Individual differences in cyber security behaviours: An examination of who's sharing passwords

Monica Whitty[1], James Doodson[1], & Sadie Creese[2], Duncan Hodges[2]

[1]Department of Media and Communications, University of Leicester, Leicester, England, United Kingdom

[2]Cyber Security Centre, Department of Computer Science, University of Oxford, Oxford, Oxfordshire, United Kingdom.

Address correspondence to:

Monica Whitty

Department of Media and Communications

University of Leicester

Leicester, Leicestershire

England, United Kingdom

Telephone: 0116 2297329

Email: mw229@le.ac.uk

Acknowledgment: *The work reported in this paper was supported by award EP/J004995/1: An Exploration of Superidentity, from the UK Engineering and Physical Sciences Research Council. Colleagues on this grant are thanked for helpful contributions to the current work.*

Individual differences in cyber security behaviours: An examination of who's sharing passwords

RUNNING HEAD: INDIVIDUAL DIFFERENCES IN CYBER SECURITY BEHAVIOURS

Abstract

In spite of the number of public advice campaigns, researchers have found that individuals still engage in risky password practices. There is a dearth of research available on individual differences in cyber security behaviours. This study focused on the risky practice of sharing passwords. As predicted, we found that individuals who scored high on a lack of perseverance were more likely to share passwords. Contrary to our hypotheses, we found younger people and individuals who score high on self-monitoring were more likely to share passwords. We speculate on the reasons behind these findings and examine how they might be considered in future cyber security educational campaigns.

Introduction

Despite the number of government education campaigns to change problematic online behaviours, many individuals still engage in risky password practices, such as sharing passwords, using the same password over multiple platforms and using passwords that can be easily cracked[1-5]. Given that such actions can potentially lead to undesirable outcomes for the individual (e.g., identity theft, theft from bank accounts, fraud, etc.) it is important to find new ways to prevent risky security practices. This is especially important given that passwords are the default authentication mechanism on all 'secure' systems on the Internet. Research that identifies the type of person who is more likely to engage in risky cyber security practices could assist in reducing the likelihood of these insecure practices. Such knowledge could help develop more appropriate campaigns as well as target the individuals who are more likely to engage in poor security practices. As Wiederhold[6] has pointed out: "psychology, through its insight into human nature, has a crucial role to play in mitigating" risky cyber security practices (p.131). This paper helps add to the literature on poor security practices by focusing on the risky practice of sharing passwords. This behaviour is of interest as it is inherently risky – not only is the person effectively surrendering their digital identity to another user (who could misuse the data it is protecting), he/she is also increasing the risk to that particular security 'token'. The person the password has been shared with might engage in risky security practices, hence dramatically increasing the risk associated to the token.

Researchers have found that individuals are typically aware of what good password management entail[7-8]. Nonetheless, it has been found that despite understanding security risks, individuals are still inclined to take risks because: they are unrealistically optimistic and believe that negative events are less likely to happen

to them[9], they are unable to perceive any immediate negative consequences[7], or they make a convenience-security trade-off[7].

In addition to the specific motivations mentioned above, there might be individual factors that distinguish users who engage in risky cyber security behaviours. To date, individual differences in problematic security practices have received little attention in the psychological literature. Identifying the type of person who is more likely to make poor security decisions could assist in improving public awareness campaigns.

This paper specifically examined the type of person who is more likely to share passwords. Given the dearth of literature available on the topic, the hypotheses are based on the scant available literature available on individual differences and online security as well as the research on how individuals with certain personality characteristics typically behave in their everyday lives. The results reported in this paper are part of a much larger study, which examined password decision-making. The hypotheses are outlined below.

Age

Older adults tend to be less knowledgeable about Internet security compared with younger users[10]. Given the 'digital divide' between younger and older Internet users our first hypothesis is that older people are more likely to share passwords compared with younger people.

Impulsivity

Individuals who score high on impulsivity questionnaires are individuals who tend to act on whim, displaying behaviours characterised by little forethought or consideration of the consequences of their actions[11]. Although impulsivity, to our knowledge, has not previously been considered with regards to online security it

would be reasonable to presume that these types of people are less secure online, as they are likely to focus on the short-term goal (getting an account) rather than the long-term security implications. The second hypothesis is individuals who score high on measures of impulsivity are more likely to share passwords compared with those who score low on impulsivity.

