ISSN 2519-9781

An Exploration of the Frequent Use of Social Networking Sites and Severity Attack among Undergraduate Students in Somalia

Dr. Abdulkadir Jeilani

Lecturer, Faculty of Computer Science and Information Technology, Mogadishu University

Dr. John M. Kandiri

Lecturer, Faculty of Computing and Information Technology (CIT), Kenyatta University, Kenya

ABSTRACT

Social networking sites play an important role in our daily life. Most of the people communicate using the online social networks. Besides the advantages in their use, social networking sites have a plethora of potential attacks. The study aimed at gaining an exploration on frequently used and severity attack. Protection Motivation Model was used as a basis to develop and confirm research model and structural equation modeling technique was applied to data analysis and used cross-sectional survey data. A total of 207usable survey questionnaires was received from students drawn from three universities in Mogadishu, Somalia. The result was drawn based on the perceived severity attack, default security and privacy settings, perceived vulnerability response efficacy and frequently use. Contributions and limitation of the study were discussed.

KEYWORDS: Social Networks, Online attacks, Perceived Attack, Vulnerability, Severity Attack, Protection Motivation Model.

1. *INTRODUCTION*

Today's social networking sites' interface attracted the eyes of the users. The simplified interface that social media sites makes them appealing for communication around the world especially among the youngsters. A social networking site is a part of web service for creating a virtual link between users with similar interests, backgrounds, and activities (Rathore, Kumar, Loia, Jeong, & Hyuk, 2017). People use this social media for different reasons such as creating/maintaining a relationship with friends and families, entertainment and seeking information. Social media change the way people receive news and movies instead of buying newspaper and CD's they have Facebook, Twitter, YouTube and its(Huang & Lu, 2017). Besides the purpose and advantages, there are some other risks related these social networking sites such stolen password, spam and spoofing(Hur, Terry, Karatepe, & Lee, 2017).

In addition, there are empirical studies that have examined the information privacy concerns, antecedents and privacy measure use in social networking sites (Mohamed & Ahmad, 2012), understanding online safety behaviors: A protection motivation theory perspective(Tsai et al., 2016), A prediction system of Sybil attack in social network usingthe deep - regression modell (Al-qurishi, Alrubaian, Rahman, & Alamri, 2017), Social network security: issues, challenges, threats and solutions(Rathore et al., 2017), User's information privacy concerns and privacy protection behaviors in social media(Adhikari & Panda, 2018).

However, from a theoretical perspective, studies still highlight a need for more empirical research about how to protect privacy issues in social media. *This study endeavored to identify* the interrelationship of frequent use of social networking sites and severity attack with the perspective of protection motivation theory(Maddux & Rogers, 1983). Specifically, the

set variables were adopted, viz: perceived severity, default security, perceived vulnerability, response efficacy and frequently use. These were meant to help understand the correlation between perceived severity attacks and frequent use of social networking sites.

1.1 Media Censorship, Social Network and Studentship in Somalia

Self-censorship among the mainstream media in Somalia has remained in force. This can be attributed to the role of government and al-Shabaab in enforcing sanctions in case-sensitive coverage, LANDINFOR (2016). Gallup (2013) study in 2013 found that majority of Somalis (65.6%) accessed news from mainstream media once per day. It was also noted that 75% of Somalis owned a mobile phone with about 22% using them to access social media sites (Gallup, 2013). Due to the censorship of mainstream media, social media provides an avenue to access to information. Previous research on the role of social media in Somalia and Sudan has focused on how its role in conflict (Lomuria, 2014, Kadoda and Hale, 2015). Student's life without social networking site is almost impossible. The main social networking sites established in the year 2004 like Facebook, this famous social media have rapidly become both basic tools for an interface of social interaction, personal identity, and network building among students(Debatin, Lovejoy, Horn, & Hughes, 2009). Social network sites play a crucial part in our daily life and using it to keep in link with our close friends and make some new friends(McLean, Edwards, & Morris, 2017) The majority of the students use social networking sites with the different approaches such as to communicate, reading news feeds, posting information to their profiles, sharing stories, uploading pictures and videos(Hoffmann, 2012).

