default ones. Another study found that men have more knowledge on the acceptable cyber hygiene norms (Cain et al, 2018) whilst in a different study, conducted only two years later, women were those with more cyber security knowledge, stringent attitudes, and practices (Neigel et al, 2020). Moreover, the HAIS-Q questionnaire, used to evaluate specific cyber hygiene attitudes towards things like password management, email and internet use, etc. (Parsons et al, 2017) has found evenly distributed scores between men and women, thus concluding that the gender had no impact on cyber hygiene, only the person’s knowledge and attitudes did.

Whilst the results are not always conclusive on the gender differences in cyber hygiene, women do appear to be the “Weak link” when it comes to the password hygiene, based on the existing research discussed. The reasons behind this, however, are not obvious.

According to the Social Cognitive Theory (Bandura, 1986), people with lower self-efficacy place less trust in their ability to accomplish something, whilst negative emotions can also have an impact on one’s self belief. Coincidentally, women have been found to have a lower computer related self-efficacy (Anwar et al, 2017), although the correlation between it and the lack of cyber hygiene has not been confirmed (Neigel et al, 2020). The stringent password policies of many existing websites can cause the user frustration too and an inability to recall the password shortly afterwards (Shay et al, 2010). Moreover, the password meters are often inconsistent, inaccurate, unhelpful, and not very appealing (Gola & Dürmuth, 2018; Ur et al, 2017). Poorly designed website components, such as the password meters, and frustrations over stringent policies, could lead to user resentment and a decrease in the self-efficacy (Grimes & Marquardson, 2019). Thus, the Social Cognitive Theory could potentially explain some of the reasons why women are more likely to have weaker passwords than men.

# **Significance, Contribution to the discipline and Research Problem**

A password meter is a visual representation of the strength of the password entered by the user, and it usually takes a form of a bar within which a traffic light scheme is implemented to advise the person of the password’s suitability. Meters can be standalone components or be used in conjunction with the list of password requirements. Basic password meters used together with stringent requirements and aesthetically pleasing meters with less strict requirements have both been found to produce stronger passwords (Ur et al, 2012).

Out of the 20 most popular websites in the UK in 2022 (smilarweb), upon the inspection, only three have been found to have password meters: BBC, Daily Mail and Reddit. This trend isn’t new: many applications and websites are designed with the perfect user in mind (Millar et al, 2021). Women especially appear to be exposed to a variety of threats on existing platforms due its developers failing to consider women specific threats and risks during the development process. As an example, social media platform default privacy settings do not provide enough protection for women (Millar et al, 2021) who are more likely to become victims of the online abuse (Storry & Poppleton, 2022); if the women fail to update default values to something more suitable, they also then suffer from the victim blaming (Millar et al, 2021).

Thus, this study fills the gap in the multidisciplinary cyber security research area by addressing the lack of research on the gender specific cyber risk and threat impact on the website and application design, specifically, password meters and how the existing meter concepts could be improved to ensure women password strength increases, so that one particular gender is not disadvantaged by the genderless design considerations.

# **Research project aims and objectives**

Whilst there exists a wide variety of password meters, the designs tend to be ad-hoc with lack of insight into what constitutes a strong password (de Carné de Carnavalet & Mannan, 2014). Those that do provide the password requirements, often use very stringent password rules resulting in frustrated users (Ur et al, 2012, Shay et al, 2010) who are unable to recall the recently created password (Shay et al, 2010).

Hence, this research aims to explore if the Social Cognitive Theory (Bandura, 1986) could be applied to the password meter designs and its suitability guidelines to trigger the desired action in women when creating new accounts, namely, the creation of a strong password.

In other words, this research aims to explore how the human factors specific to women could be used to improve the women’s password strength in order to improve their password hygiene.

