

A Conceptual Model to Evaluate Secure Intention Behavior in Online Game Addiction Among Adolescents

Wan Mohd Yusoff Wan Yaacob¹, Nur Haryani Zakaria^{2*}, Zahurin Mat Aji²

¹Department of Communication and Information Technology, Politeknik Tuanku Syed Sirajuddin, Pauh Putra, 02600, MALAYSIA.

²School of Computing, Universiti Utara Malaysia, Sintok, 06010, MALAYSIA.

*Corresponding Author Designation

DOI: <https://doi.org/10.30880/mari.2023.04.01.027>

Received 15 October 2022; Accepted 30 November 2022; Available online 15 January 2023

Abstract : Recently, there is enormous views of potentially non-substance addictive behaviors which become humongous threat among the adolescents such as digital addiction especially in online game addiction. This study argues that all type of addictions including online game addiction is related to common addiction components such as salience, mood modification and tolerance. Despite the plethora of digital addiction protection motivation, there is no standards or benchmarks used in secure intention behavior which involved the element of cybersecurity perspective in online game countermeasures. Hence, this study was organized to develop a conceptual model based on the former Protection Motivation Theory (PMT) in order to evaluate the secure intention behavior in online game addiction among adolescents. Driven by previous studies of online game addiction, we adopt all the distinct common components to measure underlying criteria which related to online game addiction to find the relationship between these constructs. As a result, this study will present the conceptual model as a secure intention behavior model in the context of online game addiction among adolescents. This conceptual model also has been validated by the expert in secure behavior together with related instruments. This conceptual model was expected to become as a reference model which can explain the relationship between human factors component and security factor like fear appeal which influence secure intention behavior in online game addiction. The researchers in this field also can use the model in different perspective and settings and thus create an avenue in paving the way towards online game addiction countermeasures especially in cybersecurity perspective.

Keywords: Protection Motivation Theory, Secure Intention Behavior, Online Game Addiction, Adolescents

1. Introduction

The major focus in this study is finding way to inspire end users including adolescents in order to increase the protection of their individual behavioral intention toward cyber threat which can be influenced by online game addiction. The recent theoretical approaches utilized to promote security compliance that are related to former Protection Motivation Theory (PMT) (See **Figure 1**) [1-3]. The majority of current research on compliance arising from sanctions, threats or fear has shifted from conceptual framework based approaches to a greater emphasis on PMT [4, 5]. Despite the fact that PMT is based on how individual react and made decision under stressful situation, it emphasizes the use of persuasive communications that warn of a personal risk and explain counteracting measures that consist of protective behavior driven by fear appeal [6]. Regarding to this study, PMT is well suited to secure intention behavior in online game addiction involving adolescents as the end users who need extra incentive to defend against cyber threat. Recently published in information systems (IS) journals are the number of research on secure intention behavior that employ PMT as the major foundation for theory development from the overview of online game addiction [7, 8].

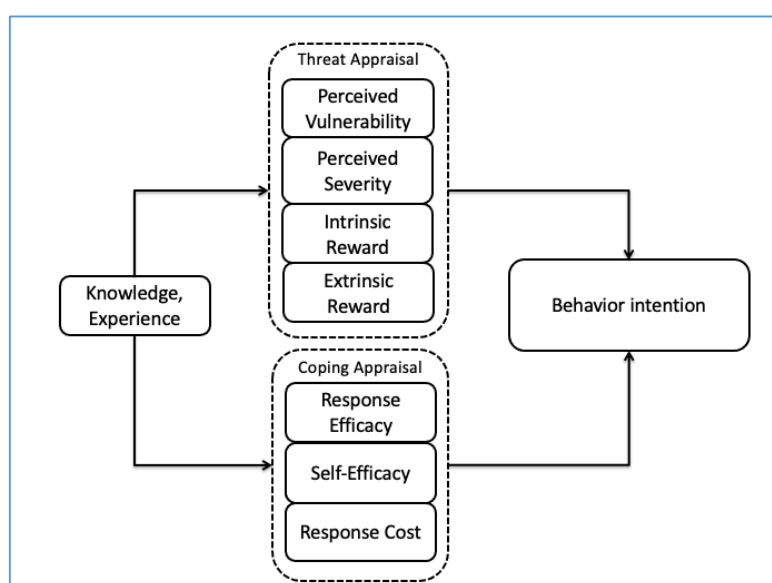


Figure 1: Former Protection Motivation Theory [9]

These studies have contributed significantly to the field of PMT based research in the context of secure intention behavior. However, the literature has not fully leveraged PMT research conducted in fields outside IS to provide a wider range of opportunities for theory and practice, especially in addictive behavior [10, 11]. Opportunities for improvement in current safe intentions practices were identified in our literature research [12, 13]. First, although the studies use many of the PMT concepts, none of them use all its core constructs which deviate dramatically from PMT without proper theoretical justification regarding to online game addiction. Second, with few exceptions [14, 15], none of the studies manipulate an actual fear appeal in the context of the research related to online game addiction among adolescents. Third, the majority of secure intention behavior studies focus on countermeasure of addictive behavioral and not on actual security behaviors in online game addiction.