Dhaha and Igale (2013) found out that the youths in Somalia used social media for “virtual companionship escape, interpersonal habitual

entertainment, self-description of own country, self-expression, information seeking, and passing time gratifications ". From the Dhaha and Igale (2013) findings, it's clear that any attack on the social media platforms might be catastrophic. This is incognizant of the fact that terrorism is a global threat and terrorist can use social media for militarization.

2. *Theoretical Framework and Hypotheses*

In this section, the researchers explore the theoretical framework and the hypothesis to be tested

2.1 Frequent Uses

In several cases of social media, such as Facebook use, mainly multimedia data are produced and shared. According to a report from(Zephoria Inc, 2017), approximately 300 million photos are uploaded per day on Facebook. Facebook becomes one of the highest average rates of watching and sharing videos after increasing day by day. Currently, around 8 billion videos per day are watched on Facebook, which is twice the total viewed in the year 2015. According to the huge amount of data accessible on Facebook, security, and privacy severity attacks are also incrementing. Cybergangs are able to share malicious information on an SNS by hiding it within multimedia data. Furthermore, individual's crucial information such as identity, username, and location can easily gain by an attacker(Venkatachalam & Anitha, 2017)

2.2 Default Privacy Settings

According to (Hoffmann, 2012) Social networking sites are set up to offer individuals with a means of communicating and cooperating with one another. To join a site, individuals sign up as a member; this method may include ensuring personal information such as an e-mail address or phone number, his or her first name and last name, and/or zip code. Since

social networking sites deliver privacy measures, users have the choices to leave as default setting or to set their privacy, but some users are unaware of this privacy issues on social networking sites will likely to fail victim or harm, individuals who have higher concerns with their information protect their privacy issues(Mohamed & Ahmad, 2012). Since social networking sites play a crucial role in individual's communication and distributing information besides these benefits, there are other troubles in this media, for example, the privacy and security problems. This indicates significant consequences for individuals such as This bring significant consequences for users such as unsuitable sharing of personal information, leakage, and exploitation of personal details using active mining(Kayes & Iamnitchi, 2015).

There are various studies which concern of the security and privacy threats caused by malicious software such as adware, worm, spyware, spam, virus and other phishing attempts outside of the user profile itself. One of the issues of social networking that hasn't been examined is the default security and privacy settings on a user's profile(Hoffmann, 2012). Individual online social networks do not take advantage of the security and privacy controls presented the majority of Facebook and Twitter has default settings(Kayes & Iamnitchi, 2015)

2.3 Protection Motivation Theory

Protection Motivation Theory (PMT) suggests that users to protect himself or herself from risks arises from three major components: perceived vulnerability, perceived severity, and response efficacy(Rogers, 1975). In order to encourage the individuals the model was adjusted to include three other main components: self-efficacy, response costs and rewards associated with risky behavior (Maddux & Rogers, 1983; Rogers, 1975). The model proposes that risks and benefits are fundamental factors to describe how users manage behavior in risky

conditions(Youn, 2005). This theory major emphases to health related field(Grindley, Zizzi, & Nasypany, 2008; T. S. Lee, Kilbreath, Sullivan, Refshauge, & Beith, 2007; Milne, Orbell, & Sheeran, 2002; Searle, Norman, Harrad, & Vedhara, 2002). Other researchers were linked the three additional components like self-efficacy, response costs and rewards to adopt an anti-plagiarism system since the model was not tested(Y. Lee, Lee, & Liu, 2007). The majority of the theory identifies health research and information(Y. Lee et al., 2007 a).

The use of PMT in the context of social networking sites however is not apparent(Adhikari & Panda, 2018; Mohamed & Ahmad, 2012). The researchers consider that PMT can significantly explore the use of social media this research perceives of the following variables: vulnerability, response efficacy, frequent, default privacy settings and severity attack. However, the current study proposes that the perceived severity attack on social networks doesn't depend the frequent use.

2.4 Perceived Vulnerability

Regarding (D. Lee, Larose, & Rifon, 2008)Perceived vulnerability is the degree to which individuals trust a threat will occur to him or her. Every new feature in social networking sites conveys many benefits, and other side vulnerabilities and possible dangers like Eavesdropping, Spoofing, Tracking, Denial of Service (DoS) and data corruption manipulation or insertion(Ed, 2013).

