THREE ESSAYS ON INDIVIDUALS' VULNERABILITY TO SECURITY ATTACKS IN ONLINE SOCIAL NETWORKS: FACTORS AND BEHAVIORS

by

Neshat Beheshti

A Dissertation Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

in Management Science

at

The University of Wisconsin-Milwaukee

May 2019

ABSTRACT

THREE ESSAYS ON INDIVIDUALS' VULNERABILITY TO SECURITY ATTACKS IN ONLINE SOCIAL NETWORKS: FACTORS AND BEHAVIORS

by

Neshat Beheshti

The University of Wisconsin-Milwaukee, 2019
Under the Supervision of Professors Fatemeh (Mariam) Zahedi and Huimin Zhao

With increasing reliance on the Internet, the use of online social networks (OSNs) for communication has grown rapidly. OSN platforms are used to share information and communicate with friends and family. However, these platforms can pose serious security threats to users. In spite of the extent of such security threats and resulting damages, little is known about factors associated with individuals' vulnerability to online security attacks. We address this gap in the following three essays.

Essay 1 draws on a synthesis of the epidemic theory in infectious disease epidemiology with the social capital theory to conceptualize factors that contribute to an individual's role in security threat propagation in OSN. To test the model, we collected data and created a network of hacked individuals over three months from Twitter. The final hacked network consists of over 8000 individual users. Using this data set, we derived individual's factors measuring threat propagation efficacy and threat vulnerability. The dependent variables were defined based on the concept of epidemic theory in disease propagation. The independent variables are measured based on the social capital theory. We use the regression method for data analysis. The results of

this study uncover factors that have significant impact on threat propagation efficacy and threat vulnerability. We discuss the novel theoretical and managerial contributions of this work.

Essay 2 explores the role of individuals' interests in their threat vulnerability in OSNs. In OSNs, individuals follow social pages and post contents that can easily reveal their topics of interest. Prior studies show high exposure of individuals to topics of interest can decrease individuals' ability to evaluate the risks associated with their interests. This gives attackers a chance to target people based on what they are interested in. However, interest-based vulnerability is not just a risk factor for individuals themselves. Research has reported that similar interests lead to friendship and individuals share similar interests with their friends. This similarity can increase trust among friends and makes individuals more vulnerable to security threat coming from their friends' behaviors. Despite the potential importance of interest in the propagation of online security attacks online, the literature on this topic is scarce. To address this gap, we capture individuals' interests in OSN and identify the association between individuals' interests and their vulnerability to online security threats. The theoretical foundation of this work is a synthesis of dual-system theory and the theory of homophily. Communities of interest in OSN were detected using a known algorithm. We test our model using the data set and social network of hacked individuals from Essay 1. We used this network to collect additional data about individuals' interests in OSN. The results determine communities of interests which were associated with individuals' online threat vulnerability. Moreover, our findings reveal that similarities of interest among individuals and their friends play a role in individuals' threat vulnerability in OSN. We discuss the novel theoretical and empirical contributions of this work.

Essay 3 examines the role addiction to OSNs plays in individuals' security perceptions and behaviors. Despite the prevalence of problematic use of OSNs and the possibility of

addiction to these platforms, little is known about the functionalities of brain systems of users who suffer from OSN addiction and their online security perception and behaviors. In addressing these gaps, we have developed the Online addiction & security behaviors (OASB) theory by synthesizing dual-system theory and extended protection motivation theory (PMT). We collected data through an online survey. The results indicate that OSN addiction is rooted in the individual's brain systems. For the OSN addicted, there is a strong cognitive-emotional preoccupation with using OSN. Our findings also reveal the positive and significant impact of OSN addiction on perceived susceptibility to and severity of online security threats. Moreover, our results show the negative association between OSN addiction and perceived self-efficacy. We discuss the theoretical and practical implications of this work.

To

my parents,

my husband,

and especially my lovely daughter (Shauna)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

First, I would like to express my appreciation to UWM Distinguished Professor Emerita Fatemeh (Mariam) Zahedi, for supporting me during my PhD studies. She patiently guided me throughout my graduate career and provided me with scientific advice. I would also like to thank my committee members: Dr. Huimin Zhao, Dr. Sanjoy Ghose, and Dr. Hemant Jain. I sincerely appreciate their insightful comments and suggestions.

I want to express my genuine appreciation and thanks to Mr. and Mrs. Lubar for their financial support of my research. I also extend my thanks to Dawn Koerten for all the support and guidance that she has given me.

Last and most importantly, I wish to express my gratitude to my family. I thank my beloved husband Mahyar Vaghefi for his love and support. I thank my parents for their enthusiasm and all sacrifices they have made for me and I thank my dear sister Mona for her positive energy and encouragement.

CHAPTER 1

Introduction

In recent years, the pervasive use of online social networks (OSNs) has become an indispensable part of individuals' daily lives. Individual users spend a considerable amount of time on OSNs to connect to other people and share their interests, opinions and daily activities. However, the popularity of OSNs makes them as main focus of attackers who can easily harm large number of online users. There are a large number of attacks in OSNs which threaten individuals and their societies. Therefore, having a safe and secure way of using OSNs is a challenging task for individuals. The study of individual-level factors that contribute to threat vulnerability can help improve security in OSNs. Individuals' connections, strength of ties, levels of activity, and types of interest are factors which can be related to threat vulnerability in OSNs. Moreover, individuals' addiction to OSNs can impact individuals' security perceptions and behaviors.

In this three-essay dissertation, we examine the security consequences of using OSNs at the individual level. We investigate individual factors and security behaviors that affect individuals' threat vulnerability in OSNs. The first essay explores the role of individuals in propagating security attacks and the factors that contribute to individuals' vulnerability to such attacks. The second essay extends Essay 1's model and investigates the impacts of individuals' interests and similarities of interest with their friends on their threat vulnerability.

The third essay explores OSN-addicts' brain systems and the effects of these systems on individuals' threat perceptions and coping efficacies in OSNs. This dissertation makes novel

contributions to theoretical development, data collection and analysis methods, and provides practical implications for promoting awareness among all entities of OSNs—individual users, organizations, policy makers and OSN administrators—about individual factors that contribute to threat propagation in OSNs as well as controlling individuals' level of OSN use to prevent addiction to these platforms, and the impact of OSN addition on security behaviors.

Essay 1: Factors Associated with Individuals' Vulnerability to Security Attacks and Their Roles in Propagating Attacks

Individuals are identified as the weakest links in security studies. However, little is known about the factors that make individuals vulnerable to security attacks and the role individuals play in spreading such attacks. In this study, we address this gap by answering two research questions: 1) What are the factors associated with individuals' threat propagation efficacy? 2) What are the factors associated with individuals' threat vulnerability? The first question focuses on the extent of individuals' roles in unwittingly propagating security threats to others in OSNs. The second question emphasizes the extent to which individuals are vulnerable to security threats due to their OSN relationships. To address these research questions, we build on a synthesis of the disease propagation epidemic theory and social capital theory to formulate a conceptual model that identifies key individual-level factors that contribute to attack propagation in OSNs. The source of data in this study is public postings on Twitter. We use data classification and data filtering to create a dataset of more than 8,000 Twitter users. The dependent variables are measured using the literature on disease propagation and vulnerability in the epidemic theory. We rely on the social capital theory to formulate our conceptual model's independent variables as patterns of connections, strengths of relationships and levels of activities. Our results identify significant

factors that play a role in individuals' propagation efficacy and threat vulnerability. This study makes novel theoretical contributions and provides managerial implications for individuals, policy makers and OSN administrators.

Essay 2: The Role of Communities of Interests in Individuals' Vulnerability to Online Security Attacks

Individuals reveal their interests online by posting on OSNs and following their favorite pages or people. OSN owners and other companies benefit from individuals' revealed interests by using the information to identify potential customers and target audiences. However, revealing interests online may have negative consequences for individuals, including violating their security and privacy. Prior studies have shown that high exposure of individuals to their topics and activities of interest can decrease their ability to evaluate the risks associated with it. Individuals with poor self-control may pursue their interests regardless of the associated risks. In online environments, this gives attackers a chance to target people based on what they are interested in. However, interest-based vulnerability is not just a risk factor for individuals themselves. It could be damaging to their friends as well. Social studies have reported that similar interest binds people and leads to friendship, and friends share common interests. This similarity can increase a sense of connectedness and increases trust among friends. This trust makes individuals more vulnerable to security attacks. Security attackers take advantage of such trust among friends in various ways, such as sending messages and emails from hacked accounts or posting fraudulent links on hacked persons' pages. This activity propagates security attacks within friendship networks.

Despite the potential importance of interest in the propagation of online security attacks, the literature on this topic is scarce. We address this gap by focusing on two research questions 1) Are revealed individuals' interests in OSNs associated with their vulnerabilities to security threats in OSNs? If so, which interest types are associated with individuals' vulnerability in such platforms, 2) Do similarities of interest among individuals and their friends play a role in individuals' vulnerabilities to security threats in OSNs? We answer these research questions by identifying the communities of interest in OSNs, computing similarity of interest and testing their associations with individuals' vulnerability to online security attacks. The theoretical foundation of this work is a synthesis of dual-system theory and the theory of homophily. Detecting communities of interest in OSNs is done with a known algorithm. The data for the empirical analysis is obtained from publicly available posts on Twitter.

The results show that certain categories of communities of interests such as pop music, video games, business leaders and political views are associated with individuals' online threat vulnerability. Moreover, our findings reveal that similarities of interest among individuals and their friends play a role in individuals' threat vulnerability in OSNs. This study contributes to both theory and practice and provides insights for individuals, OSNs administration and policy makers.

Essay 3: The Role of Addiction to Online Social Networks in Individuals' Online Security Behaviors

Individuals use OSNs to build and maintain their social relationships. As people enjoy their online connectedness and access to information about family, friends, and other individuals, the probability of excessive use of OSNs increases. Uncontrolled and compulsive behavior in using

OSNs with unpleasant consequences can be examined from an addiction perspective. Addiction to OSNs is a part of technology addiction that is defined as an individual's maladaptive psychological state of dependency on IT use. In spite of the importance of OSN addiction and the risks it can pose, there is inadequate research on OSN-addicted users' brain-system functionalities, online security perceptions, and security behaviors. We address these gaps by answering the following research questions: 1) What are the roles of brain systems in OSN addiction? 2) What is the role of OSN addiction in the addicted users' security perceptions and security behaviors? To address these questions, we develop the Online Addiction Security Behavior (OASB) theory and conceptual model by synthesizing two theories: dual-system theory from cognitive-neuroscience and the extended protection motivation theory. The conceptualized model is tested based on 691 survey observations from OSN users. The analysis method is structural equation modeling (SEM). Our results show that OSN addiction is rooted in an imbalance between two brain systems. OSN addicts have strong impulsive cognitive-emotional preoccupation with using OSNs. Our results also reveal the significant impact of OSN addiction on perceived threat susceptibility, severity and self-efficacy in coping with threats. OSN addiction is associated with individual's threat susceptibility and severity perceptions about online security threats. Moreover, OSN addicts have low self-efficacy in dealing with security threats. Our finding accentuates the importance of security from OSN addicted perspectives and provides insights for the managers and policymakers regarding the role of OSN addiction in online security threats.

CHAPTER 2

Essay 1: Factors Associated with Individuals' Vulnerability to Security Attacks and Their Roles in Propagating Attacks

2.1. Introduction

Along with increasing reliance on the Internet, security threats have increased exponentially. People use online social networks (OSNs) to share personal information and stay connected (Utz 2015). OSN is defined as a web-based service with four main attributes: 1. digital profile, 2. relational ties, 3. search and privacy, and 4. network transparency (Kane et al. 2014). Compared to traditional social networks, OSNs entail new opportunities and risks. In OSNs, the spread of information happens easily and quickly—almost in real time. The volume of shared information is high, and individuals share information globally. In doing so, however, individuals get exposed to potential threat attacks (Gross and Acquisti 2005).

Security threats in OSNs are classified into four broad types: privacy breaches, viral marketing, network structural attacks and malware attacks (Gao et al. 2011). Among these threats, malware attacks include worms such as Trojan horses, spyware, and viruses, and they pose growing problems in OSNs (Guo et al. 2016). Examples of malware attacks include Koobface worms which target OSNs, and a clickjacking worm that propagates malicious links and entices users to click on a link that leads them to a fake page (Grier et al. 2010). Malware attacks are propagated in OSNs due to the high frequency of interactions among people in such

environments (Gao et al. 2011). In addition, interactions in OSNs promotes users' trust in their friends' posts and links, thus facilitating the propagation of malware (Mansfield-Devine 2008). Hackers abuse this trust by compromising individuals' accounts on OSNs to lure and infect their friends. Furthermore, it takes individuals some time to discover that their accounts have been infected, thus giving hackers plenty of time to carry out their criminal activities (Eagle et al. 2013). According to a 2009 Kaspersky Labs report, OSNs propagate spam and malicious threats faster than other hacking methods such as email spams. It is estimated that about 8% of the links posted on Twitter are malicious links that contain scam, malware or phishing websites that lure people with free offerings, such as music, games, books, jewelry, and electronics (Grier et al. 2010). Thus, hackers and cybercriminals have many opportunities to attack users in OSNs and make them vulnerable to fraud (Liang and Xue, 2010, Vance at al. 2012). Such security attacks could be costly at personal and business levels. Hackers abuse users' sensitive information such as social security or credit card numbers for financial fraud, and accumulate individuals' other personal information for further attacks and profit. In a 2012 security breach, the personal information of about 117 million users in the LinkedIn network was compromised and sold in dark websites (Franceschi-Bicchierai 2016).

Although OSNs offer security policies to protect users' profile information, they cannot prevent attacks propagated by their neighbors. Therefore, individuals lack the information and tools to protect themselves from all breaches and attacks. The literature has reported extensively that individuals' online behaviors impact the security of both internet users and the internet infrastructure (Noyes 2007, Anderson and Agarwal 2010), making users the weakest points in cybersecurity (Schneier 2000, Anderson & Agarwal 2010). However, little is known about what makes a person more vulnerable to security attacks and how an infected person spreads the attack.

In this study, we address this gap by investigating the factors that play a role in individuals' vulnerability and individuals' contagion. This study focuses on malware threat propagation as one of the main types of the threat propagation in OSNs, which is shown as malicious links, malicious posts or photos in OSN that propagate from one user to another through an OSN. We investigate malware threat propagation efficacy and threat vulnerability. We define threat propagation efficacy as the extent of an individual's role in propagating the security threat infection to others in their neighborhoods within the OSN; and we define threat vulnerability as the extent to which individuals are vulnerable to security threats through their pattern of relationships in OSNs. Thus, our research questions are: 1) What are the factors associated with individuals' threat propagation efficacy? 2) What are the factors associated with individuals' threat vulnerability?

To answer the research questions, we draw on the spread of infectious diseases and epidemics. The process of malware propagation has a parallel in the epidemic theory, which studies transmission of diseases in a social network. The epidemic theory identifies the status of individuals regarding the epidemic and how individuals' status change over the time. Since epidemic theory studies propagation of a disease through a social network, there is a need to examine the features of the social network. We, therefore, synthesize the epidemic theory with the social capital theory to conceptualize factors that contribute to individuals' role in malware propagations in OSNs.

Epidemic theory demonstrates that network structure and individual's characteristics have direct relation to both the extent of a disease propagation and the degree of vulnerability of individuals (Rothenberg et al. 1995, Pastor-Satorras and Vespignani 2001, Meyers et al. 2005 and Christley et al. 2005). In the context of security attacks, research reports that network

structures and nature of the connectivity could play a role in the initial stage of diffusion (Yan et al. 2011). However, there is little insight about the way individuals' characteristics and their activities could influence the contagion and the speed of hacking propagation in OSNs. Moreover, there is little research investigating individual factors related to users' vulnerability to malware attacks. Our research strives to address these gaps.