2. Materials and Methods

The purpose of this study is to propose the conceptual model as a secure intention behavior model in the context of online game addiction among adolescents. This study has identify security factor for potential theoretical and methodological improvements on which to build this literature by proposing reincarnation of PMT based on behavioral addiction studies. Notably, we propose the reincarnation involved a study that used the main constructs of PMT, that is “core nomology” based on Jansen [12]

and improving fear appeals and online game addiction factors by adding salience, mood modification and tolerance in the model. Salience behavior happen when games become dominant in though, feeling and conduct while tolerance is an increm(ent of game activity to achiece pleasure and mood modification is refer to the gaming behavior which used as coping mechanism from bad mood to good mood. This study was useful in reintroducing the impact of fear appeals and online game addiction factors that construct into PMT and assessing actual behavior along with secure intention behavior. **Figure 2** depicts the reincarnation of PMT along with proposed construct nomologies.

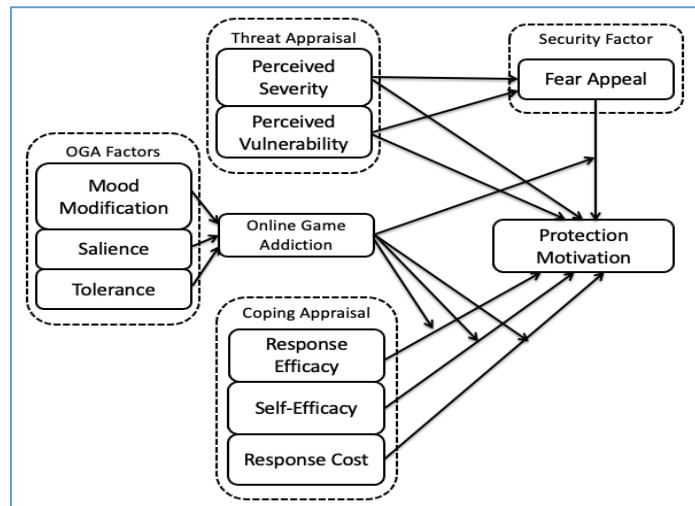


Figure 2: Reincarnation of Protection Motivation Theory

3. Results and Discussion

PMT key assumptions are similar with threat appraisal and coping appraisal which related to two components of PMT (threat appraisal and coping appraisal) as shown in **Figure 2** that shape the protection behavior. The essential behind PMT is that the threat appraisal process is initiated by a fear appeal towards cyber threat. In order for a person to respond adaptively, there are two things should occur: First, the cyber threat that inspire protection motivation must first be given greater weight in the threat appraisal process than maladaptive incentives gained by not participating in online game. Second, in order to engage in the protection behavior, a person's response effectiveness and self-efficacy must be greater than the response costs in online game. Concern about cyber threats is not the same thing as a fear appeal, this distinction has to be made clear when discussing threat assessment. PMT characterizes fear as a "relational construct, awakened in reaction to a circumstance that is evaluated as threatening and toward which protective action is taken" [9], [16]. Furthermore, a fear appeal is a distinct stimulus intended to activate the fear response with the threat assessment and coping appraisal processes. In an ideal world, a fear appeal would do more than simply enhance threat [12], [17]. It would also boost effectiveness by providing a way for the responder to cope with the threat. The most effective fear appeals increase both threat and efficacy, or how well they work by focusing on the threat and the individual's coping mechanisms [18–20].

4. Conclusion

The concept of secure intention behavior is just part of what makes up a fear appeal and this should be kept in mind by the adolescents who infected by online game addiction. Just because a message is there condemning a certain kind of insecure conduct in online game addiction doesn't mean it will be convincing or scary. An effective fear appeal relies on a convincing message that ideally and emphasizes the gravity of the cyber threat and the degree to which the target is exposed to it. Meanwhile, the fear appeal towards cyber threat has to deal with things that boost confidence and make responses more effective while cutting down on the hassle they cause. In order to effectively counteract fear

appeals towards cyber threat, campaigns, interventions and training are usually necessary. More frequent applications throughout time are necessary in order to get optimal results in mitigating this issue. In conclusion, a successful fear appeal with online game addiction factors towards cyber threat motivates a protective and adaptive reaction rather than a negative and dismissive one by influencing the receiver to change how they think about the threat and how they may deal with it. We want our studies to convince the adolescents of the usefulness of appealing to users' worst fears and to provide them with compelling reasons to comply with behavioral security policies towards secure intention behavior.

Acknowledgement

This research was supported by Ministry of Higher Education (MoHE) through Fundamental Research Grant Scheme (Ref: FRGS/1/2020/ICT03/UUM/02/1). The content of this article is solely the responsibility of the authors and does not necessarily represent the official views of the MoHE, Malaysia.

