The Influence of Graphical Representations of Password Strength on the Behaviour of Potential Victims of Cybercrime

Aljoscha Ocko

University of Twente

Bachelor Psychology; 201000150

Iris van Sintemaartensdijk

26th of February, 2021

Abstract

Cybercrime is a problem of increasing importance in the digitalised world. One important aspect of cybercrime prevention is password security and the question of how to motivate potential victims of cybercrime to choose secure passwords. Using the framework of Protection Motivation Theory and taking findings from other areas into consideration, this study seeks to investigate whether or not participants can be influenced by presenting them with a colour-coded graphical representation of password strength. Results indicate that being presented with a graphic does not increase participants' intent to change passwords and also does not increase the reported level of information gained. Implications and limitations of the study are discussed.

Introduction

Background

With the advent of commercial computers and widespread public access to the internet, a new type of crime emerged and drastically increased both in scale and impact. This new type of criminal behaviour is commonly referred to as cybercrime, which is defined as any crime that involves a computer and a network (Moore, 2014). Broadly defined as it is, cybercrime includes a vast array of crimes, ranging from historically common crimes that found new applications through recent technological developments (e.g., blackmail/ransomware) to those crimes that have been given a whole new significance or were made possible entirely by technological means (e.g., identity theft, computer viruses, phishing) (Jahankhani; Al-Nemrat, & Hosseinian-Far, 2014).

Norton (2017) lists the five most common cybercrimes in the United States as part of its Cyber Security Insights Report, with three out of five of the listed crimes being related to password security. Moreover, accessing another person's account is one of the most common offenses in civil litigation cases concerning cybercrime (Krohn, Hendrix, Hall, & Lizotte, 2019), with 54% of technical circumvention claims involving password theft (Mayer, 2016). Further adding to this problematic are other risk factors, like the vast number of login credentials (i.e., separate passwords and usernames for different web services) each individual needs to remember (over 100 for the average UK citizen), leading to passwords being used for multiple accounts, including work-related passwords that might give criminals access to whole organizations (Eddolls, 2016). Furthermore, an analysis carried out by the British intelligence agency GCHQ (2019) revealed that a large number of victims of cybercrime used insufficiently strong passwords (23.3 million victims using "123456"; 3.6 million "password" as their password). Another study asked over nine hundred people about their use of passwords and found that half of respondents used passwords with less than six characters, 80% only used letters and never changed their passwords, and 78% used personal information to create their passwords (Zviran & Haga, 1999).

The purpose of this study will, therefore, be to explore a way to persuade potential victims of cybercrime to select secure passwords. If successful, insights gained through this research might help online service providers inform their users more effectively on how to choose a sufficiently strong password. To get an idea on what approach could be useful in respect to finding a suitable intervention and inform the ultimate study design, different theories are considered and their applicability discussed.

The Problem

The problem of lacking awareness of password security does not only pose a threat to the bank accounts of individuals and corporations, it may also threaten national and international security. In wake of the 2016 US presidential election a scandal arose when hackers broke into the email account of John Podesta, former Chief of Staff under Bill Clinton and chairman of the Hillary Clinton presidential campaign, and leaked all his communications to Wikileaks (Matishak, 2016). Although the hackers managed to do so via a phishing attack, the leaked information revealed that Podesta not only used passwords of questionable strength for someone in his position ("Runner4567" and "p@ssword"), but also once asked his assistant to email his password to him, used the same password for multiple services, and apparently failed to change his password even after the leak happened.

Next to this most recent example of hackers breaching supposedly secure government(-connected) networks by cracking, guessing, or phishing passwords, there are numerous other known cases in history. Namely, German hackers cracking passwords of accounts belonging to military networks to obtain sellable information (Stoll, 1988); hackers guessing passwords of 150 accounts belonging to the Israeli parliament (DiDio, 1998); passwords being cracked at the US Department of Defense (DiDio, 1998); and a teenager breaching computers belonging to the Pentagon and inadvertently almost causing a war with North Korea (Ungoed-Thomas, 1998). Notably, in three out of four of these cases the culprits were not foreign government agencies with considerable resources, but merely teenagers working with minimal consumer-grade equipment. Perhaps unsurprisingly, as in the last-mentioned case, the hacker managed to bypass security by guessing that the password for a Pentagon computer was “guest”. These various examples make it clear that it is of upmost importance to educate people on proper password security and motivate them to apply some general rules to avoid becoming vulnerable to these types of attacks. Based on the fact that computers have become more popular and knowledge regarding their use more accessible, we may assume that since the 1990s there has been a rise in awareness concerning cybercrime, especially concerning government networks containing sensitive information. However, the circumstances of the Podesta case make this assumption questionable at best.

It should be mentioned that there is a multitude of alternative security concepts that have been proposed to replace the traditional system of user passwords. For instance, some systems require users to pass one additional step of authentication, like confirm a code sent to them via SMS, or by making use of a separate TAN system, as many banks do (Krol, Philippou, De Christofaro, & Sasse, 2015). There are also systems called “password managers” which enable users to manage and encrypt their passwords within one browser by using one master password. However, none of these concepts have proven to be superior to the contemporary system, as they often lack in terms of usability or sometimes security, for example, in case someone uses a password manager on their phone and loses their phone (Bonneau, Herley, Oorschot, & Stajano, 2012). The same was found to be true for two-factor authentication, which is already mandatory for most banks and optional for some other web-based services (Krol et al., 2015). Due to this circumstance, it might prove more effective to focus on encouraging protective behaviours within the current system, at least until a viable alternative to passwords arises.

Apart from advising against some of the more obviously careless actions regarding cybersecurity highlighted in the aforementioned cases, we should consider one important aspect of password security, which is the question of what makes a strong password. Even if people refrained from including any personal information in their passwords, as was reported by Zviran and Haga (1999), they still would be vulnerable to cyberattacks, since the vast majority (70%) of security breaches are committed by outsiders, rather than people familiar to them, as was found by Verizon in der 2020 Data Breach Investigations Report. Furthermore, they found that of those breaches affecting web applications, 80% were committed via "stolen or brute-forced login credentials". Similarly, Leukfeldt and Yar (2016) found that the degree of online activity ("visibility") is the best predictor of victimization for all kinds of cybercrime and that contact with strangers, such as adding them on online platforms, further increases likelihood of victimization.

In context of cybercrime, a brute force attack is a common method of cracking passwords, whereby a computer program is employed to automatically go through every possible combination of ciphers until it finds the password in question. The success of and time required for this process depends on the password itself (i.e., number of characters and complexity), the processing power of the tools available to the hacker (i.e., CPU/GPU and potential botnets), as well as the software that carries out the attack, since each software may use a different method (Álvarez, Montoya, Romera, & Pastor, 2004; Shankdhar, 2020). Due to these circumstances, the question whether or not a brute-force attack will be successful is almost entirely dependent on the password, as the average time required to crack can vary from a fraction of a second to many quintillions of years. Brute-force attacks are a highly prevalent method to access restricted networks (Abraham, Lloret Mauri, Buford, Suzuki, & Thampi, 2011; Alata, Nicomette, Kaaniche, Dacier, & Herrb, 2006). Conolly and Wall (2019) investigated cyberattacks at twenty-one different organizations, twelve of which were attacked via brute-forcing passwords. Since there is no way of controlling the means by which hackers may attempt to break into accounts, the only way to effectively reduce this specific type of cybercrime is to educate potential victims on the importance of secure passwords and motivate them to make use of techniques by which they can minimize the risk of being victimized by cybercriminals.

Most of the major online service providers, such as Facebook or Google, already made it standard practice to require users to choose a secure password by making a certain length or use of special characters mandatory. However, this practice may not be universally enforced by smaller providers or private networks used by corporations or governments, as illustrated by some of the previously mentioned examples. For this reason, it may be more viable to focus our efforts on finding ways to motivate the users themselves to take necessary action to protect themselves. This way potential victims of cybercrime would be able to minimize risks across all platforms, regardless of the platforms' policies. Additionally, if the average user made it a habit to use secure passwords on every platform, some of the alternative systems to increase security (e.g., two-factor authentication) would either not be necessary or further increase security, instead of acting as the linchpin of the whole system.

Protection Motivation Theory

Probably the most longstanding and best-established psychological theory with respect to protective behaviours is Protection Motivation Theory, which was formulated by Ronald Rogers in 1975 and has since been refined. It postulates that the question of whether or not a person will take protective action towards a threat is determined by four factors: (1) the perceived severity of a threat; (2) the perceived chance of the occurrence; (3) the efficacy of the protective measure; (4) the perceived self-efficacy, meaning how likely a person believes their implementation of the protective measure to be. PMT has previously been applied to online protective behaviour and it has been shown that messages focussing on coping-appraisal were more effective than those focussing on threat-appraisal (Tsai, Jiang, Alhabash, LaRose, Rifon, & Cotten, 2016; Van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019). Following this, any intervention aimed at making subjects select stronger passwords should prioritize delivering a coping-message over a fear-appeal if necessary. This assumption is also confirmed by research that looked at password security in particular, which found that most users simply don't perceive themselves to be at risk of falling victim to password breach (Weirich & Sasse, 2001).