2.5 Perceived Response Efficacy

Response efficacy is the belief in the effectiveness of the protections(Tsai et al., 2016). There are some common guidelines to keep prevented from information offenses on social networking sites. First, use long passwords that consist of letters and numbers with unique characters. Second, only let people you actually know and trust to access your profile. Third, be cautious with games and applications. Finally,

check the social networking site's security settings weekly(Hoffmann, 2012). Individuals those trust that preventive action can be taken to keep it up the consequence of losing privacy information through social media is more likely to be concerned with the information privacy(Mohamed & Ahmad, 2012)

2.6 Perceived Severity Attack

Perceived severity is described as the degree to which user observes that negative consequences caused by a malicious IT will be severe(Liang & Xue, 2010). Individuals who perceive severe consequence as a result of losing information privacy through social media are more likely concerned with information privacy (Mohamed & Ahmad, 2012). Therefore, the research proposes that individuals who perceive severe consequences have higher concerns with their information privacy on social networking sites.

Based on the above theory, the researchers proposed the following hypotheses:

H1. The perceived severity attack is negatively related to frequent use by SNSs users.

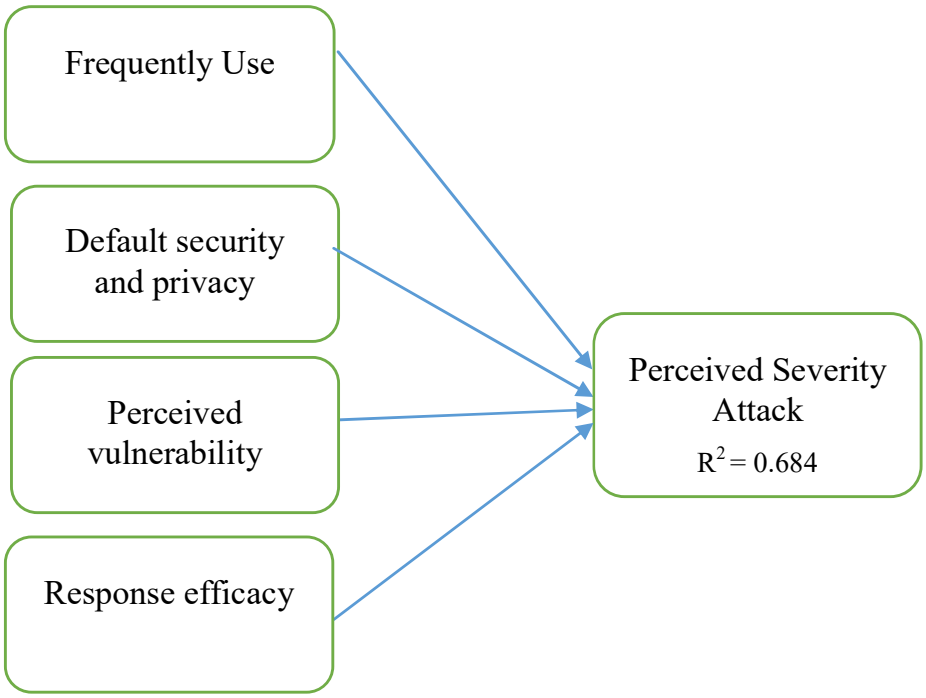
H2. Default security settings are positively related to having fallen victim to severity attack with SNSs users.

H3. A perceived vulnerability is positively related to severe attack with SNSs users.

H4. Response efficacy is negatively related to severe attack with SNSs users.

2.7 Research Model

Figure 1 Research representation model



3. *Methods*

3.1 Sample and Data Collection Process

The study used to investigate the frequently use and severe attack on social media. The sample consisted of 207 undergraduate students from 3 universities in Mogadishu, the capital city of Somalia. The survey was conducted for eighteen days from March 5 to 22, 2018. An online questionnaire survey was used to collect data for analysis using a combo data collect and items of the questionnaire were rated using a Likert - type scale (strongly disagree, disagree. neutral, agree and strongly agree).

3.2 Data Analysis Tool

The result was analyzed using Amos IBM SPSS and Excel so the researchers tested the following set of variables: perceived severity, default security, perceived vulnerability, and response efficacy and frequently use to help understand the correlation between perceived severity attacks and frequent use of social networking sites.

