THE PENNSYLVANIA STATE UNIVERSITY
SCHREYER HONORS COLLEGE

COLLEGE OF INFORMATION SCIENCES AND TECHNOLOGY

An Exploratory Study of the Information Security Behavior of Gamers

JOHN ZHUANG
SPRING 2023

A thesis
submitted in partial fulfillment
of the requirements
for a baccalaureate degree
in Cybersecurity Analytics and Operations
with honors in Cybersecurity Analytics and Operations

Reviewed and approved* by the following:

Yubo Kou
Assistant Professor of Information Sciences and Technology
Thesis Supervisor

Michael Hills
Teaching Professor of Information Sciences and Technology
Honors Adviser

* Electronic approvals are on file.

ABSTRACT

Information security has continued to remain a critical issue in society. Gamers are a population of interest that contain more technological mastery than most due to their extended time with devices and technical gaming matters. Consequently, gamers may display various behaviors or traits that can encourage information security related behaviors. However, gamers are under-represented in security research studies. This study addresses this research gap by examining factors that motivate gamers' information security behaviors. The protection motivation theory (PMT) provides a theoretical framework for understanding user security behavior that is adopted in the model. A survey of 122 responses from gamers is used to test the designed model using Partial Least Squares regression to analyze relationships among variables. Results demonstrate that gamers are motivated to practice information security behavior if high levels of vulnerability, severity, self-efficacy, and response cost are perceived. However, response efficacy did not influence the security behavior of gamers. The findings suggest that gamers' information security behaviors are generally effective with potential for future research into strengthened security behavior.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to begin by thanking my thesis advisor, Dr. Yubo Kou, for his unwavering support, mentorship, and kindness throughout my undergraduate career. I am especially grateful for his advice, time, and patience given to this project. Thank you to my committee members, Dr. Ting Wang and Dr. Xinning Gui, for their guidance and feedback.

I would also like to thank Dr. Michael Hills for serving as my honors advisor and supporting me throughout my Schreyer Honors College pursuits.

I would like to give a special thanks to my family for their continued support throughout this entire process.

Chapter 1
Introduction

The use of computers and the Internet are integral parts of our lives as many societal functions have been digitized. Today, we are able to work, shop, bank, game, and more, all from the convenience of our own devices. We have become dependent on technology for these capabilities and many others. However, in doing so, we have also become exposed to many serious information security threats such as malware, spam, phishing, and social engineering attacks (Bendovschi, 2015). These cyber threats will only continue to increase in number with the introduction of new technologies, leading to new exploits.

Consequently, effective information security behaviors are a critical skill to all technology users to protect against these threats. If these behaviors are not adopted, the potential consequences are severe, including threats to digital assets such as devices, forced access to private information, and unauthorized use of financial assets (Clough, 2015). Other impacts can also affect users' social and affective lives. Financial losses and the forced disclosure of private information can be extremely stressful and take a toll on their wellbeing (Liang & Xue, 2010). An attack such as ransomware can induce panic and cause further distress, preventing users from accessing their personal devices and files without paying a ransom. Through these examples, it is clear to see that cyber-attacks can have devastating consequences without effective information security behaviors.

While these cyber-attacks can be complex in nature, their corresponding preventative measures are quite simple. Examples include installing antivirus software and being aware of signs of phishing, both of which are well-documented and require little effort to perform (CISA, 2019). The upkeep of these preventative measures is also very inexpensive as prior attacks such as phishing do not change drastically in form, and software such as antivirus only require updates which are often automatic. Today, there is little that a technology user has to do in order to obtain effective information security behaviors. Yet, there are still many users who lack these critical skills (Furnell et al., 2018).

Specifically, users often engage in unsafe technological behaviors such as browsing unsafe websites, downloading suspicious software, sharing passwords, and implementing insufficient host and network protections. Factors behind these behaviors include convenience as well as a lack of protective security knowledge. As a result, significant information security risks still exist without the adoption of effective information security behaviors.

To encourage these behaviors, I have decided to examine an often-overlooked population: gamers. In recent years, security breaches at notable gaming companies such as Electronic Arts, Rockstar, and Riot Games have occurred. These incidents have raised concerns about the effectiveness of security measures at these companies as well as the safety of gamer data and personal information. In turn, experience with breaches may allow gamers to have more effective security habits. Additionally, gamers contain more technological mastery than most, choosing to spend more time with technology and often pursuing more technical matters related to games (Sanford & Madill, 2006). I believe that gamers may display various behaviors or traits that can encourage information security related behaviors. If found, these aspects of gamers can be used to devise better methods of encouraging effective information security behavior habits among other populations as well.

This study uses the protection motivation theory (PMT) to understand what drives information security behaviors among gamers. This paper contributes to research on security by examining a scarcely studied population to develop an extended model for information security behavior motivation.

Research Question

The aim of this study is to provide a better understanding of gamers' information security behaviors by discussing the following research question:

1. What are the factors that motivate gamers' behaviors towards information security?

Information security behaviors are defined as taking on recommended security precautions to ensure the safety of one's own computers, laptops, smartphones, and other technological devices.

Chapter 2

Literature Review

The purpose of this study is to determine the most important factors that affect information security habits among gamers. As such, a focus will be placed on the theoretical frameworks that have been used to predict users' behavior in the information security domain. An overview of research that has been conducted in the video game domain will be discussed as well.

Theoretical Frameworks

The following sections discuss the major dimensions involved in this research which include the theoretical foundation, video game literature, and a brief summary.

Health Belief Model

In the 1950s, social psychologists Hochbaum, Rosenstock, Leventhal, and Kegeles developed the Health Belief Model (HBM). It was originally developed to explain the failure of individuals to participate in government health programs but has since extended into many different health-related behaviors. The HBM proposes that an individual's combined beliefs about a health threat and the effectiveness of a health treatment will indicate the likelihood the person seeks out the treatment. Although the HBM originally focused on a very narrow range of health behaviors, it has since been applied to broad healthcare areas such as symptoms and diagnoses, even extending into other disciplines such as information security.

The HBM originally contained four main principles: perceived susceptibility, perceived severity, perceived benefits, and perceived barriers. As time passed, more research was done on HBM, resulting in two more principles being added to the model as shown in **Figure 1**. In total, there are six principles as follows:

Perceived susceptibility - A person's perceived perception of the risk of contracting illnesses and beliefs can serve as a main catalyst for change to healthier behaviors. This principle is subjective and can vary greatly from person to person.

Perceived severity - The principle of perceived severity is described as an individual's attitude towards the contraction of a disease. As with perceived susceptibility, this principle is highly subjective and can pose a wide variation between people.

Perceived benefit - When considering health threats and treatments, one component in the decision to adopt a healthier behavior is the benefits that result from doing so. Both perceived susceptibility and perceived benefits are considered when deciding on a behavior to adopt, and a person is more likely to follow through with the new behavior when they believe there are benefits to be gained.

Perceived barriers - While there may be benefits to be gained through healthier behavior, it is also likely that there are obstacles as well. Some barriers could be as simple as inconvenience, while others can relate to cost and potential side effects. A cost-benefit analysis is typically conducted to compare the effectiveness and obstacles of a particular health action.

Cues to action - The principle of cues to action is caused by external or internal stimuli. Internal cues such as personal symptoms can cause a person to begin a healthy behavior, and external cues such as news articles can have the same effect.

Self-efficacy - Self-efficacy is one's own belief in themselves to succeed at doing something. This is an important component in behavioral theory because people do not usually perform a behavior unless they have faith that they will succeed. This principle was added to the HBM in 1988, the newest component of the model.

