Contemporary Management Research
Pages 227-245, Vol. 15, No. 4, 2019
doi:10.7903/cmr.19394

Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers

Ramakrishna Ayyagari
College of Management, University of Massachusetts
E-Mail: r.ayyagari@umb.edu

Jaejoo Lim
University of Arkansas – Fort Smith
E-Mail: jlim@uafs.edu

Olger Hoxha
Boston, MA
E-Mail: olger.hoxha@gmail.com

ABSTRACT

Why don't individuals follow the best information security practices? We address an aspect of this question by focusing on one of the most common authentication methods – passwords. To promote better password habits, security experts consistently recommend the use of password managers as a best practice, but recent research shows their usage rate is low. Therefore, understanding the factors that influence the use of a password manager is important. We contribute to this cause by drawing on information security and technology adoption literature. Survey results from 120 participants with varying numbers of internet accounts yield some counterintuitive findings. As proposed, perceived severity and perceived vulnerability of password loss strongly influenced intent to use password managers. However, perceived ease of use diminished the intent to use password managers, and trust is only partially supported. Our results indicate that 'security' aspects of password managers are more important than 'usability' aspects. The implications of these findings for password management are discussed.

Keywords: Security, Passwords, Password managers, Perceived severity, Perceived vulnerability

INTRODUCTION

Individuals often ignore the best information security practices. Why? For example, individuals often create ‘weak’ passwords. Although passwords are used to protect and restrict access to sensitive information, a recent survey of American users has found that users share, reuse, and use weak passwords (Pew Research Center, 2017). The password authentication method is easy-to-use; however, users are bad at managing passwords. Users create passwords that are easy to guess. An examination of 32 million users’ password data suggests that 5,000 passwords accounted for 20% of user accounts (Vance, 2010). Users typically used simple passwords like '123456' or 'abc123'.

Given the stronghold of passwords as an authentication method (Herley & Oorschot, 2012), researchers have studied users' password behaviors. Research and anecdotal evidence suggest that users have lousy password habits such as reusing and writing down passwords (Komanduri et al., 2011; Wash, Rader, Berman, & Wellmer, 2016; Yan, Han, Li, Zhou, & Deng, 2015). Besides, users overestimate the security of their passwords and do not have a good understanding of password strength (Ur et al., 2016). It is also easy to trick users to divulge their passwords for simple rewards (Happ, Melzer, & Steffgen, 2016).

Given these issues with passwords, researchers have suggested options to improve on passwords. Password research explored the use of passphrases and graphical passwords as options for creating and remembering secure passwords (Nelson & Vu, 2010). However, usability issues with these methods remain. For example, although graphical passwords might be more secure, they are also easy to shoulder-surf (Tari, Ozok, & Holden, 2006). The use of passphrases is proposed as another way to increase the strength of passwords and at the same time, make it easier to recall. Passphrases typically use a phrase that has meaning to the user. For example, a phrase like 'ILikeManchesterUnited' could be used. Although passphrases are suggested to improve the strength of passwords, users face issues of memory recall, typographical issues that limit the usability of passphrases (Keith, Shao, & Steinbart, 2007).

Another way in which a significant password benefit can be obtained is with the use of password managers. Password managers are applications/programs that act as a vault in storing users' usernames and passwords. This is akin to using safe deposit lockers in banks. A key opens the safe deposit locker containing valuable items. Similarly, password managers have a powerful master password that provides access to users' various other accounts and passwords. In this way, users have to remember only one strong password (i.e., password to enter the password manager). Security experts consistently recommend the use of password managers (Huth, Orlando, & Pesante, 2012). However, the use of password managers is sparse (Alkaldi & Renaud, 2016; Pew Research Center, 2017; Stobert & Biddle, 2014). It presents an interesting dilemma

where the benefits of a tool like a password manager exist; however, it is not widely adopted. Therefore, we investigate the users' intention to use password managers. We do this by combining literature on individuals' behaviors when faced with risk and technology adoption.

Our study contributes to an essential aspect of individuals' digital lives – protecting and managing passwords. Specifically, our study yields interesting findings such as

- Counterintuitive finding that ease of use of password manager actually diminishes the intention to use the password manager
- Trust in password managers is found to be only partially significant

The rest of the paper is organized as follows. First, we present background work on password managers and develop our hypotheses. Next, the methodology used in our study is presented. The paper ends with a discussion of our results and implications on how to improve the use of password managers.