4. *Results*

4.1 Profile of Response

A number of 282 survey questions were distributed. A total of 207 usable responses was received as summarized in table1, a 73% response rate. Nulty (2008) reported that show that face-to-face administration results in higher response rates. Therefore, a 73% response rate was acceptable in this study. From the responses, 83.1% were male and female made up 16.9%. The majority of the students, 79.7% were the age between 18 – 24, between 25-34 of 19.8% and 35 – 44 made up 5%. On frequently used social networking site was, Facebook recorded 96.6%, Twitter had 5% and SnapChat recorded 0.5%. According to the number of accounts, the majority of the students, 76.8% had one account, 20.8% have two accounts and the small number of 1.4% have three accounts. 90.3% of the students have more than 2 years and the other remaining have 1 year. 62.3% of the students spend their time on social media chatting with their friends and families, were 23.3% spend between 2 and 4 hours, 9.2% spend between 1 and 2 hours final 5.3% of the student spend less than 1 hour. 64.3% of the respondents spend 4 hours or more on the Facebook reading news, posting and browsing friends' profiles, 25.1% of the respondents spend between 2 and 4 hours, between 1 and 2 hours final spend less than 1 hour.

4.2 Profile of the Study

Table 1 Profile of the study

Profile	Item	Frequency	Percentage (%)
Gender	Male	172	83.1
	Female	35	16.9
Age	18-24	165	79.7
	25-34	41	19.8
	35-44	1	5
Social Networking sites	Facebook	200	96.6
	Twitter	5	2.5
	SnapChat	1	0.5
Number of Accounts	1	159	76.8
	2	43	20.8
	3	3	1.4
How long have you had a Facebook account	Less than 1 year	6	2.9
	Between 1 and 2years	14	6.8
	More than 2 years	187	90.3
About how much time do you spend on Facebook chatting with friends and families	Less than 1 year	11	5.3
	Between 1 and 2 hours	19	9.2
	Between 2 and 4 hours	48	23.2
	4 hours or more	129	62.3
About how much time do you spend on Facebook reading your news, posting and browsing friends' profiles?	Less than 1 year	11	5.3
	Between 1 and 2 hours	19	9.2
	Between 2 and 4 hours	48	23.2
	4 hours or more	129	62.3

4.3 Factor Loading

Table 2 Factor Loading, SMC. CR, AVE

Construct	Items	Factor Loadings	SMC	CR	AVE
Frequent use	FU1	.741	0.549	0.835	0.633
	FU2	.860	0.739		
	FU3	.695	0.483		
Default security and privacy	SP1	.957	0.916	0.841	0.578
	SP2	.570	0.325		
	SP3	.740	0.548		
	SP4	.724	0.524		
Perceived vulnerability (PV)	PV1	.603	0.364	0.79	0.575
	PV2	.751	0.564		
	PV3	.894	0.799		
Response efficacy (RE)	RE1	.929	0.863	0.811	0.591
	RE2	.781	0.609		
	RE3	.653	0.426		
Perceived severity attack (PSA)	PSA1	.546	0.298	0.843	0.583
	PSA2	.822	0.676		
	PSA3	.681	0.464		
	PSA4	.946	0.895		

4.4 Reliability and Validity

This article was applied using the structural equation modeling technique to identify correlation among construct variables. The researchers identified two types of validity which are convergent and discriminant validity regarding (Brown, 2006) defines convergent validity as internal consistency of set questions or items. It represents the

strong correlation between items that are forecasted to represent a single latent variable. Table 2 indicates the range of factor loadings between 0.546 and 0.957. According to(Byrne & van de Vijver, 2010)factor loadings must be more than 0.5. In convergent validity high average variance extracted (AVE) should greater than 0.5(Fornell and David F. Larcker, 1981) above the table 2 indicates the AVE between 0.575 and 0.633. The construct reliability is similar to Cronbach alpha and should be greater than 0.7(Hair, Black, Babin, & Anderson, 2010). All composite reliability was greater than 0.7 as the above table those are not meeting the criteria was removed from the analysis, in short, the convergent validity was achieved. Discriminant validity was also achieved (Fornell and David F. Larcker, 1981) by calculating the squared average variance extracted(AVE) as the below table 3 indicates.

