Generational Differences in Password Management Behaviour

Burak Merdenyan
University of York
York, United Kingdom
burak.merdenyan@york.ac.uk

Helen Petrie
University of York
York, United Kingdom
helen.petrie@york.ac.uk

Passwords still remain a very common authentication method for online accounts. Many studies have investigated people's risky password management behaviour, including reusing passwords, writing them down, and sharing them with others. However, most studies provide limited information about the demographics of their participants. There may be substantial differences in password management behaviour between younger and older people, as they represent very different generations with different experiences of the Internet, and investigation of these differences could be a first step to helping people manage their passwords more appropriately. An online survey asked 45 younger and 47 older people about their password management behaviour. Significant generational differences were found in password behaviours including storing passwords, sharing them with others, forgetting them, and logging in from a shared computer. There were also significant differences in respondents' ratings of their password security knowledge and password strength. Finally, there was a significant social desirability bias in answers to several questions.

Password security, password management, risky password behaviour, generational differences, older respondent, younger respondent, social desirability bias.

1. INTRODUCTION

Passwords still remain the most popular method of authentication for online accounts (Bonneau et al., 2015; Das et al., 2014; Seitz et al., 2017) in spite of the development of more sophisticated authentication methods such as biometrics, hardware tokens, and 2-factor authentication. Email, online banking, and social networking sites (SNSs) are amongst most common online services that require password authentication. The number of passwords that users require is increasing, as they continue to acquire more and more online accounts (Woods & Siponen, 2018). Even a decade ago, a large-scale study conducted with half a million users on web password habits revealed that on average people managed 25 online accounts that require passwords (Florencio & Herley, 2007). A more recent small-scale password behaviour study confirmed this result, finding that on average British respondents manage 22.3 online accounts requiring passwords (Petrie & Merdenyan, 2016).

The management of passwords and ensuring their security for large numbers of online accounts is not easy for users. Studies have shown that users report difficulties in managing their passwords (Gaw & Felten, 2006; Stobert & Biddle, 2014), and that they adopt risky coping strategies such as reusing passwords, writing them down, and sharing them with others (Grawemayer & Johnson, 2011; Shay et al., 2010; Zviran & Haga, 1999).

But, what do we know about the users involved in these password behaviour studies? Many studies (*see* Background section) investigating password management behaviour have been conducted with university students, faculty members and staff, and employees from different organisations, and provided very limited information about the demographics of their participants. There might be substantial differences in the general password behaviour between young and older users, as they have different views and experiences of life. People currently in their 20s have grown up with the Internet and online accounts: someone who is currently 25 years old was born in 1993, about the time when the general public began to use the Internet. Whereas people currently in their 60s and 70s have lived most of their lives without the Internet, and may have greater suspicions about using it.

Previous studies have revealed that age is one of the most important variables that affects usage of the Internet (Fox & Madden, 2006; Van Deursen & Van Dijk, 2014; Zillien & Hargittai, 2009). News about security breaches might have a different

impact on the password behaviour of younger and older users. Older people might also have different attitudes when it comes to creating and recalling passwords, they may be more worried about forgetting complex passwords and more likely to write them down and re-use familiar passwords.

In addition, password behaviour studies until now have failed to consider the effect of social desirability in responses from participants. Researchers have assumed that the self-report responses of participants are largely accurate, but participants undoubtedly are aware that they should not be undertaking risky activities such as reusing passwords, so the frequency of risky behaviour may be even higher than research indicates. In addition, previous research has found a correlation between age and social desirability, indicating higher propensity to socially desirable responses with advancing age (Soubelet & Salthouse, 2011). Thus, older people might be more susceptible to socially desirable responses when it comes to reporting their password behaviour than younger people. The social desirability effect can be measured using the Marlowe-Crowne Social Desirability Scale, a short version of which has been developed by Strahan and Gerbasi (1972) and used extensively in psychological research.