Self-monitoring

Individuals who are high self-monitors are more likely to observe and regulate their expressive behaviours. These individuals are typically sensitive to social and situational cues and alter their behaviour accordingly[12]. Given that individuals who score high on self-monitoring tend to consider their social surroundings prior to acting out we might expect them to be more considerate of how others would view them should they undertake risky practices. The third hypothesis is individuals who score high on measures of self-monitoring are more likely to share passwords compared with those who score low on self-monitoring.

Locus of control

Locus of control refers to an individual's belief about control over his/her environment. People who have an internal locus of control have the conviction that events are contingent upon one's behaviour. Those with an external locus of control believe that events do not depend upon their actions, but rather upon luck, chance or fate[13]. Those with an external locus of control have been found to engage in more risky activities[14]. If individuals believe that they have little control over whether someone compromises their data, it is reasonable to presume they will be less likely to behave securely online. The forth hypothesis is that individuals who score high on

measures of internal locus of control are more likely to share passwords compared with those who score high on external locus of control.

Knowledge of cyber security

Although the research has found that the general population are typically aware of online security[7], there are still clear distinctions between experts and non-experts regarding basic security behaviours, such as patching and updating software[15]. Having a greater knowledge about online security could impact on cyber security practices. Therefore our fifth and final hypothesis is that individuals who believe they are more knowledgeable about cyber security issues are more likely to share passwords compared with those who believe they are less knowledgeable.

Method

Participants

Participants were invited to take part in the study via professional association mailing lists. One list focused on cyber security issues and five lists focused on the arts or social sciences. We focused on these lists to ensure we included both cyber security experts and non-experts in our sample. Overall, the sample represented a broad range of knowledge about cyber security issues.

In the period from 5th June 2013 to 7th September 2013, 910 participants accessed the survey. Of these, 630 completed the survey in full and indicated that their data could be used for analysis. In order to avoid cultural bias, we only included those residing in the UK in our final sample. Additionally, one individual was excluded for being too young to give consent to complete the survey (16 years) and two individuals were excluded for providing an unlikely age (103 and 107 years).

After excluding participants, 497 participants (295 male, 202 female) remained with a mean age of 41.86 years (*SD* = 13.38), ranging from 18 to 72 years.

Materials

Data were collected using a questionnaire hosted on the Qualtrics online survey platform. The questionnaire comprised a number of scales, represented online using individual or matrix-style layouts with responses entered via radio buttons, drop-down menus or free text entry as appropriate. Password sharing was assessed using a single yes/no question: "Have you ever shared any of your passwords with anyone?"

Impulsivity was measured using the UPPS-R Impulsivity Scale[11]. The 45-item scale measures a person's tendency to act on whim, displaying behaviours characterised by little forethought or consideration of the consequences of their actions. The scale comprises four subscales: lack of premeditation (11 items), urgency (12 items), sensation seeking (12 items) and lack of perseverance (10 items). Possible scores range from 11 to 44 for the lack of premeditation subscale, from 12 to 48 for both the urgency and sensation seeking subscales, and from 10 to 40 for the lack of perseverance subscale. A lower score indicates low impulsivity for that dimension. In the current study, each of the subscales demonstrated good internal consistency (Cronbach's α=.85, .89, .87 and .82 for lack of premeditation, urgency, sensation seeking and lack of perseverance, respectively).

Self-monitoring was measured using the original version of the Self Monitoring Scale[12]. The 25-item scale measures a person's tendency to monitor (regulate, control and observe) their behaviour and image in interpersonal relationships and social situations. For each item on the scale, participants indicate whether a statement is true or false description of how they act or react in social situations. Possible scores range

from 0 to 25, with a lower score indicating low self-monitoring. In the current study, the scale demonstrated good internal consistency (Cronbach's α=.74).

Locus of control was measured using the Internal-External Control scale[13]. The 29-item scale measures a persons' general tendency for an internal or external locus of control. For each item on the scale, participants indicate which of two statements they agree with most. Possible scores range from 0 to 23, with a lower score indicating a more internal locus of control insofar as a participant believes that everyday events are contingent his or her own behaviour. In the current study, the scale demonstrated good internal consistency (Cronbach's α=.75).