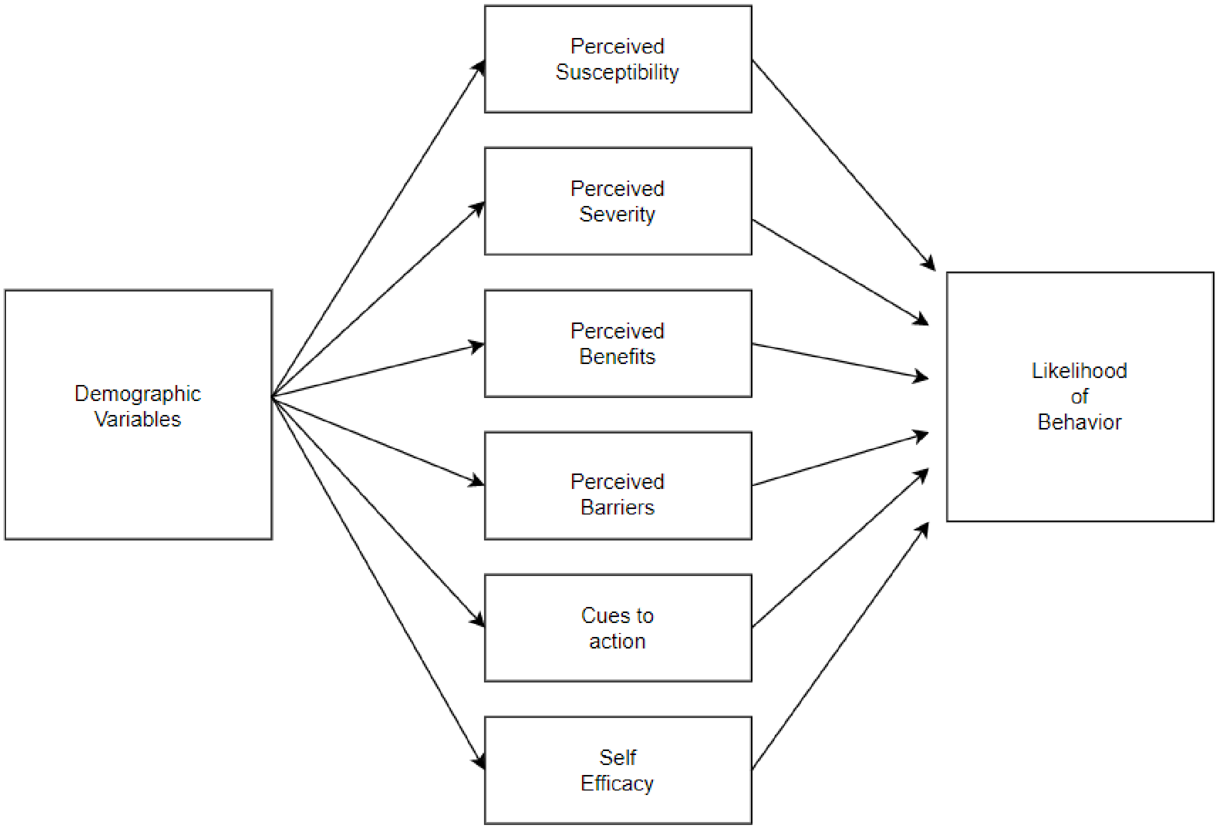


Figure 1. Health Belief Model: Adapted from Rosenstock (1974); Stretcher and Rosenstock (1997)

Technology Threat Avoidance Theory

One of the original theories that attempts to explain information technology (IT) behavior is the Technology Threat Avoidance Theory (TTAT). Liang and Xue (2009) created TTAT to provide "a broader approach focused on avoidance" aimed at providing "a complete understanding of the phenomenon", one that draws upon the fields of psychology, risk analysis, healthcare, and information systems (p. 71). TTAT attempts to explain threat avoidance behavior in IT users at the individual level. A further study was then conducted by Liang and Xue (2010) to test their TTAT with the model shown in **Figure 2** below:

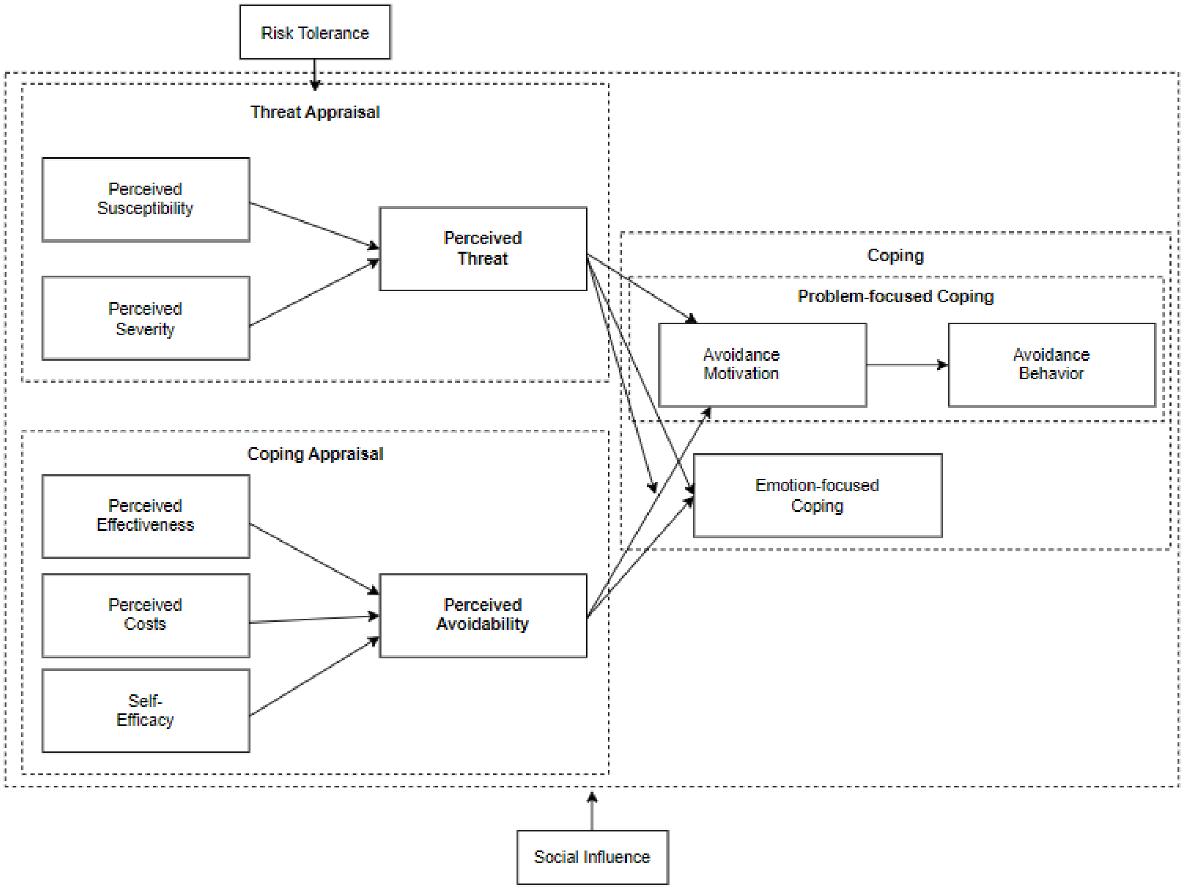


Figure 2. Technology Threat Avoidance Theory: Liang and Xue (2010)

The TTAT contains two main processes: appraisal and coping. Threat appraisal and coping appraisal are antecedents of the coping process. Within threat appraisal, perceived threat is defined as the degree of harm that an individual assesses from malicious IT. The two antecedents to perceived threat are perceived susceptibility and perceived severity. Perceived susceptibility is the individual's belief of the probability of a security incident negatively affecting them. Perceived severity is the individual's perception of the damage severity of such an occurrence.

Within coping appraisal, perceived avoidability is an individual’s belief in the ways they can detach themselves from the malicious IT. The three antecedents of perceived avoidability are perceived effectiveness, perceived costs, and self-efficacy. Perceived effectiveness is the individual’s belief in the safeguard to avoid the threat. Perceived costs are the “individual’s physical and cognitive efforts that are needed to use the safeguarding measure such as time, money, inconvenience, and comprehension” (Liang & Xue, 2009, p. 82). Self-efficacy is the individual’s confidence in themselves to implement the safeguard.