This study aims to fill the gap in password behaviour research by investigating potential differences in password management behaviours of participants from two different generations: participants in their late teens/early 20s and participants over 60 years of age. It also considers the effects of social desirability on responses and investigates whether these differ for these two generations. In this study, we also aim to compare our results with previous studies conducted with young people, particularly university students, in order to investigate whether young people's password behaviour have changed over the last decade, and if they become more careful on managing their passwords after numerous online security breaches reported on news, and public advice campaigns. These results will throw light on the specific requirements on password management support for different age groups, and could be used for the design of password management systems and the education of users about safe password management.

2. BACKGROUND

There have been many studies on password behaviour conducted with university students, faculty members, and staff (Boothroyd & Chiasson, 2013; Brown et al. 2004; Bryant & Campbell, 2006; Gaw & Felten, 2006; Grawemayer & Johnson, 2011; Riley, 2006; Shay et al., 2010; Stobert & Biddle, 2014; Ur et al., 2015), employees from various organizations (Adams & Sasse, 1999; Inglesant & Sasse, 2010; Zviran & Haga, 1999), children (Meter & Bauman, 2015), married couples (Singh et al., 2007), and the general public (Florencio & Herley, 2007; Kaye, 2011). But to the best of our knowledge, there are only three studies that have reported differences between younger and older people in their password behaviour: Bryant and Campbell (2006), Kaye (2011), and Whitty et al. (2015).

Table 1 summarises a range of studies which have collected information about people's password management behaviour, including the participant demographics and findings. These studies span the last 15 years of research on password management behaviour. It can be seen that the participant samples are often not well specified, failing to provide information about the country where participants are located (Furnell & Bär, 2013; Hoonakker et al., 2009), age information (Brown et al., 2004; Furnell & Bär, 2013; Kaye, 2011; Tam et al., 2010), or gender information (Boothroyd & Chiasson, 2013; Brown et al., 2004; Furnell & Bär, 2013; Riley, 2006). There are sensible reasons for this lack of information, researchers often want to make their surveys as anonymous as possible, as passwords are a sensitive topic for respondents. However, this lack of information makes it difficult to explore individual and group differences within and between samples. Samples are also often very heterogeneous, mixing university staff and students (Kumar, 2011; Shay et al., 2010) or university students with the general public (Boothroyd & Chiasson, 2013; Furnell & Bär, 2013), again making it difficult to explore differences between different groups in society.

Three studies have drawn conclusions about age or generational effects. Bryant and Campbell (2006) conducted a survey of the password behaviour of 884 undergraduate students from the business faculty of an Australian university. Although all the participants were undergraduate students, there was a considerable age range, from under 26 years (797/90% of participants) to over 35 years (32/3.6% of participants). Unfortunately, the authors do not report the maximum age of participants. And despite the very unbalanced age distribution of participants, the authors concluded that young people do not change their passwords as frequently as older participants (It might be better to say 'young aged older participants', as they are only over 35 years), but they are less likely to forget their passwords than older people.

Kaye (2011) conducted a survey with respondents from many countries and presumably a wide range of people (he publicised the survey on Facebook, but due to a low response then used snowball sampling from his own Facebook and Twitter contacts). He found that older men (49 – 69 years) shared their passwords significantly more often, although there was no similar significant effect for women. Whitty et al. (2015) with a sample of participants from 18 to 72 years also found that older