BACKGROUND AND HYPOTHESES

A stream of research from computer science has addressed technical issues of creating better tools – better ways to manage passwords. Previous research on password managers has focused mostly on the 'tool' rather than factors that influence the use of the 'tool'. For example, researchers propose a tool to make web browsers' password managers more secure (Zhao & Yue, 2014), use of dual authentication as a solution to develop secure password managers (McCarney, Barrera, Clark, Chiasson, & van Oorschot, 2012). Other studies identify security flaws in password managers and provide guidance on designing better password managers (Li, He, Akhawe, & Song, 2014). In this stream of research, the emphasis is on the tool itself – i.e., how to develop or design a better tool. However, the tools are useless unless users adopt and use those tools.

Besides, some research also focused on the usability of password managers. Here the focus is on user interactions and behaviors when using the tool. For example, Chiasson, Oorschot, and Biddle (2006) compared two browser plug-in options and found that users are unable to use the password managers appropriately, and are uncomfortable relinquishing control of their passwords to a password manager. Similarly, Karole, Saxena, and Christin (2010) compared online versus portable (phone and USB) password managers. Contrary to expectation, users did not prefer the online password manager which had better usability features. It is suggested that the lack of trust in the online password manager supersedes the usability features. A thematic analysis of users' responses to password managers has also highlighted trustworthiness

as a concern (Alkaldi & Renaud, 2016). This research indicates that trust in password managers plays a role in users' adoption of password managers.

Trust plays a vital role in individuals' acceptance of new technologies (Bahmanziari, Pearson, & Crosby, 2003). Previous research indicates that trust reduces individuals' uncertainty when faced with dealing with new technological methods. For example, trust plays a key role in individuals' acceptance of online retailing, banking, and mobile technologies (Gu, Lee, & Suh, 2009; Hillman & Neustaedter, 2017; Luarn & Lin, 2005; Ong & Lin, 2015; Yu, Balaji, & Khong, 2015). One of the influential papers in e-commerce has identified trust as a key variable in the acceptance of e-commerce (Yang, Wang, & Chen, 2017). Individuals can be trusting of technology in general (trust in general technology) and also be trusting of the features and abilities of a particular technology (like password managers) (Mcknight, Carter, Thatcher, & Clay, 2011). Taken together, the role of trust in accepting new technologies and individuals' apprehension about trusting password managers leads to the following hypothesis

H1a: Perceived trust in general technology will be positively related to intention to use password managers.

H1b: Perceived trust in password managers will be positively related to intention to use password managers.

One of the key reasons behind the use of password managers is that it reduces the chance of passwords being compromised. In a sense, password managers are similar to protective technologies like antispyware or antivirus. In these cases, the use of antivirus reduces the chance that computing resources are compromised. Previous research has used protective motivation theory (PMT) to explain individuals' intention to use such security tools (Chenoweth, Minch, & Gattiker, 2009; Gurung, Luo, & Liao, 2009; Martens, De Wolf, & De Marez, 2019; Thompson, McGill, & Wang, 2017).

PMT explains users' behaviors when faced with threats (Rogers, 1975). PMT indicates that users appraise threats and choose behaviors accordingly. Two key variables in appraising threats are perceived vulnerability and perceived the severity of threats (Rogers, 1975). Individuals choose protective behaviors if they perceive they are vulnerable to perceived threats, and the potential damage is severe from these threats. Perceived vulnerability addresses the probability of realizing the threat, whereas perceived severity addresses the impact or damage from the threat. In the context of passwords, if users believe that they might lose their passwords, then they are likely to take protective actions. Besides, since users often reuse passwords, the threat of password loss will be perceived as problematic because the same password is used for multiple accounts. When faced with a breach, it is common practice for businesses to

request users to reset passwords for all the other accounts where that account information is used (UnderArmour, 2018). Previous research on security behaviors has found support for perceived vulnerability and perceived severity (Chenoweth et al., 2009; Crossler & Belanger, 2014; Liang & Xue, 2010; Martens et al., 2019; Thompson et al., 2017). Therefore, we hypothesize

H2: Perceived severity of password loss will be positively related to intention to use password managers.

H3: Perceived vulnerability of password loss will be positively related to intention to use password managers.

