Perceptions of the risks of password related activities

Burak Merdenyan
Human Computer Interaction Research Group
Department of Computer Science
University of York
York YO10 5GH UK
bm815@york.ac.uk

Helen Petrie
Human Computer Interaction Research Group
Department of Computer Science
University of York
York YO10 5GH UK
Helen.petrie@york.ac.uk

Many studies have investigated people's risky password related activities such as writing down passwords, sharing them with other people and re-using them across accounts, but few studies have investigated people's perceptions of the risks of these activities. This paper reports on an online survey with 129 people rating the risks of 11 different password related activities in four domains (social networking, email, eBanking and eCommerce). There were fewer differences between the perceived riskiness of activities due to domain than expected, but differences between the activities and the numbers of respondents who said they would engage in the different activities. There were interesting patterns of differences in the ratings of the riskiness, severity of the consequences, usefulness and likelihood of encountering the different activities, which may help explain why people undertake risky password activities.

Passwords, password management activities, risk perception.

1 INTRODUCTION

Authentication using passwords is still the most common method for digital services (Ur et al., 2016; Bonneau et al., 2015). Users create and manage passwords in order to log-in, and use the services of their online banking, email, social networking accounts, amongst many others. Managing a password and ensuring its security are the responsibility of a password holder. However, recalling the right password for a specific account is not easy. A recent study in password behaviours showed that on average British respondents manage 22.3 total systems requiring passwords (Petrie and Merdenyan, 2016).

The management of passwords for that many systems requires a substantial effort. Prior studies have shown that users have difficulties in managing their passwords (Stobert and Biddle, 2014; Gaw and Felten, 2006), and exhibit risky password management activities such as re-using passwords, writing them down, and sharing passwords with others (Shay et al., 2010). But, how do users perceive the risks when they undertake these activities? Despite numerous studies on password behaviour (see Background section, below), little attention has been given to understand how users perceive the risks of different common password related activities. Moreover, there is no study to our knowledge investigating the password management activities through a range of different digital domains. As users' risk perceptions differ for different website domains (LeBlanc and Biddle, 2012), it is important to investigate whether users have different perceptions of the risks of password management activities in different domains.

Therefore this study investigated people's perceptions of the risk of a range of password related activities in a range of different domains. It also investigated people's attitudes to other aspects of the activities, such as whether people would engage in the activity, their perception of the severity of the consequences of a password compromise due to the activity, the usefulness of the activity and the likelihood of encountering the activity in real life. All these attitudes may throw light on people's perception of risk.

2 BACKGROUND

Despite a considerable literature on password activities, there is little work that has investigated users' perceptions of these activities and the risks associated with them. Areas of password activities that have been investigated include password content and creation processes (Egelman et al., 2013; Ur et al., 2012; Grawemeyer and Johnson, 2011; Komanduri et al., 2011; Bonneau, 2010; Shay

et al., 2010; Bryant and Campbell, 2006; Brown et al., 2004), password strength, security and usability (Ur et al., 2016; Mazurek et al., 2013; Ur et al., 2012; Kumar, 2011; Voyiatzis et al., 2011; Inglesant and Sasse, 2010; Shay et al., 2010; Vu et al., 2007; Bryant and Campbell, 2006; Yan et al., 2004; Proctor et al., 2002; Sasse et al., 2001; Adams and Sasse, 1999; Zviran and Haga, 1999; Adams et al., 1997; Morris and Thompson, 1979), and password management strategies such as re-using, sharing and writing down passwords (Meter and Bauman, 2015; Whitty et al., 2015; Stobert and Biddle, 2014; Boothroyd and Chiasson, 2013; Grawemeyer and Johnson, 2011; Kaye, 2011; Singh et al., 2007; Gaw and Felten, 2006).

Two studies which have addressed users' perceptions of password management are Notoatmodjo and Thomborson (2009) and Creese et al. (2013). Notoatmodjo and Thomborson (2009) conducted a survey with 26 university students in New Zealand to investigate their perceptions of their password. They found that students were aware of the possible security risks of re-using passwords and that they were able to mentally categorize accounts according to their importance: online banking accounts were categorized as *high importance* accounts, whereas online newspapers were categorized as *low importance* accounts. Using this categorization, it was found that the participants tended to re-use passwords for low importance accounts, whereas they avoided re-using passwords for high importance accounts. Nonetheless, the participants also stated that having multiple accounts forced them to re-use passwords as they were unable to remember a distinct password for each account.

Creese et al. (2013) asked fifty security experts from industry and academia and fifty non-expert participants to rate the level of risk they perceived in relation twenty potentially risky online and offline (real world) activities. There were a number of significant differences between the ratings of the two groups, for example non-experts rated 'not-updating operating system, web browser, and applications' significantly lower in risk than experts, whereas experts rating 'emailing credit card details' significantly lower than non-experts. Despite these differences, the authors concluded that in general non-experts and experts provided similar risk assessments.

