International Journal of Economic Research

ISSN : 0972-9380

available at http: www.serialsjournals.com

Volume 14 • Number 19 • 2017

The Relationship between Perceived Severity and Login Management Among Students at Universiti Utara Malaysia

Rajoo Ramanchandram[a], Shahmir Sivaraj Abdullah[a], Noor Fareen Abdul Rahim[b], Zaini Yahaman[c] and Sidi Bello Alkasim[d]

[a] *School of Business Management, Universiti Utara Malaysia, Malaysia, E-mail: rajoo@uum.edu.my; shahmir@uum.edu.my*
[b] *Graduate School of Business, Universiti Sains Malaysia, Malaysia, E-mail:noorfareen@usm.my*
[c] *Lz Portal Ventures, Lot F-2-19, Jalan BG 38/1, Bangi Gateway 38, 43650 Bandar Baru Bangi, Selangor, Malaysia*
E-mail: zaini@lzportal.com.my
[d] *Department of Marketing, CABS, Umaru Ali Shinkafi Polytechnic, Sokoto State, Nigeria*
E-mail: alkasimsidi32@gmail.com

Abstract: Online communication creates a lot of security issues for users. High reliance on computers and the Internet invariably exposes students as well as consumers to information security threats. However, university students have different attitudes towards information security as opposed to regular consumers. This may be due to ignorance, naivety or a basic lack of understanding the risks involved when communicating online. This paper measured perceived severity (IV), and their willingness to login (DV) in relation to information security behaviour when logging into websites by 83 randomly sampled undergraduate students in Universiti Utara Malaysia (UUM). It was found that there is a significant positive relationship between the IV and the DV (p=.000. The variables explained 7.65% of the variance. The constructs showed reliability (Cronbach's alpha) of .925 for the perceived severity construct (IV) and .795 for the login management construct (DV). Perception of severity is an important element of safe login management behaviour when students login to a particular website. Other variables can be added to this model to gain a better understanding of information security behaviour of students in all other universities in Malaysia before expanding it nationally. In the future this can influence national information security policy.

Keywords: Perceived severity, login management, undergraduate students

INTRODUCTION

The Internet today is inextricably linked to almost every aspect of an individual's life. It plays an important role when engaging with the outside whether to do business or just for social engagement. With this phenomenon online security invariably has become a prime concern for firms and users alike (Anderson,

2006, Anderson and Moore, 2006). Online security intrusion very often leads to substantial losses either directly or indirectly such as fund depletion from bank accounts fraudulently or the loss of critical data held by firms. Consumer perceptions of a firm which is deemed to have a lackadaisical attitude towards security protocols may be disastrous to firms as it will affect consumer trust levels which in turn will have negative consequences on the brand itself (Yenisey, Ozok & Salvendy, 2005).

Good password management may be considered to be a part of login management (Scheiner, 2006). This is important for anyone using the Internet to be aware of when logging in to websites. Online security is often overlooked as users tend to be either naïve or in the other extreme very trustful of the Internet (Campbell, Greenauer, Macaluso & End, 2007). The normal user predominantly exhibits the 'it will not happen to me' syndrome when dealing with 'Internet security. This syndrome aptly explains why almost all users including IT professionals manage their login credentials badly (Powell 2006).

LITERATURE REVIEW

Perceived Severity

Fear at the significance of threats influences perceived severity (Yoon, *et al.,* 2012). When students are aware of the perceived threat to information security, it is more than likely that they will engage in some form of action related to security and have a tendency to adopt appropriate behaviour (Blythe, Coventry & Little, 2015). The possible loss of finances or identity is not the only threats that are faced by users when private information is compromised. There will be lower levels of trust when customers have no control of the distribution or misuse of information that has been by illegal access towards themselves or businesses. This inadvertently creates uncertainty and reluctance when asked to disclose private information (Liao *et al.,* 2011).

When related to information or computer security the perceived severity an individual feels may not only be confined to the damage that happens to the data in a system or the system itself but the effect it exerts on the individual's job or the firm he or she is employed by (Ng, Kankanhalli & Xu, 2009). It must be noted that in the case of the firm the data that is compromised is owned by the firm which consequently affects the confidence and integrity of the firm as well as the job functions of its employees (Ng, Kankanhalli & Xu, 2009). On the other hand, when employees do not exercise appropriate computer security behaviour then they may be held accountable for any loss or theft of data. In situations such as these the consequences of the security breach might be very severe. However, employees may differ on how they perceive the severity and the levels of damage that has been incurred.