We use Twitter as the source of data in our investigation. Twitter is a popular platform that has more than 200 million users, who post about 400 million tweets per day (Fiegerman 2012, Tsukayama 2013). The widespread and high frequency uses of Twitter around the world makes it an attractive environment for hackers to propagate spams and malwares. Since Twitter is one of the largest OSNs, security threats could impact many users across the globe. The main hacking method in Twitter is compromising accounts, which subsequently are used to spread malware, to access people's messages, and to hack their profiles (Zangerle and Specht 2014).

Subjects in our data are Twitter users, who have tweeted that their Twitter accounts were hacked from July 24, 2017 to October 21, 2017. We measure the patterns of connection, the strengths of relationships and the levels of activities as independent variables in the two proposed models—one model for user propagation efficacy and a second model for user vulnerability.

The method of estimation is regression, which tests the effects of these three independent variables on user efficacy and user vulnerability as the dependent variables. The results show that in-degree centrality, level of activity and strength of relationships have statistically significant effects on both user threat propagation efficacy and user threat vulnerability.

This study makes a number of theoretical and practical contributions. First, this research conceptualizes threat propagation efficacy as users' effectiveness to spread threat to other people; and threat vulnerability as users' ability to take risk from their neighbors. These

conceptualizations provide a new approach for finding influential and vulnerable users in security attacks in OSNs. Our work contributes to the literature by identifying significant individuals within social networks that promote individuals' threat propagation efficacy and individuals' vulnerability. At the practical level, our study provides insights for individuals, platform managers and policy makers who are interested to understand and counter security threat propagation in OSNs. In this research, we demonstrate that individuals have impact on their online friends and also are vulnerable to threats emanating from them. This shows that individuals' protections alone do not guarantee full security in OSNs. Platform managers should provide policies to secure connections and protect trust among users and their friends.

2.2. Literature Review

The literature on information systems security is based on two types of studies: technical context of security models and socio-technical security behaviors (Anderson and Agarwal 2010). Although there is strong literature on information systems security, there is not enough attention to diffusion of threat and determining specific factors which affect diffusion of threat among members of an OSN.

Information diffusion refers to the process of disseminating a piece of information through social interactions. Information diffusion processes are beneficial for all users in OSNs from personal and organizations views. However, diffusion has harmful aspects for both individuals and the whole network when it is performed by malicious people. Therefore, malware diffusion is a special type of information diffusion. This type of diffusion considers the process of transmission malware instead of information. Karyotis and Khouzani (2016, p. 4) define

malware diffusion as “all types of malicious software dissemination in various types of networks”. In the concept of malware diffusion, they refer to two different mechanisms, spreading and propagation. Spreading determines dissemination of malicious software from an attacker to legitimate users. Propagation refers to malicious transfer from one infected legitimate user to another legitimate user. In this study, we study diffusion of malware among infected legitimate users. Therefore, we use the term propagation.

Malware propagation has a long history in literature of small-world networks, scale-free networks, mobile networks and email networks (Watts and Strogatz 1998, Moore and Newman 2000, Pastor-Satorras and Vespignani 2001, Zou et al. 2002 and 2004, Griffin and Brooks 2006, Fleizach et al. 2007). However, malware propagation in OSNs is quite different. In recent years, there are few works related to malware propagation in OSNs. Faghani and Saidi (2009) simulated spread of two worms, XSS and Koobface, in OSNs and proposed that users’ attitude to visit other’s posts, the initial number of infected users and clustered networks are parameters that impact on propagation of XSS. Spreading malware in BrightKite—which is a location-based OSN—is studied using a simulation approach (Yan et al. 2011). The results showed that threat propagation is increased by high cluster networks, users’ activities, initial number of infected users, and probability of clicking on links. Research has also found that number of friends, number of followers and user’s influence (Klout score) can be used in predicting the most vulnerable individuals in Twitter (Wald et al. 2013). Similarly, another study, using simulation, reported the number of followers and probability of clicking on the link are factors which affect the speed of malware propagation (Sanzgiri et al. 2013). A comparison of malware diffusion in fake accounts and compromised accounts in OSN was illustrated by Almaatouq et al. (2016).

A theory-based understanding of security attack dissemination in OSNs networks provides a deeper insight about the process of malware propagation. Developing models for attack dissemination can help assess the process of diffusion and how to control it. Epidemic models are similar to attack propagation. A disease such as influenza, Flu or AIDS can transfer from infected people to non-infected ones in a social network. In a malware dissemination, security attack is the disease and infection constitutes propagation, moving from one infected user to the other.

Furthermore, security attack propagation has some similarity to information diffusion in social networks, albeit harmful and costly type. Research in information diffusion has utilized the epidemic models as well. There are two classical epidemic models, SIS (Susceptible-Infected-Susceptible) and SIR (Susceptible-Infected-Removed). Both models are used in studying propagation of different types of information in social networks such as rumor (Zanette 2002, Kawachi 2008, Shah and Zaman 2011, Zhao et al 2012), financial information (Shtatland and Shtatland 2008, Shive 2010, Burnside et al. 2016), information in mobile networks (Khelil et al. 2002, Kivelä et al. 2012), file sharing in peer-to-peer systems (Euster et al. 2004, Leibnitz et al. 2006) and email (Wu et al. 2004, Wang et al. 2011).

Online information diffusion has been studied using real data from OSNs such as blogs (Adar and Adamic 2005, Gruhl et al. 2004, Leskovek et al. 2007), Twitter (Cha et al. 2010, Kwak et al. 2010, Lerman and Ghosh 2010, Suh et al. 2010, Wu et al. 2011, Romero et al. 2011, Myers et al. 2012), Facebook (Sun et al. 2009, Viswanath et al. 2009, Bakshy et al. 2012) and Flickr (Cha et al. 2009). Recently epidemic models have been used to analyses online information diffusion (Woo and Chen 2016). Recent works about applying epidemic models to online information diffusion are shown in Table 2.1.

Table 2.1 Overview of Applications of Epidemic Theory in Online Information Diffusion Research

Context	Study	Finding
Information Diffusion	Pei et al. 2014	-The best spreaders are located in the k-core across dissimilar social platforms. -Sum of the nearest neighbors' degree is a reliable measure for users' influence when the complete global network structure is unavailable.
	Chen et al. 2012	-Developing a new measurement (local centrality) as a tradeoff between degree-centrality and time-consuming measurements (betweenness centrality and closeness centrality) for finding influential users in spreading information. -This measure is based on nearest and next nearest neighbors of a user. -Comparing with well-known centrality measures, the proposed measure performs better than degree and betweenness centrality, and almost as good as the closeness centrality measure with much lower computational complexity.
	Xiong et al. 2012	-Study information diffusion based on retweeting mechanism in OSNs. -Develop an information propagation model considering a decision state in which users need a time to decide about retweeting the topic. -Individual decision making for retweeting mainly depends on the topic itself.
	Ver Steeg et al. 2011	-People are less likely to become spreaders of information with repeated exposure. -High clustered social networks put individuals in a position that they are exposed to the same information multiple times. -This structural feature slows down the diffusion process and does not contribute to individuals' decisions.
News Diffusion	Abdullah and Wu 2011	-Structure of Twitter facilitates the process of news diffusion among individuals. -Individuals' similarity in terms of location or interest can directly affect the process of diffusion.
Topic Diffusion	Woo and Chen 2016	-SIR model is a proper model for topic diffusion in the web forum. -Expected number of initial authors, duration and extremity of each topic can be predicted by the model. -Sale topics have fewer initial authors, high infection rates and low recovery rates compared to stock topics.
	Woo et al. 2011	-Order propagation of rough topics in a web forum and the number of authors for each topic.
URL Diffusion	Lü et al. 2011	-Developing a new random-walk based ranking (LeaderRank) for identifying influential people in information diffusion. -LeaderRank outperforms PageRank in terms of ranking effectiveness, and robustness against manipulations and noisy data.
Emotion Diffusion	Wang et al. 2015	-Users prefer to repost messages with happy emotions whereas few users repost tweets that reflect anger. -Retweets do not change the emotion of the original tweets.
Video Diffusion	Li et al. 2014	-Activeness is the main factor for user to initiate and watch videos in OSN. -Active users that share hundreds of videos do not necessarily watch that many. -Videos can quickly be propagated among friends in the OSN. -The process of video sharing is different in OSNs compared to other platforms such as email because of difference in the property of propagated content and system design.

		-Initiating more video shares does not necessarily help attract more friends for a user.
Meme Diffusion	Bauckhage 2011	-The main memes propagations happen in homogenous online communities and OSNs.
Product Diffusion	Xu et al. 2008	-Frequency and volume of interaction among users in an OSN determine influential individuals in product adoption. -Number of followers of a user positively affect adoption of a product by the others. -User's age and number of days as ae member in a social network negatively affect product adoption.
	Leskovec et al. 2007	-Number of recommendations in a blog has a positive effect on the probability of purchasing a product before gaining a saturation point. -Increasing the number of recommendations among the same users decreases the probability of purchasing the product. -Structure of connection in communities have positive effect on product diffusion.
Rumor Diffusion	Cheng et al. 2013	-Degree of information propagation depends on the trustworthiness of connections between users. -Likelihood of propagation increases in strong ties. -Users having higher connections can maximize spread of rumors.
	Zhao et al.2011	-Determining refusing rate and forgetting rate as constraints for continues spreading rumor in online communities.
Malware propagation	Guo et al. 2016	-There is a difference between malware propagation in social networks and technology networks. In social networks a virus spreads more slowly but infects a larger number of computers in the end. -Random-walk betweenness and subgroup structure of both social network and technological network have significant impacts on malware propagation.

While these studies are helpful for understanding the process of information diffusion in OSNs and determining which users are most effective in propagation, there is insufficient theory-based research on malware propagation in OSNs. Guo et al. (2016) show malware propagation in an organizational environment. They construct real organizational networks and simulate a malware propagation process. Organization networks consist of networks of users (social network) and their computers (technology network) in the network. For constructing a social network, they collected data from all students in a university who have an account on Myspace and extracted

their connection with other students in this network. They considered the local area network (LAN) of the university to be a technology network. Then, they mapped nodes in the social network to nodes in technology network. After constructing both networks, due to the lack of real infection data, they simulated malware propagation on these networks based on the SIR model. They showed impact of structural network on malware propagation in both networks.

The literature indicates a gap in research about the importance of individuals' role in malware propagation in OSNs. There is a need to identify individuals' characteristics and structural positions that play a role in their efficacy in malware propagation and vulnerability to infection.

Although attack propagation is similar to information diffusion, there is a major difference between propagation of security attacks and the information diffusion process. Contrary to information diffusion, in which individuals can make decisions about sharing the information or control receiving it, in the epidemiology of diseases as well as in security propagation, being exposed to infection or attacks is not under individuals' control and they do not have the ability to accepts or reject it (Wu et al. 2004, Zafarani et al. 2014). This feature of epidemiology is common between disease and malware propagation in that individuals are not able to decide whether to become infected or infect others. Therefore, epidemic theory is a more appropriate theoretical framework for the study of malware propagation. Furthermore, the place of individuals in the social network plays a role in the propagation of both diseases in epidemiology as well as in malwares propagation. We rely on the social capital theory to identify the place of individuals within the OSNs.

2.3. Theoretical Framework

The epidemic theory and social capital theory form a framework for this study.

2.3.1. Epidemic Theory

Epidemic theory explains the process by which infectious diseases are transmitted within a society. In reality, the structure of connection among individuals is dynamic and contagious diseases can go back and forth within the population. In the epidemiology literature, two comprehensive models are used to conceptualize the network structure of contagion—SIR and SIS (Anderson and May 1992). SIR (Susceptible-Infectious-Removed) models people's health status in the epidemic as three conditions: (i) Susceptible: not yet infected with the disease (ii) Infectious: infected with the disease (iii) Removed: recovered or died (Bailey 1975). In this model, considering a predetermined rate, susceptible individuals can take the disease from infected individuals. Moreover, because of the immunity systems for each individual, this model assumes individuals will recover after being infected and will not be able to get the disease again (Newman 2002). Also, this model considers some cases when an individual cannot recover, and dies from the disease. Therefore, SIR model is more compatible with reality.

However, in some infectious diseases, recovered individuals may get infected again. Such cases are modeled as SIS (Susceptible-Infected-Susceptible). This model assumes that there is no removed condition in the process (no one dies from the disease) and individuals can become susceptible after completing their infectious period. The SIS model assumes each healthy individual becomes infected with a given rate when he contacts at least one infected individual in a network. Also, infected individuals recover again with a given rate and become susceptible once more (Pastor-Satorras and Vespignani 2001). Since this model does not have a recovery

step, it is applied to diseases which are common and when having the infection does not provide immunity from getting the disease again.

We use the SIR model in our investigation since our study is a short-run investigation of threat propagation. We argue that people who are infected will be more cautious in the short run and take stronger security measures to avoid infection. We checked this assumption against the information in our dataset. Fewer than 3 percent of users in our data set mentioned that they were hacked again within one month of their first report, which indicated that the probability of recurrence of infection is low in the short run. Also, Zou et al. (2004) state that the SIS model is not appropriate to study propagation of email worms. They believe that removed users will not be re-infected by the same types of email worms.

In epidemic theory, one of the fundamental factors is the basic reproductive ratio (R_0). R_0 is a measure to check whether an infection will propagate through a society or not. R_0 is defined as the average number of secondary individuals infected by a single individual in his/her infectious period in a susceptible population (Heesterbeek and Dietz 1996). Reproduction ratio is related to the number of contaminated people connected to each person, the likelihood of transmitting infection from the infected person to a susceptible person and finally the period of infection (Jeger et al. 2007).

R_0 has been used in various outbreaks to model the spread of infectious diseases and to find optimal ways to halt pandemic diseases and provide timely immunization programs (Hill and Longiri 2003, Keeling et.al 1999). In recent years, there is a pattern of using R_0 for complicated and real situations (Heesterbeek 2002). For example, researchers have used R_0 to assess the risk of spreading diseases, such as SARS (Lipsitch et al. 2003 and Meyers et al. 2005), Influenza (Mills et.al, 2004), Ebola (Chowell et al. 2004 and Althaus, 2014) and sexually transmitted diseases

(Diekmann et al. 1991 and Kretzschmar and Morris, 1996). Therefore, it is more tangible and dominant to use a reproduction ratio to study infectious diseases and apply it to data (Heesterbeek 2002).

In this study, we use epidemic theory to capture the characteristics of security attack propagation in a social network. There is a perfect match between epidemiology and social network theory (Klovdahl, 1985; May and Anderson1987, Rothenberg et al. 1995, Danon et al. 2011). That the patterns by which infectious diseases spread throughout a society can be specified not just by the characteristics of the threats but also by the structure of the network (Easley and Kleinberg 2010). Some social network metrics have been used to measure the effect of an infected individual in a network (Rothenberg et al. 1995, Wang et al. 2003, Christley et al. 2005).

We apply epidemic theory to investigate the spread of hacking in Twitter. We use a basic reproductive ratio to develop a probabilistic measure of reproduction in a dynamic network based on the SIR model. In our conceptualization, R_0 measures the *threat-propagation efficacy* of each individual in the network. More accurately, we define threat-propagation efficacy as a hacked individual's basic reproductive ratio-proportion of all individuals in a network who have been hacked by the individual. Moreover, we measure the threat vulnerability of each individual in the network. We define this variable as the proportion of all individuals in a network who have impact on individuals' vulnerability to be hacked. We study factors that influence individuals' threat propagation efficacy and individuals' threat vulnerability.