With this caveat taken into consideration, our focus for successfully persuading people to change their passwords should be on the two factors related to coping-appraisal, namely the perceived efficacy of the protective measure and the perceived self-efficacy. This means that any measure aimed at being persuasive should ideally suggest to the user that it is both highly effective at preventing their passwords from being breached, as well as being easy and quick to implement. Considering that most people do not perceive this type of cybercrime to be a big threat to them, it is likely that most people would also not be willing to invest too much time and energy into processing information related to a threat they do not perceive to be important. For this reason, cognitive load should be taken into consideration when designing any interventive measures and short, concise messages should be prioritized over long-winded explanations.

The Right Presentation

Protection Motivation Theory unfortunately does not give us any insight regarding the visual presentation of information that goes beyond the precise framing in regards to coping- and fear-appraisal. For this reason, we need to consult other research with respect to presentation, as well as to decide what information to present. As the research by Zviran and Haga (1999) as well as the GCHQ report made clear, there seems to be a substantial lack in understanding of the importance and mechanics of password security among the population, as most seem to prioritize usability over security. We should, therefore, focus our efforts on informing users on these issues. One way to educate and motivate potential victims of cybercrime might be by presenting to them concise information on password strength in the form of a graphical representation. This could help with addressing the problem of cognitive load and might help users understand that by merely adding one or two characters to their passwords would already greatly reduce their risk of falling victim to this type of cybercrime, thereby also addressing PMT's factors of self-efficacy and protective efficacy.

Past research has shown that graphical representations can greatly increase post-exposure interest in presented information (Park & Lim, 2004) and positively influence health-related protective behaviours (Rosenblatt et al., 2018; Steurer-Stey, Zoller, Chmiel Moshinsky, Senn, & Rosemann, 2010), as well as behaviours related to waste-reduction (Farr-Wharton, Foth, & Choi, 2012). Additionally, graphics that are specifically colour-coded were shown to motivate behaviour to avoid hazards (Braun & Silver, 1995) and improve decision making as long as information complexity is low (So & Smith, 2002). It should also be noted that, due to passwords being used almost universally on coloured screens, there is no cost to using colour in the way of presenting the information, while there is seemingly a high potential for benefits.

Following this line of research, we aim to investigate which effect a colour-coded graphical representation of password strength might have on the intended behaviours of potential victims of cybercrime. Information gained this way could potentially inform service providers on how to address users and increase awareness of password security. For instance, instead of simply requiring users to pick a secure password, online platforms could briefly show a graphic highlighting the importance of a strong password, thereby possibly shielding users from data breach on their platforms and beyond. This is where a graphical representation may prove effective, both in informing potential victims about password security, as well as shaping intentions for increasing security. We believe that these two potential effects are the most worthwhile to investigate. The optimal effect would probably be that a user immediately changes his or her password in accordance with the learned information. However, this is only effective if the user also gained any useful information from looking at the graphic, since otherwise changing the password would have no effect. To possibly answer these questions, the following hypotheses were investigated:

H_1: The group exposed to the graphical representation is more likely to report the intention to change their passwords than the control group.

H_2: The group exposed to the graphical representation is more likely to report that they are more informed about password security than the control group.

Methods

Participants and Design

After removing data points, which were invalid due to incomplete responses, the final dataset was comprised of 131 participants. The sample was primarily female (n = 88) and from Germany (67.9%), with another 23.7% of the sample coming from the Netherlands and 8.4% of participants coming from various other countries. Ages ranged from 18 to 66 years old, with the mean age being 26.5 years and median being 21 years, with a standard deviation from 12.5 years. Most participants reported a high school degree as their highest completed education (67.9%), followed by a Bachelor's (16.8%) and Master's (13%) degree. Two participants reported not to have finished school (1.5%) and one had a PhD (.8%). Participants were recruited partly through the SONA credit system of the University of Twente and partly by being invited directly by the researcher. Participants were informed about the nature of the study and ensured that their data would be handled anonymously and not shared with third parties. Furthermore, it was emphasized that they could choose to withdraw consent and stop the participation at any point. Based on this, informed consent was obtained from all participants in the dataset.

The study had a one-factor between-participants design with the independent variable being MoP, meaning Method of Presentation (graphical representation versus bullet point list) and the dependent variables being Feeling Informed (low versus high) and Intent to Change PW (low versus high). “Feeling Informed” refers to the degree to which participants felt informed by the study and “Intent to Change PW” to their reported intent to change their passwords following the study. Both dependent variables were recorded with a five-point Likert scale ranging from “strongly disagree” to “strongly agree”.

Materials

Risk Perception Questionnaire

A risk perception questionnaire was constructed to measure perceived risks related to cybercrime, in order to see if this plays a role in the outcome (for instance, whether or not risk-averse people are more likely to respond to the intervention). The questionnaire consisted of ten questions and required the participant to consider if he or she agrees with various statements regarding perceptions and feelings surrounding cybercrime. A five-point Likert scale was utilized, which ranged from “strongly disagree” at 1 to “strongly agree” at 5. The mean response to this questionnaire was at 3.2, which mostly corresponds to the “neither agree nor disagree” option, with a standard deviation of .58. Exploratory factor analysis as well as Cronbach’s test of reliability were carried out for this and all other questionnaires that were constructed by the researcher. The risk perception questionnaire passed the threshold of acceptable reliability ($\alpha = .72$). However, factor analysis revealed that the scale measured three factors in total, with the second factor (four items; factor loadings from .50 to .85) explaining 16.3% of the variance and seemingly representing items related to financial worries (e.g., online banking and shopping) and the third factor accounting for 11.8% of the variance and seeming to be an artifact of the framing of the items, as only the two positively worded items loaded on this third factor (factor loadings .73 and .79). Factor one explained 29.5% of the variance and was comprised of four items, with factor loadings ranging from .48 to .82.

Actual and Perceived PW Strength

Another scale was used to assess participants' actual and Perceived PW Strength, by asking them questions about their subjective thoughts and feelings about their respective passwords and directly inquiring about the characteristics of their passwords. This way we could control whether participants' subjective perception as well as the actual strength of their passwords would in any way influence the results. This was done via a five-point (agree/disagree) Likert scale. The first four items of the password strength questionnaire, which were meant to measure Perceived PW Strength, had a mean response of 3.30, a standard deviation of .77, and were not reliable (α = .59). However, after removing the first item the scale did meet Cronbach's requirements (α = .70), for which reason this item was removed for any subsequent analysis. The second half of the questionnaire, which was supposed to measure Actual PW Strength, had 4.27 as its mean, .60 as SD, passed the reliability test (α = .74) and no item had to be removed.

Exploratory factor analysis was carried out on the questionnaire as whole. With the exception of the first item, all items supposed to measure Perceived PW Strength loaded most strongly on the second factor, with factor loadings ranging from .52 to .86 and the total factor explaining 20.4% of the variance. The second half of the questionnaire (items 5 to 11), meant to measure Actual PW Strength, was mostly explained by the first factor, which accounted for 30.8% of the variance (factor loadings .72 to .83). The only exception to this being item 7, which was more attributable to the second and third factor with equal loadings (.57), as well as item 11, which mostly loaded on the third factor (.62). Notably, these two items are the only ones asking about the use of special characters, indicating that only a certain subset of participants utilize special characters in their passwords. Factor three and four together accounted for 22.5% of the variance, while the intended factors one and two explained 51.3% cumulatively.

Feeling Informed by the Study / Intent to Change Password Questionnaire

To measure the dependent variables, a five-point Likert scale questionnaire was constructed asking participants with each three questions how informed they felt by the study and how inclined they felt to change their passwords following the study. The items measuring the degree to which participants feel more informed about password security than before the study yielded an average response of 3.75(SD = .86) and proved to be very reliable (α = .83). The same applies to the second variable (µ = 3.03; SD = 1.00) (reported motivation to change one's password after the study), which had a Cronbach's alpha of .85. Exploratory factor analysis for this scale revealed no other factors other than those intended and the items loaded onto the factors in the expected manner. The first factor explained 53.3% of the variance with factor loadings ranging from .75 to .76. The second factor accounted for 23.1% of the variance and its items loaded onto this factor from .52 to .53.