The coping process is split into two categories: problem-focused and emotion-focused. Problem-based coping can occur when the individual judges whether the IT threat is avoidable. When problem-based coping is employed, the individual undertakes efforts to ensure that safeguarding measures are being utilized to protect assets. In contrast, the individual may use an emotion-based coping strategy in an unavoidable situation where a security incident will occur.

Protection Motivation Theory

The Protection Motivation Theory (PMT) was created by Rogers in 1975 to better understand fear appeals. The original model can be seen in **Figure 3** below. This theory was later extended to understand the cognitive processes behind behavioral change, particularly with persuasive communication.

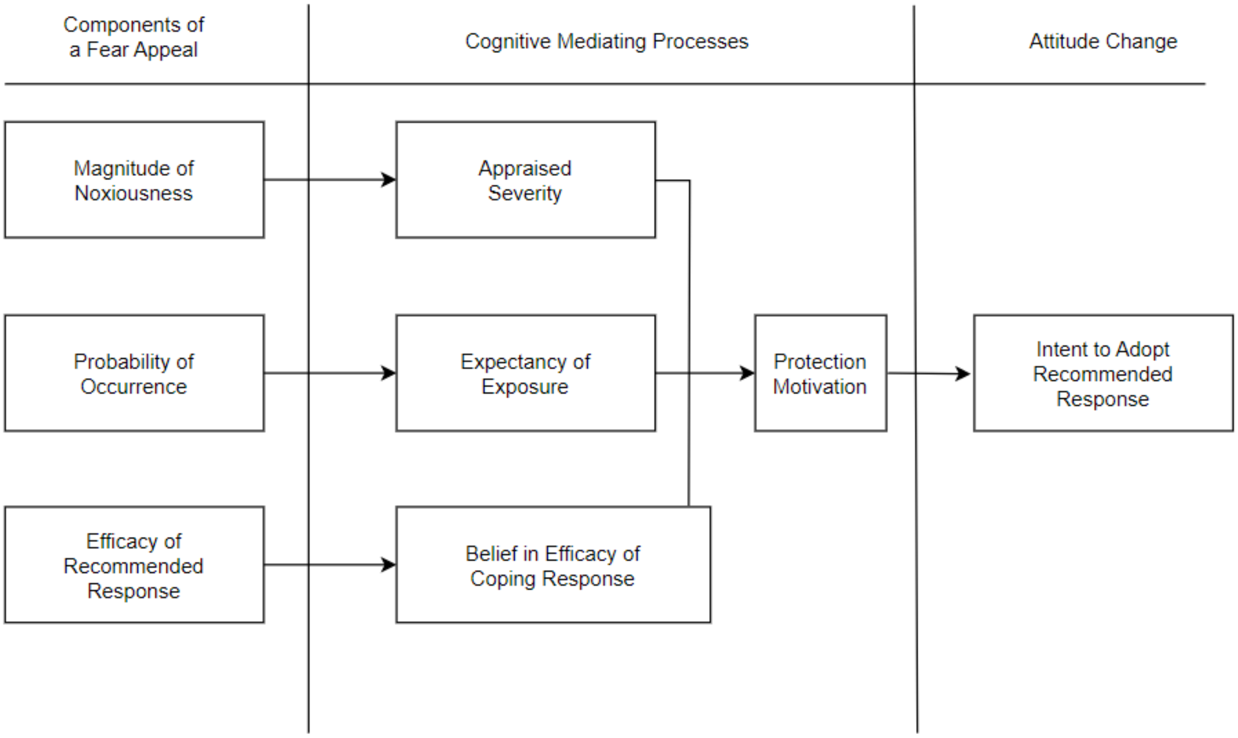

Components of a Fear Appeal
Cognitive Mediating Processes
Attitude Change
Magnitude of Noxiousness
Appraised Severity
Probability of Occurrence
Expectancy of Exposure
Protection Motivation
Intent to Adopt Recommended Response
Efficacy of Recommended Response
Belief in Efficacy of Coping Response

Figure 3. Protection Motivation Theory: Rogers (1975)

Protection motivation is influenced by three main factors: perceived severity, perceived vulnerability, and response efficacy. Perceived severity is an individual's estimate of the degree of harm from a disease on their life. Perceived vulnerability is an individual's appraisal of the probability of contracting a disease. Response efficacy is the individual's belief on the effectiveness of the recommended health behavior in combating the threat. These three factors determine the individual's decision to adopt the recommended behavior or not, a process that can be extended to fields outside of healthcare and psychology.

The extension of the PMT was done by Rogers in 1983. Determinants of protection motivation were split into two main categories: threat appraisal and coping appraisal. Threat appraisal is influenced by perceived susceptibility (perceived vulnerability) and perceived severity. Coping appraisal is determined by self-efficacy (one's belief in themselves to effectively perform the protective action), response efficacy, and response cost. A simplified version of the model can be seen in **Figure 4**:

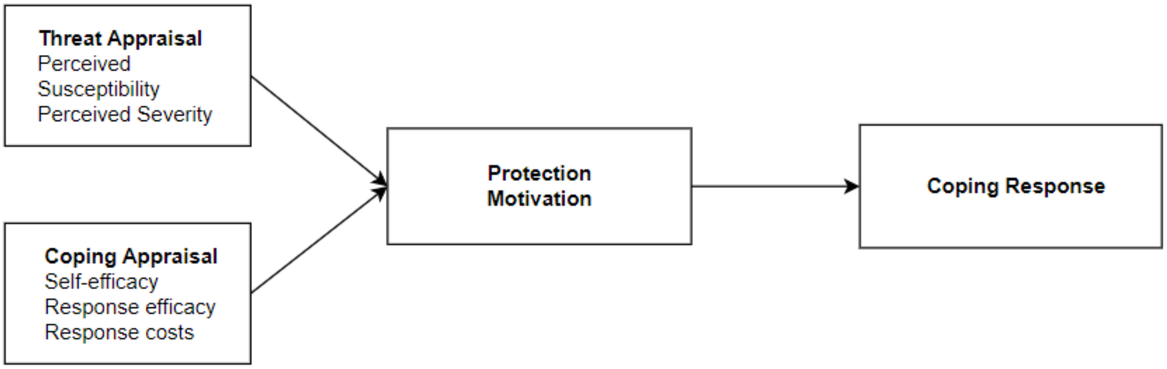


Figure 4. Protection motivation theory: Adapted from Rogers et al. (1983)

Video Games and Security

Video games are defined by Merriam Webster as ”an electronic game in which players control images on a video screen”. They have been studied extensively across a few different domains. Specifically, a large amount of research has been done on gaming addiction and other disorders (Hussain et al., 2012; Kuss, 2013; Lam, 2014). Aside from this focal point, other research has focused on various aspects of gamers such as gamer types and behaviors (Eklund, 2016; Hewett et al., 2020), motivation (Veltri et al., 2014), and genre preferences (Entertainment Software Association, 2021). Regarding video games and its intersection with other fields of study, it appears that the area is often limited to education and how games can be incorporated in various curriculums and tools (Royse & Newton, 2007; Zirawaga et al., 2017).

In terms of education, video games have been studied as a possible medium to improve security awareness. Cone et al. (2007) introduces a video game by the name of CyberCIEGE that helps support organizational security training objectives. Sheng et al. (2007) describes an online game called Anti-Phishing Phil used to teach players about good habits in avoiding phishing attacks. Konig and Wolf (2018) demonstrate how GHOST, a competence developing game, can be used as another quality form of cybersecurity awareness training. Although these studies have demonstrated the effectiveness of incorporating video games as security awareness tools, more research is required to combat the issues surrounding the implementation of security awareness programs with video games.