2.3.2. Social Capital Theory

Social capital is defined as "resources embedded in a social structure that are accessed and/or mobilized in purposive action" (Lin 2002 p. 29). Social capital facilitates the interpretation of activities among people when their relationships are considered (Coleman, 1988). Social capital theory posits that networks of relationships are valuable resources for the individual or organization (Inkpen and Tsang 2005). Nahapiet and Ghoshal (1998) proposed social capital as all available and potential information that are based on relationships between individuals and groups in social networks. There are three types of social capital: structural, relational and cognitive (Nahapiet and Ghoshal 1998). Structural social capital focuses on the types of connections and interactions among people in a social network. Relational social capital explains factors in personal relationships that influence individuals' behaviors, such as respect, trust and friendships. Cognitive social capital considers cognitive abilities that influence understanding and interpreting of relations among the members of social networks. These dimensions of social capital have been used in studies of individuals, communities and organizations (Nahapiet and Ghoshal 1998; Seibert et al. 2001; Dess and Shaw 2001; Chua 2002; Wasko and Faraj 2005; Inkpen and Tsang 2005; Tsai and Ghoshal 1998; Chow and Chan 2008; Faraj et al. 2015). Of the three types, we use the structural and relational aspects of social capital for finding valuable factors embedded within and derived from the network of individuals' relationships to investigate threat-propagation efficacy.

2.3.2.1. Structural Social Capital

Social capital represents the quality of individuals' relationships within their groups (Burt 2009). For individuals, structural social capital focuses on the individual's relationships within a network (Borgatti et al. 1998). These relationships can be derived from network connections of

individuals in a network. These connections are the main source of transferring information among individuals and provide social capital for individuals (Adler and Kwon 2002, 2009, Chow and Chan 2008). There are several methods for measuring structural social capital. Since structural social capital is embedded within social networks (Lin 1999), social-network metrics could be used to represent and measure various aspects of individuals' structural social capital. These metrics are generally called centrality-based measures. They quantify the position and connection of individuals within a network (Burt 1984, Marsden 1987). Individuals with high centrality are considered influential individuals in a social network (Borgatti et al. 2009, Cha et al. 2010). There are different methods for measuring an individual's centrality. Among them, ego-network metrics such as degree are used the most (Burt 1984, Marsden 1987, Albert et al. 2000). Also in OSN there are several studies which consider different centrality measures for identifying influential people, such as degree, betweenness, closeness, and page rank (Goldenberg et al. 2009, Heidemann et al. 2010, Hinz et al. 2011, Kim and Han 2009, Lerman and Ghosh et al. 2010).

Among them, degree centrality was the main factor used for finding influential people. Research reports that degree centrality works better than other measures to find influential people in an OSN (Lerman and Ghosh et al. 2010). This type of metric considers the number of linkages from an individual to others in a network (Freeman 1979). This impacts on accessibility of individuals in the network and ease of information exchange and diffusion (Burt 1992, Lin 1999, Chow and Chan 2008). Therefore, individuals with a higher degree centrality are considered influential individuals in a social network (Burt 1992, Lin 1999, Fang and Hu 2016).

2.3.2.2. Relational Social Capital

Relational social capital demonstrates the effect of direct relations among individuals in the network (Chow and Chan 2008). It refers to "assets roots in these relationships" (Tsai and Ghosl 1998, p. 465). There are a number of the factors such as strength of ties, trust, norms and others to measure relational social capital. We concentrate on strength of ties because of its impact on increasing interactions and enhancing trust (Tsai and Ghosal 1998, Coleman 1988, Bapna et al. 2017). Trust is defined as "an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon" (Rotter 1967 p. 651). Moreover, trust has been identified as confidence in a partner and accepting vulnerability and uncertainty (Coleman 1990, Moorman et al. 1992). Both definitions emphasize the importance of confidence in others.

An individual's trust in others means giving the responsibility of decision making to the other individuals and accepting the risks of this faith. Based on relational social capital, trust is one of the main aspects of interactions among individuals (Lewis and Weigert 1985, Rousseau et al. 1998). Previous studies show the role of trust in social networks and its effect on security (Gray et al. 2003, Adali et al. 2010). Trust plays a significant role in determining influential individuals and information diffusion in a social network. Studies demonstrate that successful interactions and information transmission are done among individuals who have more trust in each other. On the other hand, having more interactions between two individuals constitutes more trust between them (Adali et al. 2010).

Interaction among people in a social network is a factor for determining social relationships and these interactions form the basis for the existing trust among them (Adali et al.2010). Strength of ties demonstrate the effect of strong relationships on existing trust among

individuals. Studies show that trust among individuals comes from social interactions and social ties (Gulati 1995; Tsai and Ghosal 1998, Chow and Chan 2008). Strong ties indicate trusted people with whom one has already established a strong relationship, whereas weak ties indicate relationships where there is less trust (Sherchan et al. 2013). There are several methods for measuring strength of ties in social networks (Sherchan et al 2013, Aral and Walker 2014, Bapna et al. 2017). Some of these measures are based on behavioral aspects such as reputations and confidence among two actors and the other methods are based on connection and ties among individuals.

Strength of ties forms differently offline than in OSNs. In offline social networks, people have more frequent face-to-face contacts and get to know each other in a variety of environments and circumstances. Individuals may face difficulties in judging the directionality and strength of their friendship (Almaatouq et al. 2016). In OSNs, individuals have connections to different people, post about their activities and interests and share information on their profiles without having any contacts and in most cases without knowing each other in offline social networks. The ability to view and track network connections is one of the main features of OSNs that distinguishes them from offline social networks (Kane et al. 2014). This feature provides direct observational information for the assessment of strength of friendship in networks. In this study, we measure friendship strength based on the reciprocity of connections among individuals in OSNs. Reciprocity in OSN is defined as a bidirectional friendship of two individuals.

2.4. Model Conceptualization

Disease epidemic literature shows that individuals' roles in disease propagation are associated with their positions and activities in the structure of social networks (Rothenberg et al. 1995, Bell 1999, Riolo et al. 2001). Rothenberg et al. (1995) argue that centrality measures are a tool to identify individuals who increase the speed of disease propagation in a network. Morris (1994) mentioned "people can be thought of as inhabiting a multidimensional space. Some of these dimensions describe their coordinates in the physical world, but the remainder describe their position in social terms, and their distance from others". This research studies the effect of social capital dimensions on an individual's propagation efficacy of malware threats in the network, and how these dimensions affect individual's vulnerability to receive threats from the network. The conceptualized models are presented in Figure 2.1.

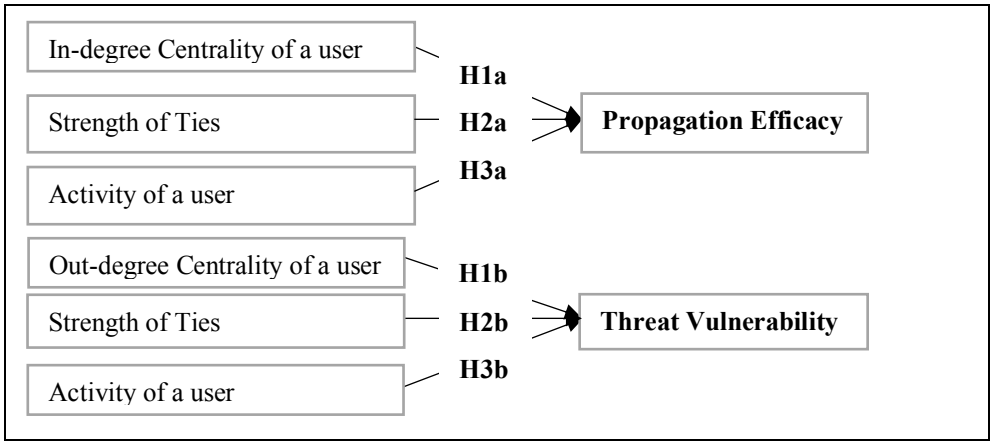


Figure 2.1. Propagation Efficacy and Threat Vulnerability Models

2.5. Hypotheses

2.5.1. Structural Social Capital

People with many connections are usually more influential to meet new people and suggest them to the others (Probst et al. 2013). Individuals with a high number of connections are targeted by companies to distribute word-of-mouth faster and use it to improve their market (Goldenberg et al. 2009). It is argued that the higher the number of communications an individual has, the greater chance he/she has of receiving credible information. Such an individual occupies a more strategic position within the network (Borgatti et.al 1998, Kiss and Bichler 2008). Moreover, individuals having central positions in a social network can be considered as trustworthy by others in the network (Tsai and Ghosl 1998). Furthermore, individuals' higher number of social ties in OSNs motivate them to share knowledge with others. Therefore, individuals having high connections with others in a society have more opportunities to impact on others' behaviors (Barabási 2003; Kiss and Bichler 2008; Van den Bulte and Joshi 2007). Moreover, the strength of connection improves individuals' influence in a society (Brown and Reingen 1987, Burt 1992). Stronger connections lead to more trust and confidence among individuals. Degree has been used to measure trust units in business as well (Tsai and Ghosal 1998).

In social networks, one of the popular ways to show structural social capital is degree centrality (Barabási 2003). Degree centrality demonstrates that individuals with many connections to others are considered as central in a network. Since in some platforms there are directed connections among individuals, we need to distinguish between two types of degree centrality: in-degree and out-degree. In-degree centrality quantifies the number of communications sent by other to an individual, whereas out-degree centrality quantifies the

number of communications sent by an individual to others. Individuals with more in-degree centrality are the more valuable resources of information and are considered as a major point for the flow of knowledge (Freeman 1979). Since the ties among users in Twitter is directional, there is a difference between in-degree centrality and out-degree centrality in Twitter. The number of Twitter users who follow an individual is the in-degree centrality of that individual. While, the number of Twitter users who the individual follows are called the out-degree centrality of that individual.

2.5.1.1. In-Degree Centrality

Based on social capital theory, in-degree centrality provides strong social capital and flow of knowledge. Individuals gain reputation and prominence on social networks due to their social status and reputation, such as celebrity status or political status. Research reports that number of followers is an indication of the amount of the audience that a user has in a social network (Cha et al. 2010). Users who create interesting and new posts obtain a large audience. It is shown that individuals with higher numbers of followers are considered influential people in Twitter (Weng et al. 2010). Such individuals occupy strategic positions within the network (Borgatti et al. 1998). Furthermore, individuals' higher number of social ties in OSNs motivate them to share knowledge with others. They are the more valuable resources of information and are considered critical nodes for the flow of knowledge (Freeman 1979). In the context of the epidemic model, a higher number of connections between an infected individual with others results in more propagation of disease and infection (Bell 1999, Christley et al. 2005). Accordingly, individuals with more connections could become hackers' targets for infecting a network (Albert et al. 2000). This is in line with the report that the number of followers and posts in Twitter indicates users' reputation and recognition, which attract security threats (Yang et al. 2011). This

recognition increases the probability of people clicking and sharing hacked information attributed to people with a high level of reputation on social networks.

Individuals with higher numbers of followers are viewed as major points for dissemination of knowledge. Therefore, individuals with high numbers of followers are in a more prominent position and have more opportunity to receive security threats. In addition, central individuals have a high risk of getting diseases in a network (Christley et al. 2005). By the same token, when their knowledge is infected by malware, they become a major point for the spread of malware. Hence, we argue that individuals with more in-degree ties with other members in the social network have more influence for transmitting a hacking threat.

> ***Hypothesis 1a****. Individuals' malware propagation efficacy is positively associated with their in-degree centrality.*

2.5.1.2. Out-Degree Centrality

Out-degree centrality is the number of communications from an individual to others in the network. In social networks, out-degree centrality occurs when an individual follows others who have similar interests or have gained their attention and recognition. Individuals following more others have accessibility to different people having different interests and knowledge. Out-degree centrality represents the extent of dependency of an individual to the others (Dess and Shaw 2005). It is argued that the higher number of communications an individual has, the greater chance of receiving credible information. Moreover, individuals with high degree centrality adopt products sooner because of the large number of connections they have in a network (Probst et al. 2013).

In the context of the epidemic model, a higher number of connections between an infected individual and others results in more propagation of disease and infection (Bell 1999). More

interactions and relations of infected users with other people in a society results in faster transition of disease (Morris and Kretzschmar 1996, Meyers et al 2005, Shirley and Rushton 2005). People having high numbers of connections in a social network are more exposed to diseases and infections of disease propagation (Newman 2002). Also, more communications from an individual to others impact on being vulnerable to a disease (Christley et al. 2005). Hence:

> ***Hypothesis 1b.*** *Individuals' malware threat vulnerability is positively associated with their out-degree centrality.*

2.5.2. Relational Social Capital—Strength of Ties

There are several factors representing relational social capital. Among them is strength of relationships because it is one of the most important factor that indicates the level of trust among friends. Friendship in social networks has different levels of strength. Strength of ties demonstrates the intensity and tightness of a friendship (Van den Bulte and Wuyts 2007). Strength of ties impacts on perceived level of interactions and the quality of individuals' engagement in a society (Moorman et al. 1993). Moreover, strength of friendship influences individuals' willingness to share information, thus increasing their social capital (Lin 2002, Putnam 1995).

Strength of ties has been used to represent the level of trust. Strong ties increase friends' influences due to a higher level of trust and increased interactions (Coleman 1988, Coleman 1990, Bapna et al. 2017). Over time, there is more trust and confidence among individuals who have strong interactions with each other in a network and as a result there is a high level of shared information among them in the network. Research has demonstrated that strong ties among individuals increases the level of trust between individuals and improves social influence.

Moreover, in online shopping and recommendation systems, trustworthy individuals have a high impact on increasing market size and their feedbacks are effective (Benbasat and Wang 2005). Although strength of ties increases social interactions and information transmission in the network (Levin and Cross 2004), it can be harmful in risky situations. Therefore, individuals expect some risks and harms from people with whom they have strong relations. In the context of disease propagation, strong relationships have significant effect on how much individuals can infect others in a social network. For example, research shows that strong romantic relationship makes people more vulnerable to sexually transmitted diseases (Jadack et al. 1997, Brady et al. 2009).

Recent studies on OSNs have shown that reciprocity in relationships are stronger than one-way relationships (Kwak et al. 2010, Shi et al. 2014). Reciprocity in relationships is instrumental for spreading online behaviors (Bond et al. 2012, Valenzuela 2014). In the context of security threats, research shows criminals target users with a high number of reciprocated relationships as a base to propagate their attacks in a network (Garriss et al. 2006, Mislove et al. 2007).

Applied to the propagation efficacy of and vulnerability to malware in OSNs, we argue that individuals with a stronger ties have higher propagation efficacy in spreading malware threats; and those individuals are more vulnerable to malware threats.

> ***Hypothesis 2a.*** *Individuals' malware threat propagation efficacy is positively associated with their strength of ties with others.*
>
> ***Hypothesis 2b.*** *Individuals' malware threat vulnerability is positively associated with their strength of ties with others.*

2.5.3. OSN Activities

Individuals' behavior could also influence their ability to diffuse information as well as to propagate security threats. In epidemiology, the high activity of infected individuals increases

propagation of diseases such as STD and SARS (Holmes et al. 1990, Riley et al. 2003). Thus, infected individuals are constrained in social activities in order to reduce propagation. This limitation can be in the form of quarantine, which is common for contagious diseases (Chowell et al. 2003, Rizzo et al. 2014).

In the context of online security threats, those having a high level of knowledge and distributing more information are considered influential individuals in a social network (Watts and Dodds 2007). In general, influential people are more active in society (Weimann et al. 2007). In OSNs, individuals reach social influence through their sustained activities and engagement. There are various OSN activities such as posts, comments or likes (Probst et al. 2013). Research reports significant associations between individuals' activities in an OSN (Facebook) and the extent of their social capital (Ellison et al. 2007). It is argued that Facebook posts and participations could be used as a measure of "bridging" social capital—where bridging social capital refers to connections between users who generate or share information with others (Ellison et al. 2007). Furthermore, people gain attention and recognition through their contributions and activities in online communities, thus increasing their social capital (Lampel and Bhalla, 2007).