Table 1: *Summary of previous research on password management behaviour.*

Authors	Year	Location	Participants			Password Behaviour Findings	
			Type	*Number*	*Age & Gender*	*General*	*Age Effects*
Brown et al.	*2004*	*USA*	*University students*	*218*	*Age: No info* *Gender: No info*	*Forget: 31%* *Reuse: 93%* *Write down: 54%*	*N/A*
Bryant & Campbell	*2006*	*Australia*	*University students*	*884*	*Age: < 26 90.2%, 26 – 35: 6.2%, 36+: 3.6%* *Gender: 57.1% Female, 42.8% Male*	*Change: 61.9% never* *Forget: 30.4%*	*Change: Young < Old* *Forget: Young < Old*
Riley	*2006*	*USA*	*University students*	*315*	*Age: 18 – 58; Mean: 25.34* *Gender: No info*	*Change: 52.7% never* *Reuse: 54.6%* *Writing down: 15%*	*N/A*
Hoonakker et al.	*2009*	*USA/ Denmark?*	*Employees*	*836*	*Age: Mean: 50 years* *Gender: 70% Female, 30% Male*	*Reuse: 18%* *Share: 5%* *Write down: 56%*	*N/A*
Shay et al.	*2010*	*USA*	*University students, faculty, staff*	*470*	*Age: 59.6% < 22, 39.4% 22+* *Gender: 51.3% Female, 48.5% Male*	*Reuse: 81%* *Share: 28%* *Write down: 13%*	*N/A*
Tam et al.	*2010*	*USA*	*University students*	*133*	*Age: No info* *Gender: 48 Female, 84 Male*	*Forget: 58.0%* *Reuse: 56.0%* *Share: 42.1%*	*N/A*
Grawemeyer & Johnson	*2011*	*UK*	*Employees, university staff, students*	*41*	*Age: late 20s to early 40s* *Gender: 25 Female, 16 Male*	*Change: 79.4% never* *Reuse: 49.1%* *Write down: 6.3%* *N.B. %s refer to passwords, not participants*	*N/A*
Kumar	*2011*	*India*	*University students, faculty, staff*	*202*	*Age: 17 – 61* *Gender: 24% Female, 76% Male*	*Change: 67% never or annually* *Forget: 66% in 6 months* *Reuse: 79%* *Write down: 84%*	*N/A*
Kaye	*2011*	*Worldwide*	*No info: general public?*	*122*	*Age: no info* *Gender: 60 Female, 62 Male*	*Share: 70.5%*	*Share: Young < Old (for male participants)*
Boothroyd & Chiasson	*2013*	*Canada*	*University, community at large*	*31*	*Age: 21 – 37* *Gender: No info*	*Reuse: 97%*	*N/A*
Furnell & Bär	*2013*	*UK/ Germany?*	*IT students, general public*	*246*	*Age: No info* *Gender: No info*	*Change: 21% regularly* *Forget: 10%* *Share: 6%*	*N/A*
Whitty et al.	*2015*	*UK*	*Professionals*	*497*	*Age: 18 – 72 Mean: 41.86* *Gender: 202 Female, 295 Male*	*Share: 51.1%*	*Share: Young < Old*

people (both men and women) were more likely to share their passwords than younger people.

Three studies have also included only university students, providing reasonably homogeneous samples of well-educated individuals who ought to be well informed about password management behaviour. Brown et al. (2004) conducted a survey with 218 participants, all students enrolled in the Introductory Psychology class at a university in the United States (although the ages and gender breakdown of participants is not given). They found that 31% of participants had forgotten their passwords in the past, 93% of the participants re-use at least one password for more than one system, 54% of participants write down their passwords. These authors also note that participants' level of education or training in security did not seem to have any impact on their password management behaviour, as most participants stated that guidelines provided are too unpractical to follow. This finding demonstrates that there are problems in translating password security information into practical behaviour by users.

Bryant and Campbell (2006) also conducted a survey with only undergraduate students at an Australian university, although as already discussed, the age range of participants include individuals over the age of 36 years. Overall, they found the 61.9% of participants reported that they never change their passwords and 31.4% reported forgetting passwords.

Finally, Riley (2006) conducted a survey with 328 undergraduate and graduate students at another university in the United States. 52.7% of participants reported that they never change their passwords. 54.6% reported that they reuse their passwords very frequently, and 33% of the participants use slight variations of the same password for multiple accounts. 15% of the participants reported that they wrote down their passwords.

All these three studies are more than a decade old and no more recent studies with solely university students in relation to password management could be found.

Overall, the set of studies, of mainly younger participants, reveal that high levels of risky password management behaviours continue. Although there is naturally much variation between studies, there is little evidence of decreases in risky password management behaviour, such as reusing passwords, and writing passwords down.