Security issues within the video game industry have also been examined. Bryant and Saiedian (2021) describe the technical implementation of 3 different networked video games, outlining vulnerabilities that may lead to potential cyber-attacks. Chen et al. (2016) also looks at various networked video games in addition to the Sony Playstation 4 (PS4) game console, highlighting features in each that can also be exploited by attackers to reveal sensitive information. Zhao (2018) focuses on security issues in online games, particularly cheating and how it relates to common security threats. Mohr and Rahman (2011) take a broader stance and examines security issues at the organizational level for video game companies, proposing possible solutions for common security concerns.

While the study of video games has been thorough, there are still many areas that have yet to be discovered. The insights drawn from studies done on gamer types, behaviors, and motivation can be applied to other types of behavior as well. Particularly, there is a significant lack of research on the intersection between video games and security behavior. Video games allow gamers to spend more time with technology, increasing their experience and expertise in the area. This increase in technological exposure through video games can influence the effectiveness of security behavior. For example, it was found that individuals who play video games contain more technological mastery than most, choosing to spend more time with technology and often pursuing more technical matters related to games (Sanford & Madill, 2006). This mastery can lead to improved self-efficacy with regard to technological behavior, improving security habits. Future investigation is required to determine whether an increase in technological experience can be used to encourage an increased adoption of effective security behaviors.

Summary

Current behavioral theories have developed a detailed understanding of the security behavior of users across different contexts. In particular, self-efficacy appears to be a consistently significant construct across multiple theories. The PMT has been widely used in the study of user security behavior, and it will be applied in this study as well. Within the PMT, in addition to self-efficacy, perceived severity and response efficacy also demonstrate strong influence on protection motivation. Video games and their players have been studied across a variety of domains and have been very useful in understanding addiction, behavior, and motivation. Despite the breadth of literature on these topics, there has been no research done on the intersection between information security behavior and gaming as far as I know. My research seeks to fill this gap by utilizing the PMT to assess the most important factors that motivate gamers' behaviors towards information security. As seen in the review above, the PMT has been widely used in the information security domain to analyze security behavior. Findings may be able to provide avenues of improvement in information security habit adoption among other populations not limited to gamers.

Chapter 3

Research Model and Hypotheses

Research Model

This study aims to understand the security behavior of gamers through the research model presented in **Figure 5**. There are five constructs derived from the PMT assessed in this study: perceived vulnerability, perceived severity, self-efficacy, response efficacy, and response cost. The coping response construct (i.e. behavioral intent) is not investigated as this is a cross-sectional rather than a longitudinal study.

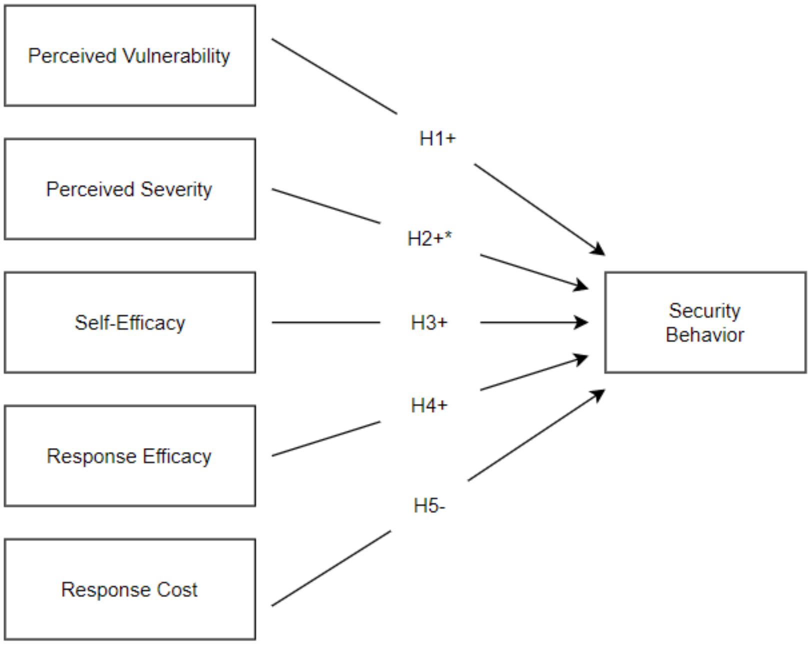


Figure 5. Research Model

Hypotheses

Threat Appraisals

Threat appraisals have been found to predict security behavior, although past studies have come up with mixed findings. Perceived vulnerability is a shared construct in other theories such as the HBM and the TTAT. For HBM, Ng et al. (2009), Schymik & Du (2018), and Claar (2011) all found perceived vulnerability to be positively significant with the former two studies analyzing email-related security behavior and Claar analyzing the adoption of computer security software among home users. For the TTAT, Liang & Xue (2010) and Forrester (2019) found perceived vulnerability to be positively significant in their studies as well. However, when performing a replication study of Liang & Xue (2010) applied to the context of spyware instead of malware, Young et al. (2016) did not find perceived vulnerability to be significant. In PMT studies, Chang et al. (2018), Tu et al. (2019), and Giwah et al. (2019) have found the construct to be positively significant, but there have been many cases where perceived vulnerability was found to be insignificant as well (Woon et al., 2005; Yoon et al., 2012; Mwagwabi, 2015; Tsai et al., 2016).

Interestingly, there have been conflicting results among different populations of the same study. Dang-Pham & Pittayachawan (2015) found perceived vulnerability to hold positive significance when analyzing university students but no significance when applied to home users in a study about malware avoidance. Crossler & Bélanger (2014) have even found perceived vulnerability to negatively predict security behavior as well. Despite mixed findings across a variety of theories for the construct of perceived vulnerability, the hypothesis aligns with the original relationship proposed by Rogers in the PMT:

H1: Perceived Vulnerability will have a positive relationship with the recommended security behavior.

Perceived severity has also received mixed findings in terms of significance from a variety of behavioral theories. For the HBM, studies seem to consistently find that perceived severity has no significance on security behavior (Ng et al., 2009; Claar, 2011; Schymik & Du, 2018). Yet, according to the TTAT, the construct seems to consistently contain significance (Liang & Xue, 2010; Young et al., 2016; Forrester, 2019). Results become increasingly conflicted with studies related to the PMT. While a large majority seem to agree on the positive significance of perceived severity (Woon et al., 2005; Herath & Rao, 2009; Vance et al., 2012; Yoon et al., 2012; Crossler & Bélanger, 2014; Dang-Pham & Pittayachawan, 2015; Chang et al., 2018; Tu et al., 2019), there are still findings that have demonstrated no significance from the construct (Mwagwabi, 2015). Giwah et al. (2019) and Tsai et al. (2016) even found that perceived severity seems to negatively predict security behavior. Consistent with perceived vulnerability, although there are conflicting findings for the significance of perceived severity, the hypothesis remains consistent with the majority of other PMT studies:

H2: Perceived Severity will have a positive relationship with the recommended security behavior.

Coping Appraisals

Generally, coping appraisals have been found to predict security behavior. Self-efficacy has more uniform findings across a large number of studies predicting security behavior based on behavioral theories. HBM studies seem to agree on self-efficacy's positive significance in predicting security behavior (Ng et al., 2009; Claar, 2011; Schymik & Du, 2018). TTAT studies appear to have similar results with consistent positive significance as well (Liang & Xue, 2010; Arachchilage & Love, 2014; Young et al., 2016; Chen & Li, 2017; Forrester, 2019). Studies based on the PMT almost mirror these results, with a vast array of positive significance for self-efficacy when predicting security behavior (Woon et al., 2005; Herath & Rao, 2009; Vance et al., 2012; Yoon et al., 2012; Crossler & Bélanger, 2014; Dang-Pham & Pittayachawan, 2015; Mwagwabi, 2015; Chang et al., 2018; Giwah et al., 2019; Tu et al., 2019). Yet, there have been deviating findings. Tsai et al. (2016) unexpectedly found self-efficacy to have negative significance on security behavior, resulting in the need for future studies and analysis. The hypothesis aligns with the results of the vast majority of studies:

H3: Self-Efficacy will have a positive relationship with the recommended security behavior.