This finding is further supported in a study reporting that individuals who have more contributions in the social network are considered more attractive and have more audiences. This motivates them further to increase their contributions and attain more recognitions (Huberman et al. 2009). Research reports that individuals with a high number of posts in Twitter are more inclined to respond to requests from a bot and become victims to more attacks (Wald et al. 2013). Applied to malware propagation, we argue that individuals with higher OSN activities have higher malware propagation efficacy. Hence,

Hypothesis 3a. *Individuals' malware threat propagation efficacy is positively associated with their level of OSN activities.*

In epidemic theory, individuals with more social activities—particularly activities with at risk people—are more susceptible to infections (Rizzo et al. 2014). This is observed more frequently in risky behaviors such as unprotected sexual contacts (Riley et al. 2003, Finlayson et al. 2011, Mukandavire et al 2009). Applied to online security threat vulnerability, we argue that users who have more OSN activities are more vulnerable to malware security threats. Hence:

Hypothesis 3b. *Individuals' vulnerability to malware threats is positively associated with their level of OSN activities.*

2.6. Data Collection, Data Classification, Data Filtering and Network Creation

This section shows the processes of data collection from Twitter and creating a social network of hacked individuals from it.

2.6.1. Data Collection of Tweets and Users

In analyzing hacked individuals in Twitter required collecting tweets about having been hacked as well as information about the individuals who posted such tweets. We collected data from Twitter using Twitter's application programming interface (API). At the first step, we searched for tweets containing the keyword "hack" with one of these verbs "got", "was", "is", "has been" and "have been". We did not collect retweets to avoid redundancy. We used a crawler to collect data from July 24, 2017 to October 21, 2017. In total, we collected 283,421 tweets.

We also collected posting times, the owner of each tweet, and the user profile information publicly available on Twitter. Profile information for each user included number of followers, number of friends, number of tweets up to the time of the tweet about hacked account, and the

creation date of Twitter account. We also collected friends' IDs for each user to construct the social network of users and their friends.

2.6.2. Classification Method

We needed to filter 283,421 tweets to identify the tweets in which users had mentioned their own Twitter accounts were hacked. We used the following filtering process. For filtering tweets, we needed to label collected tweets as relevant or irrelevant. To do so, we randomly selected 10% of the tweets. The selected tweets were labeled manually to separate the tweets that mentioned their owners' accounts were hacked (relevant) from the tweets which mentioned that others people's accounts were hacked (irrelevant). After labeling the selected 10% of tweets in our data set, we applied classification methods to label the remaining 90% of 283,421 tweets.

We applied two popular classification methods for tweet classification: Support Vector Machine (SVM) and Maximum Entropy (Maxent). Each classification method was performed using a 10-fold cross validation, which means that tweet dataset was divided into ten subsets. Nine subsets were used as the training dataset and the remaining subset was used to test the performance of the labeling classification. This work was done ten times. Therefore, we have ten different results from the performance of each classification method. Performance of each method is measured based on accuracy, precision, recall and F1 score. Classification methods and average of their performance for our data set are reported in Table 2.2. Our results showed that the SVM method had the better performance. Our finding is in line with research that reports SVM as having the best performance among classification methods (Benevenuto et al. 2010). Hence, we selected SVM for filtering the rest of the tweets.

Table 2.2. Performance of Filtering Methods

Performance Metric	SVM	MAXENT
Accuracy	0.936	0.886
Precision	0.963	0.927
Recall	0.874	0.907
F1 Score	0.964	0.916

2.6.3. Data Filtering

Using the SVM method, we classified the remaining tweets and added to those identified manually. Since our focus is hacked twitter accounts, we needed tweets that stated users' Twitter accounts were hacked. Therefore, we added keywords "twitter" and "tweet" and different derivation of these keywords in captured tweets to filter the collected tweets. The set of filtered tweets contained 32,406 tweets in which users stated their twitter accounts were hacked. We applied another filter for tweets as follows. In an online propagation setting, the hacking date of a user is the date when the user first mentions the information about infection (Rodriguez et al. 2014). Therefore, we kept the first tweet of a user tweeting about his/her hacking problem and removed the rest of the user's tweets. This reduced the number of tweets to 22,513 by the same number of users.

We filtered users as follows. When users are hacked in Twitter, they may create a new account and use the new accounts tweet that their previous accounts had been hacked. In order to avoid inaccuracies due to hacked accounts outside the time frame of our dataset and to prevent double counting, we removed users whose accounts were created less than one week prior to their announcement that they were hacked. This reduced users to 16,074.

The goal of this research is to find the propagation efficacy of users in a social network and the degree of their threat vulnerability in the social network. Therefore, we needed to find connections among the hacked users in this network. We further filtered users in one more

round. In order to find the effect of hacked users on each other, we considered that threat propagates forward in time. It means that, if user *i* has a direct connection to user *j* and $t_j < t_i$, then user *j* with hacking time t_j can infect user *i* at time t_i. Therefore, from all the connections in the social network, we kept those connections and users that the hacked time of target users is later than the hacked time of source users. Target users are those who follow other users in the network and source users are those who are followed by others in the network. We call the resulting social network as the "hacked network". The hacked network has 8,271 users. The process of data collection and creation of the network is shown in Figure 2.2.

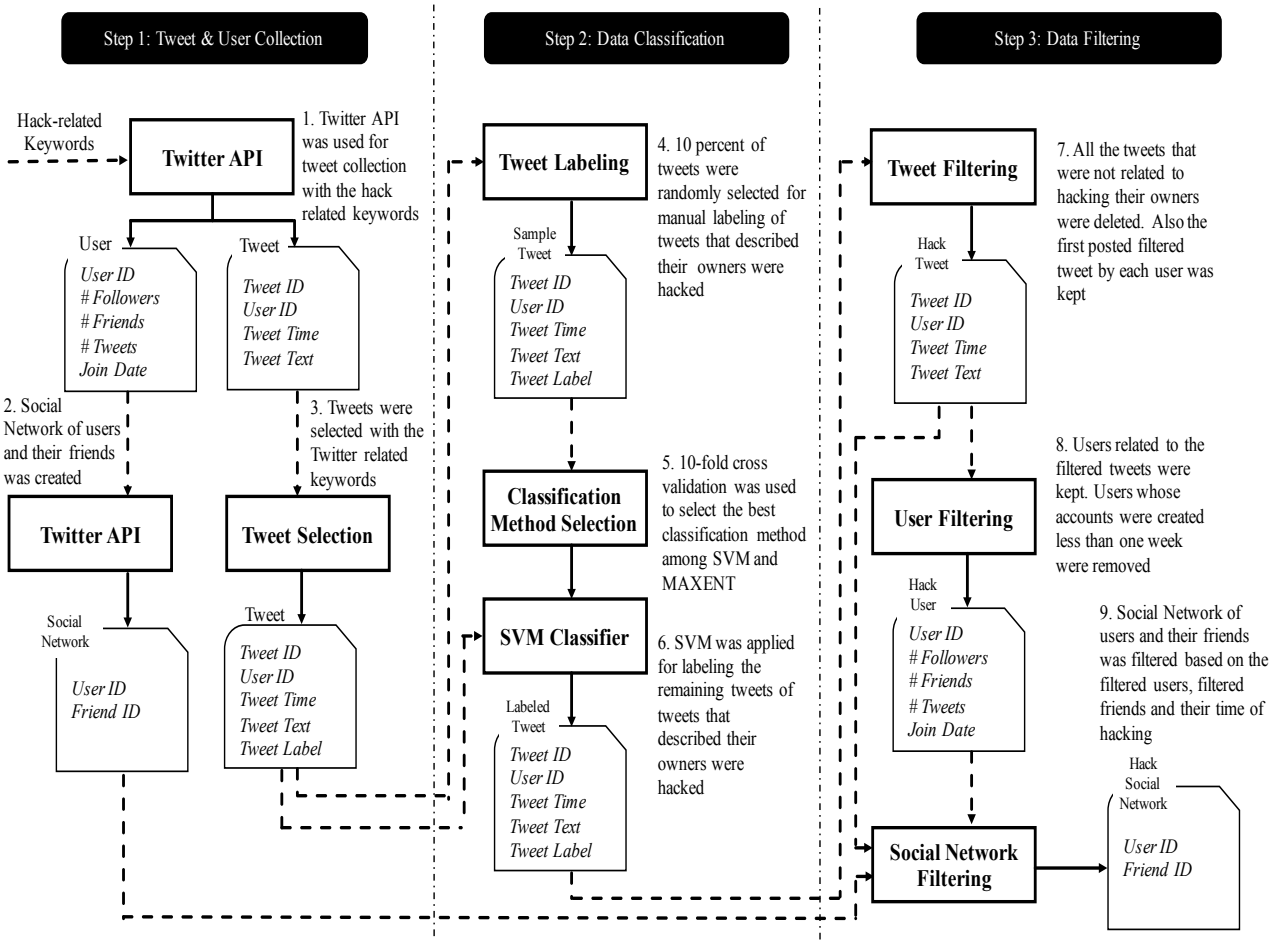


Figure 2.2. The Process of Data Collection, Classification and Creation of Hacked Network

2.7. Variable Measurement

2.7.1 Notations. G represent a set of N users, i represents a user in the OSN. $i \in G$, $i = 1,2, \ldots . N$. E denotes a set of connections among users in an OSN. In Twitter connections are directed. Table 2.3 shows the notations used in this study.

Table 2.3. Notations

Notation	Meaning
G	set of users in the hacked network
i	user $i \in G$
P_i	propagation efficacy score of user i (see Eq. 2.1)
p_{ik}	probability that user i infects user k (see Eq. 2.2)
V_i	vulnerability score of user i (see Eq. 2.3)
t_i	infection time of user i
$d(t_k\text{-}t_i)$	probability distribution of time differences between infection time of users k (t_k) and user i (t_i)
R_i	the number of user i's reciprocal friends
F_i	set of user i's infected followers
O_i	set of infected users who user i follows
m_i	user i's strength of ties as the one who infects others
z_i	user i's strength of ties as the one who is infected by others
L_i	user i's in-degree count in the hacked network
H_i	user i's out-degree count in the hacked network

2.7.1. Measurement of Dependent Variables

This research has two dependent variables. Propagation efficacy and threat vulnerability.

2.7.1.1. Propagation Efficacy

In the context of threat propagation in OSNs, the effectiveness of propagation is directly related to the power of individuals who convey it. Influential people are defined as "individuals who were likely to influence other persons in their immediate environment" (Katz and Lazarsfeld 1955, p. 3). We use this definition for our first dependent variable; propagation efficacy. In this study, the propagation efficacy of each user is measured based on the reproductive ratio in

epidemic theory that has been used for measuring the speed of propagation of different kinds of diseases (Hefernan et al. 2005). For computing each user's propagation efficacy, we applied the method used by Wallinga and Tenuis (2004). In this work, they compute likelihood-based estimates of reproductive ratio thorough pairwise computation (Wallinga and Teunis 2004):

$$P_i = \sum_{k \in F_i} p_{ik} \quad (2.1)$$

$$p_{ik} = \frac{d(t_k - t_i)}{\sum_{j \in O_k} d(t_k - t_j)} \quad (2.2)$$

where p_{ik} is the relative likelihood that user *k* was infected by user *i*, and is computed as the probability distribution of infection-time differences of users *k* and *i* ($d(t_k - t_i)$). F_i is the set of infected followers of user *i*, and O_k is the set of infected users followed by user *k*. The normalized relative likelihood that user *k* will be hacked by user *i* is computed by dividing p_{ik} by the sum of probabilities that user *k* will be infected by the infected users who user *k* follows. In computing p_{ik} we assume that there is no dependency between *i* and *k*. The estimated influence for user *i* is computed as the sum of relative likelihood that each user is infected by user *i*.

2.7.1.2. Threat Vulnerability

The second dependent variable is user's threat vulnerability (V_k). This variable measures the level of vulnerability of a user to be infected by the other users in the network. This measurement is based on the method suggested by Myers et al. (2012) for computing the probability of individuals' exposure to information by others in an OSN. For this measurement, the likelihood-based estimate of user's vulnerability is computed as the sum of the probability distribution function of exposure propagation that user *k* has been infected by user *i* (who is infected before user *k*).

$$V_k = \sum_{i \in O_k} d(t_k - t_i) \quad (2.3)$$

where t_i is the infection time of user i and O_k is the set of infected users followed by user k.

2.7.2. Measurement of Structural and Relational Social Capital

Structural and relational social capital are base of our two independent variables.

2.7.2.1. Structural Social Capital

Propagation of infection among individuals in a society is consistent with the study of the structure of the network. Social network measures and centralities have been widely used for analyzing the effect of individuals on spreading the infection and disease (Bell 1999). We take into account two metrics for centralities within the Twitter OSN. The first is in-degree centrality, which measures the number of people who follow a user in Twitter, which is known as "number of followers". The second centrality is out-degree centrality, which measures the number friends a user has or the number of people a user follows. We have captured each user's number of followers and the number of people he/she follows directly from the Twitter. We normalized in-degree and out-degree centrality metrics by dividing each by its range.

2.7.2.2 Relational Social Capital

We use strength of ties as the measure of relational social capital. Interactive relationships among individuals are critical to improving trust in a society (Wilson et al. 2009). Users connect to others for various reasons. Therefore, it is not easy to identify real friendship connections (Viswanath et al. 2009). However, one can observe the strength of ties in OSNs through the type of individuals' connections. In OSNs like Twitter, there are two types of connections between a pair of users: one-way connection and two-way connection. A one-way connection occurs when one user desires to connect with a second user and knows about his/her activities in the OSN, but the second user has no desire to connect with the first one. In other words, a connection is one-

way if user *i* follows user *j*, but user *j* does not follow user *i*. In a two-way (or reciprocal) connection, both individuals desire to connect with each other, therefore, they follow each other. A pair of users in a two-way connection are friends who have more information about each other and have formed more intimate knowledge about each other, which strengthen their ties and increase their mutual trust and confidence (Adali et al. 2010).

Since we have two conceptualized models, we measure strength of ties two ways. In the propagation efficacy model the dependent variable is the efficacy of individuals in infecting their followers. Therefore, for each OSN user, strength of ties is computed as the number of reciprocal friends (with whom the user has a two-way connection) divided by the total number of his/her followers in the hacked network. Thus, for user *i* who infects others we measure strength of ties as:

$$m_i = \frac{R_i}{L_i} \qquad (2.4)$$

where R_i is the number of user *i*'s reciprocal friends and L_i is the number of user *i*'s followers.

In the threat vulnerability model, the dependent variable is individuals' vulnerability to security attacks from friends in Twitter. For each user in this case, strength of ties is computed as the number reciprocal friends (with whom the user has a two-way connection) divided by the total number of people the user follows (H_i) in the hacked network. Thus, we measure strength of tie for user *i* who is infected by others as:

$$z_i = \frac{R_i}{H_i} \qquad (2.5)$$

2.7.2.3. Measurement of OSN Activity

In OSNs, particularly in Twitter, users with high numbers of posts and connections are targeted by hackers to spread security attacks (Yang et al. 2011). We examine the association of OSN activities with malware propagation through the network. OSN activity is defined as a user's extent of participation in OSN, and represents the extent of a user communications with others in

the network. OSN activity is measured as user's total number of posts in Twitter divided by the age of the user's account. Therefore, this measurement takes into account all of the user's posts (covering all tweets, retweets and comments for the others) and the creation date of the user's account. Thus, this variable represents the average daily post of a user. Variable measurements are reported in Table 2.4 and discussed below.