Although there is little study of risk perceptions of password behaviour, the study of risk and its perception in other areas is a major topic. The development of risk perception started in 1960s, with the rapid rise of new technologies, especially nuclear technologies. The necessity of risk comparisons was first suggested by Sowby (1965), to balance the benefits and risks of the nuclear power. Risk perception differences amongst laypeople and experts were found in relation to nuclear technologies. It was interesting that laypeople perceived the risks of some activities (e.g. smoking, driving) as being lower than the risks of nuclear technologies (Sjöberg et al., 2004). Later, Starr (1969) claimed that the reason of this difference relies on the *voluntariness of the activity* (risk) taken. His claim explained the reason why laypeople accepted the risks of smoking but not of that nuclear technologies. His work lead to a raised awareness and interest on discovering how people accept, tolerate, and perceive risks.

In 1970s, researchers investigated the perceived risks associated with gambling and lotteries. Langer (1975) made several studies and found that people perceived the risk of winning a lottery higher when they were given the chance to pick numbers. It was found that people perceive risks lower when they think that the situation is under control. This phenomenon was called '*illusion of control*'.

Fischhoff et al. (1978) used *psychometric procedures* to reveal quantitative judgments of perceived risk, and perceived benefit. Psychometrics is the science of measuring mental processes; hence, the psychometric paradigm is a methodological approach to explore the characteristics of risk perception (Breakwell, 2007). Researchers using the psychometric paradigm ask participants to rate the riskiness of a set of hazardous activities, and to express their desires for risk reduction of that hazard, within various domains. The paradigm assumes that people can provide answers to difficult questions such as '*What is the risk associated with the use of nuclear power?*' (Slovic, 2000). The paradigm suggests that risk is subjectively defined by people who are influenced by various psychological, social, cultural, and institutional factors, and assumes that with appropriate design of surveys it is possible to quantify and model the interrelationships of these factors (Slovic, 2000).

Our study was influenced by the psychometric approach to risk and investigated a number of psychological factors which might influence people's perception of the risk of password related activities, including their perception of the severity of the consequences of a password compromise due to the activity, the usefulness of the activity and the likelihood of encountering the activity in real life.

3 METHOD

3.1 Design

The study used an online survey via Amazon Mechanical Turk (MTurk).

11 potentially risky password related activities were created (*see* Table 2) based on an analysis of the

relevant research on password management. These activities were related to four domains in which people typically have passwords: social network sites (SNSs), email, eBanking and eCommerce. These domains were chosen because users have different types of information stored in these domains and may regard them as having different levels of importance and privacy. Not every activity seemed appropriate to every domain, so a total of 35 specific activities resulted. As asking respondents to answer questions about this number of activities, they were divided into four sets with only one activity per set and a range of different domains. Different respondents did each set (due to an oversight in materials preparation for Activity 4, two versions of this activity went in the same set, which complicated the statistical analysis – it meant that repeated measures analyses had to be conducted for this activity).

On each activity, respondents were asked a number of questions, including Likert rating items and open-ended questions. These covered how risky they thought the activity was, whether they would engage in it, how severe they thought the consequences would be and whether they thought the activity is useful.

3.2 Respondents

Respondents were recruited through the MTurk crowdsourcing service. A total of 129 individuals responded and provided sufficient data for analysis. Table 1 summarises the demographics of the sample which was close to gender balanced (55.8% male, 43.4% female, 0.8% preferred not to say). The mean age of respondents was 33.4 year (range: 19 - 62 years). 80 respondents were from the USA, 35 were from India and 14 from other countries.

Respondents were quite evenly divided between the four sets of activities: two groups had 31 respondents, one group had 32 and one group had 35.

3.3 Materials

Four versions of an online questionnaire were developed with 8 or 9 activities. For each activity there were 5 questions:

How risky is the activity? (Likert)

Would you ever engage in the activity? (Yes/No)

If your password were compromised as a result of engaging this activity, how severe do you think the negative consequences would be? (Likert)

How useful is the activity? (Likert)

How likely do you think you are to face the activity in real life? (Likert)

For each Likert item questions, respondents were invited to explain their rating by an optional open-ended question (why did you give that rating?)

After completing the 8 or 9 sets of activity questions, respondents were asked to complete a brief demographic questionnaire.