Prior Knowledge

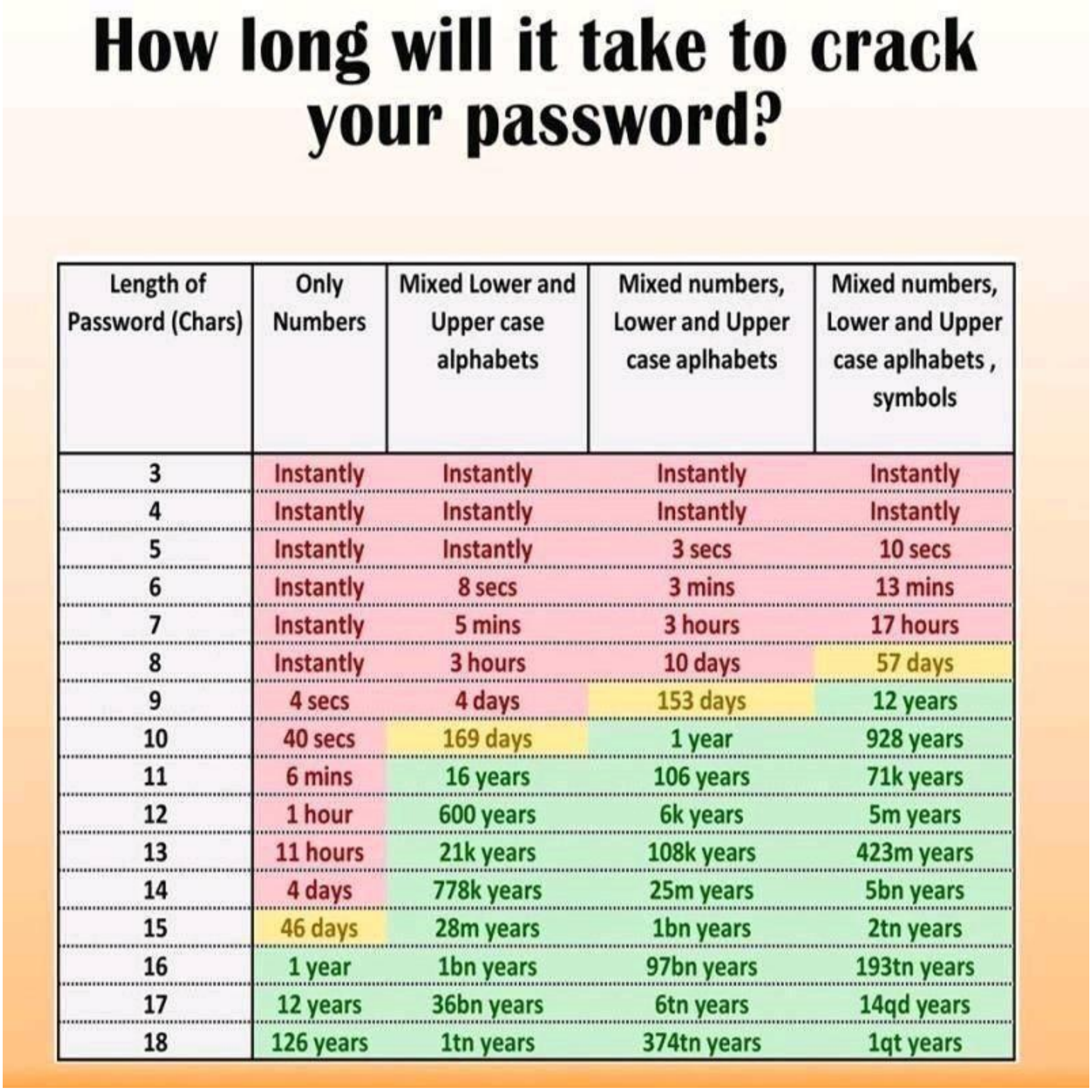
Apart from the self-constructed scales, a quiz was used to assess the prior knowledge participants brought into the study concerning cybercrime, which was later used to assess how much prior knowledge might have affected the outcome. The quiz was obtained from Pew Research Center (2020) and included ten multiple-choice questions, each with only one correct answer, dealing with concepts related to cybercrime in general, with two questions directly concerning password security in particular. The more correct answers a participant got, the more prior knowledge he or she brought into the study. The mean score was 5.2 with a standard deviation of 1.9, indicating that the vast majority of participants scored between three and seven points on the quiz. Cronbach’s alpha for the quiz was at .61, making it sufficient yet not very reliable.

Method of Presentation

In order to investigate whether a colour-coded graphical representation of password strength would be able to influence the outcome measured by the dependent variables, such a graphic was obtained from Quora (2019), the original source of which could not be located (see Figure 1). The graphic shows the number of characters of a password on the y-axis and the number of character sets (e.g., numbers, letters, or symbols) used on the x-axis. Where the rows and columns meet, each cell contains the amount of time it would take a hacker to crack a given password using a brute force attack, with unsafe passwords coloured red, safe passwords coloured green, and borderline passwords coloured yellow. Estimated cracking times range from instantly to one quintillion years. The bullet point list participants in the control condition were given contains three examples from each column of the graphic provided to the experimental group, amounting to twelve examples in total. The bullet points were chosen in a way that would ensure that the information is equivalent to that which is presented in the experimental condition, while not including every single example to reduce cognitive load.

Figure 1

Graphical Representation of Password Strength used for the Experimental Condition



How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Demographics Questionnaire

A basic questionnaire was included requiring participants to disclose information about their education level, sex, age, and country of origin. The questions regarding sex and education gave participants a few options to pick from, while the other two questionnaires had participants fill in their information manually. Manually entered information was subsequently coded for analysis.

Procedure

After being informed about the purpose and nature of the study, as well as being asked for consent under the conditions of anonymity, voluntary participation, and the possibility to withdraw consent at any point, participants filled in the questionnaires, starting with the Risk Perception questionnaire, followed by the quiz on cybersecurity assessing prior knowledge of the topic, and the questionnaire about actual and Perceived PW Strength. Following this, participants were randomly assigned to look either at the graphic on password strength (experimental condition) or a few examples taken from the graphic in bullet point form (control condition). In each test condition, participants were told to look at the graphic/list for some time and get familiar with its content. This was followed up by a few demographic questions (age, gender, nationality, and education) and another questionnaire about the intent of participants to change their password, as well as their perceived gain of knowledge concerning password security. Finally, participants were debriefed and thanked for their participation. Additionally, they were asked to voluntarily leave their Email address, in case there was a follow-up study they would like to participate in. As part of the informed consent form, they were informed that entering their email address would de-anonymize their data.

Results

Preliminary analyses

A preliminary analysis was carried out to explore possible associations between all variables that were part of the final model, as well as demographic information. This will help to get a general idea of what associations exist in the data, help with interpreting the results of the main analyses, and make it possible to rule out potentially collinear and redundant variables. Bivariate correlations indicate that some of the investigated variables are associated with one another (see Table 1). Some of the findings seem rather intuitive (e.g., the positive correlation between prior cybercrime knowledge and password strength) but others are worth pointing out. For instance, the overall strongest correlation is between Perceived PW Strength and the intent to change passwords, making it likely Perceived PW Strength will play a role in the final model.

Furthermore, Risk Perception was negatively correlated to Perceived PW Strength (-.23), indicating that the higher someone's Risk Perception towards cybercrime in general was, the more likely they were to rate their passwords as potentially unsafe. Concerning both dependent variables, the degree to which someone felt informed by the study correlated at .40 with the intent to change one's passwords, suggesting that participants who felt like they gained information by taking part in the study also felt more inclined to increase the security of their passwords. Based on this we can say that the dependent variables are definitely related but not collinear and could each give us different insights in the main analyses.

Table 1

Bivariate Correlation-Matrix for Independent Variables

		PK	Age	Risk Perception	Actual PW strength	Feel informed	Intent to change PW	Perc. PW strength
Prior Knowledge (PK)	Pearson correlation	1	-.146	.032	.229**	.015	-.177*	-.254**
	Sig. (2-tailed)		.096	.716	.009	.867	.043	.003
Age	Pearson correlation	-.146	1	-.195*	.082	-.218*	.044	.105
	Sig. (2-tailed)	.096		.025	.351	.012	.622	.233
Risk Perception	Pearson correlation	.032	-.195*	1	-.018	-.028	-.165	-.233**
	Sig. (2-tailed)	.716	.025		.835	.747	.060	.008
Actual PW strength	Pearson correlation	.229**	.082	-.018	1	-.034	-.088	-.143
	Sig. (2-tailed)	.009	.351	.835		.697	.317	.102

Feel informed	Pearson correlation	.015	-.218*	-.028	-.034	1	.395**	.098
	Sig. (2-tailed)	.867	.012	.747	.697		.000	.264
Intent to change PW	Pearson correlation	-.177*	.044	-.165	-.088	.395**	1	.497**
	Sig. (2-tailed)	.043	.622	.060	.317	.000		.000
Perc. PW strength	Pearson correlation	-.254**	.105	-.233**	-.143	.098	.497**	1
	Sig. (2-tailed)	.003	.233	.008	.102	.264	.000	

*. $p < .05$. **. $p < .01$.