Login Management

Having a plethora of login credentials whilst not only bothersome but creates serious security issues within the Internet environment. When users have many login credentials, the way these credentials are managed creates security concerns. More often than not it will be written down somewhere either on paper or just stored in the devices that they own. Other generic behaviour patterns include the use of the same login credentials on different websites. Collectively, these form of actions leads to serious security breaches. However, having strong security protection by itself does not necessarily guarantee that the systems utilized are completely secure from breaches. These instances become even more acute when user practice or

behaviour shows a disregard for maintaining security. Such mistakes are the easiest point for hackers through which system security is breached. Consequently, it can be surmised that security is only effective when both the technical and behaviour perspectives are present (Katuk, Halim, Tahir, Ahmad & Yusof, 2013).

Instances where passwords are hijacked to gain unauthorised access to user accounts are omnipresent. Using randomly generated or difficult to remember default passwords has the tendency to be forgotten and subsequently written down are easily accessible (Tam, Glassman & Vandenwauver, 2010). The focus of Internet security should be focussed on the user to enhance understanding the importance of login management. However, making people understand the importance of security while going online is a major people based issue (Wilson 2006). The human factor impacts the level of security when using passwords with the ever multiplying use of the Internet (Gehringer, 2002). Based on these arguments the following hypothesis was generated; Perceived severity has a significant effect on login management. The research framework is presented in Figure 1 below.

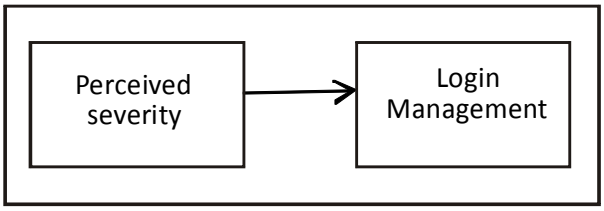

Figure 1: Research Framework

RESEARCH METHODOLOGY

The respondents for this quantitative study were undergraduates' students. The respondents were selected based on the random sampling technique. A total of 150 questionnaires were distributed and 93 was duly completed and returned. The total number of questionnaires received was 93 (62%). Of this only 83 (55%) were deemed usable or valid.

Profile of the Respondents

The demographic profiles of the respondents revealed that males (10=12%) formed the majority with females consisting 88% (73). All respondents were BBA undergraduate students.

Instrumentation

The five point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree) was used for the questions to indicate a degree of agreement or disagreement with each of the statements related to the stimulus objects. The questionnaire comprised two sections. Section 1 comprised the demographics and section 2 comprised the independent and dependent variables. The survey instrument was adopted and further adapted to suit this research from previous studies that were conducted.

Data Analysis Techniques

This study used SPSS version 24 for statistical analysis namely descriptive and inferential statistics on the data. The descriptive statistics that was employed has enabled this study to profile the sample population

based on gender. Other demographic differences were nominally similar because all the respondents were students. . This was then followed by the use of inferential statistics to achieve the objectives of the study. Tests for reliability and construct validity were conducted for this study.

Reliability

Table 1
Reliability Measures

Variable	*Cronbach's Alpha*	*No. of Items*
Login Management	0.795	5
Perceived Severity	0.925	6

According to Hair *et al.,* (2014) the minimum acceptable Cronbach's Alpha is 0.60 but scores above 0.70 are acceptable with scores above 0.80 preferred (Pallant, 2010). All the scores for internal consistency of the constructs (as presented in Table1) are above 0.70 and therefore are acceptable for use by the study.

Outliers

The use of multivariate analysis will confirm and identify outliers and if necessary the appropriate action can be taken to resolve it. To achieve this, the study conducted a multivariate analysis using SPSS 24. The output from this analysis will provide a Mahalanobis score (Pallant, 2010; Hair *et al.,* 2010). The Mahalanobis distance score can be extracted from the chi-square table by looking for X^2 for (df=V) p<.001. The X^2 (chi-square) for 2 variables at a significance value of 0.001 is 13.82. Any value that falls beyond this value is

Table 2
Residual Statistics

Residuals Statistics[a]

	Minimum	*Maximum*	*Mean*	*Std. Deviation*	*N*
Predicted Value	2.5992	3.8492	3.4627	.25126	83
Std. Predicted Value	–3.437	1.538	.000	1.000	83
Standard Error of Predicted Value	.097	.347	.131	.039	83
Adjusted Predicted Value	2.1551	3.9708	3.4587	.27101	83
Residual	–2.84922	2.40085	.00000	.87358	83
Std. Residual	–3.242	2.731	.002	1.013	83
Stud. Residual	–3.310	2.973	.002	1.013	83
Deleted Residual	–2.97076	2.84486	.00391	.90852	83
Stud. Delected Residual	–3.537	3.131	–.002	1.040	83
Mahal. Distance	.014	11.810	.988	1.542	83
Cook's Distance	.000	.818	.021	.093	83
Centered Leverage Value	.000	.144	.012	.019	83

a) Dependent Variable LOGIN

considered to be an outlier and needs to be checked (Tabachnick & Fidell, 2007). To complement this and identify any other strange cases which may have any undue influence on the model as a whole a Cook's distance measure can also be analysed. When ascertaining Cook's distance any values above 1 are considered problematic (Pallant, 2010).