Table 1: *Demographic information for the respondents*

Number and Gender	129 Women: 56 (43.4%) Men: 72 (55.8%) PNS: 1 (.8%)
Age	19 – 62 years mean: 33.4
Education	School: 35 (27.1%) Bachelor: 65 (50.4%) Masters: 25 (19.4%) PhD: 4 (3.2%)
Employment	Student: 16 (12.4%) Employed: 98 (76.0%) Other: 15 (11.7%)

Table 2: *Password related activities and domains*

Activity	Domains covered
Storing passwords on paper at home	All 4
Storing passwords in a wallet	All 4
Storing passwords in digital devices	All 4
Sharing passwords with partner	All 4
Sharing passwords with colleagues	Email
Sharing passwords with friends	SNS, Email
Re-using passwords across different accounts	All 4
Using slight variations of passwords for other accounts	All 4
Not changing passwords at regular intervals	Email, eCommerce
Logging-in to account from a shared computer outside home	All 4
Logging-in to account from an unknown person's digital device	Email

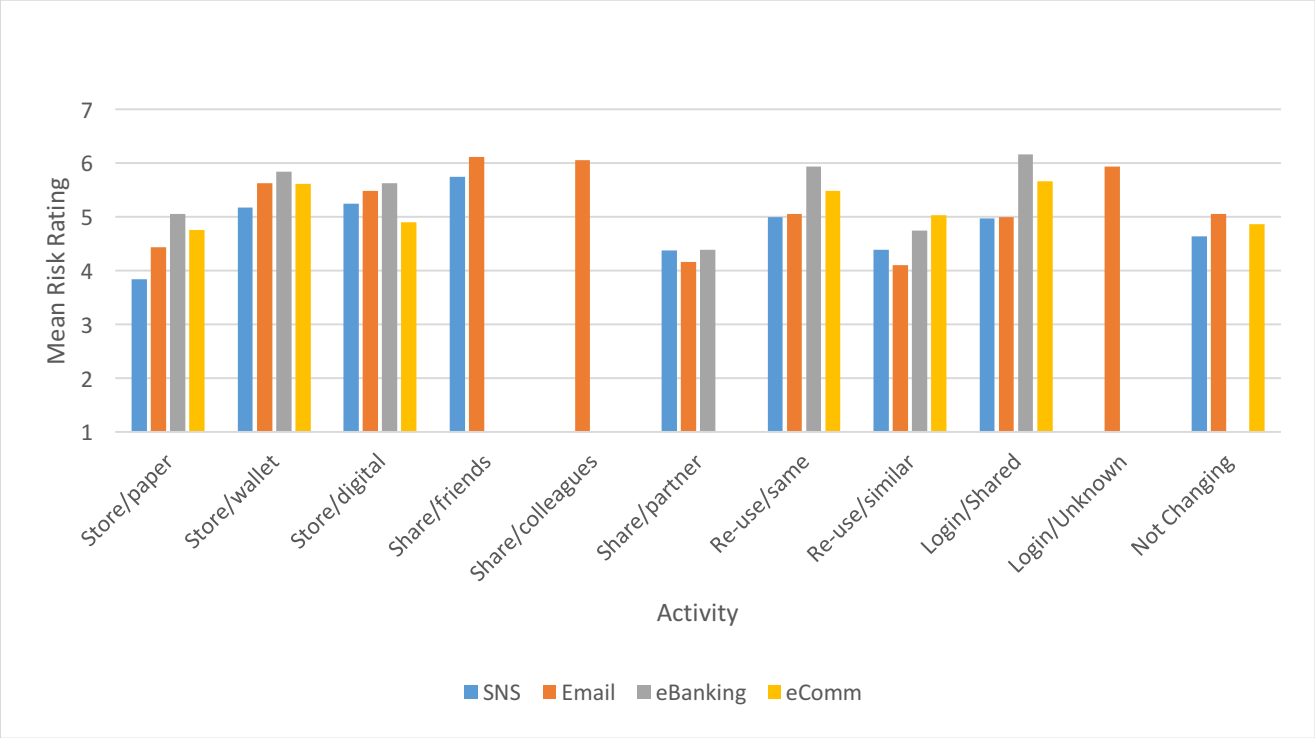

Figure 1: *Mean ratings of risk of activities by domain*

3.4 Procedure

The online survey was distributed via MTurk. No specific qualification was required to be a respondent, and there were no geographical restrictions to complete the survey. In the description of the task respondents were informed about the approximate completion time of the survey (15 minutes, established via a pilot study conducted with researchers at the University of York). Potential respondents were informed that all information they provided would be confidential and that they would not be asked for any of their passwords or any information that might compromise the security of their passwords.

All respondents who completed the survey and provided sufficient information were rewarded USD 0.50 (£0.40 at the time of the study).

The aim was to have 40 respondents complete each of the four sets of activities. However, it was necessary to reject 31 responses (for incomplete or totally inappropriate responses), which resulted in the final sample of 129 responses.

4. RESULTS

The rating scale variables were normally distributed, so parametric statistics were used for the analyses.