Knowledge of cyber security was measured using a single question**.** Participants were asked to rate their knowledge about cyber security issues on a five-point likert scale. Overall, 24% rated themselves 'very knowledgeable', 41% as 'somewhat knowledgeable', 26% as 'about average', 6% as 'somewhat unknowledgeable' and 2% as 'very unknowledgeable'. Cyber security experts were significantly more knowledgeable about cyber security than non-experts, Mann-Whitney U=15803.500, W=37958.500, Z=-9.563, p<.001.

Procedure

Participants were asked to complete a number of demographic items, followed by the password sharing and knowledge of cyber security question and finally the personality questionnaires. They were debriefed at the end of the questionnaire and given a summary of their personality scores. They were also given the opportunity to leave contact details to be entered in a draw for a £500 Amazon voucher (the opportunity to enter the draw was explained in the initial participant information). Finally, they were given details of where they could access a summary of the findings once the study had been completed.

Results

All five hypotheses were tested simultaneously using standard forced entry binary logistic regression, with password sharing as the outcome variable – participants had either shared passwords in the past or they had not. As summarised below, a few of our hypotheses were supported.

Overall, 51.1% had shared their passwords in the past. Table 1 summarises the descriptive statistics for means broken down by those who had shared and not shared passwords.

INSERT TABLE 1 ABOUT HERE

Impulsivity was considered using the four subscales. The overall model was statistically significant in predicting whether an individual had shared passwords, $\chi^2(8)=49.69$, $p<.001$, though the amount of variance explained was low (Cox and Snell $R^2=.10$) The model correctly predicted whether participants had shared passwords for a good proportion (62.6%) of cases.

Table 2 demonstrates that only one of our hypotheses supported (and only in part), with those who scored high on lack of perseverance more likely to share their passwords ($B=0.05$, $Wald=4.29$, $p=.04$). We obtained two further significant results; however, in the opposite direction to what was predicted. Younger people were more likely to share passwords compared with older people ($B=-0.02$, $Wald=5.06$, $p=.02$) and those who scored high on self-monitoring were more likely to share passwords compared with those who scored low ($B=0.07$, $Wald=9.65$, $p<.001$).

INSERT TABLE 2 ABOUT HERE

Discussion

There is a dearth of research on the psychological characteristics of those who engage in risky cyber security practice. This study highlighted the importance of

understanding the types of people who are more likely to engage in the risky behaviour of sharing passwords. Importantly, we identified a number of significant variables, suggesting that personality, in part, plays a role in predicting the type of person who is more likely to share passwords. However, we did find that only one of our hypotheses was supported.

Demographic characteristics

Age was a significant predictor of sharing passwords; however, the direction of the result was the opposite of what we hypothesised. Younger people were more likely to share passwords compared with older people. It would be interesting to learn more about whom younger people are sharing passwords with and why younger people are more likely to share passwords. It might be that younger people have more opportunities to share passwords, given they potentially have more family and friends who are active online compared with older people. Although this result is the opposite of what we predicted, it is nonetheless an important finding. It suggests that educational campaigns need to ensure they are including young people as their target audience

Personality variables

For our hypothesis on impulsivity we found that only one of the subscales was significant: perseverance. Perseverance measures the ability to remain with a task until completion and avoid becoming bored. It might be that one of the motives for sharing passwords is to delegate an online task to others to complete in order to minimise boredom and personal effort on the task. This might explain why those who score high on a lack of perseverance were more likely to share passwords. The non-significant results for lack of premeditation, urgency and sensation seeking also

suggest that those who are more rash, more likely to make spur of the moment decisions and seek out risky activities, are not more likely to share passwords.

Self-monitoring was a significant predictor of sharing passwords; however, the direction of the result was the opposite of what we hypothesised. Instead, we found that those who score high on self-monitoring were significantly more likely to share passwords compared with those who score low on this measure. Although the result is opposite to what we expected, it is an important finding. Perhaps those who score high on self-monitoring are more likely to feel pressured by others to share their passwords, thereby compromising security to appease other people. Future research is needed to test out this explanation.