Table 2

Descriptive Statistics for both Dependent Variables in each Test Condition

Method of Presentation		N	Mean	Standard deviation
Bullet-Point	Feel informed	64	3.83	.84
	Intent to change PW	64	3.06	1.00
Graphic	Feel informed	67	3.66	.88
	Intent to change PW	67	3.00	1.00

Note. Each variable was measured on a five-point Likert scale, with 1 = “strongly disagree” and 5 = “strongly agree”.

Main analyses

In order to test the hypotheses, a general linear model was applied. The model included both dependent variables (i.e., Intent to change PW and Feeling Informed), Method of Presentation, as well as the covariates Risk Perception, Prior Knowledge, Actual PW Strength and Perceived PW Strength. Additionally, each of the covariates was investigated for interaction effects with the Method of Presentation to test if any of the covariates moderated the effect of the independent variable. Multivariate analysis revealed that MoP by itself had no significant effect on either of the dependent variables. For intent to change password MoP had no effect; $F(1, 121) = 0.221$, $p = .639$. Concerning feeling informed, presenting participants with a graphical representation of password strength also had no significant effect: *F*(1, 121) = 3.578, *p* = .061 (see Table 3). Based on these findings, both hypotheses were rejected.

Table 3

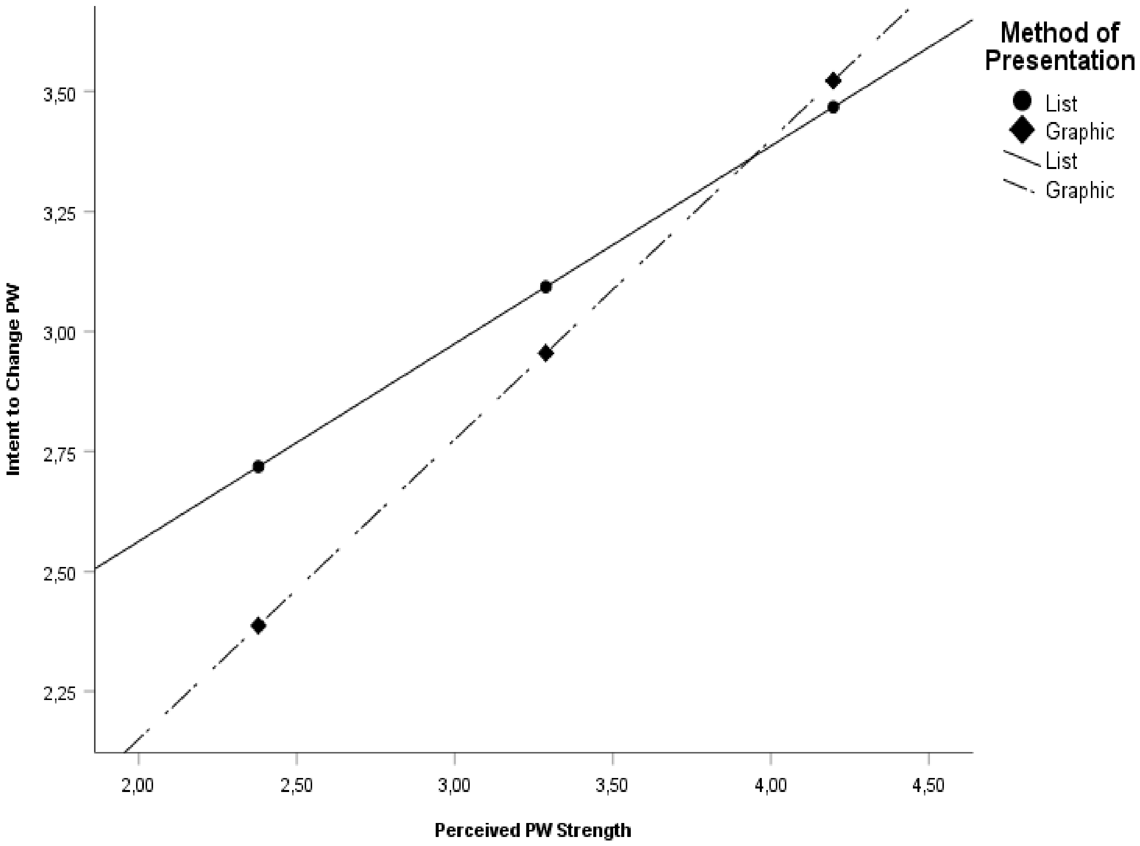
Tests of Between-Subject Effects

Source	Dependent variable	df	Mean square	F	Sig.	Partial Eta-square
MoP	Feel informed	1	2.540	3.578	.061	.029
	Intent to change PW	1	.169	.221	.639	.002
Prior Knowledge	Feel informed	1	.030	.043	.837	.000
	Intent to change PW	1	.432	.564	.454	.005
Risk Perception	Feel informed	1	.143	.202	.654	.002
	Intent to change PW	1	.694	.907	.343	.007
Actual PW strength	Feel informed	1	.048	.068	.795	.001
	Intent to change PW	1	.000	.000	.990	.000
Perc. PW strength	Feel informed	1	.645	.908	.342	.007
	Intent to change PW	1	22.965	30.007	.000	.199
MoP * Prior Knowledge	Feel informed	1	2.792	3.932	.050	.031
	Intent to change PW	1	1.356	1.771	.186	.014
MoP * Risk Perception	Feel informed	1	5.668	7.982	.006	.062
	Intent to change PW	1	.226	.295	.588	.002
MoP * Actual PW strength	Feel informed	1	.150	.211	.647	.002
	Intent to change PW	1	.875	1.144	.287	.009
MoP * Perc. PW strength	Feel informed	1	.194	.274	.602	.002
	Intent to change PW	1	1.584	2.070	.153	.017
Error	Feel informed	121	.710			
	Intent to change PW	121	.765			

There was, however, one main effect from one of the other variables that were investigated and were not part of the hypotheses. Of the covariates that were analysed, Perceived PW Strength had a significant effect on the intent to change one's password; $F(1, 121) = 30.007$, $p < .001$, $\eta_p^2 = .199$, such that the weaker someone estimated their passwords to be, the more they were intending to change their passwords to make them more secure (see Figure 2). This effect was independent of Method of Presentation, as there was no statistically significant interaction effect between Perceived PW Strength and having been shown a graphical representation of password strength. Furthermore, Perceived PW Strength had no effect on the degree to which participants felt informed by the study. Of all significant effects that were measured, this one had the largest effect size and lowest *p*-value.

Figure 2

Simple Slopes Analysis of Intent to Change PW and Perceived PW Strength

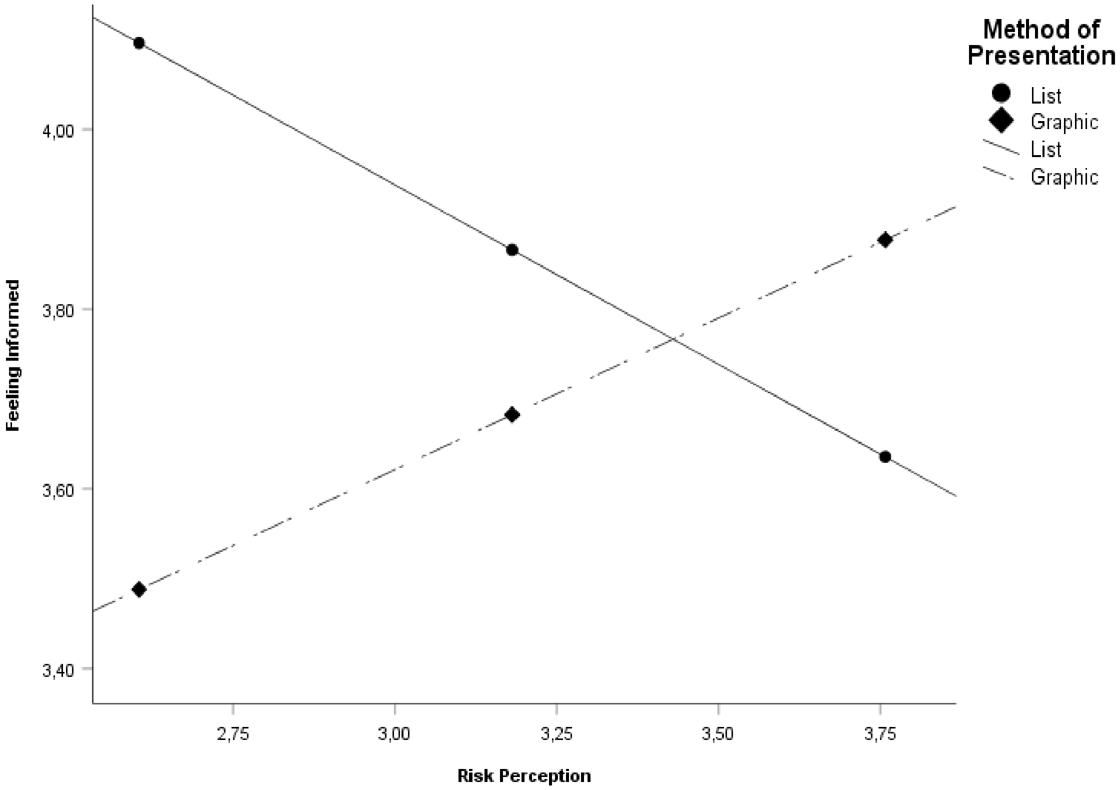


Note. Both axes show mean scores of each variable. Scores were measured on a five-point Likert scale. High scores for Perceived PW Strength indicate low password strength. High scores on Intent to Change PW indicate high intent.