Information systems literature has a long tradition of studying factors that influence the adoption of technologies (Davis, 1985). Perceived usefulness and perceived ease of use are often identified as important variables explaining intention to use technologies (Lau, Lam, & Cheung, 2016; Lee, Kozar, & Larsen, 2003; Marangunić & Granić, 2015). Therefore, we control the impact of perceived usefulness and perceived ease of use in this study on the intention to use password managers by modeling them as control variables.

The proposed research model is shown in figure 1.

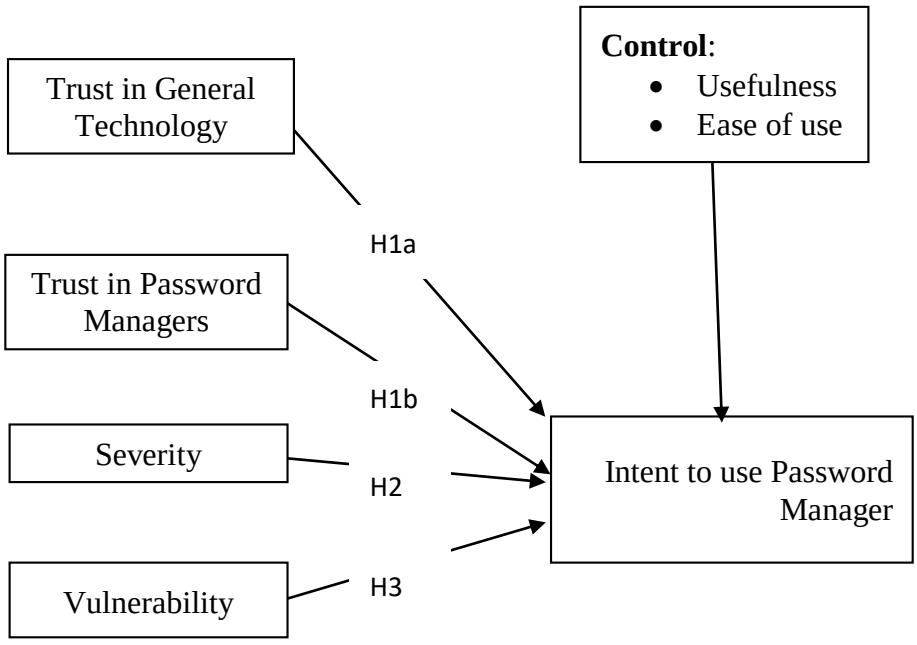

Figure 1 Proposed Research Model

RESEARCH METHOD

To test our hypotheses, we surveyed undergraduate students at two universities geographically located in the southwest and the northeast area of the USA, respectively. To ensure that respondents are aware of password managers, we first showed a two-minute long video clip on password managers that explained the functionality of password managers. Previous researchers have used a similar approach (Alkaldi & Renaud, 2019). Then, we distributed a paper-based survey questionnaire containing items related to the variables used in the study (Table 1). Participants were asked to indicate their agreement to each questionnaire using a five-point Likert scale from "Strongly Disagree" (1) to "Strongly Agree" (5). Further, demographic data, such as age and gender, were also collected.

All of the variables and scale items used in this study are drawn from previous research and modified to the password manager context. For example, perceived severity is described as "How serious the individual believes that the threat would be" to him- or herself (Milne, Orbell, & Sheeran, 2002, p. 108)". Previous research has used items such as "If I were to lose data from my hard drive, I would suffer a lot of pain (Boss, Galletta, Lowry, Moody, & Polak, 2015, p. A9)" and "If my computer were infected by malware, it would be severe (Boss et al., 2015, p. A10)" to measure perceived severity. True to the 'severe' concept of this item, our item is worded as "If I were to have my password compromised, I would suffer a lot of pain." Further, perceived usefulness and perceived ease of use are drawn from Davis (1989), trust variables are drawn from Mcknight et al. (2011). Table 1 provides descriptions of constructs and sample items used to measure them.