3. METHOD

3.1 Design

A between participants design was used, the independent variable was age group: participants in their late teens/early 20s and participants over 60 years of age. An online survey system was used to collect data. The survey consisted of 27 questions with a mixture of Likert item, multiple choice, and open-ended responses. Topics included: risky password management activities (e.g. frequency of storing, sharing, re-using, and using different variations of passwords, logging-in from a shared computer), positive password management strategies (usage of password managers, changing passwords at regular time periods), behavioural changes in password management (after exposure to news items and information from trusted people), self-ratings of password security knowledge, following specific password security guidelines and advices, and personal experiences of problems with password security via several open-ended questions. The respondents were also asked to complete the short version of Marlow-Crowne Social Desirability Scale (Strahan & Gerbasi, 1972), which consists of 10 items such as "I am always willing to admit it when I make a mistake". This scale was presented to respondents as a short personality questionnaire. All the survey questions are online at goo.gl/9qXEph.

3.2 Respondents

92 respondents (*see* Table 2) provided sufficient data for analysis, 45 young respondents and 47 older respondents. The educational and employment backgrounds of the older respondents was varied. Only one older respondent stated that they any background in computer science, as they had worked as a software developer for 43 years. Respondents were entered in a prize draw for one of 10 gift vouchers worth £10 (approximately USD 14 at the time of the study).

3.3 Procedure

An invitation email including the link to the survey was sent to computer science students at the University of York and to a local online community. The email to the online community as for volunteers aged 60 years and older (previous requests to this community for research participants had yielded an excellent response from older participants). In the email, potential respondents were informed about the topic of the survey, and the approximate time it would take to complete it (5 - 10 minutes). Respondents completed an online consent form in which they were informed that at no point in the survey would they be asked for their passwords or any information that would compromise their security of passwords.

Table 2: *Demographic information for younger and older respondents.*

	Younger Respondents (N = 45)	**Older Respondents (N = 47)**
Age	*18-22 years* *Mean: 18.8*	*60-83 years* *Mean: 68.8*
Gender	*Male: 39 (86.7%)* *Female: 5 (11.1%)* *Transgender: 1 (2.2%)*	*Male: 22 (46.8%)* *Female: 25 (53.2%)*
Education	*Comp. Science Bachelor's Students: 45 (100%)*	*No Schooling: 2 (4.3%)* *High School: 13 (27.7%)* *Bachelor's: 25 (53.2%)* *Master's: 7 (14.9%)*
Employment	*Student: 45 (100%)*	*Actively Working: 7 (14.9%)* *Retired / Not working: 40 (85.1%)*

4. RESULTS

The short Marlow-Crowne Social Desirability (SD) Scale is scored from 0 (very low susceptibility to SD) to 10 (very high susceptibility to SD). We divided scores into Low SD (scores of 0 to 3), Medium SD (scores of 4 to 6) and High SD (scores of 7 to 10). Using this categorization, we found there was a significant difference in the distributions of younger and older respondents, with significantly much older respondents in the High SD group (42.6%) than younger respondents (17.8%) (chi-square = 6.97, $p < .05$). Therefore, for each of the questions about password management, we investigated the possibility of a social desirability bias in responses.

4.1 Risky password management behaviours

Respondents were asked if they write down and store their passwords. Table 3 shows the distribution of answers, which were significantly different for young and older respondents (chi-square =40.45, $p < 0.001$). Less than 50% of younger respondents report that they store their passwords (42.2%), whereas over 90% of older respondents report that they store their passwords (93.6%). Of the 26 (57.8%) younger respondents who declared that they do not store their passwords, only 5 (19.2%) of them had a High SD score. Responses to an open-ended follow-up question reveal that password managers are a common way of storing passwords digitally. There was no tendency for High SD respondents to answer in the more socially desirable way (that they do not store their passwords).