Knowledge about cyber security

It is especially interesting that knowledge about cyber security did not distinguish between those who share passwords and those who do not share passwords. Researchers have found that individuals are generally aware of what constitutes good cyber security practices[7] and as with previous research our study demonstrates that knowledge is not enough to change problematic cyber security behaviours, when it comes to sharing passwords. Our research cannot speak for the motivations behind individuals' decisions to share passwords; however, we have learnt that personality, at least, plays a minor role. The results of our study provide evidence that campaigns need to go beyond providing information about cyber security if poor practices are to be changed.

Conclusions

As Wiederhold[6] has empathically argued, psychology plays an important role in providing answers to why individuals engage in risky cyber security practices. This

research reinforces this view. We found a number of variables that predicted the risky practice of sharing passwords: age, perseverance and self-monitoring. Although not all our significant results were in the direction we hypothesised they nonetheless provide us with an important picture of who is sharing passwords. We have speculated on the reasons why these types of people are more likely to engage in such risky practices. Further research is needed into testing out our speculations. Those creating public awareness campaigns could benefit from our study to help them re-focus on the messages they tell individuals as well as the types of individuals they choose to target.

Author Disclosure Statement

No competing financial interests exist.

Acknowledgements: *The work reported in this paper was supported by award EP/J004995/1: An Exploration of Superidentity, from the UK Engineering and Physical Sciences Research Council. Colleagues on this grant are thanked for helpful contributions to the current work.*

References

1. Carstens DS. (2009) Human and social aspects of password authentication. In: Gupta M, Sharman R, eds. *Social and human elements of information security: Emerging trends and countermeasures.* Hershey, PA: Information Science Reference Global, pp. 1-14.

2. 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,* San Antonio, TX: SAGE Publications, pp. 459-463.
3. Lorenz B, Kikkas K, Klooster, A. (2013) "The Four Most-Used Passwords Are Love, Sex, Secret, and God": Password Security and Training in Different User Groups. In: *Human Aspects of Information Security, Privacy, and Trust (Lecture Notes in Computer Science 8030*), Las Vegas, NV: Springer-Verlag Berlin Heidelberg, pp. 276-283.
4. Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviors. Computers & Security 2005; 24:124-133.
5. Zviran M, Haga WJ. Password security: an empirical study. Journal of Management Information Systems 1999; 15:161-186.
6. Wiederhold BK. The role of psychology in enhancing cybersecurity. Cyberpsychology, Behavior and Social Networking 2014; 17:131-132.
7. Tam L, Glassman M, Vandenwauver M. The psychology of password management: a tradeoff between security and convenience. Behaviour & Information Technology 2010; 29:233-244.
8. Von Zezschwitz E, De Luca A, Hussmann H. (2013) Survival of the Shortest: A Retrospective Analysis of Influencing Factors on Password Composition. In: *Human-Computer Interaction–INTERACT 2013, Cape Town, South Africa:* Springer-Verlag Berlin Heidelberg, pp. 460-467.
9. Campbell J, Greenauer N, Macaluso K, End C. Unrealistic optimism in internet events. Computers in Human Behavior 2007; 23:1273-1284.

10. Grimes GA, Hough MG, Mazur E, Signorella ML. Older adults' knowledge of Internet hazards. Educational Gerontology 2010; 36:173-192
11. Whiteside SP, Lynam DR. The five factor model and impulsivity: Using a structural model of personality to understand impulsivity. Personality and individual differences 2001; 30:669-689
12. Snyder M. Self-monitoring of expressive behavior. Journal of Personality and Social Psychology 1974; 30:526-537.
13. Rotter JB. Generalized expectancies for internal versus external control of reinforcements. Psychological Monographs 1966; 80:Whole No. 609.
14. You X, Ji M, Han H. The effects of risk perception and flight experience on airline pilots' locus of control with regard to safety operation behaviors. Accident Analysis and Prevention 2013; 57:131-139.
15. Creese S, Hodges D, Jamison-Powell S, Whitty M. (2013) Relationships between Password Choices, Perceptions of Risk and Security Expertise. In: *Human Aspects of Information Security, Privacy, and Trust (Lecture Notes in Computer Science 8030*), Las Vegas, NV: Springer-Verlag Berlin Heidelberg, pp. 80-89.