4.5 Square-root Average Variance Extract

Table 3 Square-root AVE

Construct	FU	DS	PV	RE	PSA
Frequent use (FU)	**.796**				
Default Security (DS)	0.420	**.760**			
Perceived vulnerability (PV)	0.537	0.345	**.683**		
Response efficacy (RE)	0.531	0.367	0.409	**.769**	
Perceived severity attack (PSA)	0.444	0.374	0.377	0.386	**.764**

4.6 Hypothesis Testing

Hypothesis 1 suggests that there is negative relationship between perceived severity attack and frequently use with SNSs users (β =.357; p<. 000) this suggests that hypothesis, not supported and shows that users of social networking sites perceived severity attack with their frequent

use. The findings concur with previous studies by Adhikari and Panda (2018).

Hypothesis 2 indicates that there is the positive relationship between default security settings on social networking sites and perceived severity attack with SNSs users (β = .508; p<.000). Kayes and Iamnitchi (2015) and(Hoffmann, 2012) findings are supported by this study.

Hypothesis 3shows that there is positive relationship between perceived vulnerability and perceived severity attack with social networking site's users regarding the beta a probability value (β =.379; p<. 000). (Mohamed & Ahmad, 2012) mentioned that there was positive relationship between vulnerability and severity attack on online social media. Thus the two studies had similar findings.

Hypothesis 4 Explores response efficacy has negatively related to the perceived severity attack with social networking site's users (β =.394; p<. 000). This supports (Mohamed & Ahmad, 2012) study findings.

TABLE 4 HYPOTHESES TESTING

Hypothesis	Finding
H1: Perceived severity is negatively related to frequent use by SNSs users	Not supported
H2: Default security is positively related to severe attack with SNSs users	Supported
H3: Perceived vulnerability is positively related to severe attack with SNSs users.	Supported
H4: Response efficacy is negatively related to severe attack with SNSs users	Supported

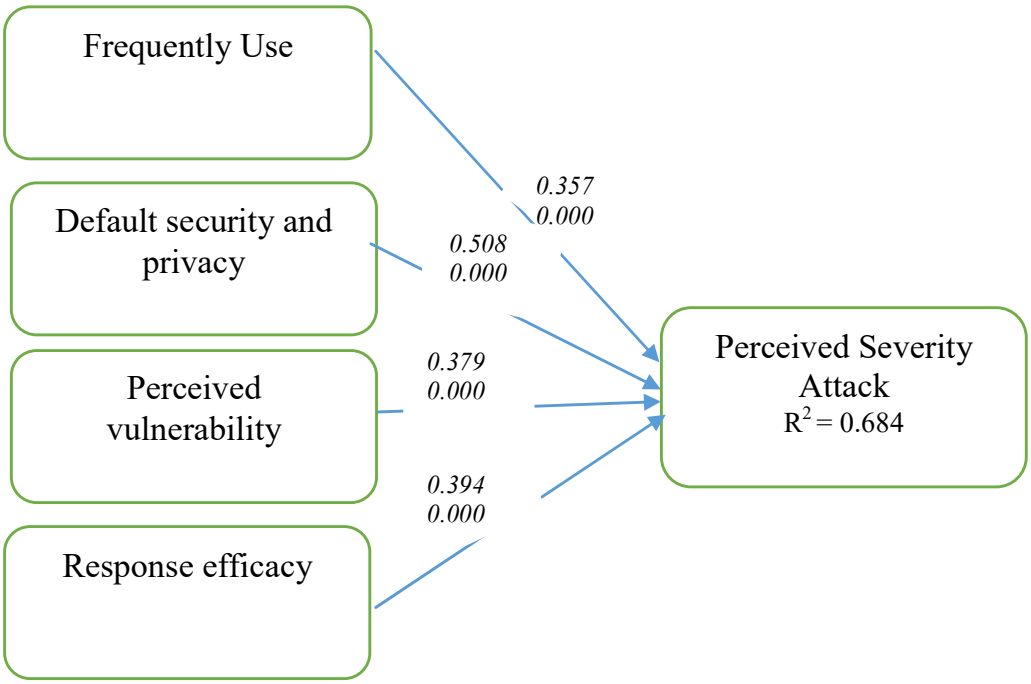


FIGURE 2 RESULT MODEL

TABLE 5 GOODNESS-FIT INDICES

Construct	Recommended value	Value calculated
Chi-square		304.538
Degree of freedom		130
Related Chi-square	<5	1.476
P- value	<0.05	0.001
GFI	>=0.90	0.918
CFI	>=0.90	0.870
Root- mean square error of approximation	<0.08	0.048