Respondents were asked if they reuse passwords across different accounts. There was no significant (n.s.) difference between young and older respondents (chi-square =2.84, n.s.). However, both age groups show very high reuse of passwords: 37 (82.2%) of young respondents and 44 (93.6%) of older respondents reported this behaviour. Respondents were also asked if they use different variations of their passwords across different accounts. Again, no significant difference was found (chi-square =0.42, n.s.) between younger and older respondents. However, again both age groups show very high use of variations of passwords: 36 (80%) of younger respondents, and 40 (85.1%) of older respondents. There was no tendency for High SD respondents to answer in the more socially desirable way on either of these questions.

Table 3: *Password storage locations for young and older respondents.*

	Younger Respondents (N = 45)	**Older Respondents (N = 47)**
On paper	*2 (4.4%)*	*19 (40.4%)*
Digitally	*16 (35.6%)*	*14 (29.8%)*
Both	*1 (2.2%)*	*11 (23.4%)*
Do not store	*26 (57.8%)*	*3 (6.4%)*

Respondents were asked if they have ever shared their passwords with others. 23 (51.1%) of younger respondents compared to only 13 (27.7%) of older respondents say they do, a significant difference (chi-square =5.31, $p < .05$). There was a significant SD effect on this question, with only 17.9% of High SD respondents saying they share passwords, compared to 63.3% of Low SD respondents (chi-square =10.11, $p < .01$). Of the 22 (48.9%) younger respondents who declared that they do not share their passwords with others, only 6 (27.3%) of them had a High SD score. On the other hand, of the 34 (82.3%) older respondents who declared that they do not share their passwords with others, 17 (50.0%) of them had a High SD score. Of the younger respondents who share passwords, 16 (69.6%) say they share them with close family members and 8 (34.8%) share them with close friends. Of the older respondents who share passwords, all say they only share them with close family members. Table 4 shows the type of accounts for which respondents share passwords share with others. Younger

respondents are more likely to share entertainment account passwords whereas older respondents are most likely to share eBanking passwords.

Table 4: *Type of accounts for which passwords are shared.*

	Younger Respondents (N = 23)	Older Respondents (N = 13)
Email	*5 (21.7%)*	*3 (23.1%)*
eBanking	*1 (4.4%)*	*5 (38.5%)*
eCommerce	*0 (0.0%)*	*1 (7.7%)*
SNSs	*4 (17.4%)*	*2 (15.4%)*
Entertainment (e.g. Netflix, gaming)	*6 (26.1%)*	*1 (7.7%)*
University account	*4 (17.4%)*	*0 (0.0%)*
All accounts	*2 (8.8%)*	*1 (7.7%)*

Respondents were asked if they have ever log in to their online accounts from a shared computer (respondents were given examples such as, in a library, in an Internet café, but they were not restricted to think of a specific location). 34 (75.7%) of younger respondents but only 15 (31.9%) of older respondents report doing this, a significant difference (chi-square =17.59, $p < .001$). There was also an SD effect on this question, with only 39% of High SD respondents reporting this behaviour, compared to 78.9% of low SD respondents (chi-square = 7.32, $p < .05$). Of the 11 (24.3%) younger respondents who declared they have never logged in from a shared computer, only 1 (0.09%) of them had a High SD score. On the other hand, of the 32 (78.1%) older respondents who declared that they have never logged in from a shared computer, 16 (50.0%) of them had a High SD score. Table 5 shows the types of online accounts which respondents say they log in to from a shared computer. Table 6 shows the places where respondents say they log-in to shared computers.

4.2 Positive password management behaviours

Respondents were asked if they change their passwords regularly (e.g. every six months). There was no significant difference (chi-square =1.61, n.s.) between younger and older respondents. Very high percentages of both younger and older respondents stated that they do not change their passwords regularly (younger: 42/93.3%; older: 40/85.1%). There was no SD effect on this question.