Moreover, two interaction effects emerged. Risk Perception moderated the effect of MoP on Feeling Informed; $F(1, 121) = 7.982$, $p < .05$, $\eta_p^2 = .062$, in such a way that in the experimental condition higher perceived risk was associated with feeling less informed, while in the control condition the inverse was the case, meaning that the less someone felt at risk of cybercrime, the less likely they were to report they felt informed by the study (see Figure 3). This interaction effect was not significant for the other dependent variable.

Figure 3

Simple Slopes Analysis of Feeling Informed and Risk Perception

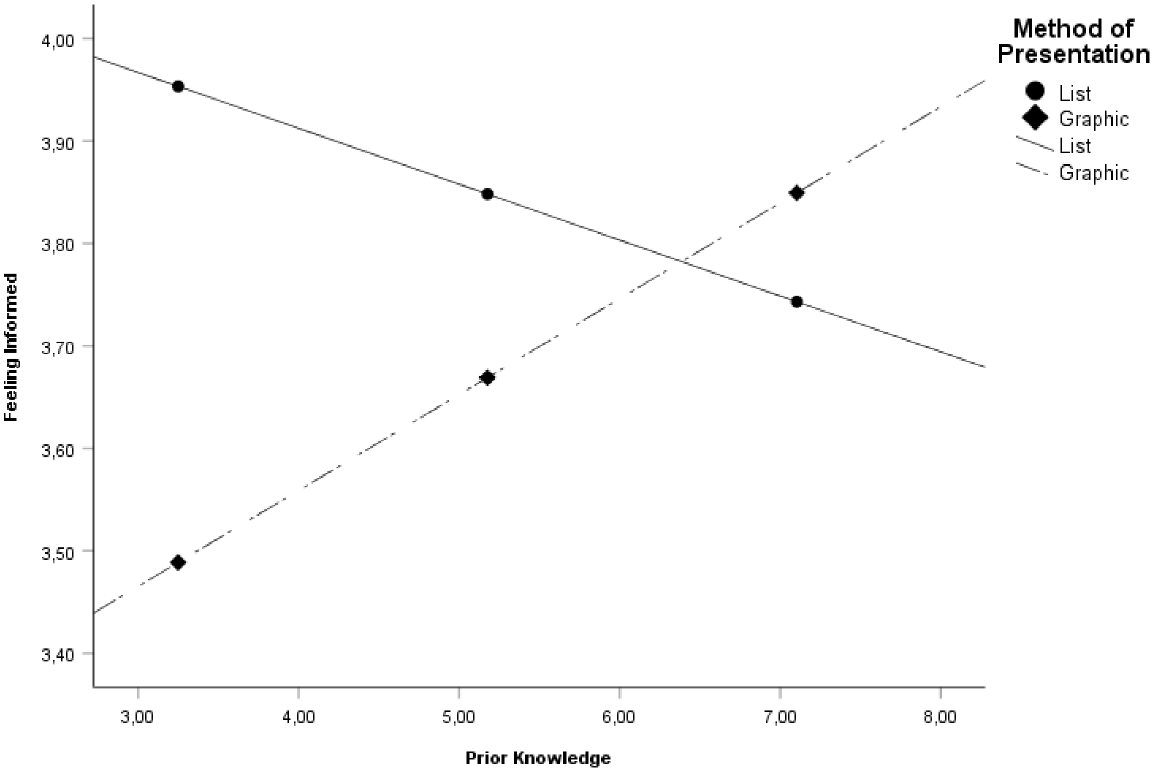


Note. Both axes show mean scores of each variable. Scores were measured on a five-point Likert scale. High scores for Risk Perception indicate a low level of perceived risk. High scores on Feeling Informed indicate a participant felt informed by the study.

Furthermore, another interaction between MoP and Prior Knowledge emerged in the analysis; $F(1, 121) = 3.932$, $p < .05$, $\eta_p^2 = .031$. As with the other interaction, whether participants were part of the control or experimental condition reversed the relationship between the dependent variable "feeling informed" and the covariate, in this case prior knowledge of cybercrime. In the control condition, more prior knowledge predicted lower levels of feeling informed by the study, while in the experimental condition the more prior knowledge participants brought into the study, the more likely they were to rate their participation as informative (see Figure 4).

Figure 4

Simple Slopes Analysis of Feeling Informed and Prior Knowledge



Note. Both axes show mean scores of each variable. Scores for Feeling Informed were measured on a five-point Likert scale (1 = not feeling informed at all; 5 = feeling very informed). Scores for Prior Knowledge were measured with a multiple-choice quiz consisting of ten answers, with ten being the maximum score and indicating high Prior Knowledge.

Discussion

The present study had the purpose of investigating a possibility to persuade potential victims of cybercrime to increase the security of their passwords. Drawing from Protection Motivation Theory and past research on its applicability to the area of cybercrime (Tsai et al., 2016; Van Bavel et al., 2019), the approach chosen was informed by the apparent advantage of choosing cope-appraisal to influence behaviour. The graphical representation chosen showed that very large differences in password security could be achieved by merely adding a small number of characters and increasing character sets. For example, someone who has a password that is eight characters long and consists of numbers and lower- and upper-case letters can increase the estimated time to have their password cracked from ten days to twelve years only by adding one special character to their password (see Appendix). This circumstance seemed to appeal to two of the four main factors behind PMT (efficacy of measure and self-efficacy), as it indicated how effective the measure was in fending off potential intruders, as well as being easy to implement. However, findings indicate that the graphic did not significantly affect either of the dependent variables.

Following research from areas other than cybercrime that showed (colour-coded) graphical representations could influence subjects in their behaviour and post-exposure interest (Park & Lim, 2004; Rosenblatt et al., 2018; Steurer-Stey et al., 2010), it was hypothesised that exposing participants to such a graphic would increase the likelihood of them reporting they felt more inclined to change their passwords after the study (1), as well as reporting they felt more informed by the study (2), when compared to a control group. However, findings indicate that the Method of Presentation (graphic versus bullet-point list) did not significantly affect the dependent variables. Of the covariates investigated, Perceived PW Strength showed a main effect. There were also two interaction effects between Risk Perception and Feeling Informed and Prior Knowledge and Feeling Informed.

Interpretation of Findings

Based on the findings from the main analyses, both of these hypotheses can be rejected. There was no statistically significant effect of the Method of Presentation on either of the dependent variables, indicating that being presented with a graphical representation of password strength alone did not influence participants in a measurable way. There were, however, different effects found that were not included in the main hypotheses. The only statistically significant main effect that was found was that of Perceived PW Strength on reported intent to change one's password, which suggests that those who perceive their own passwords to be weaker also feel more inclined to change them following the study. This effect was independent of which Method of Presentation participants were assigned to and also happened to be the effect with the largest effect size in the study.

Although this effect is perhaps the most intuitive that was measured, there are a few things to point out. For instance, it is notable that while Perceived PW Strength had this strong an influence on Intent to Change PW, there was no significant effect of Actual PW Strength on the same variable. This means that even people who potentially already had very secure passwords, felt the need to change them following the study. Conversely, people with unsecure passwords did not feel this need, so long as they perceived their current passwords to be sufficiently strong. This is especially interesting, considering there seems to be no correlation between perceived and Actual PW Strength, suggesting that people in general seem to have a weak intuition about what constitutes a strong password.

Furthermore, Actual and Perceived PW Strength are correlated with Prior Knowledge of cybercrime to approximately equal degrees, indicating that whatever mismatch there is between Actual and Perceived PW strength can most likely not be explained by participants' cybercrime knowledge. This is somewhat strange, since we would expect any discrepancy between actual and perceived PW strength to stem from insufficient knowledge on what constitutes a strong password. However, this is possibly explained by the fact that the cybercrime quiz measuring Prior Knowledge did not solely focus on password security, so different results might be expected with a quiz that more precisely measures knowledge concerning password security. Moreover, it is interesting that this variable more closely corresponds to fear-appraisal than coping-appraisal in context of Protection Motivation Theory, which contradicts our assumption based on prior research that coping-appraisal would be the more significant factor when it comes to persuasion in context of cybercrime.