Table 2.4. Variable Measurements

Variable	Definition	Metric	Computation
Dependent Variables			
Propagation Efficacy	Individual's ability to infect others in a society	Sum of the likelihoods that an infected individual *i* has infected others (Wallinga and Teunis 2004)	$P_i = \sum_k p_{ik}$ $p_{ik} = \frac{d(t_k - t_i)}{\sum_{j \in F_j} d(t_k - t_j)}$
Threat Vulnerability	Individual's exposure to infected individuals	Sum of the likelihoods that an individual *k* has been infected by other infected individuals (Myers et al. 2012)	$V_k = \sum_{i \in F_i} d(t_k - t_i)$
Independent Variables			
In-Degree Centrality	Number of in-coming links—structural capital	User *i*'s total number of followers in Twitter	Captured directly from Twitter
Out-Degree Centrality	Number of out-going links—structural capital	User *i*'s total number of people she/he follows in Twitter	Captured directly from Twitter
Strength of Ties	Level of an individual's strong relations in a society—relational capital	Reciprocal connections divided by the total number of all followers a user has (for dependent variable #1)	$m_i = \frac{R_i}{L_i}$
		Reciprocal connections divided by the total number of people a user follows (for dependent variable #2)	$z_i = \frac{R_i}{H_i}$

OSN Activity	Extent of an individual's engagement and activities in the OSN	Total number of a user's posts (covering all tweets, retweets and comments) since the creation of the user's account divided by the number of days the account has been in existence.	

2.8. Analysis and Results

As mentioned in the measurements of two dependent variables, we need to compute the relative probability distribution of difference in users' infection time. Several distribution functions such as power law, exponential and Weibull distribution were used to study the propagation of infectious diseases and information diffusion in social networks (Myers and Lavesco 2010, Myers et al. 2012). For this study, as the first step, we compute time differences between hacking dates of users in the hacked network. The second step involves identifying the best distribution function for the time differences. Since our data is discrete and the time differences are based on days, we need to find the best discrete distribution function for time differences. We used different discrete distribution functions. Distribution functions were compared to each other based on several metrics: the fit between empirical and theoretical densities, the fit between the empirical and theoretical cumulative distribution functions (CDF), Q-Q plot, P-P plot and AIC. The comparisons of the empirical and theoretical densities as well as the comparison of the empirical and theoretical cumulative distribution functions (CDF) show the level of fit between our observed data and the theoretical density and the CDF of the selected distribution. Quantile-quantile (Q-Q) plot is a graphical technique for demonstrating if a data set is generated from a

given probability distribution. A Q-Q plot compares the quantiles of an empirical distribution formed from a data set with the quantiles of a standardized theoretical distribution from a given family of distributions. The fourth metric is P-P plot. A P-P plot compares the empirical CDF of a data set with the theoretical CDF of a given probability distribution. AIC estimates the relative quality of a model developed for a given data set as compared to the other possible models.

Using the above four metrics, we found the exponential distribution with the parameter equal to 0.036 to be the best distribution function for hacked-time differences in our hacked network. Figure 3 shows the four metrics for the exponential distribution. In Figure 2.3, parts a and b show that the density and CDF of our data have the best fit with exponential distribution. Part c shows data points fit close to the exponential distribution. Part d shows that our data points fit close to the CDF of exponential distribution.

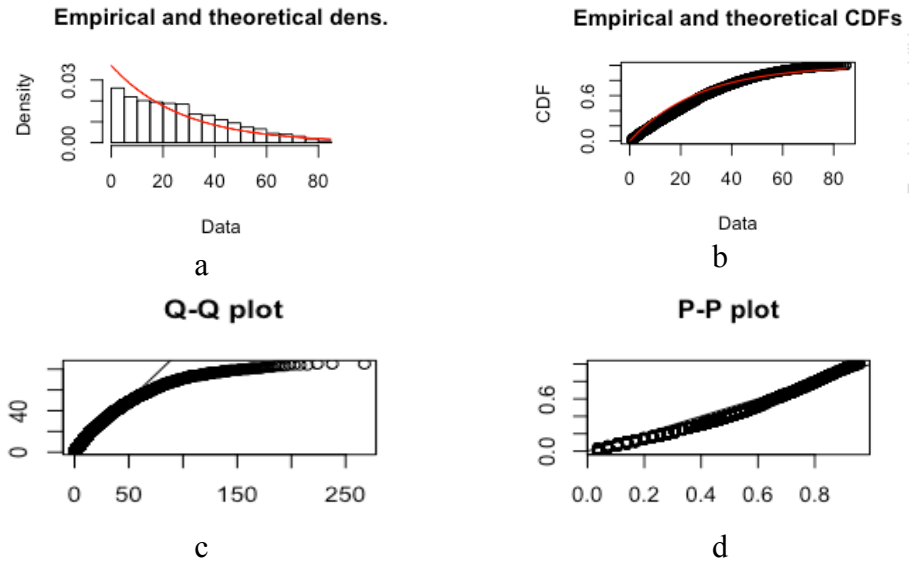


Figure 2.3. Results of Exponential Distribution Fit with the Data

Moreover, the AIC of the exponential model is 162,515.7, which is lower compared to the other distributions' AIC. Therefore, we concluded that the exponential distribution is the best fit with our data. Using the selected exponential distribution, we computed the probability of time

difference between hacking dates of user *k* and the infected user *i* that he/she follows in the hacked network using Equation 2.2. We then computed the propagation efficacy of user *i* based on Equation 2.1. We carried out a similar computation for each user's vulnerability by applying the exponential distribution in Equation 2.3. The final data set consisted of six variables. Table 2.5 reports the Pearson correlation values.

Table 2.5. Variable Correlation

	1	2	3	4	5	6
1.Propagation Efficacy	1					
2.Threat Vulnerability	0.1	1				
3.In-Degree Centrality	0.5	0.0	1			
4.Out-Degree Centrality	0.2	0.4	0.09	1		
5.Strength of ties with followers	0.0	0.2	0.03	0.08	1	
6.Strength of ties with friends	0.0	0.1	-0.03	0.10	0.0	1
7. OSN Activity	0.0	0.1	0.06	0.06	0.1	0.1

We estimated the two models using the regression method. Tables 2.6 and 2.7 report the estimated regression results of the two models.

Table 2.6. Estimation Results for the Propagation Efficacy Model

Coefficient	Value
Intercept	0.32***
In-Degree Centrality	97.13***
Strength of ties with followers	0.51***
OSN Activity	0.00**
R^2: 0.32	

**** p<0.001, ** p<0.01, * p< 0.05*

Table 2.7. Estimation Results for the Vulnerability Model

Coefficient	Value
Intercept	0.01***
Out-Degree centrality	1.83***
Strength of ties with friends	0.06***
OSN Activity	0.00***
R^2: 0.24	

**** p<0.001, ** p<0.01, * p< 0.05*

Per Table 2.6, in the propagation efficacy model in-degree centrality is significant (beta=97.13, $p<.001$) and supports H1a. Furthermore, strength of ties with followers is also significant and has a positive effect on propagation efficacy (beta=.51, $p<.001$). Therefore, the result supports H2a. In addition, user activity is significant (beta=.00, $p<.01$). The result confirms user participation in an OSN is associated with propagation efficacy within the network, this supporting H3a.

Per Table 2.7, in the vulnerability model, out-degree centrality of users in an OSN has a positive and significant effect on users' threat vulnerability (beta=1.83, $p<.001$). This result supports H1b. Also, having threat vulnerability has a significant relation to strength of ties with friends (beta=.06, $p<.001$). It increases the ability of users to be infected more easily. Therefore, it supports H2b. A user's activity is alone significant when we study threat vulnerability of users in an OSN (beta=.00, $p<.001$). It supports H3b. Thus, the results showed support for the importance of structural social capital, relational social capital and activity of individuals in OSNs in the strength of propagation efficacy of individuals and their threat vulnerability. Table 2.8 summarizes estimation results for each hypothesis. To check for robustness of the estimated models, we randomly selected smaller samples of users and re-estimated our models using different sample sizes. Appendix A shows the graphs for the coefficients and p-values of the factors in the model using eight different sample sizes. Each sample was selected randomly. The results support the robustness of our estimated model and validate our findings.

Table 2.8. Supported Hypotheses

Hypotheses	**H1a**	**H2a**	**H3a**
Propagation Efficacy	yes	yes	yes
Hypotheses	**H1b**	**H2b**	**H3b**
Threat Vulnerability	yes	yes	yes

2.9. Discussions

The first research question in this study was to identify significant factors contributing to an individual's malware propagation efficacy in an OSN. Using epidemic, social capital and social network theories, we developed a model based on reproductive ratio to reveal that social capital and user's network activity can be used to identify the propagation efficacy of users. We emphasize the self-reported status of individuals in Twitter who mentioned their accounts were hacked. We stated that the amount of a user's propagation efficacy in his/her neighborhood depends on centrality parameters, having strength of ties and the user's activity.

First, the empirical result of estimating propagation efficacy model reveals that individuals who have more in-degree centrality or more followers in OSN have more ability to infect others in the network. We found strong impacts of number of followers through Twitter on propagation efficacy. This finding is in line with prior studies on the effect of an individual's connection in social networks, which show that individuals with high centrality have more power for knowledge contribution, sharing information and even disease prevalence in social networks. There are also studies that confirmed these finding for OSNs. Faraj et al. (2015) identified leaders in online communities as individuals with high central positions compare to the others. Second, our study reveals that strong ties in OSN affect a user's propagation efficacy. The strength of connections between a user and his/her followers (as measured by having reciprocal connections with followers) can significantly increase the individual's propagation efficacy. This finding is consistent with the previous study and shows that having strong connections and interactions increase an individual's ability to cause others to follow his/her behavior. Third, our results showed that a high level of activity in an OSN (in terms of posting a message) strongly correlates with a

user's propagation efficacy and increases chances to user will spread the threat. This finding was supported by a previous study in which in OSNs, popularity and contributions, are considered factors for identifying influential people as well (Heidemann 2010, Cha et al. 2010, Eirinaki et al. 2012). Moreover, researchers find influence of people in a social network is primarily based on an individual's connectivity and activity (Probst et al. 2013).

The second research question is this study was to identify the individual's factors improving the malware threat vulnerability of individuals in OSNs. For this research question, we also used epidemic theories along with social capital and social network theories. We developed a model to reveal the role of individuals' positions in a network, their trusted relationships and activities on threat vulnerability in OSN. First, our study showed that out-degree centrality or number of friends in OSN has a significant positive association with the threat vulnerability of individuals. This confirmed prior studies in which individuals having more are looking for more people and tend to follow others' activities, behavior and characteristics. Therefore, these users can be more affected by the others they follow, and this issue can increase the probability of being exposed to various attacks in a social network. Second, the empirical result of the estimating threat vulnerability model showed that, strong ties could influence an individual's vulnerability. We showed that having more reciprocal connections with friends in OSN increases the level of threat vulnerability. This result is in line with prior studies that levels of interaction and trust impact the effectiveness of individuals. Third, our analysis showed that more vulnerable users have high activity in OSN in terms of posting and sharing many contents.

Overall, our results show that the advantage of the centrality position along with strength of relationships and amount of participation affect a user's ability to propagate the thread and user's vulnerability to take attacks in OSNs, especially within the Twitter platform.

2.10. Theoretical and Practical Implications

This research makes a number of theoretical and practical implications.

2.10.1. Theoretical Implications

In a social network, individuals' belief, attitude and behavior are affected by others in a network (Burt 1987, Erchul and Raven 1997). Recognition of vulnerable individuals and individuals with high ability to infect others can promote controlling and inhibiting procedures (Rothenberg et al. 1998, Christely et al. 2005). However, the influential factors contributing on propagating infection is not clear and there is an immense concern to study the effect of individual's characteristics in threat propagation (Pastor-Satorras and Vespignani, 2001, Christely et al. 2005). The results of our study provide useful managerial implications for malware prevention strategies and other security decisions in OSNs.

First, our approach in collecting hacked users and forming the hacked network within an OSN, shows a new way in observational study of the threat propagation in an OSN. It demonstrates the great potential of OSNs for being infected on a large scale. Second, combining structural network theories with a disease spreading theory provides a conceptual framework for studying threat propagation and shows the influential individuals'-level factors on it. This research determines which features of social structure encourage the emergence of social relations that facilitate spreading of threat in an OSN. It also shows which features can be influential in enhancing a user's vulnerability in an OSN. This study could motivate researchers to focus on an individual's characteristics to study security and malware propagation in social media. Moreover, finding highly vulnerable individuals' in our neighborhood increase our chances to be infected by

them. This study helps users in OSNs understand both their own vulnerability and vulnerability to their neighbors to improve their security. Furthermore, identifying the characteristic of individuals who are targeted by hackers can be used for preventive strategies.

2.10.2. Practical Implications

Our work presented metrics to identify individual's characteristic in malware propagation in OSNs. If IT managers consider these metrics, they can decrease the level of malware propagation and start their preventive strategies from the influential users. In the other words, identifying the most influential individuals in a network in terms of transmitting threat to the other members of a network can contribute to reducing the propagation of infection. Once the most influential individuals have been determined, the theories outlined in this research can be used to define the minimal coverage needed to ensure elimination of the infection through the network. To ensure security managers completely understand emerging security incidents at the early stages, they should control individuals with a high level of activities and positions in a network. These users might be the source of new incidents and threats; managers must be aware of them throughout the network. Moreover, increasing trust among individuals in OSN increases the level of their threat vulnerability. Therefore, individuals should be aware about the potential risks embedded in their trust of other users and the content they share in these environments to be safe from security threats in OSNs. Most security policies in OSNs are related to an individual's protections from strangers and IT managers don't consider the security attacks which individuals may encounter from their friends in OSNs. This study shows individuals are vulnerable from their friends' behavior as well as their own behaviors. To guard against malware threat propagation in these platforms, managers

should provide multiple policies for informing users of threats coming from their neighbors even they are protecting their personal accounts.

2.11. Limitations and Future Research Direction

Like all empirical research, this study has limitations. Due to practical limitations, we can only crawl a portion of the total tweets and our crawled data set may still have sampling bias. The second limitation relates to the static nature of captured social network data. While tweets have been collected over a two-month period, the connections among individuals were captured at one time during that period. However, collecting an ideal large data set from Twitter, a real and dynamic OSN, without any bias is an almost impossible mission. Since most users have more than thousands of followers or friends, collecting the actual network of hacked users which are infected users with all their followers and friends in Twitter is not easy. Thus, the third limitation in this study relates to focusing on the hacked network, which is the collection of all hacked users with their infected friends and followers. Moreover, in this research we studied users who know their accounts were hacked. Therefore, we filtered all tweets which mentioned others' accounts (e.g. his/her friends' accounts) were hacked. In order to have a large network with more hacked users, we can extract the information related to the users who were hacked and mentioned by others to inform about their situation.

In this study, we investigated several individual-level factors in relation to social network metrics, social activity and trust. Future studies need to investigate the effect of other individuals' characteristics which are related to their psychological and psychographic attributes. Furthermore, our work can be extended to study the role individual's members of different communities and

subgroups play in malware threat propagation in OSNs. Finally, the future extension of our work could be related to malware propagations in other OSNs, to see learn of any difference of influential factors in these platforms.

CHAPTER 3

Essay 2: The Role of Communities of Interests in Individuals' Vulnerability to Online Security Attacks

3.1. Introduction

In last few years, online social networks (OSNs) have facilitated the process of interaction and communication among people. Research has shown that the structure of OSNs is formed around topics of interests (Mislove et al. 2010, Li et al. 2014) where people interact and make friends with those who have similar interests and preferences. This similarity of interests allows people to get a high rate of approval and positive feedback for their disclosed behaviors and shared contents (Han et al. 2015). Furthermore, the more similar two individuals are, the more they will have trust to each other (Tang et al. 2013). People tend to trust similar others in recommending products, discussion about their personal matters or asking help (Winter and Kataria 2013).