The significance of response efficacy has had very consistent results across a variety of behavioral studies. Studies based on the TTAT have found positive significance (Liang & Xue, 2010; Young et al., 2016; Chen & Li, 2017), and a variety of PMT studies have found positive significance as well (Woon et al., 2005; Herath & Rao, 2009; Vance et al., 2012; Yoon et al., 2012; Crossler & Bélanger, 2014; Dang-Pham & Pittayachawan, 2015; Mwagwabi, 2015; Tsai et al., 2016; Chang et al., 2018; Giwah et al., 2019; Tu et al., 2019). Consistent with these findings, the hypothesis is as follows:

H4: Response Efficacy will have a positive relationship with the recommended security behavior.

Past studies have obtained mixed findings on the effects of response cost. HBM studies have found response cost to have no significance in studies relating to security behavior (Ng et al., 2009; Claar, 2011; Schymik & Du, 2018). As for the TTAT, some studies have found negative significance for response cost (Liang & Xue, 2010; Young et al., 2016), while others have found the construct to be insignificant (Chen & Li, 2017; Forrester, 2019). A large number of PMT studies have found response cost to be negatively significant (Woon et al., 2005; Herath & Rao, 2009; Vance et al., 2012; Yoon et al., 2012; Dang-Pham & Pittayachawan, 2015; Tsai et al., 2016; Chang et al., 2018; Tu et al., 2019), but there have also been conflicting findings in the PMT domain with some studies discovering no significance for the construct (Crossler & Bélanger, 2014; Mwagwabi, 2015; Giwah et al., 2019). Consistent with the original relationship of the PMT, the hypothesis is as follows:

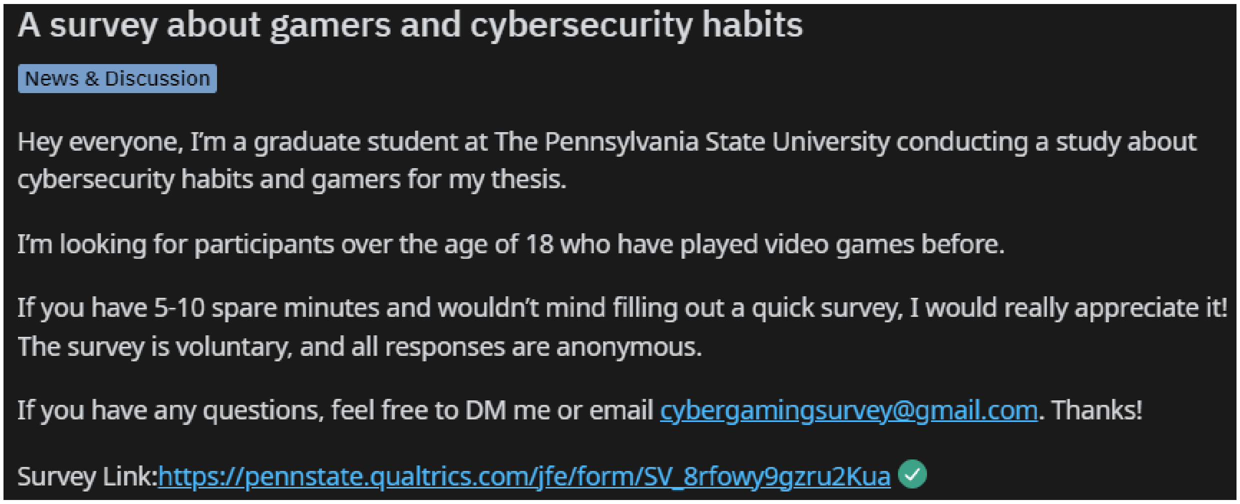
H5: Response Cost will have a negative relationship with the recommended security behavior.

Chapter 4

Methodology

Data Collection

In this study, a self-reported web survey hosted by Qualtrics was used to test the theoretical model derived from the PMT. General security behaviors and beliefs are assessed to gain a holistic understanding of an individual's security intentions. The method collection consists of a snowball sampling technique of members of the author's social network in addition to convenience sampling in the social media community, Reddit. A variety of popular gaming-focused subreddits were sampled. The participants for this study consisted of adults 18 years or older who have played video games before. No personal identifiable information was collected from the participants. An example of a survey invitation post on Reddit is shown in **Figure 6** below:



A survey about gamers and cybersecurity habits

Hey everyone, I'm a graduate student at The Pennsylvania State University conducting a study about cybersecurity habits and gamers for my thesis.

I'm looking for participants over the age of 18 who have played video games before.

If you have 5-10 spare minutes and wouldn't mind filling out a quick survey, I would really appreciate it! The survey is voluntary, and all responses are anonymous.

If you have any questions, feel free to DM me or email cybergamingsurvey@gmail.com. Thanks!

Survey Link:https://pennstate.qualtrics.com/jfe/form/SV_8rfowy9gzru2Kua

Figure 6. Survey Invitation Post on Reddit

Measurements

The survey consists of 15 questions. All questions assessing PMT constructs will be conducted using a 5-point Likert scale with responses ranging from “Strongly disagree” to “Strongly agree”. Other qualitative questions are self-developed to provide context and investigate other experiences that gamers may have had. The web survey consists of 4 sections. The first section contains demographic items. The second section contains items for gaming habits and preferences. The third section contains PMT items for perceived susceptibility, perceived severity, self-efficacy, response efficacy, and response costs in addition to an attention check question. The final section contains an optional open-ended question for the participants to include any information they may feel is relevant to the study. Items that had been validated in relevant behavioral security research studies were selected to ensure their validity and reliability when measuring the model. These items were slightly reworded for general device use as necessary. All relevant items in the survey for data analysis are presented in **Appendix A**.

Data Screening

Data screening was performed to identify responses that may have impacted the data quality. Incomplete responses were not included in the study. Survey responses that failed the attention check question or contained zero variance were removed as well. A total of 129 responses were collected. Among these, 7 responses were discarded for failing the attention check question, leaving a total of 122 responses for data analysis.

Chapter 5

Results

Table 1 provides detailed descriptive characteristics about the respondents. Approximately 49% of the respondents are in the age group 18-24, and over 86% of respondents have been playing video games for more than 10 years.

Measure	Value	Frequency (%)
Gender	Male	76 (62.3)
	Female	34 (27.9)
	Non-binary	11 (9.0)
	Prefer not to say	1 (.8)
Age Range	18-24	60 (49.2)
	25-34	36 (29.5)
	35-44	19 (15.6)
	45-54	5 (4.1)
	55-65	1 (.8)
	65+	1 (.8)
Total Gaming Time	< 6 months	0 (0)
	6 months - 1 year	1 (.8)
	1 year - < 5 years	3 (2.5)
	5 years - < 10 years	12 (9.8)
	10 years+	106 (86.9)

Table 1: Descriptive Statistics Table

Table 2 displays the device categories that are used to play video games. Personal computers are the most popular gaming device of choice with use from approximately 87% of respondents, while mobile devices only serve as gaming devices for approximately 45% of respondents.

Measure	Value	Frequency
Device Type	Mobile Device	55 (45.1)
	Game Console	73 (59.8)
	Personal Computer	106 (86.9)

Table 2: Gaming Device Table

Table 3 shows the usage distribution of different console types among the respondents that use gaming consoles. The Nintendo Switch is the most popular console with usage from approximately 63% of respondents that game on a console, while the Wii is only used by approximately 15% of the same group.

Measure	Value	Frequency
Console Type	Nintendo Switch	46 (63.0)
	Xbox	25 (34.2)
	PlayStation	33 (45.2)
	Wii	11 (15.1)
	Other	19 (26.0)

Table 3: Console Type Table

Table 4 displays the game genres that respondents play on a regular basis. Approximately 57% of respondents regularly play fighting-type games, while only approximately 10% of respondents often play rhythm games.