Table 1 Constructs Definitions and Measurement Items

Construct Definition	Sample Items
Perceived Ease of Use - “The degree to which a person believes that using a particular system would be free of effort.” (Davis, 1989)	• Learning to operate a password manager would be easy for me. • I would find it easy to get a password manager to do what I want it to do.
Perceived usefulness - "The degree to which a person believes that using a particular system would be free of effort." (Davis, 1989)	• Using a password manager would enable me to manage passwords more quickly. • I would find a password manager useful in managing my passwords.
Perceived Vulnerability - The degree to which users believe that using a particular system would be necessary for them. (Chiasson et al., 2006)	• I need to use a password manager to protect my passwords. • My passwords are safe, even without using a password manager.
Perceived Severity - "'How serious the individual believes that the threat would be' to himself- or herself." (Boss et al., 2015; Milne et al., 2002)	• If I were to have my password compromised, I would suffer a lot of pain. • Having my password hacked would be likely to cause me major problems.
Trust (password managers) - “Users consider whether the technology delivers the functionality promised by providing features sets needed to complete a task.” (Mcknight et al., 2011)	• has the functionality I need. • has the ability to do what I want it to do.
Trust (general technology) - “The degree to which users believe that positive outcomes will result from relying on technology.” (Mcknight et al., 2011)	• My typical approach is to trust new technologies until they prove to me that I shouldn’t trust them. • I generally give technology the benefit of the doubt when I first use it.

One hundred twenty-six responses were collected. After six missing cases, one hundred twenty responses were used for further analyses. All of the participants were undergraduate students. Of the participants, 67 were male, and 53 were female. The participants' ages ranged between 19 and 40, with a mean of 22 and a standard deviation of 4.2 years. Sixty-eight percent of the participants reused their passwords across different accounts (Table 2). About 46 % of the participants had less than ten internet

accounts that required id and passwords, while 54% of students had more than ten accounts (Table 3 provides details on the number of accounts). Forty-eight percent of the participants reported that they use at least one password with 1+ special characters, 1+ uppercase characters, etc.

Table 2 Demographics

	Female	Male	All
Age			
Minimum	18	18	18
Maximum	39	40	40
Mean	21.4	22.3	21.9
Std. Dev.	4.0	4.4	4.2
Reusing password	41 (77.4%)	41 (61.2%)	82 (68.3%)
Total	53	67	120

Table 3. Number of Subscribed Internet Accounts

# of Internet Accounts	Count	Percentage
0-5	13	10.8
6-10	43	35.8
11-15	31	25.8
16-20	14	11.7
21 +	19	15.9
Total	120	100%

DATA ANALYSIS AND RESULTS

The dependent variable in the study (Intent to use a password manager) was measured as a binary variable. Therefore, logistic regression was used to test the proposed research model, i.e., 'Intent to use Password Manager' as a dependent variable and six variables, including the two control variables as explanatory variables. Cronbach's alpha and loadings for the explanatory variables are presented in Table 4 and meet the suggested requirements of Cronbach's alpha > 0.7 (Santos, 1999). Table 5 provides descriptive statistics, and items are averaged to represent each variable in further analysis.

Table 4 Loadings and Reliability

Variables	Loading	Cronbach's Alpha
Trust in General Technology	0.675-0.885	0.742
Trust in Password Managers	0.687-0.879	0.867
Severity	0.707-0.920	0.864
Vulnerability	0.917-0.927	0.723
Usefulness	0.744-0.766	0.775
Ease of Use	0.603-0.954	0.705

Table 5. Descriptive Statistics

Variables	N	Minimum	Maximum	Mean	Std. Dev.
Trust in General Technology	120	1.0	5.0	3.353	.866
Trust in Password Managers	120	1.0	5.0	3.558	.818
Vulnerability	120	1.0	5.0	2.883	.812
Severity	120	1.0	5.0	4.129	.969
Usefulness	120	1.0	5.0	4.025	.806
Ease Of Use	120	1.0	5.0	4.081	.744

To test our proposed model, we used various measures of fit for logistic regression. The overall percentage correct for the predicted reached 85.1%, while 93 percent of intention to use the password manager was correctly predicted, which is considered very high for logistic regression models (Bogard, 2011). Since there is no universally accepted goodness of fit measure, we report statistics like -2 log likelihood, Cox & Snell, and Nagelkerke R square values, as shown in Table 6. The R square values in logistic regression cannot be interpreted like R square values from the ordinary least squares model. The values of R squares reported in Table 6 indicate a good fit of the logistic regression model (Allison, 2014; Cohen, West, & Aiken, 2014; Kneidinger-Müller, 2017). Besides, we also ran the Hosmer-Lemeshow test (HL test) as another goodness of fit measure (Hosmer, Hosmer, Le Cessie, & Lemeshow, 1997). The null hypothesis for the HL test indicates that the proposed model is a good fit for the data. The p-value (.830) for the HL test was above alpha=0.05, and so the null hypothesis is not rejected, indicating a good fit of the data for the model (Table 7).