Figure 2 and table 4 indicates the satisfactory model fit and confirmatory of the theoretical model for frequent use of social networking sites and severity attack. Specifically, frequently use, default

security and privacy, perceived vulnerability perceived response efficacy variables significantly contribute to the dependent variable perceived severity attack. The chi-square =302.538, df = 130, related chi-square / df =1.48, probability value =0.001 and other model fit goodness of fit index (GFI) = 0.92, CFI=0.87 and RMSEA = 0.048. However, the results indicate that the model is fit for the structural equation model.

5. *Conclusion*

The study shows that frequent use of social media doesn't depend to fail severity attack the only thing wished is to awareness security and privacy setting should change frequently. Awareness is the extremely important role in educating users on do's and don'ts in the social media. Lack of awareness of the user will cause serious damages and loss of data (Yati Yassin and Zahri Yunos, 2006). The researchers have developed the concept of frequent use of social networking sites in the Somalia context. Firstly, the major of the social networking sites users have a default of security and privacy settings (Gross, Acquisti, & Heinz, 2005), so the study indicates that most of the users do not take the advantage security and privacy control available on the social media this causes to fall severity attack. Secondly, the previous studies suggest those who believe an attack will happen to them through social networking sites will be more concerned their security and privacy settings(Mohamed & Ahmad, 2012). In context, this study the perceived vulnerability is positively related to being fallen severity attack on social networking sites. Third, the study identifies that perceived efficacy explore whether users enable their security and privacy measure in-home wireless security(Woon, Tan, & Low, 2005). In the context of this study, response efficacy is negatively related to the severity attack. Finally, the study suggests that the perceived severity attack has no effect using social networking sites frequently, so users believe to have intention and protection. According to (T. S. Lee et al., 2007) individuals should have

the intention to embrace virus protection behavior. Other research indicates to use anti-spyware software(Chenoweth, Minch, & Gattiker, 2009).

6. *Research Contributions*

The study makes a number of contributions to theory and practice. First, the user should avoid using the same password to various social networking accounts, no matter how the user frequent use of this social media. Second, in order to protect the severity attack on this social media, the users should not leave their security and privacy as a default, it's extremely better to change. Finally, social networking site's users have different viewpoints on existing severe attack on social media some of them lack of awareness of this attack and other their aware one of the effective way to protect these harms on social media to educate the users and provide more guidance.

7. *Limitations and Suggests for Future Research*

There are several limitations to this research, first, the sample size was 207, and only undergraduate students at three universities were included. The population and sample were drawn only higher education, so these findings could not be generalized to the entire institutions. Second, the study has only used the questionnaire to obtain qualitative data. Future research may consider requesting individuals to sit a computer, and take the screenshot on both security and privacy settings using snipping tool later to send as capture through email to the researchers and interviewing social networking sites may provide deeper insights into perceptions of frequent use.

Acknowledgement

First of all we all thank to the Almighty. It's our pleasure to have a great chance to complete this article of an excellent topic "An exploration of the frequent use of social networking sites and severity attack among undergraduate students in Somalia" Secondly, we would like to thank the students, for their busy time to fill the questionnaire with their complicate them .

References

Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *Journal of Global Marketing*, *1762*, 1–15. https://doi.org/10.1080/08911762.2017.1412552

Al-qurishi, M., Alrubaian, M., Rahman, S. M., & Alamri, A. (2017). A Prediction System of Sybil Attack in Social Network using Deep-Regression Model. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.030

Brown, T. A. (2006). *Confirmatory Factor Analysis for Applied Research*. *Methodology in the Social Sciences*. https://doi.org/10.1198/tas.2008.s98

Byrne, B. M., & van de Vijver, F. J. R. (2010). Testing for measurement and structural equivalence in large-scale cross-cultural studies: Addressing the issue of nonequivalence. *International Journal of Testing*, *10*(2), 107–132. https://doi.org/10.1080/15305051003637306

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. In *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*. https://doi.org/10.1109/HICSS.2009.74

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Ed, M. F. (2013). *Cyber Security and Privacy*.