References

- [1] R. C. Plotnikoff and L. Trinh, "Protection motivation theory: Is this a worthwhile theory for physical activity promotion?," *Exerc Sport Sci Rev*, vol. 38, no. 2, pp. 91–98, 2010, doi: 10.1097/JES.0b013e3181d49612.
- [2] K. MacDonell, "A Protection Motivation Theory-Based Scale for Tobacco Research among Chinese Youth," *J Addict Res Ther*, vol. 04, no. 03, 2013, doi: 10.4172/2155-6105.1000154.
- [3] J. Ophoff and M. Lakay, *Mitigating the Ransomware Threat: A Protection Motivation Theory Approach*, vol. 973. Springer International Publishing, 2019. doi: 10.1007/978-3-030-11407-7_12.
- [4] K. Y. Chen and C. F. Yeh, "Factors affecting adoption of smart meters in the post-Fukushima era in Taiwan: an extended protection motivation theory perspective," *Behaviour and Information Technology*, vol. 36, no. 9, pp. 955–969, 2017, doi: 10.1080/0144929X.2017.1317363.
- [5] W. Al-ghaith, "Extending Protection Motivation Theory to Understand Security Determinants of Anti-virus Software Usage on Mobiles Devices," *International Journal of Computers*, vol. 10, pp. 125–138, 2016.
- [6] Donna L. Floyd, "A Meta-Analysis of Research on Protection Motivation Theory," *Psychologist*, vol. 21, no. 1, pp. 16–19, 2008.
- [7] Z. Xu, O. Turel, and Y. Yuan, "Online game addiction among adolescents: Motivation and prevention factors," *European Journal of Information Systems*, vol. 21, no. 3, pp. 321–340, 2012, doi: 10.1057/ejis.2011.56.
- [8] S. Bekir and E. Çelik, "Examining the factors contributing to adolescents' online game addiction," *Anales de Psicologia*, vol. 35, no. 3, pp. 444–452, 2019, doi: 10.6018/analesps.35.3.323681.
- [9] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *J Psychol*, vol. 91, no. 1, pp. 93–114, 1975, doi: 10.1080/00223980.1975.9915803.
- [10] K. MacDonell, "A Protection Motivation Theory-Based Scale for Tobacco Research among Chinese Youth," *J Addict Res Ther*, vol. 04, no. 03, 2013, doi: 10.4172/2155-6105.1000154.

- [11] R. A. Amaral, A. Malbergier, D. R. Lima, V. C. V. Santos, C. Gorenstein, and A. G. de Andrade, "Intention to Drive after Drinking among Medical Students: Contributions of the Protection Motivation Theory," *J Addict Med*, vol. 11, no. 1, pp. 70–76, 2017, doi: 10.1097/ADM.0000000000000276.
- [12] J. Jansen and P. van Schaik, "Persuading end users to act cautiously online: a fear appeals study on phishing," *Information and Computer Security*, vol. 26, no. 3, pp. 264–276, 2017, doi: 10.1108/ICS-03-2018-0038.
- [13] J. Jansen and P. van Schaik, "Comparing three models to explain precautionary online behavioural intentions," *Information and Computer Security*, vol. 25, no. 2, pp. 165–180, 2017, doi: 10.1108/ICS-03-2017-0018.
- [14] D. P. Johnson and D. Johnson, "How Attitude Toward the Behavior , Subjective Norm , and Perceived Behavioral Control Affects Information Security Behavior Intention This is to certify that the doctoral study by," 2017.
- [15] B. Fatokun Faith, S. Hamid, A. Norman, O. Fatokun Johnson, and C. I. Eke, "Relating Factors of Tertiary Institution Students' Cybersecurity Behavior," *2020 International Conference in Mathematics, Computer Engineering and Computer Science, ICMCECS 2020*, pp. 0–5, 2020, doi: 10.1109/ICMCECS47690.2020.246990.
- [16] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *J Exp Soc Psychol*, vol. 19, no. 5, pp. 469–479, 1983, doi: 10.1016/0022-1031(83)90023-9.
- [17] K. Renaud and M. Dupuis, "Cyber security fear appeals: Unexpectedly complicated," *ACM International Conference Proceeding Series*, no. December, pp. 42–56, 2019, doi: 10.1145/3368860.3368864.
- [18] D. C. Orazi, A. C. Johnston, and M. Warkentin, "Integrating construal-level theory in designing fear appeals in IS security research," *Communications of the Association for Information Systems*, vol. 45, no. 1, pp. 397–410, 2019, doi: 10.17705/1CAIS.04522.
- [19] D. Burgos, B. Fernández-Manjón, and G. Richards, "Examining the Relationship of Organizational Insiders' Psychological Capital with Information Security Threat and Coping Appraisals," *Comput Human Behav*, vol. 24, no. 6, pp. 2475–2476, 2008, doi: 10.1016/j.chb.2008.03.008.
- [20] D. J. Lemay, R. B. Basnet, and T. Doleck, "Examining the relationship between threat and coping appraisal in phishing detection among college students," *Journal of Internet Services and Information Security*, vol. 10, no. 1, pp. 38–49, 2020, doi: 10.22667/JISIS.2020.02.29.038.