Respondents were asked if they use password managers to deal with their passwords. No significant difference was found (chi-square =1.84, n.s.) in the use of password managers between younger and older respondents. 13 (28.9%) of younger respondents, and 8 (17.0%) of older respondents reporting use of password managers. '*LastPass*' is the most commonly mentioned password manager (by 12 respondents). There was no SD effect on this question.

Table 5: *Account types respondents logged in from a shared computer.*

	Younger Respondents (N = 34)	Older Respondents (N = 15)
Email	*29 (85.3%)*	*12 (80.0%)*
eBanking	*0 (0.0%)*	*2 (13.3%)*
eCommerce	*1 (2.9%)*	*0 (0.0%)*
SNSs	*12 (35.3%)*	*2 (13.3%)*

Respondents were asked how often they forget their passwords (Likert item: 1 = Quite rarely, to 7 = Very often). Older respondents rated their forgetting as significant more frequent (Median: 5) in comparison to younger respondents (Median: 1) (Mann-Whitney $U = 618.5$, $p < .001$). There was no SD effect on this question.

Table 6: *Places where respondents log in to a shared computer.*

	Younger Respondents (N = 34)	Older Respondents (N = 15)
Library	*25 (73.5%)*	*7 (46.7%)*
Internet Café	*3 (8.8%)*	*2 (13.3%)*
Airports	*0 (0.0%)*	*1 (6.7%)*
Not specified	*6 (17.6%)*	*5 (33.3%)*

4.3 Knowledge of password security issues and changing behaviour

Respondents were asked how they would rate their knowledge about password security and management issues (Likert item: 1 = Not at all knowledgeable, to 7 = Extremely knowledgeable. There was a significant difference between younger (Median: 5) and older (Median: 4) respondents (Mann-Whitney $U = 563.0$, $p < .001$), with younger respondents rating themselves as more knowledgeable. Respondents were also asked how they would rate the strength of their passwords (Likert item: 1 = Not at all strong, to 7 = Extremely strong). There was a significant difference between younger (Median: 6) and older (Median: 5) respondents (Mann-Whitney $U = 782.5$, $p < .05$), with younger respondents rating their passwords as stronger. There was no SD effect on these questions.

Respondents were asked if they have ever changed their passwords after reading about password security issues in the mass media. There was no significant difference (chi-square =0.16, n.s.) between young and older respondents. 22 (48.9%) younger respondents and 21 (44.7%) older respondents stated that they have changed their

passwords in these circumstances. Respondents most frequently mentioned news about security breaches as a reason for changing their passwords (19/86.4% of younger respondents; 11/52.4% of older respondents). Table 7 provides information about the source of the information. There was no SD effect on this question.

Table 7: *Sources of information about password security issues.*

	Younger Respondents (N = 22)	**Older Respondents (N = 21)**
Online source	*15 (68.2%)*	*9 (42.9%)*
In an email	*2 (9.1%)*	*3 (14.3%)*
TV/Radio/ Newspaper	*4 (18.2%)*	*10 (45.5%)*
Cannot remember	*1 (4.5%)*	*3 (14.3%)*

Respondents were also asked if they have ever changed their password management behaviour after reading about password security issues in the mass media. There was no significant difference (chi-square = 3.65, n.s.) between younger and older respondents. 13 (28.9%) younger respondents, and 6 (12.8%) older respondents stated that they have changed their password management behaviour as a result of reading news in the mass media. There was no SD effect on this question.

Table 8: *Advice followed by respondents.*

	Younger Respondents (N = 20)	**Older Respondents (N = 12)**
Character types in password	*11 (55.0%)*	*9 (75.0%)*
Number of characters in password	*2 (10.0%)*	*1 (8.3%)*
Content of password	*8 (40.0%)*	*2 (16.7%)*
Not reusing passwords	*3 (15.0%)*	*0 (0.0%)*

Respondents were asked if they have ever changed their password management behaviour after talking to someone. There was no significant difference (chi-square =1.15, n.s.) between younger and older respondents. 5 (11.1%) younger respondents, and 9 (19.1%) older respondents stated that they have changed their password management behaviour after talking to someone. There was no SD effect on this question.