4.1 Differences in perception of risk between the different domains

When the perception of risk of the activities was compared across the four different domains, there were fewer differences than might be expected. Figure 1 shows the mean ratings of the perception of how risky the activity was for the 11 activities and the four domains (note for some activities not all four domains were asked about, see section 3.1). For only three of the 9 activities in which more than one domain was investigated were there significant differences. These were on "storing a password on paper at home" ($F_{3, 124} = 2.84$, $p = .04$; post-hoc tests revealed that this was perceived as more risky for eBanking and eCommerce than for SNS, email was intermediate and not significantly different from the other three domains); on "re-using a password across different accounts" ($F_{3, 125} = 3.25$, $p = 0.03$; post-hoc tests revealed that eBanking was perceived as more risky than either SNS or email); and "logging onto a shared computer" ($F_{1, 124} = 3.85$, $p = 0.01$, post-hoc tests again revealed that eBanking was perceived as more risky than either SNS or email).

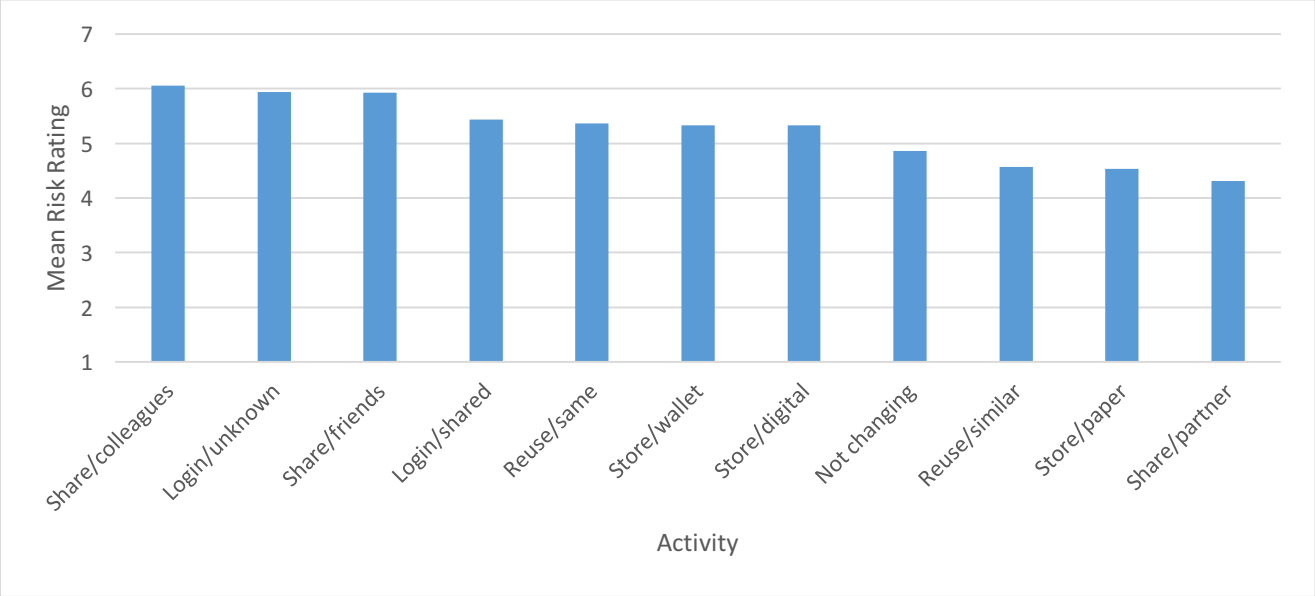

Figure 2: *Mean ratings of risk for the 11 activities*

4.2 Differences in perception of risk between the different types of task

As the perception of risk was not substantially affected by domain, the perception of risk of the different activities was investigated, averaging across the four domains. Figure 2 shows the 11 different activities organized from that perceived as most risky (sharing a password with colleagues, mean risk rating: 6.06/7, standard deviation: 1.24) to that perceived as least risky (sharing a password with a partner, mean risk rating: 4.31, standard deviation: 2.05). However, it is interesting to note that the standard deviation on sharing a password with a partner was over 65% higher than the standard deviation for sharing with a friend, and was by far the highest standard deviation, so there is much more disagreement about the risk of sharing a password with a partner. All the mean ratings, apart from that of sharing with a partner are significantly above the midpoint of the rating scale, so respondents perceive all these activities to be substantially risky.

4.3 Propensity to engage in the activities, relationship to perception of risk consequences, usefulness and likelihood of encountering the activities

Respondents were asked whether they would engage in each of the activities. Table 3 presents the numbers who said they would and would not for each of the activities, with a chi-square test of whether the distribution differed significantly from random. It can be seen that the activity respondents most frequently said they would engage in was re-using a password with slight variation across accounts, with over 60% of respondents saying they would do this, a significantly large proportion of the sample. The activity participants least frequently said they would engage in was sharing a password to an SNS with friends, with only approximately 5% of respondents saying they would do this, a significantly low proportion of the sample. (Sharing passwords for SNSs and email with friends were not combined across domains for this analysis as these were presented to the same respondents).