While belonging to supportive communities is enjoyable, it has its own negative effects. One dark side of it relates to the possibility of reduction in individuals' level of self-control. Prior studies have shown that high exposure of individuals to their topics and activities of interest can decrease the ability of individuals to evaluate the risks associated with it (Gino et al. 2011). In online environments, this gives a chance to attackers to target people based on their interest online (Gao et al. 2011, Yan et al. 2011). In doing so, attackers post contents on topics of interest with links to third party scam sites outside OSNs. It was reported that attackers earn

millions of dollars using this approach every year.[1] This type of vulnerability can be seen more in friendship networks. The reason behind that is individuals in their friendship networks have more trust in each other and accept any reaction of their friends (Mayer et al. 1995, Roussen et al. 1998). Despite the importance of this topic, no prior studies have investigated the direct role of communities of interest and similarity of interests with friends on individuals' vulnerability to security attacks.

To address this gap, this research asks: 1) Are revealed individuals' interests in OSNs associated with their vulnerabilities to security threats in OSNs? If so, which types of interest are associated with individuals' vulnerabilities in such platforms? 2) Do similarities of interest among individuals and their friends play a role in individuals' vulnerabilities to security threats in OSNs?

To answer these questions, we rely on s syntheses of the dual-system theory and the theory of homophily. Dual-system theory considers two distinct systems in a human brain. These two systems are 1) impulsive system and 2) controlling system. Processed information by these two systems allows individuals to make decisions about continuing or inhibiting certain behaviors. (Hofmann et al. 2009, Turel and Qahri-Saremi 2016). Imbalance is generated in the human brain when a strong persistent desire to do interest-based activities leads to a weakened controlling system. This reduces the ability of individuals to evaluate the rationality of their behaviors (Bechara 2005, Evans 2008, Hofman et al. 2009, Turel and Bechara 2016). Consistent with the dual-system theory, interest-based stimuli can strengthen the impulsive system and reduce the individual's control over the behavior.

[1] https://www.theguardian.com/technology/2013/aug/28/facebook-spam-202-million-italian-research (Accessed in April 2018)

Furthermore, we use the theory of homophily to capture individuals' interests and preferences. According to the theory of homophily, people with similar interests have a higher tendency to interact with each other and form denser social networks (McPherson et al. 2001). This allows researchers to identify individuals' interests and preferences using patterns of connectivity in OSNs. In this study, we use a homophily-based interest detection method (Sharif Vaghefi 2018) to capture the shared interests of individuals and further compute the level of individuals' similarities in OSNs.

We use Twitter API for our data collection and collect the tweets and social network information of individuals' who had reported hacking vulnerability on their social network accounts. Using this novel dataset, we capture the association of individuals' interests with the observed vulnerability of individuals and conduct a comparative analysis to compare the effect of different type of interests. Moreover, we examine the effect of interest-based similarity on their vulnerability as well. Eight different communities of interest were found for the infected individuals in Twitter. We use multiple regression methodology for our model estimation and hypothesis testing. The results of our analysis show that an individual's vulnerability in OSNs is associated with the individual's interests. The magnitude of this association is different for each type of interest in OSNs. Furthermore, our analyses show that similarity of interest among individuals and their friends has a significant association to their vulnerability from their friends in OSNs.

This research makes a number of theoretical and practical contributions. First, our work contributes to the literature by identifying individuals' interests that promote their threat vulnerability. At the practical level, our study provides insights for individuals, platform managers and policy makers who want to understand and counter security threat propagation in

OSNs. We demonstrate that individuals are vulnerable from their friends. This study shows that an individual's protection alone doesn't guarantee a full security for individuals in OSNs. Also, OSN administrators should provide policies to have more control on security of the communities of interests.

3.2. Literature Review

3.2.1. Vulnerability in Online Social Networks

Vulnerability is a common term used by scientists in social science fields and refers to individuals' susceptibility to harm (Adger 2006, Eaking and Luers 2006, Anderson and Agarwal 2010). Vulnerability is the outcome of being exposed to threats and can be exacerbated by lack of adequate resources that allow timely threat prevention (Schröder-Butterfill and Marianti, 2006). In highly connected platforms such as online social networks, vulnerability of individuals and technologies themselves have been considered a severe form of security threat that can create big problems for the whole platform (West et al. 2009, Algarni et al. 2015). In security literature, individuals' behaviors have been recognized as one of the main sources of vulnerability to security failures (Furnell and Clarke 2012, Willison and Warkentin 2013). In fact, individuals are "the weakest links" in a security chain (Schneier, 2000, Sasse et al. 2001).

However, not all the individuals are the same. Individuals' characteristics and personalities make some individuals more vulnerable than others (Halavi et al. 2013). The main factor that makes people vulnerable is a lack of control (Halevi et al. 2013, Hu et al. 2015). Individuals with high desire to achieve pleasure, immediate gain, and being liked by others suffer more from their insufficient level of self-control. These individuals can easily become the target of attackers

(Irani et al. 2011). Prior research shows low level of self-control is a prominent attribute of individuals who are highly engaged in risky and imprudent behaviors (Piquero and Tibbetts 1996).

Table 3.1 reports a selected list of recent works that study the impact of individuals' behaviors on their vulnerability in OSNs.

Table 3.1. Overview of Individual's Vulnerability to Threat Attacks in OSNs

Study	Summary of Findings
Algarni et al. (2015)	The result of this study shows that perceived sincerity, competence, attraction, and worthiness of a source are significant predictors of individuals' vulnerability in social engineering. Source characteristics including number of friends, presence of individuals' real name, and number of posts in OSNs have significant impact on perceived sincerity. Being a celebrity, educational level, and wealth have a significant impact on perceived competence. Good looks and good writing skills have significant impacts on perceived attraction. Authority, sexual compatibility, and reciprocity have significant impacts on perceived worthiness. Finally, gender, age and security knowledge have significant impacts on vulnerability to social engineering.
Wald et al. (2013)	This study found that number of friends, number of followers and Klout score (user's influence in online social network) are important factors in predicting vulnerable individuals in Twitter.
He (2012)	This paper studies social media risks and offers strategies to reduce threats around organizations.
Modic and Lea (2012)	This study found a direct relationship between individuals' vulnerability and personality traits. Premeditation, extroversion, agreeableness and educational level of participants have significant effect on the level of individuals' vulnerability.
Irani et al. (2011)	There are three types of attack in OSNs: recommendation-based, demographic-based and visitor-tracking based. In recommendation-based approach, attacker suggests users follow or contact bogus pages based on their preferences. In demographic-based approach, attackers not only consider individuals' preferences but also their demographic factors. Finally, in visitor tracking-based approach, users are enticed to connect to users who visited their online profiles.
Li et al. (2011)	Disclosure of profile information such as demographic factors and individuals' preferences make users more vulnerable.
Yan et al. (2011)	This paper studies the spread of malwares in location-based OSNs by using a simulation approach. Their findings show that presence of high clustered networks, level of users' activities, number of infected users in early stages of malware propagation and high probability of clicking on the shared links can significantly improve the degree of malware propagation in the OSNs.

Faghani and Saidi (2009)	This study used a simulation approach to simulate the spread of two types of worm in OSNs. They found that visiting posts of non-friend users and current number of infected users in clustered networks are the parameters that impact on propagation of worms.

Vulnerability in online social networks can manifest in the forms of privacy vulnerability and security vulnerability. In privacy vulnerability, individuals' disclosed information is used by third-parties or attackers to gain benefits without the users' awareness (Pierson 2012). In security vulnerability, users become targets of malware attacks from attackers who purposefully try to harm groups of users in the OSN platforms based on the factor of trust (Coronges et al. 2012). Attackers mimic the structure of trustworthy entities in OSNs and convince people to run malicious codes. The way these malwares propagate through social networks is similar to disease propagation in a network. In contrast to privacy vulnerabilities, users generally play active roles in the formation and propagation of security vulnerabilities. In this study, we focus on the security form of vulnerability and discuss how individuals' interests and preferences can play a detrimental role in formation of such vulnerabilities.

3.2.2. Interest in Online Social Networks

Individuals' interests and preferences are among the main reasons behind their security vulnerability (Irani et al. 2011, Li et al. 2011). Interest and preference shape attitudes and behaviors (Miller 1999, Ranter and Miller 2001, Hidi 2006). Individuals' interest-based attributes make significant contributions to what people pay attention to and remember (Ebbinghaus 1964, James 1983). Research demonstrates that interest can facilitate learning, improve understanding and stimulate effort and personal involvement (Miller and Ranter 1998).

The influential theories of human motivation assume that people actively pursue their interests in order to maximize their utility, reinforcement, or the pursuit of pleasure (Miller and

Ranter 1998). Moreover, it is well-established that there is a direct relation between individuals' interests and their level of self-control (Wilcox and Stephen 2012). Individuals who have high tendency and interest toward a subject generally have low self-control about it (Gino et al. 2011). In the context of security vulnerability, research shows that victims are often targeted based on their interests and emotional triggers (Halevi et al. 2013).

In OSNs, individual users follow their favorite pages and users, upload photos and post comments based on their interests (Probst et al. 2013). Demonstrating categories of individuals' interests are feature of the most OSNs (Liu and Maes 2005). Such categories may include indications of a person's literary or entertainment interests, as well as political and sexual ones (Gross and Acquisti 2005). Most of the connections in OSN among unknown people are formed based on common interests. In OSNs, the benefits of following interests offer self-presentation, enjoyment and capability to keep social connections (Wilcox and Stephen, 2012). Accordingly, in this study, we consider observed individuals' interest-based attributes in OSNs and argue how different types of interest can play a role in individuals' level of security vulnerability. The next section provides the theoretical foundation for our research.

3.3. Theoretical Foundations

The dual-system theory and the theory of homophily form our theoretical framework in this study.

3.3.1. Dual-System Theory

The human brain seeks to find appropriate motivational activities. This requires overcoming two main challenges (Miller 1999, Scot 2000, Hofmann et al. 2009). First, how activities are reasonable to be performed? Second, how activities meet with individuals' pleasure. Dual-system theory indicates that there are two different systems in the human brain which control whether to persist or avoid a behavior (Hofmann et al. 2009). The first system is the impulsive system, and the second system is the controlling system. The impulsive system generates motivations and incentives to engage in the behavior while the controlling system analyzes the behavior and determines whether it matches with rational behaviors (Hofmann et al. 2009, Turel and Bechara 2016). These two systems work together to overcome challenges and determine motivational activities for individuals. Prior research shows that individuals with a weak controlling system may be chronically at risk from their impulses and urges to do activities based on their interests. In contrast, people who have a strong controlling system are more successful in resisting the urge to perform an activity even if it is in line with their interests (Friese and Hofmann 2009).

There are many empirical supports for dual-system theory in experimental psychology and neuroscience (Viswanathan and Jain 2013). The dual-system theory has been used in clarifying the notion of problematic and risky behaviors such as gambling, drinking, smoking, overeating and excessive use of OSNs (Evan 2008, Turel and Qahri-Saremi 2016). In all these problematic behaviors, the individuals' mind puts a higher value on smaller but immediate rewards. Accordingly, people with a higher interest and temptation toward problematic behaviors have less self-control. Hofmann et al. (2010) also discuss that the presence of stimulus items with high consummatory aspects of reward (e.g. smoking, sexual behavior) can make the process

of self-control increasingly difficult. In this study we rely on the problematic aspects of individuals' interests and assert that certain types of interest can impact individuals' level of vulnerability in OSNs.

3.3.2. Theory of Homophily

Homophily is defined as an individuals' tendency to interact with others who are similar to them (McPherson et al. 2001). The level of similarity can be determined by various sociodemographic and psychographic attributes within social networks (McPherson et al. 2001, Gu et al. 2014). "Homophily limits people's social worlds in a way that has powerful implications for the information they receive, the attitudes they form, and the interactions they experience." (McPherson et al. 2001 p. 415). There are two types of homophily: "status" homophily and "value" homophily (Lazarsfeld and Merton 1954, McPherson et al. 2001, Sherchan et al. 2013). Status homophily refers to the phenomenon where individuals with similar social status characteristics such as race, age and ethnicity are more likely to interact with each other. Value homophily refers to the phenomenon where individuals with similar interests, values, and attitudes have a greater tendency to interact with each other (Brechwald and Prinstein 2011). The tendency of developing relationships with similar others are based on the fact that individuals have more chance to be liked or confirmed by similar others (Gu et al. 2014). Additionally, it is easier for people with similar mindsets to develop trust-based relationships with each other (Winter and Kataria 2013, Tang et al. 2013). The more similar two individuals are, the more likely that they trust each other. Trust is the basis of a strong friendship (Hatfield 1984, Winter and Kataria 2013) and homophily can facilitate development of such relationships (Winter and

Kataria 2013). In this study we argue that while individuals' level of similarity can increase the level of trust, it increases vulnerability of individuals in online social networks.

3.4. Model Conceptualization

3.4.1. Communities of Interest and Individual's Threat Vulnerability

Rational decision making is a process in which individuals make risk-averse decisions in pursuing their goals (Halevi et al. 2013). However, people tend to underestimate present risks in their choices (Kahneman and Tversky 2013). They will accept costs and risks associated with their choices to gain pleasure (Hofmann et al. 2009). People who put more weights on pleasure have stronger impulsive systems and have less control over their behaviors.

Individuals' interests and preferences are pathways to pleasure. They are the basis of motivational activities. Research shows that individuals' interests impact their level of self-control (Gul and Pesendorfer 2004). In fact, strong interests and preferences toward an object leads to temptation and lower level of self-control (Baumeister 2002). People with low self-control tend to underestimate the negative consequences of their past behaviors and do not refrain from pursuing those behaviors. Research shows that this group of people are take more risk and pay less attention to security indicators and alerts (Dhamija et al. 2006). This can increase the level of individuals' vulnerability to security threat in OSNs.

OSNs facilitate the process of following interests and preferences. They allow individuals to join communities of interest that represent their interests, preferences, and way of thinking (Zillmann and Bryant 1985, Zillmann 1988). In doing so, individuals follow social pages that are

compatible with their interests and form their social environment within the platforms (Han et al. 2015). Being in such a social environment puts individuals into a less risk-averse situation. In fact, individuals tend to take higher security risks in order to enjoy features of online platforms and follow their own interests (Govani and Pashley 2005). In other words, individual users follow their interest in OSNs and have the perception that the benefits of pursuing their interests are larger than the associated costs of any security threat. On the other hand, individuals' interests and preferences can be used by OSN administrators and commercial companies to identify their potential audiences and identify targets for advertisements. These factors can compromise individuals' security (Gupta et al. 2016). As a result, communities of interest in OSNs expose individuals to security risks and domains (Halevi et al. 2013). We argue that this lack of self-control in communities of interest allows hackers to target people within the communities and increases individuals' vulnerability. Hence:

> ***Hypothesis 1.*** *Individuals' threat vulnerability is positively associated with strength of following communities of interest in OSNs.*

3.4.2. Overall Similarity of Interest and Individual's Threat Vulnerability

Similarity of interests would be a viable source of making connections and friendships among users. Similar users are more likely to establish trust relations (Tang et al. 2013). Trust among friends make them influential (Colquitt et al. 2007). A recent study shows that similarity can enhance the persuasion power of individuals. Security attackers can take advantage of such persuation power (Fang and Hu 2016). Individuals influence their friends to participate in risky behaviors (Valente et al. 2005, Brechwald and Prinstein 2011). For instance, literature reports the influential power of peers in the formation of individuals' tobacco and alcohol consumption habits (Hoffmann et al. 2007, Trucco et al. 2011, Simon-Morton and Farhat 2010).