Thus, this research project objectives are as follows:

1. To shortlist the reasons and hypothesis believed to be responsible for the women’s poor password hygiene.
2. To determine the visual cues, colours, tone of messages, message phrasing and page layout believed to help with increasing women’s self-efficacy as per the Social Cognitive theory (Bandura, 1986).
3. To assess whether a password meter designed with a women’s self-efficacy in mind could improve the women’s password strength.
4. To assess whether the proposed password meter changes positively influence password strength of other genders.

# **Research question(s)**

This research project aims to answer the following three questions: can the password meter and guidelines designed to improve women’s self-efficacy improve their password strength, can the password meter and guidelines designed with women’s self-efficacy in mind improve men’s password strength and whether the passwords created by different genders using the proposed password meter and guidelines are comparable in strength?

# **Research methodology**

A literature review and analysis of the existing research is to be conducted to better understand the drivers behind the weak password choices made by women and to find ways to mitigate it. This will be completed by using the Google Scholar, Semantic Scholar, Research Gate, and the University of Essex Online Library platforms whilst focusing on the work from the last 7 years, which is not to be restricted by any publishing language or geography. Some predating seminal studies will be included too, where necessary. Further insight into the current password meter usage and practices will be obtained by inspecting the most popular webpages within the UK.

To be able to test the participant’s response to the proposed password meter and its guidelines, a fictitious website will be built as well as a new user registration form, where the password meter is to be implemented. The website will be hosted either using Github pages or another free or low cost platform; upon the start of the project additional research will be conducted to ensure the most suitable and secure option is used. The website will log the time spent registering and the passwords provided.

Whilst the proposed meter design and the password creation guidelines could be showcased in a mock-up screenshot format within the survey itself, the research would then be limited to the questions of a speculative nature to find out how the participants feel about the proposed changes. It is believed that that by requesting the users to undergo through a simulation of the registration process, their password choices will provide a better representation on how the rest of the population creates theirs.

The online registration form will be accompanied by a survey, to obtain demographic data on the participants’ gender, age, occupation, and the level of the computer self-efficacy. Moreover, the survey will use open ended follow up questions to better understand the user views towards the proposed changes, what they liked and did not like about it.

The study will focus on the UK’s working age population only (aged 16 to 64 years) and there will be no additional demographic restrictions applied. Any gender will be permitted to partake in the survey, since whilst this research is focused on women and their password hygiene, it is important to understand the impact the proposed changes have across all genders, for comparison.

The study will be distributed by emails and on social media platforms such Facebook and LinkedIn, aiming to achieve a total of 385 respondents for a p-value of 5% (Qualtrics, 2022) based on the UK’s working age population size of 41 million (Office for National Statistics, 2022). It is believed that this sample size will provide a good representation of the UK’s working age population.

Both types of qualitative and quantitate data analysis will be performed using the survey results. The responses to the open ended user experience questions will be analysed qualitatively to get some further insights into the user’s views towards the password meters. The quantitative analysis will be performed using the demographic user data from the survey, the passwords entered and other metrics, such as the amount of time spent on the website.

# **Ethical considerations and risk assessment**

The research participants will have to consent to participating in the study by completing the consent form which will provide the research description and its goals, information about who is conducting the survey, what data is to be collected and how it will he be used, whist also addressing the voluntary participation principle and the participant’s right to opt out from the research.

To be able to test the password meter impact on the password’s strength, the user provided passwords will have to be stored. Because of the potential security risks in case of participants using their everyday passwords, any personal identifiers will not be collected or stored by this survey (even if provided on the fictitious website), only demographic related metrics such as the age, gender, and occupation and the user entered password.

Additionally, any existing research work used by this project, will be referenced throughout the work. This research results will be published in full, and no data will be manipulated to support the researcher’s personal beliefs.

# **Description of artefact(s) that will be created**

During this research project, a registration form will be created on a fictitious website, where the users will be able to create a new account by populating the registration form and submitting it.

A password meter together with acceptable password guidelines will be implemented within this registration form to test the research questions. The password meter and guidelines will be based on the outcome from the literature review and analysis.

# **Timeline of the proposed activities**

The activities needed to complete this research project will be undertaken in the order and time specified in the table. The estimates are based on a project with a duration of 30 weeks.