The perceptions of the respondents who said they would and would not engage with each activity were compared on their other perceptions about the activity. These analyses are summarized in Table 4. This shows that on all but two activities, respondents who said they would engage in the activity rated is as significantly less risky than respondents who said they would not engage in the activity. The two exceptions were sharing passwords with colleagues and sharing passwords for SNS with friends (again sharing passwords for SNSs and email with friends were not combined across domains for this analysis as these were presented to the same respondents).

However, the ratings of the severity of consequences of their password being compromised through the activity, there were no significant differences between the respondents who said they would engage in the activity and those who would not.

Table 3: *Distribution of respondents who said they would or would not engage in each activity*

Activity	Would they engage in the activity?	
	Yes	**No**
Re-using password, with slight variation	61.2% (79)	38.8% (50)
	$X^2 = 6.08$, $p = 0.01$	
Not changing passwords at regular intervals	55.1 (54)	44.9% (45)
	$X^2 = 0.64$, n.s.	
Re-using password across different accounts	51.9 (67)	48.1 (62)
	$X^2 = 0.20$, n.s.	
Storing passwords in digital devices	51.1 (48)	48.9 (46)
	$X^2 = 0.02$, n.s.	
Storing passwords on paper at home	41.1 (53)	58.9 (75)
	$X^2 = 3.44$, n.s.	
Logging in to shared computer outside home	39.5 (51)	60.5 (78)
	$X^2 = 5.24$, $p = 0.02$	
Logging-in to a/c from unknown person's device	35.5 (11)	64.5 (20)
	$X^2 = 2.06$, n.s.	
Storing passwords in digital devices	33.3 (43)	66.7 (86)
	$X^2 = 2.06$, n.s.	
Sharing passwords (email) with friends	17.1 (6)	82.9 (29)
	$X^2 = 13.82$, $p < 0.000$	
Storing passwords in a wallet	14.0 (18)	86.0 (111)
	$X^2 = 65.65$, $p < 0.000$	
Sharing passwords with colleagues	9.7 (3)	90.3 (28)
	$X^2 = 18.58$, $p < 0.000$	
Sharing passwords (SNS) with friends	5.7 (2)	94.3 (33)
	$X^2 = 27.46$, $p < 0.000$	

The ratings of the usefulness of the activity again showed a pattern of significant differences. For all but one activity, the respondents who would engage in the activity rated it as significantly more useful, often by a very substantial amount. The exception was sharing SNS passwords with friends.

Finally, the ratings of likelihood of encountering the activity in real life again showed a pattern of consistent differences, with respondents who would engage in the activity rating it significantly more likely that they would encounter the activity in real life in nine activities, with a marginally significant result in a tenth ($p = 0.06$) and a significant difference in two activities.

5. DISCUSSION AND CONCLUSIONS

This study investigated perceptions of the risk of a range of password related activities in four different domains and associated attitudes towards the severity of the consequences of the risk, the usefulness of the activity and the likelihood of encountering the activity in real life.

Four different domains were investigated as it was expected there would be differing perceptions of the risk of the different password related activities would vary with domain, with eBanking being the domain which participants would consider the most risky. However, the differences between the domains were not as great as expected, with only three of the nine activities investigated showing a significant difference in the perception of risk between the domains. However, in all three cases, it was eBanking for which the risk was considered significantly highest, with eCommerce being also considered highest in one case.

Comparing the different activities, all but one activity was rated significantly above the midpoint of the risk perception scale, suggesting that respondents viewed them all as quite risky. The exception was sharing passwords with partners which did not differ significantly from the midpoint. But interestingly, there was considerable disagreement amongst respondents on this activity (as evidenced by the high standard deviation), suggesting that some respondents trust their partners a lot more than others.

The activity which the most respondents said they would engage in was re-using a password with a slight variation on different accounts, with just over 60% of respondents saying they would do this. This result corresponds well with previous studies, for example Brown et al. (2004) found that approximately 65% of password use involved duplication of the password, a similar figure to ours. Gaw and Felten (2006) and Florencio and Herley (2007) also found high levels of password re-use, although percentages of participants reporting this behaviour were not reported by those studies.

Recording passwords was also an activity many respondents said they would engage in, with just over half saying they would record them digitally and just over 40% saying they would store them on paper. Again, these results correspond well with earlier findings, Brown et al. (2004) found that approximately half their participants keep a written record of passwords.