Respondents were asked if they follow specific password security advice or guidelines. There was no significant difference (chi-square =3.63, n.s.), 20 (44.4%) younger respondents, and 12 (25.5%) older respondents stated that they follow specific password security advice or guidelines. Table 8 summarises the advice followed by respondents. There was no SD effect on this question.

5. DISCUSSION AND CONCLUSIONS

This study investigated generational differences in password management behaviours, comparing self-reports of behaviours between a sample of undergraduate university students in computer science and a sample of people over the age of 60 years.

As we found a significant difference in the distribution of SD scores between younger and older respondents, we further investigated the possibility of social desirability bias for each question. Only 2 questions out of the 14 in the survey ('Logging in from a shared computer', 'Sharing passwords with others'), showed a significant tendency to answer in a socially desirable way. Further analysis reveal that, of the older respondents who declared that they do not undertake both activities, half of them had High SD scores. This finding may explain the reason for the low percentages in self-reported password sharing and logging in to shared computers by older respondents in comparison to younger respondents. These results show that researchers should not solely rely on self-report responses from their participants, as there may be an effect of social desirability, especially in relations to some risky password behaviours. Of course, in password research, it is very difficult to observe actual behaviour of individuals in ecologically valid settings, so imaginative approaches are needed, as well as triangulation of different sources of information.

It is noteworthy that older respondents store their passwords significantly more frequently than younger respondents. A possible reason for this might be that older respondents forget their passwords significantly more often than younger respondents and possibly worry about forgetting their passwords more. Thus, older respondents do not solely rely on their memory for passwords, and they need secure ways to store their passwords. The important point here is that older respondents should be informed about the importance of storing passwords in safe places, as 40% of older respondents stated that they store their passwords on paper. Further studies need to be conducted about appropriate password storage methods and requirements for these, especially for older respondents. Password management systems are now available, but as yet are not widely used.

Reusing passwords across different accounts is also an important security threat for users. Our results show very high percentages of password reuse by both younger and older respondents. Comparing with previous research, we can see that young people have continued to undertake the risky behaviour of password reuse, with little evidence of

improvement in the past 15 years of research on this topic. This finding reveals that public advice campaigns on secure password behaviour have not been successful in preventing password reuse, and this risky behaviour continues to exist.

Younger respondents significantly differed from older respondents on the self-rating questions of password security knowledge and password strength: younger respondents rated their knowledge of password security and password strength significantly higher than older respondents. Nonetheless, the high percentage of password reuse by younger respondents is problematic, and somewhat contradicts their high self-ratings of password security knowledge. It may be that they do know the potential security issues caused by password reuse, but they still continue to behave insecurely. This set of attitudes has been found in a number of previous studies on password management behaviour (e.g. Gaw & Felten, 2006; Tam et al., 2010). It may be that different kinds of strategies are needed to educate people to avoid risky behaviours such as reusing passwords.

The study also found that the effect of security breaches reported in the mass media, which might be a good motivator for better password management behaviour, appeared to be a weak predictor of changes to passwords and password management behaviour of both younger and older respondents. This result suggests that both younger and older respondents are reluctant to change their own password management behaviour. However, this line of investigation warrants further research.

Comparing undergraduate computer science students with a sample of older people may seem unbalanced. Naturally, it might be imagined that computer science students are amongst the best informed young people about best practices in password management, however this notion might be illusionary. The content for undergraduate students at the university where the respondents were recruited does not include any module related to cyber-security or secure password management. Being an undergraduate student in computer science (or in any other course) in fact neither means being an expert in password management practices, nor applying the best password practices all the time (e.g. Brown et al., 2004), unless the student has a specific interest in the area. With respect to general educational level, nearly 70% of the older sample of respondents had an undergraduate or master's qualification and all the older respondents have considerable life experience. Therefore, the younger and older samples are reasonably balanced for a mixture of their education, knowledge, and life experience.