In OSNs, self-disclosed information by individuals is a source of peer influence (Sharif Vaghefi 2018, Huang et al. 2014). Individuals have a biased perception about their friends' online behaviors and accept them with little hesitation (Huang et al. 2014). Moreover, the strong trust relationship among individuals in OSNs is one of the main reasons attackers focus more on this platform (Gupta et al. 2016). Since trust is greater among friends with more similarities, this makes individuals vulnerable to the risky behavior of their like-minded friends. Hence, we argue that similarity of individuals' interests makes individuals vulnerable in their relationships in OSNs. Therefore, we posit:

> ***Hypothesis 2.*** *Individuals' threat vulnerability is positively associated with the level of individuals' interest-based similarity to their friends in OSNs.*

3.5. Data Collection and Measurement

3.5.1. Data Collection and Network Creation

Data for this study was collected from Twitter. Twitter is a platform in which users talk about their daily activities and share their life events. To collect our dataset, we used the proposed data collection framework in Essay 1. We identified hacked users through keyword matching in Twitter API. Over a three-month time period (24 July – 21 October 2017), we captured 32,406 tweets in which users explicitly mentioned that their Twitter account had been hacked. Next, we used Twitter API once again to find the pattern of relationships among hacked users. We ended up with a network called a hacked network of 8,271 connected hacked users in Twitter.

3.5.2. Variable Measurements

In this study, we argue that individuals' vulnerability from online social networks is associated with two types of individuals' interest-based factors: 1) individuals' interests and preferences within online social networks, 2) interest similarity of friends in the hacked network with individuals. Accordingly, at the first step we review the measurement of vulnerability in online social networks (our dependent variable) and then describe the measurement of individuals' interests and similarity factors in detail.

3.5.2.1. Measurement of Vulnerability

V_k measures the level of the individual's vulnerability to security attacks from hacked friends in the OSN. For this measurement, we compute the likelihood of becoming infected for each user by calculating the sum of the probability that each individual is exposed to infection content posted by infected friends who were hacked before them.

$$V_k = \sum_{i \in O_k} d(t_k - t_i) \tag{3.1}$$

where t_k is the infection time of user k, $d(t_k - t_i)$ is the probability distribution of time differences between infection time of user k (t_k) and user i (t_i), O_k is the set of infected users that user k follows.

3.5.2.2 Measurement of Individuals' Interests

In order to identify individuals' interests, we adopt the proposed Homophily-based Interests Detection (HID) method offered by Sharif Vaghefi (2018). This method identifies communities of interest based on the extended bipartite graphs within online social networks. An extended bipartite graph in online social networks consists of two separate networks: the social network of individuals and the bipartite network of individuals and social pages. A social network of individuals refers to a graph in which a node represents an individual and an edge indicates the existence of reciprocated relationship between two individuals. A bipartite network of

individuals and social pages is a graph that has two types of node (individuals and social pages), and edges represent the pattern of following social pages by individuals (Sharif Vaghefi 2018).

At the first step, we formed a network of hacked-users who have a two-way connections (each pair of users follow and are followers of each other) by removing the one-way connections in the network. In the second step, we identified social pages that followed by at least 1% of users. We formed the bipartite network based on the pattern users followed these pages.

In the next phase, we identified communities of interest by clustering social pages into distinct groups. In doing so, we followed the HID method and performed the following steps: (i) network simplification, (ii) network clustering and (iii) cluster labeling.

(i) Network simplification: this step converts our extended bipartite graph into a weighted graph of social pages. To accomplish this task, the HID method computes the similarity of social pages based on the network structure of their followers using the following formula:

$$Sim(N_{SA}, N_{SB}) = \frac{(|V(N_{SA},N_{SB})|+|E(N_{SA},N_{SB})|)^2}{(|V(N_{SA})|+|E(N_{SA})|)\ .(|V(N_{SB})|+|E(N_{SB})|)} \quad (3.2)$$

Where N_{SA}, N_{SB} represent the network of followers for social pages A and B. V is the number of nodes and E is the number of links (relationships) in networks. $Sim(N_{SA}, N_{SB})$ has a value between 0 and 1.

(ii) Network clustering: at this step, the weighted graph of social pages is clustered into different groups using the Louvain clustering method (Blondel et al. 2008). This step resulted into eight distinct communities of interest. (iii) Cluster labeling: this step assigns labels to identified clusters. The labels represent latent groups based on common attributes of social pages in each cluster. In order to find the labels, we collected the description of social pages from Twitter and Wikipedia. Next, we created aggregated documents using unique words found in description of

social pages within each cluster. We then applied the TF-IDF method to find unigram keywords that distinguish one cluster from the others, where unigram keyword is defined as keyword that consists of a single word.[2] TF-IDF stands for time frequency-inverse document frequency method, which is a standard tool in text mining (Salton and McGill 1983). This method represents each document by a weighted vector with the size of its overall vocabulary $(v_1, v_2, \dots, v_n)$, where v_i is calculated as:

$$IDF_i = \frac{Total\ number\ of\ documents}{Number\ of\ documents\ contain\ term\ i} \quad (3.3)$$

$$TF_i = The\ term\ frequency\ of\ term\ i\ in\ document\ D \quad (3.4)$$

$$v_i = TF_i \times log\ (IDF_i) \quad (3.5)$$

Using these terms, a proper label was assigned to each cluster. We refer to each cluster as one community of interest. Figure 3.1 shows an example of captured terms for the Rap & Hip-Hop Music community of interest. The captured high ranked terms for the remaining communities of interest are in Appendix B.

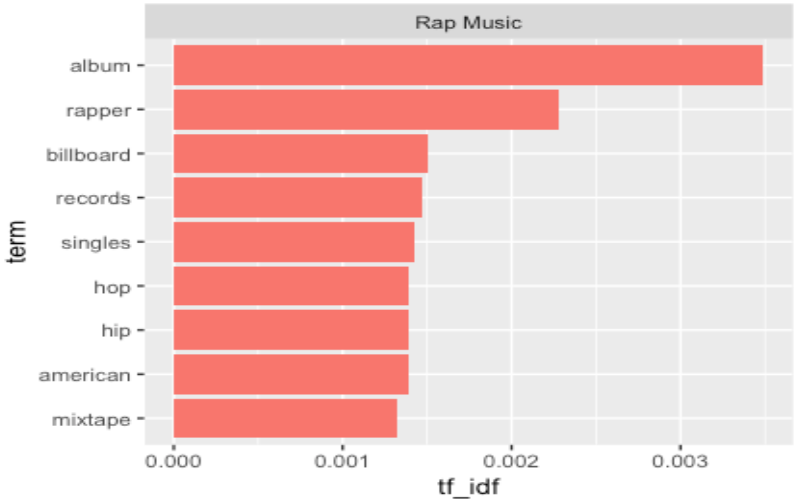


Figure 3.1. Terms with High TF-IDF Weight in Rap Music Community of Interest

[2] https://en.wikipedia.org/wiki/N-gram

Table 3.2 shows labels for all eight detected communities of interests.

Table 3.2. Communities of Interest

Labels	Number of Pages
Media & Technology	640
Pop Music	613
Rap Music	482
Liberal Politics	369
Business Leaders	234
Video Games	182
Conservative Politics	124
Indian Personalities	31

Table 3.3 demonstrates the top ten followed social pages within each community. After formation of the communities of interest, we measured individuals' level of interest toward each of the above communities of interest by computing the normalized value of followed number of social pages/accounts by each individual within each community of interest.

Table 3.3. Sample of Social Pages in Each Community of Interest

Community of Interest	Top Ten Social Pages
Media & Technology	YouTube Twitter Instagram Google LLC Netflix National Geographic BuzzFeed Inc. Marvel Entertainment Apple Music TED
Pop Music	Ariana Grande Justin Bieber Kim Kardashian Taylor Swift Katy Perry Selena Gomez Lady Gaga Miley Ray Cyrus Demi Lovato Kylie Jenner

Rap Music	Rihanna Drizzy Chance Owbum Wiz Khalifa Kendrick Lamar Nicki Minaj Tyler Okonma Kevin Hart J. Cole Lil Wayne
Liberal Politics	Barack Obama President Obama Hillary Clinton CNN Breaking News The New York Times CNN BBC Breaking News Michelle Obama Bernie Sanders The Washington Post
Business Leaders	Ben Landis Harjinder Singh Kukreja Murray Newlands Aimee Beck Ken Rutkowski John Rampton Denise Landis Roger James Hamilton Ari Sytner Nathan Allen Pirtle
Video Games	PlayStation Xbox Markiplier Rockstar Games Nordan Shat FaZe Clan Twitch Jacksepticeye IGN World Wrestling Entertainment (WWE)
Conservative Politics	Donald J. Trump President Trump The White House Melania Trump WikiLeaks Fox News Vice President Mike Pence Ivanka Trump Donald Trump Jr. Mike Pence

Indian Personalities	Narendra Modi and PMO India Priyanka Shah Rukh Khan Amitabh Bachchan Aamir Khan Salman Khan Sachin Tendulkar Deepika Padukone Virat Kohli Hrithik Roshan

3.5.2.3. Measurements of Average Similarity of Interests

The next independent variable is the average interest similarity of an individual and his/her friends in the social network. Two people are more similar when they have more common attributes. For computing similarity, we measure the pairwise similarity between individual and his/her friends' interest scores. In doing so, we computed Euclidean distance between the interest scores of individual users *i* and *j* as:

$$Euc(i,j) = \sqrt{\sum_{n=1}^{N}(i_n - j_n)^2} \quad (3.6)$$

where *N* is the number of communities of interest, and i_n is user *i*'s interest score in community *n*. We then normalized $Euc(i,j)$ by dividing it by the maximum distance between interest scores of users *i* and *j* as:

$$Norm.Euc(i,j) = Euc(i,j)/Max(Euc(i,j)) \quad (3.7)$$

We computed the similarity of interest between two individuals by converting distance to similarity as follows:

$$\mathrm{Sim}\ (\mathrm{i},\mathrm{j}) = 1 - \mathrm{Norm.Euc}(\mathrm{i},\mathrm{j}) \quad (3.8)$$

Finally, we computed the average interest similarity between each individual and his/her friends. Thus, the overall average similarity of interest between individual user *i* and his/her friends is:

$$\mathrm{OSim_i} = \frac{1}{\mathrm{K}}\sum_{\mathrm{j}\in F_i}\mathrm{Sim}(\mathrm{i},\mathrm{j}) \quad (3.9)$$

where K is the number of people with whom users i has a two-way connection, and F_i is the set of user i's two-way connections

3.5.2.4. Control Variables

For studying the relationship between interest and an individual's threat vulnerability, we controlled for the individual's factors discussed on Essay 1. Accordingly, we considered the individual's out-degree centrality, strength of ties with friends and his/her OSN activity as control variables. See Table 2.4 for the measurement method of each control variable.

3.6. Model Estimation and Analysis of Results

3.6.1. Check for Multicollinearity

Multicollinearity refers to a linear relation between two variables. For multicollinearity diagnostics between the independent variables, we examined two methods: variance inflation factors (VIF) and condition index. When testing VIF, the general rule of thumb is that VIFs greater than 10 cause concern about multicollinearity and need more investigation (Neter et al. 1989, Menard 2002). Since the largest VIF in our case is 2.05, multicollinearity does not appear to be a problem with the data used in this study. Based on the condition index method, an index greater than 30 is an indicator of multicollinearity in the data (Dormann et al. 2013). In our case, the highest value of condition index is 5.88, which shows multicollinearity does not pose a threat.

3.6.2. Estimation of Vulnerability Distribution

The first step in determining individuals' vulnerability in a network is finding the threat propagation distribution in the network. We used the same procedure discussed in Essay 1 for determining the propagation distribution. We tested several distributions and exponential distribution was found to be the best distribution function.

3.6.3. Model Estimation

Appendix C reports the Pearson correlation values. We applied a multiple regression model to test our hypotheses. Table 3.4 shows the final estimation results. We added variables in a stepwise format to show the robustness of our model. Model 1 tested the relation between an individual's interest and his/her vulnerability. In Model 2, we added similarity of interest to create the full model, which examines the associations between an individual's interests, his/her similarity of interest with his/her friends and his/her threat vulnerability in the network. Moreover, to check for robustness of the estimated models, we randomly selected smaller samples of users and re-estimated our models using different sample sizes. Appendix D shows the graphs for the coefficients and p-values of the factors in the model using eight different sample sizes. Each sample was selected randomly. The results support the robustness of our estimated model and validate our findings.

Table 3.4. Estimate Results for Vulnerability Model

Coefficient	Model 1	Model 2
Intercept	0.00***	-0.01***
Pop Music	0.13***	0.10***
Business Leaders	0.16***	0.18***
Conservative Politics	0.03***	0.03***
Liberal Politics	0.22***	0.21***
Video Games	0.09***	0.08***
Rap Music	0.03*	0.03
Indian Personalities	0.02*	0.01
Media & Technology	-0.29***	-0.30***
Avg. Similarity of Interest		0.04***

Control Variable		
Out-degree centrality	1.53***	1.52***
Strength of ties with friends	0.05***	0.03***
Activity	0.00***	0.00***
R^2: 0.32	**0.32**	**0.36**

*** *p<0.001, ** p<0.01, * p< 0.05*

Results indicate that having interests in Pop Music, Business Leaders, Politics (both conservative and liberal) and Video Games have positive and significant relations to an individual's threat vulnerability (p<.001). Among the above-mentioned interests, having interest in Liberal Politics has the highest coefficient (beta= .21). Thus, individuals who had interest is people and news with Liberal Politics had the highest level of vulnerability in our data collection time period.

The next community of interest is Media & Technology. In contrast with our expectation, results show that having interest in this community has a significant negative association with individuals' vulnerability (beta= - .30, p<0.001). One possible explanation for this unexpected result can be due to the level of awareness in this group of people. We will discuss with more detail in discussion section. Our result also indicates that having interest in Rap Music and Indian Personalities communities of interest does not have significant impact on individuals' level of vulnerability.

Considering all the results, we found that the association of interest and threat vulnerability is the context dependent factor. Further analysis is needed to find the factors inside each community of interest that can contribute to its level of vulnerability.

The other independent variable in our model is individuals' average level of similarity. Our results indicate that the average similarity of interest between individuals and their friends has positive and significant effect on individuals threat vulnerability from their friends in the OSN (beta = .04, p<0.001). Therefore, the results support our second hypothesis (H2).

3.7 Discussion

This study investigated whether individuals' interests play any role in their vulnerability to security threats in OSNs. While some studies show the association between individuals' demographic factors and their levels of vulnerability through social engineering and phishing attacks (Jakobsson et al. 2007, Vishwanath et al. 2011), no study addresses the relation of individuals' interest to their level of vulnerability in OSNs. This study addresses this gap by collecting a novel dataset of hacked users and their social networks within Twitter. The first research question in this study is how communities of interest affect individuals' threat vulnerability in OSNs. The second research question addressed the role of interest-based similarity of individuals and their friends in the level of vulnerability in OSNs. Guided by a synthesis of dual-system theory and the theory of homophily, we developed our research model and answered our research questions by extracting observed individuals' preferences in OSNs with the use of the HID method (Sharif Vaghefi 2018). In total, we identified eight communities of interests: Pop Music, Business Leaders, Conservative Politics, Liberal Politics, Video Games, Rap Music, Indian Personalities, and Media & Technology. The estimation of the model has revealed how individuals' interests toward these communities can impact their level of vulnerability.

First, we found that the magnitude and direction of relation between individuals' preferences and their level of vulnerability depends on the type of preferences. Our results indicate that interests in Pop Music, Business Leaders, Conservative Politics, Liberal Politics, and Video Games communities of interest have positive and significant associations with levels of vulnerability. Findings also show that interests in Media & Technology have a significant and

negative association with individuals' vulnerability to security threats. We have not found significant results for Rap Music or Indian Personalities.

Second, communities of interest that are positively associated with vulnerability level have different natures. Some communities of interest like Video Games generally are followed by the younger people. The desire to gather immediate information from this group of users might be the main reason behind the positive association with threat vulnerability. Other communities of interest such as political communities are generally followed by adults who are interested in politics and political parties. These users might be targeted by hackers through their social networks. Further analysis on patterns of hacking in these diverse communities of interest would give us a better picture of the contributing factors in different communities of interest.