Measure	Value	Frequency
Game Genre	Shooter	45 (36.9)
	MOBA	48 (39.3)
	MMORPG	17 (13.9)
	RPG	21 (17.2)
	Action	22 (18.0)
	Adventure	56 (45.9)
	RTS	13 (10.7)
	Turn-based Strategy	15 (12.3)
	Platform	32 (26.2)
	Rhythm	12 (9.8)
	Sports	19 (15.6)
	Fighting	70 (57.4)
	Racing	19 (15.6)
	Other	31 (25.4)

Table 4: Game Genre Table

Data Analysis

Data analysis occurred in a two-stage process. First, a confirmatory factor analysis was conducted to validate the measurement items. Then, a structural equation modeling method is used to assess the research model. Partial Least Squares (PLS) regression, a structural equation modeling method, is used to test the model. Many prior studies in the security behavior domain utilize PLS as their method of choice, supporting its usage in similar studies as well (Yoon et al., 2012; Tsai et al., 2016; Hanus & Wu, 2016).

Reliability and Validity of Measurement Items

Convergent validity is established when the loadings of each item were all significant and above the cut-off value of 0.60 (Hulland, 1999). The t-values and factor loadings of the measure items can be seen in **Table 5**. All t-values are above 1.96. The factor loading of all items are also significant and loaded highly.

Construct		1	2	3	4	5	6	T-value
PV	PV1	**.771**	.079	-.096	.084	.130	.025	6.466
	PV2	**.759**	.170	.064	.016	-.025	.060	6.627
	PV3	**.754**	.121	-.123	-.126	.123	.102	6.027
	PV4	**.777**	-.031	-.147	-.092	.090	.092	6.287
	PV5	**.834**	.223	-.006	-.183	.090	-.018	4.622
PS	PS1	.211	**.809**	-.065	.140	-.006	.080	6.117

	PS2	.157	**.810**	-.028	.122	.100	.003	6.140
	PS3	-.008	**.912**	-.034	-.013	.045	-.018	4.579
	PS4	.135	**.816**	-.208	-.025	-.009	.019	6.170
	PS5	.078	**.711**	-.039	-.162	.090	.228	6.936
SE	SE1	-.084	-.123	**.779**	.080	-.306	.172	5.057
	SE2	-.170	-.136	**.877**	.097	-.151	-.043	3.939
	SE3	-.038	-.088	**.797**	.029	-.296	.114	5.386
RE	RE1	-.060	.091	.207	**.820**	-.081	.084	4.728
	RE2	-.058	.059	.113	**.868**	-.012	.047	2.698
	RE3	-.103	-.090	-.136	**.823**	-.027	-.165	6.190
RC	RC1	.111	.017	-.031	.064	**.795**	-.039	6.560
	RC2	.130	.011	-.183	-.120	**.769**	-.055	6.035
	RC3	-.007	.142	-.299	-.011	**.791**	-.132	3.660
	RC4	.118	.042	-.220	-.074	**.744**	.026	5.890
SB	SB1	.143	.071	.210	-.058	-.103	**.836**	7.304
	SB2	.076	.133	-.008	.035	-.065	**.891**	7.437

Table 5: Confirmatory Factor Analysis Results

Discriminant validity was confirmed by meeting the following criteria: (1) measurement items load highly on their assigned construct compared to other constructs in a confirmatory factor analysis, and (2) when the square root of the average variance extracted (AVE) of each construct is larger than the correlation between that construct and any other construct (Gefen and Straub, 2005). **Table 5** demonstrates that all the measurement items loaded were stronger on their respective factors than on other constructs. **Table 6** also shows that the square root of the AVE between two constructs is larger than the correlations between both constructs.

Construct	1	2	3	4	5	6	CCR	AVE
PV	**.78**						.86	.61
PS	.336	**.81**					.91	.66
SE	-.204	-.239	**.82**				.86	.67
RE	-.131	.082	.167	**.84**			.88	.70
RC	.187	.188	-.493	.099	**.78**		.86	.60
SB	.124	.106	.167	-.030	-.183	**.86**	.85	.75

CCR: Composite Construct Reliability
AVE: Average Variance Extracted
Bold = Square root of AVE

Table 6: Average Variance Extracted and Correlation Matrix

In Table 6, composite construct reliability coefficients were calculated to assess the reliability of measurement items. All composite reliabilities were above 0.70, and all AVEs were above 0.50. As a result, high levels of reliability were obtained for the measured items.

Hypothesis Testing Results

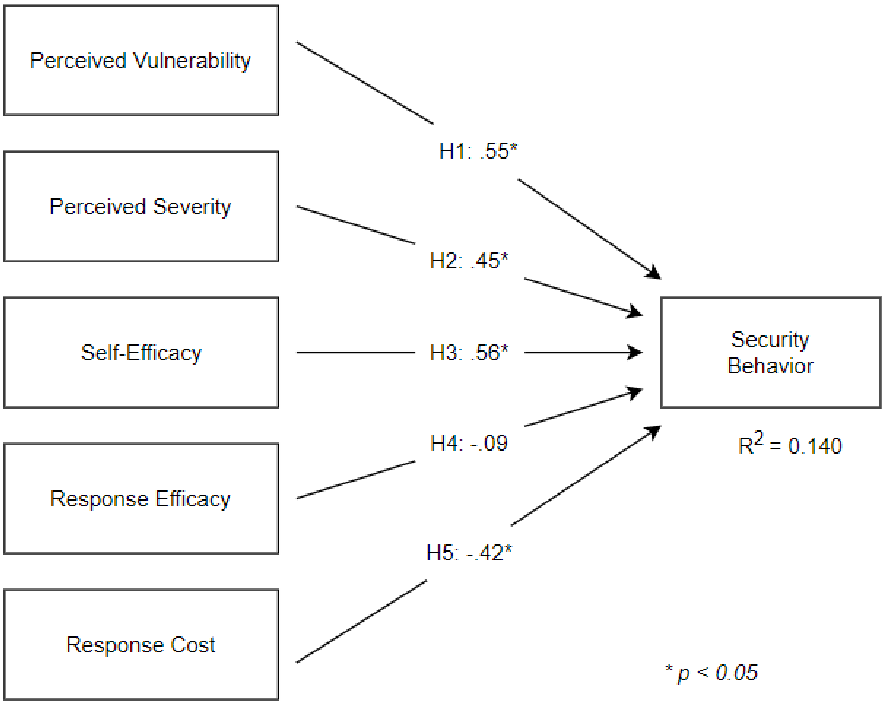


Figure 7: Research Model Results

Having assessed the structural model, hypothesis testing was consequently performed. **Figure 7** displays the paths and their significance on the structural model. **Table 7** contains the coefficients and their t-values for each dependent construct as well as the coefficient of determination (R^2) for the independent construct. The results show that the majority of hypotheses were supported.

Hypothesis	Path	Path Coefficient	t-value
H1	PV -> SB	.55	2.399*
H2	PS -> SB	.45	2.120*
H3	SE -> SB	.56	2.413*
H4	RE -> SB	-.09	-.517
H5	RC -> SB	-.42	-.1963*
Security Behavior R^2: 0.140			*Significant at the 0.05 level

Table 7: Hypothesis Testing Results

Chapter 6

Discussion

The primary purpose of this research was to examine the factors that affect the information security behavior of gamers. The research model contains a total of 5 hypothetical relationships that were tested using PLS regression and explains 14.0% of the variance in computer security behavior. The results demonstrate that certain constructs found in the PMT are more effective than others in motivating gamers to adopt security behavior. Perceived vulnerability, perceived severity, response cost, and self-efficacy were found to have a strong impact on security behavior. However, response efficacy had no significant impact on security behavior.