The output from Table 2 indicates that the Mahalanobis score is only 11.81 indicating no outliers. The Cook's distance indicated .000 which is well below 1.0 thereby indicating no strange cases exerting undue influence on the model.

Skewness and Kurtosis

From the Skewness and Kurtosis test that were conducted for all the items, it was found that all items fell within the acceptable range of <2 and <7 respectively. For instance, skewness values were less than 2; the kurtosis values, were less than 7.

Linear Regression Test

The linear regression test that was conducted was to identify the effect of the independent variable on the dependent variable. The results of the test are provided in Table 5 below. Perceived severity is a significant predictor of login management ($\beta = 0.276$, $p<.01$). The model as a whole (Table 3&4) was found to be able to predict a significant amount of login management ($F(1, 81) = 6.701$, $p < .01$, $R^2 = .076$, $R^2_{Adjusted} = .065$). As such, the perceived severity construct has a significant effect on login management.

Table 3
Model Summary

Model Summary

Model	*R*	*R Square*	*Adjusted R Square*	*Std. Error of the Estimate*
1	.276[a]	.076	.065	.87895

a. Predictors : (Constant), PSEV

b. Dependent Variable: LOGIN

Table 4
ANOVA

ANOVA

Model		*Sum of Squares*	*df*	*Mean Square*	*F*	*Sig.*
1.	Regression	5.177	1	5.177	6.701	.011b
	Residual	62.577	81	.773		
	Total	67.754	82			

a. Dependent Variable: LOGIN

b. Predictors (Constant), PSEV

Table 5
Linear Regression Output

Coefficient												
		Unstandardized Coefficient		Standardized Coefficient			95.0% Confidence	Interval for B	Correlations			Collinearity Statistics	
Model		B	Std. Error	Beta	t	Sig.	Lower Bond	Upper Bond	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)	2.287	.464		4.924	.000	1.363	3.211					
	PSEV	.313	.121	.276	2.589	.011	.072	.553	.276	.276	.276	1.000	1.000

CONCLUSION AND RECOMMENDATIONS

Perceived severity, even though is personal in nature must be taken into account when using the Internet for any form of activity. The realisation of the severity does influence the user when intending to login in to websites. The creation of passwords seems to be a factor when undergraduate students use the Internet.

The management of the university have to highlight that enhanced awareness of password. This must become a policy when students enrol at the university. Obviously emphasising on such security issues will further improve protection. The use of non-common passwords will have a positive effect of improving personal and institutional security.

Other measures would be the use of different passwords for different websites and the reduction of the use of common passwords such as birthdays etc.

REFERENCES

Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, *25*(2), 160-171.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610-613.

Blythe, J. M., Coventry, L., & Little, L. (2015, July). Unpacking security policy compliance: The motivators and barriers of employees' security behaviours. In *Symposium on Usable Privacy and Security (SOUPS). USENIX Association, Ottawa* (pp. 103-122).

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in human behavior*, *23*(3), 1273-1284.

Gehringer, E. F. (2002). Choosing passwords: Security and human factors. *Technology and Society, 2002.(ISTAS'02). 2002 International Symposium on* (pp. 369-373) IEEE.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2014). *Multivariate data analysis*. Upper Saddle River, NJ: Prentice Hall.

Katuk, N., Halim, M. S., Tahir, H. M., Ahmad, A., & Yusof, S. M. (2013). Behavioural Analysis of Students' Login Credentials Management in Mobile Environment. *Journal of Industrial and Intelligent Information*, *1*(3).

Liao, C., Liu, C. C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications*, *10*(6), 702-715.

Wilson, T., (2006). *It's the people, stupid*. www.darkreading.com/document.asp

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behaviour: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

Pallant, J. (2010). SPSS survival manual: A step by step guide to data analysis using SPSS. Maidenhead.

Powell, J. (2006). *How security breaches impact your brand*. Enterprise Systems: USA.

Schneier, B. (2006). *Beyond fear: Thinking sensibly about security in an uncertain world*. Springer Science & Business Media.

Tabachnick, B. G., & Fidell, L. S. (2007). Multivariate analysis of variance and covariance. *Using multivariate statistics*, *3*, 402-407.

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

Yenisey, M. M., Ozok, A. A., & Salvendy, G. (2005). Perceived security determinants in e-commerce among Turkish university students. *Behaviour & Information Technology*, *24*(4), 259-274.

Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviours in information security. *Journal of Information Systems Education*, *23*(4), 407.