Overall, these results indicate that both young and older people continue to undertake many risky password management behaviours. The study has shown that younger and older people do behave differently on some password management activities. Further research should investigate relevant strategies and solutions to change their risky password management behaviour, taking into consideration the somewhat different requirements of young and older people revealed in this study.

6. ACKNOWLEDGEMENTS

We thank all the respondents to our survey for their time and effort.

7. REFERENCES

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

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

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

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

Bryant, K. & Campbell, J. (2006). User behaviors associated with password security and management. *Australasian Journal of Information Systems* 14(1), 81 - 100.

Charles, S. T., Reynolds, C. A. & Gatz, M. (2001). Age-related differences and change in positive and negative affect over 23 years. *Journal of Personality and Social Psychology*, *80*(1), 136.

Das, A., Bonneau, J., Caesar, M., Borisov, N. & Wang, X. (2014, February). The Tangled Web of Password Reuse. In *NDSS* (Vol. 14, pp. 23-26).

Florencio, D. & 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.

Fox, S. & Madden, M. (2006). Generations online (demographic report). *Pew Internet & American Life Project*.

Furnell, S. & Bär, N. (2013). Essential lessons still not learned? Examining the password practices of end-users and service providers. In L. Marinos and I. Askoxylakis (Eds.) *HAS/HCII 2013. LNCS 8030*. (pp. 217 – 225). Springer.

Gaw, S. & 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. & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), pp.256-267.In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 2). ACM.

Gross, J. J., Carstensen, L. L., Pasupathi, M., Tsai, J., Götestam Skorpen, C. & Hsu, A. Y. (1997). Emotion and aging: Experience, expression, and control. *Psychology and Aging*, *12*(4), 590.

Hoonakker, P., Bornoe, N. & Carayon, P. (2009). Password authentication from a human factors perspective: results of a survey among end-users. In *Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting*. HF&E Society.

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

Kumar, N. (2011). Password in practice: an usability study. *Journal of Global Research in Computer Science*, 2(5), 107 – 112.

Meter, D.J. & 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), 437-442.

Notoatmodjo, G. & Thomborson, C. (2009). Passwords and perceptions. In *Proceedings of the 7th Australasian Information Security Conference (AISC 2009)*. Australian Computer Society.

Petrie, H. & 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*. ACM.

Riley, S. (2006). Password security: What users know and what they actually do. *Usability News*, *8*(1), 2833-2836.

Seitz, T., Hartmann, M., Pfab, J. & Souque, S. (2017, May). Do Differences in Password Policies Prevent Password Reuse?. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 2056-2063). ACM.

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

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G. & 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.

Soubelet, A. & Salthouse, T. A. (2011). Influence of social desirability on age differences in self-reports of mood and personality. *Journal of Personality*, *79*(4), 741-762.

Stobert, E. & Biddle, R. (2014, July). The password life cycle: user behaviour in managing passwords. In *Symposium on Usable Privacy and Security (SOUPS).* ACM.

Strahan, R. & Gerbasi, K. C. (1972). Short, homogeneous versions of the Marlow-Crowne Social Desirability Scale. *Journal of Clinical Psychology*, *28*(2), 191-193.

Tam, L. Glassman, M. & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour and Information Technology*, 29(3), 233 – 244.

Teachman, B. A. (2006). Aging and negative affect: the rise and fall and rise of anxiety and depression symptoms. *Psychology and Aging*, *21*(1), 201.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., Christin, N. & Cranor, L. F. (2015, July). "I added '!' at the end to make it secure": Observing password creation in the lab. In *Symposium on Usable Privacy and Security (SOUPS).* ACM.

Van Deursen, A. J. & Van Dijk, J. A. (2014). The digital divide shifts to differences in usage. *New Media & Society*, 16(3), 507-526.

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

Woods, N. & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*, *111*, 36-48.

Zillien, N. & Hargittai, E. (2009). Digital distinction: Status-specific types of internet usage. *Social Science Quarterly*, *90*(2), 274-291.

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