Table 4: *Mean ratings (and standard deviations of risk, consequences, usefulness and likelihood of encountering the activities for respondents who would engage with them or not*

ACTIVITY	HOW RISKY?		CONSEQUENCES?		USEFUL?		LIKELIHOOD OF ENCOUNTERING	
	YES	NO	YES	NO	YES	NO	YES	NO
Re-use/variation	4.33 (1.62)	4.96 (1.51)	4.99 (1.71)	5.50 (1.85)	5.18 (1.94)	3.04 (2.22)	5.61 (1.40)	2.82 (1.85)
	$t_{127} = -2.21$, $p = 0.03$		$t_{127} = -1.60$, n.s.		$t_{127} = 5.76$, $p < 0.000$		$t_{127} = 9.68$, $p < 0.000$	
Not changing frequently enough	4.35 (1.49)	5.48 (1.41)	4.50 (1.94)	5.18 (1.78)	4.61 (2.09)	2.73 (2.18)	5.28 (1.80)	3.34 (2.28)
	$t_{96} = -3.81$, $p < 0.000$		$t_{96} = -1.79$, n.s.		$t_{96} = 4.36$, $p < 0.000$		$t_{96} = 4.71$, $p < 0.000$	
Re-use/same	5.03 (1.48)	5.73 (1.24)	5.03 (1.88)	5.58 (1.81)	5.37 (1.83)	2.55 (2.05)	5.93 (1.56)	2.11 (1.88)
	$t_{127} = -2.88$, $p = 0.005$		$t_{127} = -1.69$, n.s.		$t_{127} = 8.27$, p 0.000		$t_{127} = 14.50$, p 0.000	
Share/partner	3.50 (1.94)	5.51 (1.83)	3.92 (2.21)	4.67 (2.14)	5.46 (1.75)	1.96 (1.78)	5.83 (1.52)	2.07 (1.67)
	$t_{92} = -4.25$, $p < 0.000$		$t_{92} = -1.69$, n.s.		$t_{92} = 9.63$, $p < 0.000$		$t_{92} = 11.46$, $p < 0.000$	
Store/paper	3.96 (1.73)	4.93 (1.71)	5.08 (1.90)	4.62 (2.09)	5.08 (2.09)	1.89 (1.55)	5.15 (1.94)	1.80 1.40)
	$t_{127} = -3.15$, $p = 0.002$		$t_{127} = 1.27$, n.s.		$t_{127} = 9.93$, $p < 0.000$		$t_{127} = 11.39$, $p < 0.000$	
Log in/shared	4.67 (1.79)	5.95 (1.43)	4.80 (1.77)	5.99 (1.50)	4.47 (2.13)	1.67 (1.45)	4.73 (1.95)	2.23 (1.60)
	$t_{127} = -4.49$, $p < 0.000$		$t_{127} = -4.49$, $p < 0.000$		$t_{127} = 8.91$, $p < 0.000$		$t_{127} = 7.95$, $p < 0.000$	
Log in/unknown device	4.91 (1.14)	6.50 (0.61)	4.00 (3.00)	5.11 (1.60)	3.45 (1.25)	1.25 (0.79)	3.55 (1.67)	2.25 (1.89)
	$t_{29} = -5.12$, $p < 0.000$		$t_{29} = -1.05$, n.s.		$t_{29} = 5.24$, $p < 0.000$		$t_{29} = 1.95$, $p = 0.06$	
Store/digital	4.72 (1.68)	5.63 (1.52)	4.86 (1.74)	5.47 (1.85)	5.28 (1.87)	2.21 (1.84)	5.51 (1.56)	1.71 (1.27)
	$t_{127} = -3.09$, $p = 0.003$		$t_{127} = -1.78$, n.s.		$t_{127} = 8.88$, $p < 0.000$		$t_{127} = 14.80$, $p < 0.000$	
Share/friends (email)	4.83 (1.94)	6.38 (1.02)	4.17 (2.48)	5.00 (1.92)	5.17 (1.84)	1.59 (1.38)	3.83 (1.84)	1.79 (1.42)
	$t_{33} = -2.87$, $p = 0.007$		$t_{33} = -0.92$, n.s.		$t_{33} = 5.49$, $p < 0.000$		$t_{33} = 3.05$, $p = 0.005$	
Store/wallet	4.28 (2.05)	5.76 (1.59)	4.56 (1.76)	5.43 (2.03)	4.22 (2.07)	1.79 (1.44)	4.72 (1.74)	1.58 (1.20)
	$t_{127} = -3.51$, $p = 0.001$		$t_{127} = -1.73$, n.s.		$t_{127} = 6.21$, $p < 0.000$		$t_{127} = 9.61$, $p < 0.000$	
Share/colleagues	5.33 (1.53)	6.14 (1.21)	4.00 (3.00)	5.11 (1.60)	3.67 (1.53)	1.46 (1.07)	3.67 (2.52)	1.75 (1.65)
	$t_{29} = -1.08$, n.s.		$t_{29} = -1.05$, n.s.		$t_{29} = 3.27$, $p < 0.003$		$t_{29} = 1.83$, n.s.	
Share/friends (SNS)	6.00 (0.0)	5.73 (1.80)	4.00 (4.24)	4.82 (1.99)	1.50 (0.71)	1.85 (1.64)	3.00 (2.82)	1.67 (1.40)
	$t_{34} = 0.21$, n.s.		$t_{34} = -0.54$, n.s.		$t_{34} = -0.30$, n.s.		$t_{34} = 1.25$, n.s.	