The first interaction effect that was measured indicates that the degree to which someone felt informed by the study was dependent on both the Method of Presentation, as well as on Risk Perception. In the experimental condition, participants felt more informed the lower they perceived their cybercrime risk to be, while in the control condition the lower Risk Perception was, the less they felt informed by the study. This is interesting, as it suggests that exposure to a graphical representation flipped the association between Risk Perception and feeling informed. One possible interpretation for this would be that people who went into the study with a greater concern for falling victim to cybercrime were already familiar with aspects of password security, while those that estimated risk to be low were not. This would mean that the graphical representation of password strength was only perceived to be informative by those who were unaware of the risks of cybercrime but yielded no additional information for those that were aware.

Another significant interaction was that between prior knowledge of cybercrime and experimental condition. As with the previous interaction, the degree to which participants felt informed by the study was influenced by Prior Knowledge in a way where Method of Presentation inverted the association. Participants that went into the study with greater cybercrime knowledge were more likely to rate their participation as informative in the experimental condition, while the opposite was true for the control condition. This effect could potentially be explained by the perceived information contained within the graphic. While people who already had prior knowledge did not gain any additional insights from being merely informed about the strength of certain passwords (as was the case in the control condition), they seem to gain more knowledge if the information is presented to them in a certain way (i.e., in a colour-coded graphic). This could mean that, since there is no actual difference between the actual information, the graphical representation contextualizes information more efficiently and makes it seem more informative to participants with prior knowledge. However, it is puzzling that participants with less prior knowledge did not feel as informed by the graphic as those with more knowledge. This may be explained by the fact that the information contained in the graphic is rather specialized and there was no explanation concerning brute-force password cracking provided, leading to uninformed participants not knowing how to integrate the presented information into their pre-existing knowledge structure, while those that already have a better understanding of cybersecurity have an easier time understanding and integrating the presented information.

Strengths and Limitations

One of the strengths of the study was the large number of covariates that were considered in the analysis. They seem to cover all the relevant factors that should be considered when investigating people's intent to change their passwords and made it possible to shine light on interesting interaction effects with the independent variable, as well as unforeseen main effects of the covariates. For instance, it is notable that Perceived PW Strength accounted for close to 20 percent of the variance for Intent to Change PW. Future research could build on this insight and take perceived password strength into account when designing an intervention to persuade people to change their passwords. Another strength would be the relatively high reliability of the scales measuring the dependent variable, as well as the fact that all of the self-constructed scales passed the threshold of acceptable reliability.

The present study has several limitations which need to be addressed. Perhaps the most pressing criticism could be the way in which the dependent variables were measured, as three items for each dependent variable are arguably not enough. Although three items are considered sufficient to measure a construct, it is generally recommended to use at least four items (Robinson, 2017). Furthermore, it would be more effective to measure the actual likelihood of participants changing their passwords, rather than just their reported intention to do so. This could have been done with a follow-up study, during which participants could have been asked whether or not they changed their passwords after the study. If both of these flaws were addressed, we could potentially achieve more conclusive results.

Another possible limitation could be the way in which prior knowledge of cybercrime was measured, or rather the focus of that measurement. While the used quiz may have been effective at measuring participants' broad understanding of cybercrime, it may have been more useful to specifically test their knowledge on password security. This way we could have made more precise inferences. For example, such a measurement may have given us more insights regarding the interaction effects that emerged, as presently it is unclear how much specific knowledge (or lack thereof) of password security impacted the interactive relationships we observed. With such improved measure it may also be possible to more precisely estimate the effect a graphical representation of password strength has on both DVs.

Future Research

Taking into consideration what we learned from this study, future research should try to include perceived password strength in any model seeking to explain people's inclination to change passwords, as this variable showed by far the strongest effect. For instance, when designing an intervention, researchers could try to manipulate participants' perceived password strength in such a way as to increase the likelihood of them changing passwords. This could likely be done somewhat independently of the whatever the actual strength of participants' passwords is, as results from this study suggest the two do not correspond to each other.

Furthermore, it would be interesting to see future research further explore the relationship between prior knowledge of password security and the degree to which participants feel informed by a graphical representation of password security, since the results from this study were highly counterintuitive. As Prior Knowledge seemed to amplify the effect of the graphic on Feeling Informed, there could be some interesting effects to be discovered, once flaws regarding the lacking specificity of the quiz assessing Prior Knowledge are addressed. Researchers could further specify their assessment of Prior Knowledge by tailoring it to fit the topic of password security more closely, for example, by including questions about brute-forcing, the method most relevant to the protective measure of increasing one's password length and complexity.

Finally, future research should investigate the dependent variable more thoroughly than was done in this study. One way to achieve this would be by conducting a follow-up study to ask participants whether or not they actually changed their passwords following the first study. This way the results and following interpretation about what is an effective measure to motivate people to change their passwords would be more conclusive.

Conclusion

All in all, the present study offered some interesting insights, which weren't necessarily intuitive or to be expected with the relevant research in mind. Although the Method of Presentation did not seem to affect Feeling Informed and Intent to Change PW on its own, it did make for two interesting interaction effects. For Feeling Informed, both of those interactions emerged in such a way that MoP inverted the relationship to the covariates (Risk Perception and Prior Knowledge). One can only hypothesize where these curious interactions stem from and they offer an interesting opportunity of further exploration for future research. Overall, Perceived PW Strength was the strongest predictor and the only variable that had a significant effect on Intent to Change PW. The relationship between those two variables was more expected than the aforementioned interaction effects, in that participants who perceived their passwords to be weaker reported more intent to change their passwords. Future research should primarily try to include a follow-up study, in order to measure the actual effect of possible interventions more rigorously. This way, it would be possible to more accurately reflect how likely participants are to change their passwords, given the fact that merely reporting the intend to do so is not comparable to actually following through with that intent.

References

Abraham, A., Lloret Mauri, J., Buford, J. F., Suzuki, J., & Thampi, S. M. (2011). A flow-level taxonomy and prevalence of brute force attacks. *Advances in Computing and Communications*, *191*, 666-675. https://doi.org/10.1007/978-3-642-22714-1_69

Alata, E., Nicomette, V., Kaaniche, M., Dacier, M., & Herrb, M. (2006). *Lessons learned from the deployment of a high-interaction honeypot*. 2006 Sixth European Dependable Computing Conference. Munich, Germany. September, 2006. https://doi.org/10.1109/edcc.2006.17

Álvarez, G., Montoya, F., Romera, M., & Pastor, G. (2004). Cryptanalyzing a discrete-time chaos synchronization secure communication system. *Chaos, Solitons & Fractals*, *21*(3), 689-694. https://doi.org/10.1016/j.chaos.2003.12.013

Bonneau, J., Herley, C., Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. *2012 IEEE Symposium on Security and Privacy*. San Francisco, USA. May, 2012. https://doi.org/10.1109/sp.2012.44

Braun, C. C., & Silver, N. C. (1995). Interaction of signal word and colour on warning labels: Differences in perceived hazard and behavioural compliance. *Ergonomics*, *38*(11), 2207-2220. https://doi.org/10.1080/00140139508925263

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

DiDio, L. (1998). Major hacks raise hackles, spur defenders. *ComputerWorld*, *32*(13), 49-50.

DiDio, L. (1998). Cyberattack prompts DoD to boost security. *ComputerWorld*, *32*(9), 14.

Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security*, *2016*(8), 5-8. https://doi.org/10.1016/s1353-4858(16)30075-7

Farr-Wharton, G., Foth, M., & Choi, J. H. (2012). Colour coding the fridge to reduce food waste. *Proceedings of the 24th Australian Computer-Human Interaction Conference on - OzCHI '12*. Melbourne, Australia. November, 2012. https://doi.org/10.1145/2414536.2414556

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, 149-164. https://doi.org/10.1016/b978-0-12-800743-3.00012-8

Krohn, M. D., Hendrix, N., Hall, G. P., & Lizotte, A. J. (2019). *Handbook on crime and deviance.* Springer Nature.

Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015). "They brought in the horrible key ring thing!" Analysing the usability of two-factor authentication in UK online banking. *Proceedings 2015 Workshop on Usable Security*. https://doi.org/10.14722/usec.2015.23001

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Matishak, M. (2016). *How Podesta became a cybersecurity poster child*. POLITICO. https://www.politico.com/story/2016/10/john-podesta-cybersecurity-hacked-emails-230122

Mayer, J. (2016). Cybercrime litigation. *University of Pennsylvania Law Review, 16, 1453–1507.*

Moore, R. (2014). *Cybercrime: Investigating high-technology computer crime*. Routledge.