Although perceived vulnerability to threats has generally been found to not influence security behavior in PMT (Mwagwabi, 2015; Woon et al., 2005; Yoon et al., 2012; Tsai et al., 2016; Giwah et al., 2019), the results of this study indicate that perceived vulnerability does influence security behavior among gamers. These results are consistent with Chang et al. (2018), Tu et al. (2019), and Giwah et al. (2019). The difference in results may imply that there is a distinct difference between gamers and other populations when perceiving risk. Gaming relies upon various forms of technology that are constantly exposed to security threats. Therefore, it is likely that many gamers have experienced some form of cyber-attack during their lives.

Survey responses show that many gamers have experienced attempted cyber-attacks. Many anecdotes detail account information not limited to gaming being compromised. However, other responses also show that gamers are aware of security threats and the implications that they have. Accordingly, perceived severity was found to have a positive influence on security behavior. These results are consistent with the large majority of prior PMT studies conducted regarding security behavior (Woon et al., 2005; Herath & Rao, 2009; Vance et al., 2012; Yoon et al., 2012; Crossler & Bélanger, 2014; Dang-Pham & Pittayachawan, 2015; Chang et al., 2018; Tu et al., 2019). A reason for this may be the surge in attention given to cybersecurity and surrounding issues in recent years. Security-related news such as database breaches and ransomware attacks have become increasingly common, exposing many more individuals, gamers included, to these attacks and their effects. Hackers and scammers in games are also commonly seen across various genres. Those with exposure to these threat actors may have a greater sense of perceived severity towards security.

Self-efficacy was found to have a significant positive impact on gamers' security behavior as hypothesized. These findings confirm the results obtained from many past PMT studies (Woon et al., 2005; Herath & Rao, 2009; Vance et al., 2012; Yoon et al., 2012; Crossler & Bélanger, 2014; Dang-Pham & Pittayachawan, 2015; Mwagwabi, 2015; Chang et al., 2018; Giwah et al., 2019; Tu et al., 2019). This may be due in part to the increased experience with technology that gamers possess, allowing them to more easily establish protective measures against security threats. Another possible explanation is the increase in security education offered today. Strong passwords, two-factor authentication, and distrust of unknown files can be considered common guidance given, especially to the younger population. A little less than 95%

of survey respondents are under the age of 45 which may further support the significance of the self-efficacy construct. Some survey respondents also indicated an increased interest in protective security behavior after experiencing a security-related issue themselves. An increased exposure to technology through gaming may cause the gamer to be at greater risk of a security threat.

Response efficacy has been generally found to have a significant positive impact on security behavior. However, the results of this study differ from prior studies (Woon et al., 2005; Herath & Rao, 2009; Vance et al., 2012; Yoon et al., 2012; Crossler & Bélanger, 2014; Dang-Pham & Pittayachawan, 2015; Mwagwabi, 2015; Tsai et al., 2016; Chang et al., 2018; Giwah et al., 2019; Tu et al., 2019) in finding that response efficacy has no significant influence when applied to the gamer population. In fact, some survey respondents indicated their confidence in protective measures to have decreased over time due to their inability to effectively prevent security attacks. Due to the prevalence of successful security attacks in recent times, this belief may be more widespread, leading to a lack of support for response efficacy.

Many prior PMT studies have found response cost to have a negative effect on security behavior. The results of this study are consistent with previous findings. Gamers are less likely to perform protective security behaviors if the costs of doing so are high.

Contributions and Implications

This study explores the factors that influence gamers' information security behaviors by proposing a research model based on the PMT and empirically supporting the model with 122 gamers. As far as the author is aware, this is the first paper done on exploring the information security behavior of the gamer population.

The results of this study show that perceived vulnerability has a positive effect on gamer security behavior. This finding has practical applications. Raising one's awareness of security threats should increase their adoption of security behaviors. Many gamers have experienced various security attacks such as phishing, malware, and ransomware firsthand, perhaps heightening their sense of perceived vulnerability. Security training should aim to include the tangible impact of these attacks in conjunction with protective information to best enhance security behavior.

This study also shows that response efficacy did not have an effect on the security behavior of gamers. In turn, the gamer perspective on protective measures should be assessed. An increase in experience with security tools as well as the failure of the tools to successfully secure data could have an impact on the effects of gamer perception of response efficacy. The effectiveness of protective security software and other measures should also be examined. Tools that successfully defend against security threats are more likely to be used, and evidence of their effectiveness should be clearly defined and easily accessible.

Other findings confirm the results of prior PMT studies. The severity of security threats should continue to be emphasized to promote effective security behavior. Teaching specific ways to implement security measures to increase self-efficacy will also help with adopting proper security habits. Security training should be a regular occurrence to reinforce the importance of cybersecurity among all populations.

Limitations and Future Research

A major limitation of this study is that the population of interest, gamers, is very large, resulting in the use of the snowball sampling method in order to distribute the invitation through Reddit to participate in the survey. Also, the survey did not collect any identifiable information from its respondents, preventing the tracking of invitations and responses that gives way to non-response bias. To further validate the results of the study, the survey should be conducted in more diverse settings using a greater number of gamers.

Data collection was also limited by the survey format - responses relied upon a single instance of self-reported measures of security behavior. To improve understanding of information security behavior, the development and usage of more validated measurement instruments and methods of direct measurement are needed. Direct observation of user behavior remains an area of security behavior research to be further explored with potential for greater insights than a survey response.

Individuals that were a member of the population of interest also expressed doubts in completing the survey. Distribution over Reddit occurred using a relatively new account, and suspicions regarding the validity of the post as well as the survey link were called into question. As a result, certain gamers did not complete the survey, resulting in a loss of data. Future recruitment methods should be improved to prevent distrust and encourage participation.

Additionally, just 14% of the variance of information security behavior ($R^2 = 0.140$) is explained by the variables of PMT. To improve the model's explanatory power, additional variables can be included to extend the framework. These potentially include subjective norm, security intentions, prior experience and more. Further studies with an extended version of the PMT can provide a richer understanding of the motivations behind gamer security behavior.

While gaming-related characteristics were not assessed in relation to security behavior in this study, future research can examine various gaming measures and determine their impact on security behavior. These measures can include types of gaming devices, game genres played, or time spent playing video games, furthering methods to form good security habits. Video games and their role in security habit adoption is another area of interest as well.

Future research can also include a greater variety of survey questions pertaining to security behavior by asking about: two-factor authentication, password strength, manual privacy settings, and more. Additional questions can also be added to measure constructs such as self-efficacy and response efficacy.

Appendix

This section contains all of the questions in the survey that were used for analysis.

Descriptive and Gaming Questions

Question	Possible Responses
What gender do you identify as?	Male, Female, Non-binary/third gender, Prefer not to say, Prefer to self describe (open-ended)
Please specify your age range:	18-24, 25-34, 35-44, 45-54, 55-64, 65+
On average, how many hours do you play video games **per week**?	0-100 hours
How long have you been playing video games for?	< 6 months, 6 months - 1 year, 1 year - 5 years, 5 years - 10 years, 10 years+
If you are willing, please share any experiences that you have had related to cybersecurity and video games (ex. gaming account hacked, console hacking etc.)	(open-ended)

PMT Questions

Measure	Items
Perceived Vulnerability	I could be subject to a serious information security threat
	I am facing more and more information security threats
	I feel that my devices could be vulnerable to a security threat
	It is likely that my devices will be compromised in the future

	My information and data is vulnerable to security breaches
Perceived Severity	A security breach on my devices would be a serious problem for me
	Loss of information resulting from hacking would be a serious problem for me
	Having my confidential information on my device accessed by someone without my consent or knowledge would be a serious problem for me.
	Having someone successfully attack and damage my device would be very problematic for me
	I view information security attacks on me as harmful
Self-efficacy	I have the resources and the knowledge to take the necessary security measures
	I can protect my devices by myself
	I can enable security measures on my devices
Response Efficacy	Enabling security measures on my devices will prevent security breaches
	Implementing security measures on my devices is an effective way to prevent hackers
	Enabling security measures on my devices will prevent hackers from stealing my identity
Response Cost	Taking security measures inconveniences me
	There are too many overheads associated with taking security measures to protect my devices
	Taking security measures would require considerable investment of effort
	Implementing security measures on my devices would be time consuming
Security Behavior	I have installed security software on my devices
	I use security software (anti-virus/anti malware)

References

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31.