Table 6 Model Summary

-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
75.560	.408	.587

Table 7 Hosmer and Lemeshow Test

	Chi-square	df	Significance
HL test values	4.287	8	.830

Since the above results indicate a good fit, we proceed to test the proposed hypotheses with regression results, as shown in Table 8. Hypothesis 1 proposed that trust will have an impact on intent to use password managers. Specifically, H1a proposed that users' trusting beliefs about general technology will impact users' intent to use password managers. The result showed a positive impact but was not significant ($p=0.242$). Similarly, Hypothesis 1b checks if trusting beliefs about password managers will impact users' intent to use password managers. The p-value for this relationship is 0.076, which indicates weak support. Hypothesis 2 and 3 posit that users' perceived severity and perceived vulnerability of the password loss impacts their willingness to use password managers. Both of the hypotheses 2 and 3 are strongly supported at the significance level of $p<0.01$. The odd ratios for severity and vulnerability indicate that the increase of one level of perceived severity and vulnerability increases users' intention to use password managers by 7.6 times and 4.8 times, respectively (Table 8).

For the two control variables, while perceived usefulness did not have a significant influence on intent (Perceived Usefulness, $p=0.264$), perceived ease of use showed a significant negative effect on the intent to use password managers (Perceived Ease of Use, $p=0.05$). It should be noted that the result of perceived ease of use is opposite to the proposed positive relationship between perceived ease of use and intent to use password managers. These results are discussed in the next section.

Table 8 Regression Result

Variables	Coefficients	S.E.	Sig.	Exp(B)
Trust - General Technology	.259	.370	.242	1.296
Trust - Password Managers	.786	.549	.076***	2.194
Perceived Severity	2.032	.454	.000*	7.629
Perceived Vulnerability	1.562	.605	.005*	4.769
Perceived Usefulness	.282	.447	.264	1.326
Perceived Ease of Use	-.914	.565	.050**	0.401

* Significant at 1%, ** at 5%, and *** at 10%.

DISCUSSION

In this paper, we investigated the factors that influence individuals' use of password managers. Based on the password manager and information security literature, we proposed a model that sheds light on individuals' intention to use password managers.

Before discussing our results, we acknowledge the limitations of our study. We used self-reports to measure the variables in the study. Although we have emphasized the confidentiality and anonymity to respondents, social desirability bias might likely have influenced self-reports. Further, we measured intentions to use password manager rather than actual password manager usage behavior. Although previous security research indicates support for using intentions for actual behaviors (Egelman, Harbach, & Peer, 2016), future research could incorporate actual usage measures. The results of this study should also be interpreted with caution as the sample size is limited. Besides, previous research has found that different groups (e.g., students, computer scientists) view password security differently (Duggan, Johnson, & Grawemeyer, 2012). Computer scientists viewed security as integral to their work, whereas students viewed security as an additional cost (Duggan et al., 2012). Since this study is based on one respondent group (i.e., students), the results from this study may not be generalizable to other respondent groups. These limitations also provide opportunities for further research. For example, this study can be replicated on different user groups to see if differences exist across groups.

Our results indicate that perceived vulnerability and perceived severity of password loss encourage the use of password managers. These variables provide levers for organizations to encourage individuals to use password managers. Individuals are

bad at assessing risk and underestimate their vulnerability to threats (West, 2008). Crime and disaster literature alludes to this principle, where individuals are often shocked that bad things like burglary, mugging happen to them (Lejeune & Alex, 1973; Roe-Burning & Straker, 1997). The illusion of invulnerability reasoning indicates that individuals underestimate personal misfortunes and overestimate others' misfortunes, therefore not prepared to deal with threats. In our context, even though individuals might be cognizant of 'password' issues, they might believe that they are not the target. Therefore, organizations need to deliver messages that challenge individuals' assumptions. For example, organizations might use news of security attacks on similar organizations to deliver the message that their organization is a potential target and very vulnerable to security attacks. Similarly, as users create/update passwords, organizations can proactively display messages indicating that similar users are targeted in security attacks and encourage the use of password managers. Future research can explore the individual's tendency to underestimate risks in password context.