However, the most interesting findings from this study are from the ratings of the risk, consequences, usefulness of the activities and likelihood of encountering the activity in real life, from respondents who said they would engage in the activities and those who said they would not. When their ratings of the level of risk of the activities were compared, it is perhaps not surprising that those who said they would engage in an activity consistently rated it significantly less risky than those who said they would not engage in it. However, it was surprising that when asked about the severity of the consequences of the activity if their password were compromised as a result of engaging in the activity, there was no significant difference between the two groups in their ratings.

Initially this seems contradictory – the groups are differing in the rating of risk, but not in the severity of the consequences? What is risk if it is not the consequences of an activity? The answer to this apparent contradiction may lie in the answers to three further questions. Firstly, respondents were asked how useful each activity was. Respondents who said they would engage in the activity consistently rated it as significantly more useful than those who said they would not engage in the activity, with a very large mean difference between the groups of 2.5 points on the 7 point Likert scale. Similarly, those who said they would engage in the activity rated the likelihood that they would encounter it in real life consistently significantly higher than those who would not engage in the activity, again with a very large mean difference between the groups of 2.6 on the 7 point Likert scale.

These results suggest that respondents who say they would engage with the activity, while agreeing about the level of the severity of the consequences of their password being compromised with those who would not engage with it, are swayed in their overall perception of the risk by the usefulness of the activity as a password management or other digital strategy. In addition, the fact that they report they are more likely to encounter the activity in real life may well reflect the fact that they have actually undertaken the activity in real life without dire consequences and this is also affecting their perception of the risk. One of the problems of risky password activities, like many other risky activities, is that negative consequences do not result from every instance of the activity, and negative consequences which do result may not be causally linked back to the instance of the action. Thus, one might share an email password with a colleague so they can access some important data for a meeting, and no negative consequences arise, even though it was a risky thing to do. So one's perception of the consequences goes down. Or, one might share an email password with a colleague, and not ever realize they have used it to send a malicious email in one's name. So one never connects the risky activity with the negative consequences that it caused.

Thinking about risk perception of password related activities through the lens of the psychometric approach developed by Slovic (1986, 2016) and considering the different aspects of people's attitudes around risky password activities, has begun to throw some interesting light on the relationships between various factors influencing the overall perception of risk of different risky activities.

However, we now realize that we need to explore much more about how people's perceptions of risk in this area are developed. For example, we did not ask people what negative experiences they had had in relation to password activities, but respondents' answers to the open-ended questions showed that this can have a very strong effect on risk perception. For example, relevant comments from respondents included:

> "..I went to a cybercafé and left the social networks open. Someone posted obscene things from my accounts, but I could change the password before they hacked me" (P1-25)
>
> "… used a computer with a keylogger on it, had social media affected. Had to go through lengthy process to change passwords across all platforms" (P1-31)
>
> "..When I lost my wallet I was afraid, whether I'd kept password inside it. Later I had to change all the passwords of all online services. Ever since I have stopped keeping passwords inside my wallet" (P2-8)

Other limitations of the current study include the fact that respondents were from many different countries, with substantial numbers from the USA and India. Previous work has shown that there are complex cultural differences in attitudes to password management (Petrie and Merdenyan, 2016), although the countries studied in that study did not include either the USA or India. But there may be differences in the attitudes of respondents from these two countries which are obscuring effects in the current study. The other limitation, shared with much research on usable security, is that we are

relying on self-reports of activities which may be influenced by social desirability factors. People know that should not share passwords or write them down, so may be less inclined to say they would engage in the activity than they actually do. Nonetheless, substantial numbers of respondents did admit to engaging in these activities and clear and interesting patterns of responses emerged.

8. REFERENCES

Adams, A. and Sasse, M.A., 1999. Users are not the enemy. *Communications of the ACM*, *42*(12), pp.40-46.

Adams, A., Sasse, M.A. and Lunt, P. 1997. Making passwords secure and usable. In *People and Computers XII* (pp. 1-19). Springer London.

Bonneau, J., Herley, C., van Oorschot, P.C. and Stajano, F. 2015. Passwords and the evolution of imperfect authentication. *Communications of the ACM*, *58*(7), pp.78-87.

Boothroyd, V. and Chiasson, S. 2013, July. Writing down your password: Does it help? In *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on* (pp. 267-274). IEEE.

Breakwell, G.M. 2014. *The psychology of risk*. Cambridge University Press.