National Cyber Security Centre. (2019). *Most hacked passwords revealed as UK cyber survey exposes gaps in online security*. GCHQ. https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

Park, S., & Lim, J. (2004). The Effect of Graphical Representation on the Learner's Learning Interest and Achievement in Multimedia Learning. *Association for Educational Communications and Technology*.

Rogers, R. W. (1975). "A protection motivation theory of fear appeals and attitude change". *Journal of Psychology*. **91** (1): 93–114. doi:10.1080/00223980.1975.9915803

Robinson, M. A. (2017). Using multi-item psychometric scales for research and practice in human resource management. *Human Resource Management, 57*(3), 739-750. https://doi.org/10.1002/hrm.21852

Rosenblatt, D. H., Bode, S., Dixon, H., Murawski, C., Summerell, P., Ng, A., & Wakefield, M. (2018). Health warnings promote healthier dietary decision making: Effects of positive versus negative message framing and graphic versus text-based warnings. *Appetite*, *127*, 280-288. https://doi.org/10.1016/j.appet.2018.05.006

Shankdhar, P. (2020). *Popular tools for brute-force attacks [Updated for 2020]*. Infosec Resources. https://resources.infosecinstitute.com/topic/popular-tools-for-brute-force-attacks/

So, S., & Smith, M. (2002). Colour graphics and task complexity in multivariate decision making. *Accounting, Auditing & Accountability Journal*, *15*(4), 565-593. https://doi.org/10.1108/09513570210440603

Steurer-Stey, C., Zoller, M., Chmiel Moshinsky, C., Senn, O., & Rosemann, T. (2010). Does a colour-coded blood pressure diary improve blood pressure control for patients in general practice: The coco trial. *Trials*, *11*(1). https://doi.org/10.1186/1745-6215-11-38

Stoll, C. (1988). Stalking the wily hacker. *Communications of the ACM*, *31*(5), 484-497. https://doi.org/10.1145/42411.42412

Top 5 cybercrimes in the U.S., from the NCSIR. (2017). Official Site | Norton™ - Antivirus & Anti-Malware Software. https://us.norton.com/internetsecurity-online-scams-top-5-cybercrimes-in-america-norton-cyber-security-insights-report.html

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Ungoed-Thomas, J. (1998, March 29). The schoolboy spy. *Sunday Times*, pp. 5-10.

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Verizon: Data breach investigations report 2020. (2020). *Computer Fraud & Security*, *2020*(6), 4. https://doi.org/10.1016/s1361-3723(20)30059-2

What Americans knows about cybersecurity. (2020). Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/

Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion. *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*. Cloudcroft, USA. September, 2001. https://doi.org/10.1145/508171.508195

Zviran, M., & Haga, W. J. (1999). Password security: An empirical study. *Journal of Management Information Systems*, *15*(4), 161-185. https://doi.org/10.1080/07421222.1999.11518226

Appendix

Informed Consent

WELCOME

You are invited to participate in a web-based online study on cybercrime and password security. This study explores how graphical representations of password strength may influence the behaviours, intentions, and perceptions of potential victims of cybercrime.

This research project is being conducted by Aljoscha Ocko, a student at the University of Twente, Netherlands. The survey takes about 10 minutes to complete.

PARTICIPATION

Your participation in this survey is voluntary. You may refuse to take part in the research or exit the survey at any time without penalty. You are free to decline to answer any particular question you do not wish to answer for any reason.

You will receive no direct benefits from participating in this research study, aside from SONA credits in case you found this study through the SONA system. However, your responses may help us to learn more about possible prevention of cybercrime.

CONFIDENTIALITY

Your survey answers will be sent to Qualtrics where data will be stored in a password-protected electronic format. Personal information, such as gender and age will be collected for demographic purposes. We do not collect identifying information such as your name, email address, or IP address. Therefore, your responses will remain anonymous. No one will be able to identify you or your answers, and no one will know whether or not you participated in the study. We will ask you some questions about the passwords you are using online. However, all of these questions will only be asking abstract questions about the strength of your passwords and at no point will you be asked to give us any of your actual passwords.

At the end of the survey, you will be asked if you are interested in participating in a follow-up study, which will be conducted about one to two weeks after the first one and give you the opportunity to earn additional SONA credits upon participation. If you choose to provide contact information such as your phone number or email address, your survey responses may no longer be anonymous to the researcher. However, no names or identifying information would be included in any publications or presentations based on these data, and your responses to this survey will remain confidential.

CONTACT

If you have questions at any time about the study or the procedures, you may contact Aljoscha Ocko [a.ocko@student.utwente.nl].

____

By ticking the "Agree" box, you confirm that you:

• are at least 18 years old
• understood all of the above information
• consent to taking part in the survey

Risk Perception questionnaire

Read the following statements and indicate to which degree you agree or disagree (1 = strongly disagree; 5 = strongly agree):

1. I rarely worry about falling victim to cybercrime.
2. When shopping online, I sometimes feel anxious about filling in my bank details/credit card information. [Removed]
3. I think my personal information is generally safe online.
4. I doubt criminals would be interested in breaking into one of my accounts. [Removed]
5. Someone stealing my personal information is something I often worry about.
6. I don’t like to use online banking due to fear of cybercriminals.
7. Shopping online seems less safe than shopping in real life.
8. Scams through email would never work on me. [Removed]
9. I try to be very careful when navigating the internet.

10. Cybercrime is a big issue in today’s time for people like me.
11. I generally feel safe when sharing personal information online. [Removed]
12. I feel safer carrying cash around than engaging in online banking.
13. Just to be sure, I change my passwords every now and then. [Removed]
14. Cybercrime poses a serious threat to my security and well-being.
15. I am always on the lookout for scammers online.

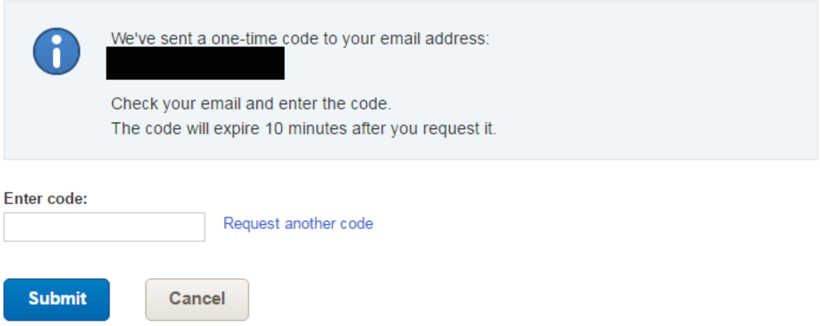
Assessment of knowledge on cybersecurity

1. What does the “https://” at the beginning of a URL denote, as opposed to "http://" (without the “s”)?
   a. That the site has special high definition
   b. That information entered into the site is encrypted
   c. That the site is the newest version available
   d. That the site is not accessible to certain computers
   e. None of the above
   f. Not sure

2. Which of the following is an example of a “phishing” attack?
   a. Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows
   b. Creating a fake website that looks nearly identical to a real website in order to trick users into entering their login information
   c. Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest
   d. All of the above
   e. Not sure

3. A group of computers that is networked together and used by hackers to steal information is called a …
   a. Botnet
   b. Rootkit
   c. DDoS
   d. Operating system
   e. Not sure

4. Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication?

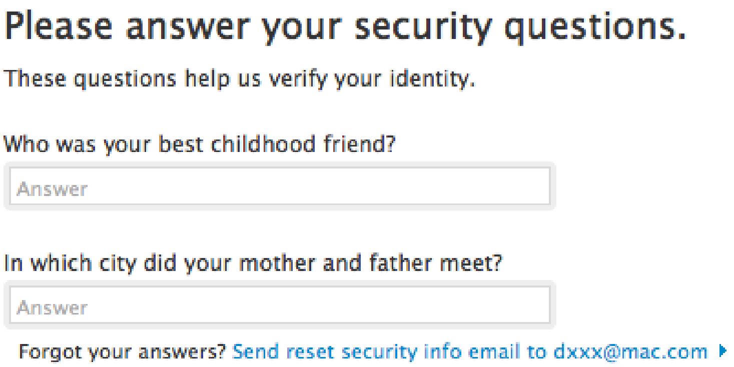


We've sent a one-time code to your email address:
[redacted]

Check your email and enter the code.
The code will expire 10 minutes after you request it.

Enter code:

a.



Please answer your security questions.

These questions help us verify your identity.

Who was your best childhood friend?