Bryant, B., & Saiedian, H. (2021). An evaluation of videogame network architecture performance and security. *Computer Networks*, 192, 108128.

Chang, S. H., Hsu, H. M., Li, Y., & Hsu, J. S. C. (2018). The influence of information security stress on security policy compliance: a protection motivation theory perspective.

Chen, H., & Li, W. (2017). Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. *Information & Computer Security*.

Chen, L., Shashidhar, N., Rawat, D., Yang, M., & Kadlec, C. (2016, February). Investigating the security and digital forensics of video games and gaming systems: A study of PC games and PS4 console. In 2016 International Conference on Computing, Networking and Communications (ICNC) (pp. 1-5). IEEE.

Claar, C. L. (2011). *The adoption of computer security: An analysis of home personal computer user behavior using the health belief model*. Utah State University.

Clough, J. (2015). Principles of cybercrime. Cambridge University Press.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *computers & security, 26*(1), 63-72.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *45*(4), 51-71.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281-297.

Eklund, L. (2016). Who are the casual gamers? Gender tropes and tokenism in game culture. *Social, casual and mobile games: The changing gaming landscape*, 15-30.

Entertainment Software Association. (2021). 2021 Essential Facts About the Video Game Industry. Washington, DC; Entertainment Software Association.

Forrester, V. V. (2019). *User Information Security Behavior in Professional Virtual Communities: A Technology Threat Avoidance Approach* (Doctoral dissertation, Nova Southeastern University).

Furnell, S., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. Computers & Security, 75, 1-9.

Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2019). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital*.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, *18*(2), 106-125.

Hewett, K. J., Pletcher, B. C., & Zeng, G. (2020). The 21st-century classroom gamer. *Games and Culture*, *15*(2), 198-223.

Hussain, Z., Griffiths, M. D., & Baguley, T. (2012). Online gaming addiction: Classification, prediction and associated risk factors. *Addiction Research & Theory*, *20*(5), 359-371.

Kranz, J., & Haeussinger, F. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior.

König, J. A., & Wolf, M. R. (2018). GHOST: an evaluated competence developing game for cybersecurity awareness training. *International Journal on Advances in Security Volume 11, Number 3 & 4, 2018.*

Kuss, D. J. (2013). Internet gaming addiction: current perspectives. *Psychology research and behavior management*, *6*, 125.

Lam, L. T. (2014). Internet gaming addiction, problematic use of the internet, and sleep problems: a systematic review. *Current psychiatry reports*, *16*(4), 1-9.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90.

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the association for information systems*, *11*(7), 1.

Mohr, S., & Rahman, S. S. (2011). IT security issues within the video game industry. *arXiv preprint arXiv:1111.1769.*

Mwagwabi, F. M. (2015). *A Protection Motivation Theory approach to improving compliance with password guidelines* (Doctoral dissertation, Murdoch University).

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

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.

Rosenstock, I. M. (1974). Historical origins of the health belief model. Health Education Monographs, 2, 328–335.

Royse, M. A., & Newton, S. E. (2007). How gaming is used as an innovative strategy for nursing education. *Nursing Education Perspectives*, *28*(5), 263-267.

Sanford, K., & Madill, L. (2006). Resistance through video game play: It's a boy thing. *Canadian Journal of Education/Revue canadienne de l'éducation*, 287-306.

Schymik, G., & Du, J. (2018). Student intentions and behaviors related to email security: an application of the health belief model. *Journal of Information Systems Applied Research*, *11*(3), 14.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99).

Stretcher, V. S., & Rosenstock, I. M. (1997). The health belief model. In K. Glanz, F. M. Lewis, & B. K. Rimer (Eds.), Health behaviors and health education: Theory, research and practice (pp. 41–59).San Francisco: Jossey-Bass.

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 & Security*, *59*, 138-150.

Tu, C. Z., Adkins, J., & Zhao, G. Y. (2019). Complying with BYOD security policies: A moderation model based on protection motivation theory. *Journal of the Midwest Association for Information Systems (JMWAIS)*, *2019*(1), 2.

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224.

Veltri, N., Krasnova, H., Baumann, A., & Kalayamthanam, N. (2014). Gender differences in online gaming: a literature review.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security.

Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of information systems education*, *23*(4), 407-416.

Young, D. K., Carpenter, D., & McLeod, A. (2016). Malware avoidance motivations and behaviors: A technology threat avoidance replication. *AIS Transactions on Replication Research*, *2*(1), 8.

Zhao, C. (2018, April). Cyber security issues in online games. In *AIP Conference Proceedings* (Vol. 1955, No. 1, p. 040015). AIP Publishing LLC.

Zirawaga, V. S., Olusanya, A. I., & Maduku, T. (2017). Gaming in education: Using games as a support tool to teach history. *Journal of Education and Practice*, *8*(15), 55-64.

ACADEMIC VITA

John Z. Zhuang

jbz5263@psu.edu
zjohn2019@gmail.com

Education

The Pennsylvania State University, University Park, PA **May 2023**
The Schreyer Honors College
Master of Science in Cybersecurity Analytics and Operations
Bachelor of Science in Cybersecurity Analytics and Operations
Dean's List
The President's Freshman Award, The Evan Pugh Scholar Senior Award

Achievements and Certifications

AWS Certified Cloud Practitioner **August 2022**

- Knowledgeable in AWS Cloud concepts and implementation of various cloud initiatives

CompTIA CySA+ Certified **August 2020**

- Proficient in analysis and defense techniques leveraging data and tools to identify risks to an organization, and apply effective mitigation strategies

CompTIA Security+ Certified **July 2019**

- Proficient on the latest trends and techniques in risk management, risk mitigation, threat management and intrusion detection

Activities & Leadership Experience

Booz Allen Hamilton **June 2022-August 2022**

- Developed a web application that visualizes MITRE ATT&CK coverage for clients by generating a heatmap
- Created MITRE ATT&CK pattern mappings for over 70 threat signatures across Carbon Black, Defender, and Splunk
- Devised Carbon Black filters to help reduce the volume of false positive alerts for the SOC

Security Risk Advisors **May 2021-August 2021**

- Assessed client networks, infrastructure, and web applications to discover security vulnerabilities
- Conducted red and purple team exercises to evaluate clients' security posture and incident response
- Prepared recommendations to strengthen security posture and mitigate identified vulnerabilities

Research Assistant **January 2021-Present**

- Author surveys and utilize statistics to develop a connection between technology usage and cybersecurity habits
- Conduct literature reviews of relevant papers to synthesize a thesis concerning cybersecurity behavior

Research Assistant **November 2019-March 2021**

- Utilized statistics and cluster maps to develop a connection between art and music
- Developed models to plot different aspects of art such as color saturation, shapes, and textures

Leadership JumpStart Program **July 2019-December 2019**

- Selected as one of 20 students in the Schreyer Honors College to participate in a semester-long program focusing on the importance of leadership and how to best implement and improve one's own leadership skills
- Contributed to the development and execution of a service plan raising awareness about kids with autism and special needs
- Participated in workshops and events with a heavy emphasis on public speaking and presentation skills

Competitive Cyber Security Organization **September 2019-Present**

- Participate in cybersecurity conferences and competitions to practice and implement skills
- Train in penetration testing, cryptography, password cracking, web hacking, and more
- Prepare and maintain virtual machines to become familiar with Ubuntu, Kali Linux, and vulnerable machines

SKILLS & INTERESTS

- Conversational Mandarin and Spanish
- Java, Python, Visual Basic, SQL, Linux, Windows, Log Analysis, Carbon Black, Splunk, AppAnyRun, MITRE ATT&CK
- Music Composition