The literature research will take 5 weeks, followed by the literature review, which is planned for another 4 weeks. Then the existing websites will be inspected for their current password meter and password policies; this will take up to 1 week. The next step will involve the design and the build of the website, the registration form, the password meter, and the password guidelines and it is planned to take 5 weeks. This is to be followed by 3 weeks of designing the survey and a further 6 weeks of the survey being live online for the participants to respond to. Lastly, the analysis of the data obtained from the survey is expected to take 3 weeks, whilst the completion of the report is also planned for a further 3 weeks.

# **References**

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. & Xu, L. (2017) Gender difference and employees’ cybersecurity behaviors. *Computers in Human Behavior*, 69, pp.437–443.

Bandura, A. (1986) Social foundations of thought and action. *Englewood Cliffs, NJ*, *1986*(23-28).

Cain, A.A., Edwards, M.E. & Still, J.D. (2018) An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, pp.36–45.

Clausnitzer, J. (2021) Restricting smartphone app data access in Finland 2018, by gender. Available from: https://www.statista.com/statistics/955247/people-restricting-smartphone-apps-data-access-gender-finland/ [Accessed 7 November 2022].

de Carné de Carnavalet, X., & Mannan, M. (2014) From very weak to very strong: Analyzing password-strength meters. In Network and Distributed System Security Symposium (NDSS 2014). Internet Society.

Golla, M. & Dürmuth, M. (2018) On the Accuracy of Password Strength Meters. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. (2018) Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, pp.345–358.

Grigas, L. (2021) Do Women and Men Have Similar Password Habits? Available from: https://nordpass.com/blog/women-men-password-habits/ [Accessed 7 November 2022].

Grimes, M. and Marquardson, J. (2019). Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems*, 119, pp.23–34.

Juozapavičius, A., Brilingaitė, A., Bukauskas, L. & Lugo, R.G. (2022) Age and Gender Impact on Password Hygiene. *Applied Sciences*, 12(2), p.894.

Millar, K., Shires, J., & Tropina, T. (2021) Gender approaches to cybersecurity: design, defence and response. *Gender approaches to cybersecurity: design, defence and response*.

Neigel, A.R., Claypoole, V.L., Waldfogle, G.E., Acharya, S. & Hancock, G.M. (2020) Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, 92, p.101731.

Office for National Statistics (2022) LFS: Population aged 16-64: All: Thousands: SA. Available from: <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/timeseries/lf2o/lms> [Accessed 13 November 2022].

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. & Zwaans, T. (2017) The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, 66, pp.40–51.

Qualtrics (2022) Determining Sample Size. Available from: <https://www.qualtrics.com/ebooks-guides/determining-sample-size/?utm_lp=blog-calculating-sample-size-inline1> [Accessed 13 November 2022].

Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. and Cranor, L.F. (2010) Encountering stronger password requirements. Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS ’10.

Similarweb (2022) Top Websites Ranking. Available from: <https://www.similarweb.com/top-websites/united-kingdom/> [Accessed 10 November 2022].

Storry, M. & Poppleton, S. (2022) Impact of online abuse and harassment revealed in new research from the Victims’ Commissioner. Available from: <https://victimscommissioner.org.uk/news/impact-of-online-abuse-and-harassment-revealed-in-new-research-from-the-victims-commissioner/#:~:text=The%20Victims'%20Commissioner's%20survey%20found,to%20be%20experienced%20by%20women>. [Accessed 12 November 2022].

Ur, B., Habib, H., Johnson, N., Melicher, W., Alfieri, F., Aung, M., Bauer, L., Christin, N., Colnago, J., Cranor, L.F., Dixon, H. and Emami Naeini, P. (2017) Design and Evaluation of a Data-Driven Password Meter. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI ’17*.

Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M.L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N. and Cranor, L.F. (2012) How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. www.usenix.org. Available at: https://www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/ur [Accessed 10 November 2022].