Our results also yielded a couple of surprising results. Previous research indicates that trust in technology is an essential antecedent to the use of technology (Bahmanziari et al., 2003; Luarn & Lin, 2005). Our results indicate that trust has a mixed relationship with the intention to use password managers. Trust in general technology had no impact, and trust in password managers has weak support once other variables (such as perceived severity, vulnerability, etc.) are accounted. The result indicates that individuals' threat assessment of password loss is a more significant driver to the use of password managers than trust in technology. Trust likely plays a more significant part when the comparison is between the options of technology vs. non-technology options. In other words, when comparing retail vs. e-retail or banking vs. online/mobile banking, users have to adopt new processes (Gu et al., 2009; Hillman & Neustaedter, 2017; Malaquias & Hwang, 2016; Yu et al., 2015). However, with the case of passwords, users need to have some level of trust to use services that require passwords. Therefore, trust in technology itself might not be that important, and overemphasis of trust might not convince users to use password managers. Future research can further investigate the complex role of trust in password managers.

Our results also indicate that perceived ease of use had a negative effect on the intention to use password managers. This result is surprising because the established tradition in information systems indicates that perceived ease of use positively impacts the adoption of technology (Hess, McNab, & Basoglu, 2014; Marangunić & Granić, 2015). The ease of use of password managers is likely seen as an indication of weakness. Since password managers are like a vault for all of the users' passwords, users may be apprehensive about the use of password managers that are very easy to use. Therefore, our study suggests that the promotion of password managers might focus on security

features rather than usability features. Further research is needed to see if ease of use is perceived as a strength or weakness by users.

In conclusion, our study indicates that perceived vulnerability and perceived severity of password loss encourages the use of password managers. However, trust and ease of use' resulted in counterintuitive findings. We hope these results provide the impetus for further research on understanding the usage of password managers.

REFERENCES

Alkaldi, N., & Renaud, K. (2016). W*hy do people adopt, or reject, smartphone password managers?* Paper presented at the EuroUSEC 2016: The 1st European Workshop on Usable Security, Darmstadt, Germany. https://doi.org/10.14722/eurousec.2016.23011

Alkaldi, N., & Renaud, K. (2019). *Encouraging password manager adoption by meeting adopter self-determination needs.* Paper presented at the Proceedings of the 52nd Hawaii International Conference on System Sciences. https://doi.org/10.24251/hicss.2019.582

Allison, P. D. (2014). *Measures of fit for logistic regression.* Paper presented at the Proceedings of the SAS Global Forum 2014 Conference.

Bahmanziari, T., Pearson, J. M., & Crosby, L. (2003). Is Trust Important in Technology Adoption? A Policy Capturing Approach. *Journal of Computer Information Systems, 43*(4), 46-54. https://doi.org/10.1080/08874417.2003.11647533

Bogard, M. (2011). *Logit models: R-square and the percentage of correct predictions*. Retrieved from http://econometricsense.blogspot.com/2011/03/logit-models-r-square-and-percentage-of.html

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864. https://doi.org/10.25300/misq/2015/39.4.5

Chenoweth, T., Minch, R., & Gattiker, T. (2009, 5-8 Jan. 2009). *Application of protection motivation theory to adoption of protective technologies*. Paper presented at the 2009 42nd Hawaii International Conference on System Sciences. https://doi.org/10.1109/hicss.2009.74

Chiasson, S., Oorschot, P. C. v., & Biddle, R. (2006). *A usability study and critique of two password managers*. Paper presented at the Proceedings of the 15th conference on USENIX Security Symposium - Volume 15, Vancouver, B.C., Canada.

Cohen, P., West, S. G., & Aiken, L. S. (2014). *Applied multiple regression/correlation analysis for the behavioral sciences.* Psychology Press. https://doi.org/10.4324/9781410606266

Crossler, R., & Belanger, F. (2014). An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *SIGMIS Database, 45*(4), 51-71. https://doi.org/10.1145/2691517.2691521

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results.* Massachusetts Institute of Technology.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-340. https://doi.org/10.2307/249008

Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies, 70*(6), 415-431. https://doi.org/10.1016/j.ijhcs.2012.02.008

Egelman, S., Harbach, M., & Peer, E. (2016). *Behavior ever follows intention?: A validation of the security behavior intentions scale (SeBIS)*. Paper presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, California, USA. https://doi.org/10.1145/2858036.2858265