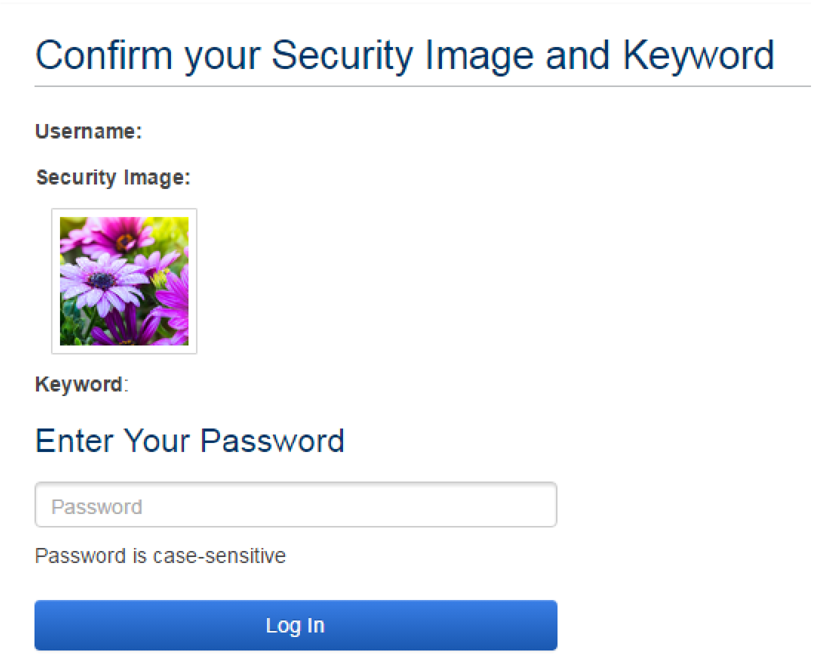
Answer

In which city did your mother and father meet?

Answer

Forgot your answers? Send reset security info email to dxxx@mac.com

b.



Confirm your Security Image and Keyword

Username:

Security Image:

Keyword:

Enter Your Password

Password

Password is case-sensitive

c.

d. None of these
e. Not sure

5. Which of the following four passwords is the most secure?
   a. Boat123
   b. WTh!5Z
   c. Into*48
   d. 123456
   e. Not sure

6. Criminals access someone’s computer and encrypt the user’s personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called …
   a. Botnet
   b. Ransomware
   c. Driving
   d. Spam
   e. None of the above
   f. Not sure

7. “Private browsing” is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?
   a. Yes
   b. No
   c. Not sure

8. Turning off the GPS function of your smartphone prevents any tracking of your phone’s location.
   a. True
   b. False
   c. Not sure

9. If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?
    a. Yes, it is safe
    b. No, it is not safe
    c. Not sure

10. What kind of cybersecurity risks can be minimized by using a Virtual Private Network (VPN)?
    a. Use of insecure Wi-Fi networks
    b. Key-logging
    c. De-anonymization by network operators
    d. Phishing attacks
    e. Not sure

Assessment of personal password strength (actual and perceived)

Think about the five most important passwords you have in mind that you are currently using. Then read the following statements and indicate to which degree you agree or disagree (1 = strongly disagree; 5 = strongly agree):

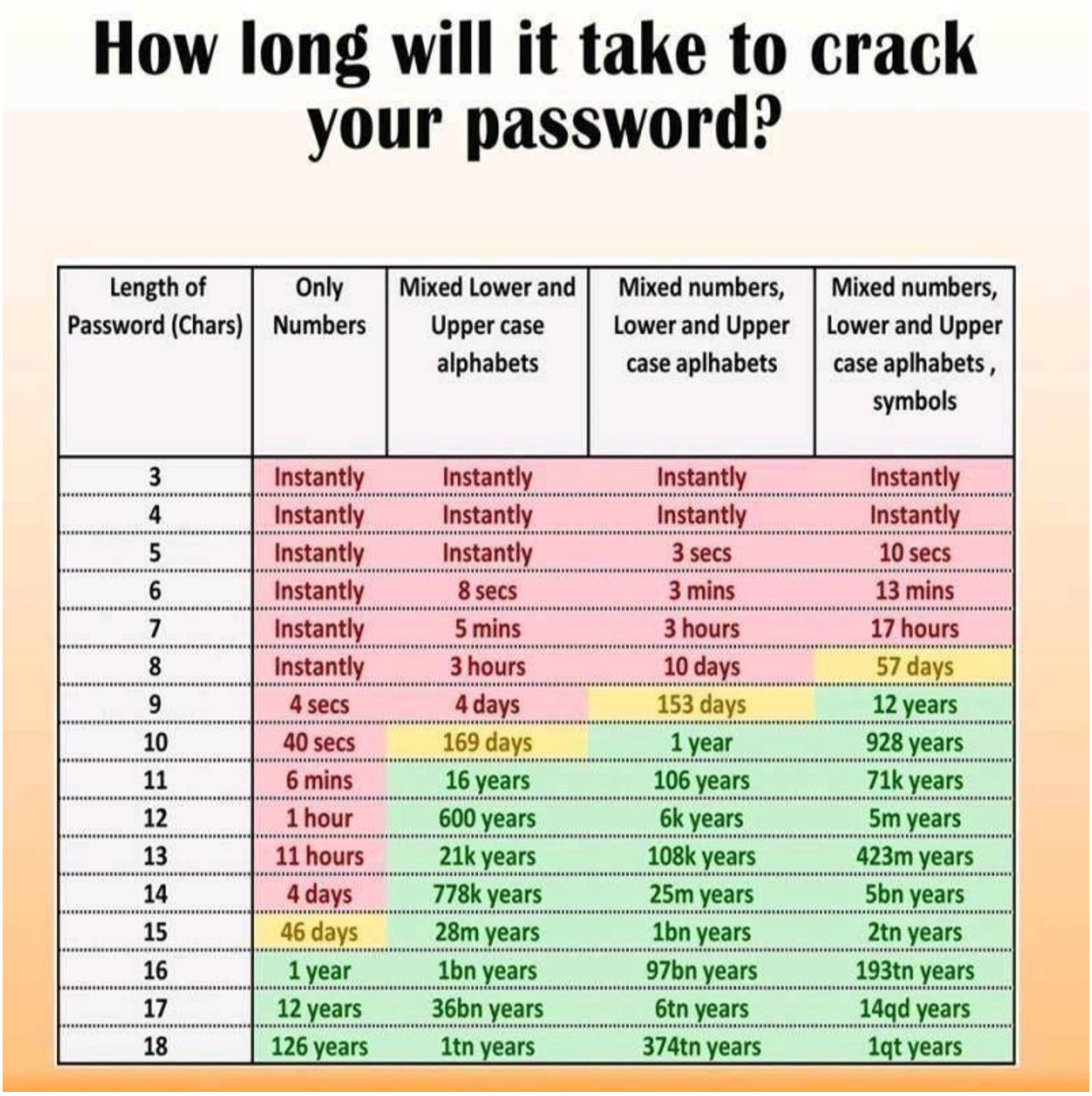
1. I never worry about one of my passwords being cracked/hacked.
2. My passwords should probably be longer.
3. Sometimes I feel anxious somebody could find out my password.
4. Sometimes I wonder if I should change my password to make it more secure.
5. My passwords only contain letters.
6. My passwords only contain numbers.
7. There are several special characters in my passwords (e.g. §$&"=#).
8. My passwords only contain special characters. [Removed]
9. My passwords contain both upper- and lower-case letters.
10. My passwords contain both letters and numbers.
11. My passwords contain upper- and lower-case letters and numbers.
12. My passwords contain letters and special characters. [Removed]
13. My passwords contain numbers and special characters. [Removed]

14. My passwords contain upper- and lower-case letters, numbers, and special characters.

Graphic vs. text

Group A (experimental condition)

Look at the following graphic for a few minutes and get familiar with its content.



How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Group B (control condition)

Below are a few examples of how long it would approximately take to crack a given password. Please read them carefully:

Only numbers, 8 characters long -> Instantly

Only numbers, 10 characters long -> 40 seconds

Only numbers, 12 characters long -> 1 hour

Lower & upper-case letters, 8 characters -> 3 hours

Lower & upper-case letters, 9 characters -> 4 days

Lower & upper-case letters, 10 characters -> 169 days

Lower & upper-case letters & numbers, 7 characters -> 3 hours

Lower & upper-case letters & numbers, 9 characters -> 153 days

Lower & upper-case letters & numbers, 11 characters -> 106 years

Lower & upper-case letters, numbers, & symbols, 9 characters -> 12 years

Lower & upper-case letters, numbers, & symbols, 10 characters -> 928 years

Lower & upper-case letters, numbers, & symbols, 12 characters -> 5 Million years

Demographics questionnaire (filler)

Age

What is your sex?

What is your nationality?

What is your highest completed education?

Questionnaire about intent/behaviour

Please read the following statements and indicate to which degree you agree or disagree (1=strongly disagree; 5= strongly agree).

1. I feel more informed about password security now than I did before this study.
2. I feel motivated to change my passwords to make it more secure.
3. After taking part in this study, I feel like I have a better understanding of what constitutes a strong password.
4. I feel like my passwords need to be updated for security reasons.
5. The information I saw in this study made me get a better understanding of password security.
6. I will change my passwords based on the information I learned in this study.