ETHICS IN INFORMATION SECURITY By Yati Yassin and Zahri Yunos. (2006), (November), 20–23.

Fornell and David F. Larcker. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, 18*(1), 39–50. Retrieved from http://www.jstor.org/stable/3151312 .

Grindley, E. J., Zizzi, S. J., & Nasypany, A. M. (2008). Use of Protection Motivation Theory, Affect, and Barriers to Understand and Predict Adherence to Outpatient Rehabilitation. *Physical Therapy*, *88*(12), 1529–1540.

https://doi.org/10.2522/ptj.20070076

Gross, R., Acquisti, A., & Heinz, H. J. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society - WPES '05* (p. 71). https://doi.org/10.1145/1102199.1102214

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate Data Analysis. *Vectors*. https://doi.org/10.1016/j.ijpharm.2011.02.019

Hoffmann, B. C. (2012). An exploratory study of a user's Facebook security and privacy settings. *Theses, Dissertations, and Other Capstone Projects*. Retrieved from

http://cornerstone.lib.mnsu.edu/cgi/viewcontent.cgi?article=1069&context=etds

Huang, L., & Lu, W. (2017). Functions and roles of social media in media transformation in China: A case study of "@CCTV NEWS." *Telematics and Informatics*, *34*(3), 774–785. https://doi.org/10.1016/j.tele.2016.05.015

Hur, K., Terry, T., Karatepe, O. M., & Lee, G. (2017). An exploration of the factors in fl uencing social media continuance usage and information sharing intentions among Korean travellers. *Tourism Management*, *63*, 170–178. https://doi.org/10.1016/j.tourman.2017.06.013

Kayes, I., & Iamnitchi, A. (2015). A Survey on Privacy and Security in Online Social Networks, *4*, 1–21. https://doi.org/10.1016/j.osnem.2017.09.001

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour and Information Technology*, *27*(5), 445–454. https://doi.org/10.1080/01449290600879344

Lee, T. S., Kilbreath, S. L., Sullivan, G., Refshauge, K. M., & Beith, J. M. (2007). The development of an arm activity survey for breast cancer survivors using the Protection Motivation Theory. *BMC Cancer*, *7*. https://doi.org/10.1186/1471-2407-7-75

Lee, Y., Lee, J.-Y., & Liu, Y. (2007). Protection Motivation Theory in Information System Adoption: A Case of Anti-Plagiarism System. In *AMCIS 2007 Proceedings* (Vol. 62, pp. 163–175).

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective* 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/10.1.1.170.5816

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

McLean, K., Edwards, S., & Morris, H. (2017). Community playgroup social media and parental learning about young children's play. *Computers and Education*, *115*, 201–210. https://doi.org/10.1016/j.compedu.2017.08.004

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

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008

Rathore, S., Kumar, P., Loia, V., Jeong, Y., & Hyuk, J. (2017). Social network security : Issues , challenges , threats , and solutions. *Information Sciences*, *421*, 43–69. https://doi.org/10.1016/j.ins.2017.08.063

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*. https://doi.org/10.1080/00223980.1975.9915803

Searle, A., Norman, P., Harrad, R., & Vedhara, K. (2002). Psychosocial and clinical determinants of compliance with occlusion therapy for amblyopic children. *Eye*, *16*(2), 150–155. https://doi.org/10.1038/sj/eye/6700086

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Venkatachalam, N., & Anitha, R. (2017). A multi-feature approach to detect Stegobot: a covert multimedia social network botnet. *Multimedia Tools and Applications*, *76*(4), 6079–6096. https://doi.org/10.1007/s11042-016-3555-3

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A Protection Motivation Theory Approach to Home Wireless Security. *International Conference on Information Systems*, 367–380.

Youn, S. (2005). Teenagers ' perceptions of online privacy and coping behaviors : A risk – benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, *49*(1), 86–110. https://doi.org/10.1207/s15506878jobem4901_6

Zephoria Inc. (2017). Top 20 Facebook Statistics. Retrieved from https://zephoria.com/top-15-valuable-facebook-statistics/