Gu, J.-C., Lee, S.-C., & Suh, Y.-H. (2009). Determinants of behavioral intention to mobile banking. *Expert Systems with Applications, 36*(9), 11605-11616. https://doi.org/10.1016/j.eswa.2009.03.024

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security, 17*(3), 276-289. https://doi.org/10.1108/09685220910978112

Happ, C., Melzer, A., & Steffgen, G. (2016). Trick with treat – reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior, 61*, 372-377. https://doi.org/10.1016/j.chb.2016.03.026

Herley, C., & Oorschot, P. V. (2012). A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy, 10*(1), 28-36. https://doi.org/10.1109/MSP.2011.150

Hess, T. J., McNab, A. L., & Basoglu, K. A. (2014). Reliability generalization of perceived ease of use, perceived usefulness, and behavioral intentions. *MIS Quarterly, 38*(1), 1-28.

Hillman, S., & Neustaedter, C. (2017). Trust and mobile commerce in North America. *Computers in Human Behavior, 70*, 10-21. https://doi.org/10.1016/j.chb.2016.12.061

Hosmer, D. W., Hosmer, T., Le Cessie, S., & Lemeshow, S. (1997). A comparison of goodness-of-fit tests for the logistic regression model. *Statistics in medicine, 16*(9), 965-980. https://doi.org/10.1002/(sici)1097-0258(19970515)16:9<965::aid-sim509>3.0.co;2-o

Huth, A., Orlando, M., & Pesante, L. (2012). *Password security, protection, and management*. Retrieved from http://aahuth.com/wp-content/uploads/sites/44/2014/02/PasswordMgmt2012-2.pdf

Karole, A., Saxena, N., & Christin, N. (2010). *A comparative usability evaluation of traditional password managers.* Paper presented at 13th the International Conference on Information Security and Cryptology, 233-251. https://doi.org/10.1007/978-3-642-24209-0_16

Keith, M., Shao, B., & Steinbart, P. J. (2007). The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies, 65*(1), 17-28. https://doi.org/10.1016/j.ijhcs.2006.08.005

Kneidinger-Müller, B. (2017). Mobile communication as invader in face-to-face interactions: An analysis of predictors for parallel communication habits. *Computers in Human Behavior, 73*, 328-335. https://doi.org/10.1016/j.chb.2017.03.055

Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., & Egelman, S. (2011). *Of passwords and people: Measuring the effect of password-composition policies*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada. https://doi.org/10.1145/1978942.1979321

Lau, M. M., Lam, A. Y., & Cheung, R. (2016). Examining the factors influencing purchase intention of smartphones in Hong Kong. *Contemporary Management Research, 12*(2), 213-224. https://doi.org/10.7903/cmr.13836

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for information systems, 12*(50), 752-780. https://doi.org/10.17705/1cais.01250

Lejeune, R., & Alex, N. (1973). On being mugged: The event and its aftermath. *Urban Life and Culture, 2*(3), 259-287. https://doi.org/10.1177/089124167300200301

Li, Z., He, W., Akhawe, D., & Song, D. (2014). *The emperor's new password manager: security analysis of web-based password managers.* Paper presented at the USENIX Security Symposium. https://doi.org/10.21236/ada614474

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394-413. https://doi.org/10.17705/1jais.00232

Luarn, P., & Lin, H.-H. (2005). Toward an understanding of the behavioral intention to use mobile banking. *Computers in Human Behavior, 21*(6), 873-891. https://doi.org/10.1016/j.chb.2004.03.003

Malaquias, R. F., & Hwang, Y. (2016). An empirical study on trust in mobile banking: A developing country perspective. *Computers in Human Behavior, 54*, 453-461. https://doi.org/10.1016/j.chb.2015.08.039

Marangunić, N., & Granić, A. (2015). Technology acceptance model: A literature review from 1986 to 2013. *Universal Access in the Information Society, 14*(1), 81-95. https://doi.org/10.1007/s10209-014-0348-1

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior, 92*, 139-150. https://doi.org/10.1016/j.chb.2018.11.002

McCarney, D., Barrera, D., Clark, J., Chiasson, S., & van Oorschot, P. C. (2012). *Tapas: design, implementation, and usability evaluation of a password manager.* Paper presented at the Proceedings of the 28th Annual Computer Security Applications Conference.