Brown, A.S., Bracken, E., Zoccoli, S. and Douglas, K. 2004. Generating and remembering passwords. *Applied Cognitive Psychology*, *18*(6), pp.641-651.

Bryant, K. and Campbell, J. 2006. User behaviours associated with password security and management. *Australasian Journal of Information Systems*, *14*(1).

Creese, S., Hodges, D., Jamison-Powell, S. and Whitty, M. 2013, July. Relationships between password choices, perceptions of risk and security expertise. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 80-89). Springer Berlin Heidelberg.

Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K. and Herley, C. 2013, April. 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.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. and Combs, B. 1978. How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy sciences*, *9*(2), pp.127-152.

Florencio, D. and Herley, C. 2007, May. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (pp. 657-666). ACM.

Gaw, S. and Felten, E.W. 2006, July. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security* (pp. 44-55). ACM.

Grawemeyer, B. and Johnson, H. 2011. Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), pp.256-267.

Inglesant, P.G. and Sasse, M.A. 2010, April. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 383-392). ACM.

Kaye, J.J. 2011, May. Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2619-2622). ACM.

Komanduri, S., Shay, R., Kelley, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F. and Egelman, S. 2011, May. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2595-2604). ACM.

Kumar, N. 2011. Password in practice: An usability survey. *Journal of Global Research in Computer Science*, *2*(5), pp.107-112.

Langer, E.J., 1975. The illusion of control. *Journal of Personality and Social Psychology*, *32*(2), p.311.

Mazurek, M.L., Komanduri, S., Vidas, T., Bauer, L., Christin, N., Cranor, L.F., Kelley, P.G., Shay, R. and Ur, B. 2013, November. Measuring password guessability for an entire university. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 173-186). ACM.

Meter, D.J. and Bauman, S., 2015. When sharing is a bad idea: the effects of online social network engagement and sharing passwords with friends on

cyberbullying involvement. *Cyberpsychology, Behavior, and Social Networking*, *18*(8), pp.437-442.

Morris, R. and Thompson, K. 1979. Password security: A case history. *Communications of the ACM*, *22*(11), pp.594-597.

Petrie, H. and Merdenyan, B. 2016, October. Cultural and Gender Differences in Password Behaviors: Evidence from China, Turkey and the UK. In *Proceedings of the 9th Nordic Conference on Human-Computer Interaction* (p. 9). ACM.

Proctor, R.W., Lien, M.C., Vu, K.P.L., Schultz, E.E. and Salvendy, G. 2002. Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods, Instruments, & Computers*, *34*(2), pp.163-169.

Sasse, M.A., Brostoff, S. and Weirich, D. 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), pp.122-131.

Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. and Cranor, L.F. 2010, July. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 2). ACM.

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G. and Furlong, M. 2007, April. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 895-904). ACM.

Sjöberg, L., Moen, B.E. and Rundmo, T. 2004. Explaining risk perception. *An evaluation of the psychometric paradigm in risk perception research*, p.33.

Slovic, P. 1986. Informing and educating the public about risk. *Risk analysis*, *6*(4), pp.403-415.

Slovic, P. 2016. *The perception of risk*. Routledge.

Sowby, F.D. 1965. Radiation and Other Risks. *Health Physics*, *11*(9), pp.879-887.

Starr, C. 1969. Social benefit versus technological risk. *Readings in Risk*, pp.183-194.

Stobert, E. and Biddle, R. 2014, July. The password life cycle: user behaviour in managing passwords. In *Proc. SOUPS*.

Ur, B., Bees, J., Segreti, S.M., Bauer, L., Christin, N. and Cranor, L.F. 2016, May. Do Users' Perceptions of Password Security Match Reality?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 3748-3760). ACM.

Ur, B., Kelley, P.G., Komanduri, S., Lee, J., Maass, M., Mazurek, M.L., Passaro, T., Shay, R., Vidas, T., Bauer, L. and Christin, N. 2012, August. How does your password measure up? The effect of strength meters on password creation. In *USENIX Security Symposium* (pp. 65-80).

Voyiatzis, A.G., Fidas, C.A., Serpanos, D.N. and Avouris, N.M. 2011, September. An empirical study on the web password strength in greece. In *Informatics (PCI), 2011 15th Panhellenic Conference on* (pp. 212-216). IEEE.

Vu, K.P.L., Proctor, R.W., Bhargav-Spantzel, A., Tai, B.L.B., Cook, J. and Schultz, E.E. 2007. Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies*, *65*(8), pp.744-757.

Whitty, M., Doodson, J., Creese, S. and Hodges, D. 2015. Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), pp.3-7.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. 2004. Password memorability and security: Empirical results. *IEEE Security &Pprivacy*, *2*(5), pp.25-31.

Zviran, M. and Haga, W.J. 1999. Password security: an empirical study. *Journal of Management Information Systems*, *15*(4), pp.161-185.