Mcknight, D. H., Carter, M., Thatcher, J. B., & Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information System, 2*(2), 1-25. https://doi.org/10.1145/1985347.1985353

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology, 7*(2), 163-184. https://doi.org/10.1348/135910702169420

Nelson, D., & Vu, K.-P. L. (2010). Effectiveness of image-based mnemonic techniques for enhancing the memorability and security of user-generated passwords. *Computers in Human Behavior, 26*(4), 705-715. https://doi.org/10.1016/j.chb.2010.01.007

Ong, C.-S., & Lin, Y.-L. (2015). Security, risk, and trust in individuals internet banking adoption: An integrated model. *International Journal of Electronic Commerce Studies, 6*(2), 343-356. https://doi.org/10.7903/ijecs.1428

Pew Research Center. (2017). *Americans and cybersecurity*. Retrieved from http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

Roe-Burning, S., & Straker, G. (1997). The association between illusions of invulnerability and exposure to trauma. *Journal of Traumatic Stress, 10*(2), 319-327. https://doi.org/10.1023/A:1024890415279

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Santos, J. R. A. (1999). Cronbach's alpha: A tool for assessing the reliability of scales. *Journal of extension*, *37*(2), 1-5.

Stobert, E., & Biddle, R. (2014). *The password life cycle: User behaviour in managing passwords.* Paper presented at the 10th Symposium On Usable Privacy and Security (SOUPS).

Tari, F., Ozok, A., & Holden, S. H. (2006). *A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords.* Paper presented at the Proceedings of the second Symposium On Usable Privacy and Security (SOUPS).

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376-391. https://doi.org/10.1016/j.cose.2017.07.003

UnderArmour. (2018). Under armour notifies MyFitnessPal Users of data security issue. Retrieved from http://investor.underarmour.com/news-releases/news-release-details/under-armour-notifies-myfitnesspal-users-data-security-issue

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). *Do users' perceptions of password security match reality?* Paper presented at the Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/2858036.2858546

Vance, A. (2010). If Your password is 123456, Just make it hackme. *The New York Times*. Retrieved from https://www.nytimes.com/2010/01/21/technology/21password.html

Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). *Understanding password choices: How frequently entered passwords are re-used across websites.* Paper presented at the Symposium on Usable Privacy and Security (SOUPS).

West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34-40. https://doi.org/10.1145/1330311.1330320

Yan, Q., Han, J., Li, Y., Zhou, J., & Deng, R. H. (2015). Leakage-resilient password entry: challenges, design, and evaluation. *Computers & Security*, *48*, 196-211. https://doi.org/10.1016/j.cose.2014.10.008

Yang, Y.-J., Wang, C.-C., & Chen, C.-C. (2017). Recent development trend of electronic commerce research: 2000 to 2016. *Contemporary Management Research*, *13*(2), 131-142. https://doi.org/10.7903/cmr.17824

Yu, P. L., Balaji, M. S., & Khong, K. W. (2015). Building trust in internet banking: A trustworthiness perspective. *Industrial Management & Data Systems, 115*(2), 235-252. https://doi.org/10.1108/IMDS-09-2014-0262

Zhao, R., & Yue, C. (2014). Toward a secure and usable cloud-based password manager for web browsers. *Computers & Security, 46*, 32-47. https://doi.org/10.1016/j.cose.2014.07.003

Dr. Ramakrishna Ayyagari (Corresponding author) received the Ph.D. degree in information systems from Clemson University, U.S.A. He is currently an associate professor in College of Management, University of Massachusetts Boston. His current research includes understanding information security behaviors.

Dr. Jaejoo Lim received the Ph.D. degree in information systems from Clemson University, U.S.A. He is an Associate Professor of MIS & Analytics at University of Arkansas - Fort Smith. His research interests include various aspects of information quality, creating business value with analytics, e-commerce strategies & applications, and IT value & investment. He has published in many academic journals including Decision Sciences, IEEE Transactions on Engineering Management, Information & Management, Journal of the AIS, Communications of the AIS, Computers in Human Behavior, and various conference proceedings.

Mr. Olger Hoxha obtained his bachelor's degree in information systems from the University of Massachusetts, Boston. He is currently working as a senior consultant at Ernst & Young. His work is focused on identifying gaps and providing recommendations to his client's business and IT processes.