Third, one unexpected result was the negative and significant association between Media & Technology communities of interest and individuals' level of vulnerability from their immediate social network. One possible explanation on this finding is the presence of higher level of awareness among people with interests toward this community. In past few years, media companies have experienced considerable number of attacks and threat propagation in their system. Huge data breaches in Yahoo and Sony Pictures are two examples of such events. These negative experiences in past can contribute to heightened awareness within these communities.

Fourth, the empirical results of this study show positive and significant association between similarity of interests in OSN and level of vulnerability. According to the concept of Homophily, individuals are more attracted to those who have similarity with them. This similarity can be in the form of having similar interests and preferences. While prior studies report that interest similarity can increase the level of individual's enjoyment from being in their group of friends, our result shows that this similarity can also increase their level of

vulnerability. The main reason behind it is that friends with higher level of similarity have higher level of trust in each other and can follow each other's behaviors with little caution.

3.8. Theoretical and Practical Implications

3.8.1. Theoretical Implications

This research makes several contributions to theory and research. First, in this study we offered a new approach for conducting studies on hacked networks in OSNs. We used Twitter, one of the popular public OSNs, to collect observational data at the individual level and to analyze the relationship of interest-based factors with their vulnerability level. Our approach can be adopted by other researchers to investigate additional contributing factors to individuals' security vulnerability.

Second, we added to the literature by adopting homophily and dual system theories to show how individuals' interest-based factors can increase their level of vulnerability in OSN. To the best of our knowledge, no study has investigated the role of interest in this domain. This provides great potential for researchers to build on this model and investigate additional aspects of individuals' interests and preferences within security domain.

Third, this work makes a novel contribution by studying the association of interest-based similarity within friends in OSNs with their vulnerability to security threats emanating from such friends. This finding indicates not only friends can be direct source of social influence in online social networks, but that their level of similarity to individuals can also make them more vulnerable to security threats in OSNs.

3.8.2. Practical and Policy Implications

The results of our study provide a number of important implications for practitioners and policy makers. Nowadays, online social networks have become ubiquitous. Research shows that people spend more time on these platforms than on any other media. Such broad levels of access and connections among individuals make them ideal platforms for hackers to propagate different forms threats. Our findings show individuals' interests and preferences can be used to attack both individuals and their friends, which has great implications for security administrators and protection agencies. They need to capture propagation of threats within communities of interest and identify potential victims of such threats to offer complementary security protection to them. That can help to control a threat before it becomes an epidemic.

Another implication of our study is for individuals. They need to know that attackers in social networks not only target them based on their personal factors but also through their close friends. They need to make sure that they are following security guidelines even in communication with their close friends. Administrators of OSNs should not only provide additional privacy and security protections for individuals who have been victimized by hackers, but also send alerts and notifications to the immediate social networks of such users notifying them about the attack and the compromised accounts in order to prevent the propagation of attacks.

Finally, we found that different communities of interest might lead to different levels of security threat vulnerability. The effect of these communities of interest may change over time as different communities become the target of attackers based on various social and political events. Hence, individuals should be more aware about threats coming from communities of interest and make sure all the content in these communities is coming from secure and safe sources.

3.9 Limitations and Future Research

This study is subject to several limitations. This research focused on individuals who encountered security threats in Twitter. Since studying the network containing the whole infected individuals with their friends is impossible, in this study we focused on the hacked network, considering infected individuals along with their infected friends. Therefore, interpretation of our results is limited to the captured population sample. Second, our analysis was limited to hacked networks within the Twitter platform. Future studies can validate our results by capturing data from other online social network platforms such as Facebook and Instagram. Third, in this research we relied on the self-reporting of individuals to capture hacked users. Future studies can expand the hacked network by collecting data at a broader level. Fourth, our study was limited to eight captured communities of interest that were extracted from the structure of OSNs. Future studies may add to this data by collecting interest and preference information from self-reported data.

CHAPTER 4

Essay 3: The Role of Addiction to Online Social Networks in Individuals' Online Security Behaviors

4.1. Introduction

In recent years, the role of online social networks (OSNs) has increasingly grown in individuals' lives. People use OSNs for their day-to-day interactions and benefit from them in their business, education, health, and entertainment. Research shows that the more people get connected to OSNs, the less control they have over their level of usage (Griffith et al. 2014, Chan et al. 2015). The tendency to use OSNs remains in an unconscious part of human brain and users do not realize how much time they have spent in these platforms (Balakrishnan and Shamim 2013). The structure of OSNs (i.e. having a like button, getting comment, joining to different communities, posting daily routines, sharing photos, and etc.) encourage individuals to engage in more activities (Griffith et al. 2014).

It was argued that OSNs are designed to get users hooked (Andreassen 2015). According to a recent study, people spend on average about five years of their life on OSNs[3]. Moreover, one survey study found that about 30% of individuals' total time in online platforms is spent in OSNs[4]. This excessive use can be problematic (Kuss and Griffiths, 2011) and leads to addiction (Orford 2001, Fenichel 2010)

[3] https://www.adweek.com/digital/mediakix-time-spent-social-media-infographic/
[4] https://www.socialmediatoday.com/marketing/how-much-time-do-people-spend-social-media-infographic

Addiction used to be thought of as uncontrolled physical dependency on substances, drugs, or alcoholic beverages. In past few years, the context of addiction has been broadened to include excessive levels of behaviors such as gambling, playing video games, overeating, television viewing, internet use and more recently, use of OSNs (Young 1998, Griffith 2005, Andreassen and Pallesen 2014, Fenichel 2010). Behavioral addiction causes disorders in decision making (Griffith 2005, Enrique 2010, Grant et al. 2010, Albrecht et al. 2007).

One of the main domains of behavioral addiction is addiction to technology. Technology addiction can be defined as an individual's maladaptive psychological state of dependence on computer-mediated activities (Turel et al. 2011). Technology addiction distorts individuals' perceptions about the system to which they are addicted (Turel et al. 2011, Bernroider et al. 2014). Technology-addicted people maintain overrated positive attitudes towards the system and in most cases exaggerate the system's attributes and functionality (Turel et al. 2011, Bernroider et al. 2014).

In the last few years, individuals' addiction to OSNs, as a type of technology addiction, has grabbed more attentions (Andreassen 2015, Kuss and Griffith 2011, Andreassen et al. 2012, Anderassen and Pallesen 2014). OSN-addicted people "engage in social networking to gain control but become controlled by their social networks" (Andreassen 2015). Research shows that addiction to OSNs has negative impact on the individual's academic/work performance, psychological and physical health, societal relationships and sense of responsibility (Kuss and Griffith 2011, Andreassen and Pallesen 2014, Ryan et al. 2014, Andreassen et al. 2014). But the negative effects of addiction to OSNs do not limit to behaviors outside the platform. It was shown that OSN-addicted users underestimate the risks involved in online platforms (Kuss and Griffith 2011, Turel and Qahri-Saremi 2016, Turel et al. 2011). This raises the concern that

OSN-addicted people may also underestimate the security measures and do activities that not only causes problems for themselves, but also for other people within their social networks. Despite the importance of the problem, there is inadequate research on the role of addiction to OSN in individuals' security perceptions and behaviors.

Additionally, prior studies provided evidences for interconnection between cognitive and behavioral aspects of using OSNs (Turel and Qahri-Saremi 2016, Zheng and Lee 2016). But, there is no study that show how different mechanisms in human's brain are related to OSN addiction.

To address these gaps, we have developed the Online Addiction Security Behavior (OASB) theory by synthesizing the dual-system theory and the extended protection motivation theory (Liang and Xue 2009, Chen and Zahedi 2016). We OASB to conceptualize a model to address the following research questions 1) What are the roles of brain systems in OSN addiction. 2) What is the role of OSN addiction in the addicted users' security perceptions and security behaviors?

To answer the first research question, we draw on dual-system theory. Dual-system theory argues that brain has two systems: impulsive system and controlling system, which promote and inhibit given behaviors (Hofmann et al. 2009). The impulsive system motivates engaging in activities regardless of their risks or costs, while the controlling system evaluates activities to find coincidence with rational behaviors and inhibits risky behaviors (Hofmann et al. 2009, Turel and Bechara 2016).

To answer the second research question, we apply the extended protection motivation theory—extended PMT—(Liang and Xue 2009, Chen and Zahedi 2016). The extended PMT argues that individuals' protective responses are formed by interactions between two processes,

namely, threat appraisal and coping appraisal (Floyd et al. 2000). These two types of appraisals in can be used to explain why people engage in maladaptive and risky behaviors. Extended PMT considers three coping behaviors: taking protective actions, seeking help and limiting use. We examine two coping behaviors (taking protective actions and seeking help) in our model. Since limiting use contradicts with the nature of addiction, limiting use is not relevant in this study.

In order to conduct this study, we collected data through a survey from a representative sample of users. The structural equation modeling (SEM) method is applied to estimate our conceptualized model. The results of our analyses show for OSN addicts, there is a strong impulsive cognitive-emotional preoccupation with using OSN. The results also revealed the significant impacts of OSN addiction on security perceptions and the coping efficacy of the individuals. OSN addiction increases individual's perceived susceptibility to and severity about online security threats. Moreover, OSN addicted users have low self-efficacy to security threats.

This research makes a number of theoretical and practical contributions. We developed a new theory to show how the brain's impulsive system can explain the behavior of OSN addicts and also how OSN addiction impacts security perception and the coping behavior of individuals. Our study provides insight for individuals, mental health practitioners, security awareness programs and policy makers to understand the relationship between addiction to OSNs and security behaviors, and decreases the possible negative security consequences of that relationship. This research can enhance individuals' awareness about the consequences of OSN addiction and how addiction can impact security perception. Policy makers and security managers can use the results of this study to develop new security measures for OSN-addicted individuals.

4.2. Literature Review

4.2.1. OSN Addiction

In late 90s, "addiction" referred to any uncontrolled dependence on physical substances such as drugs and alcohol. Later, the term "addiction" moved beyond this definition to include the behaviors where drugs are not involved such as gambling, video game playing, overeating, and television viewing (Young 1998). This type of addiction is defined as a behavioral addiction. There are similarities between behavioral and substance addictions, but both of them have biopsychosocial support (Griffith, 2005, Albrecht et al. 2007). Behavioral addiction causes disorders in making decisions. Symptoms such as salience, mood modification, tolerance, withdrawal, conflict and relapse are similar among all addictive behaviors and are known criteria for identification and diagnosis of behavioral addiction (Sutton 1987, Turel et al. 2011, Griffith 2005, Albercht et al. 2007, Sussman et al. 2011).

In IS, behavioral addiction is defined as a technology addiction which covers any mental dependence on a technology (Turel et al. 2011). Technology addiction is defined as a psychological state of maladaptive dependency on the use of a technology to such a degree that the typical behavioral addiction symptoms arise (Turel et al. 2011). Technology addiction can take the form of internet addiction (Young 1998, Griffith 1999, Yellowlees and Marks 2007), smartphone and mobile device addiction (Bernroider et al. 2014, Turel and Serenko 2010), online gambling addiction (Griffith and Parke 2008, Mehroof and Griffith 2010) and online shopping addiction (Peters and Bodkin 2007, Turel et al. 2011). Internet addiction encompasses a broad category of behaviors and leads to impulse-control problems (Young et al. 1999). Prominent types of internet addiction are computer addiction (i.e. addiction to computer game

playing), information overload (i.e. addiction to web surfing), net compulsion (i.e. addiction to online gambling, online trading or online shopping), cyber-sexual addiction (i.e. addiction to online sex or pornography sites) and cyber-relationship addiction (i.e. addiction to online relationships). Since the main purpose of OSNs is to increase connection and communication through online platforms, addiction to OSN is a type of cyber-relationship addiction (Kuss and Griffith 2011).

Several terms have been used for studying OSN addiction: social network site addiction (Kuss and Griffith 2011, Andreassen and Pallesen 2014), social network dependency (Wolniczak et al. 2013, Thadani and Cheung 2011), social network disorder (Van den Eijnden et al. 2016), problematic use of social networking sites (Spraggins 2009, Meena et al. 2012, Chen and Kim 2013, Turel and Qahri-Saremi 2016), addiction to social networking sites (Wu et. al 2013), and compulsive use of social networking sites (Aladwani and Almarzouq 2016).

However, OSN addiction is different from the concepts of high engagement in OSN and habit (Davis 2001, Charlton and Danforth 2007, Andreassen 2015, Turel et al. 2011). Contrary to OSN addiction which is related to a psychological dependency of a person to OSNs and degree of his/her symptoms (salience, mood modification, tolerance, withdrawal, conflict and relapse) over using OSNs, habit and high engagement are not associated with psychological dependence on OSN (Turel et al. 2011). These behaviors stem from learning and are considered as controlled behaviors (Turel et al. 2011, Griffith 2010, Andreassen 2015). Moreover, habit is the result of cognitive processes or willful acts that cannot explain the irrational and out-of-control aspects of OSN addiction (Rosenstein and Grant 1997, LaRose et al. 2003).

According to the literature, excessive use of OSNs turns into social, psychological and professional conflicts and health problems for individuals (Kuss and Griffith 2011, Andreassen

and Pallesen 2014, Ryan et al. 2014). Problematic use of OSN is associated with the poor brain performance and leads to poor academic performance in university students (Turel and Qahri-Saremi 2016). OSN users have problems with postponement, distraction, and time-management (Kirschner and Karpinski, 2010). In addition, there is a negative association between time spent on OSNs and interactions with colleagues in work environments (Barker 2009). Research has demonstrated that women addicted to OSN have lost their jobs because of overuse of OSN (Karaiskos et al. 2010). In the context romantic relationships, overuse of OSNs is related to jealousy and relationship dissatisfaction (Luscombe 2009, Elphinston and Noller 2011). Moreover, disclosure of personal and private information on OSNs can lead to interpersonal electronic surveillance by a person's partner (Muise et al. 2009, Tokunaga 2011). In terms of psychological problems, OSN addicts lack ability to communicate in society (Xu and Tan 2012). They are more prone to experience negative feelings like anxiety and loneliness than others (Koc and Gulyagci 2013). Furthermore, OSN addicts experience low self-esteem and have low well-being scores (Valkenburg et al. 2006, Shaw and Gant 2002). OSN usage has led to problematic behaviors such as impulsivity and risky behaviors. (Turel and Bechara (2016). OSN addiction distorts the sleep pattern, causes back, eye and heart problems and decreases the activity. There is a relationship between OSN addiction and poor sleep. OSN addicts reported problems with delayed bedtimes (Wolniczak et al. 2013, Andreassen et al. 2012). Although the findings show the improper consequences of using OSNs, the impact of OSN addiction on individuals' thoughts and behaviors have not been fully investigated. Despite increasing security issues in OSN, research on the security consequences of using OSNs remains unexplored.

Recent studies have demonstrated concerns about security issues in OSN (Shin 2010, Gao et al. 2011, Zhang et al. 2010). Scholars claimed that individuals are the weakest point in

security of the systems. Individuals' beliefs regarding the importance of security protections may arise from their understanding of security threats and the effectiveness of security measures (Herath and Rao 2009). However, for OSN addicts, perception of online security threats may be distorted by their addiction. In general, technology addiction distorts the user's perception about the system to which they are addicted. Addicts are more positive about the system and exaggerate the system's attributes and functioning (Turel et al. 2011, Bernroider et al. 2014). This distortion causes variations in decision making about the behavior, and can lead to risky and thoughtless activities (Kuss and Griffith 2011, Turel and Qahri-Saremi 2016, Turel et al. 2011).

To understand the link between OSN addiction and security, one needs to understand if addiction to OSN is related to the imbalance between impulsive system and controlling systems in brain and whether OSN addiction have any impact on the security perception and coping behaviors. We expect that the conflict between the impulsive and controlling mental systems causes problems in proper decision making about using an OSN and affect addiction to OSN. We study whether perceptions distorted by OSN addiction impact the addict's security perception and coping behaviors of users in OSN as they encounter online security threats in OSNs.

4.3. Theoretical Background

The dual-system theory and the extended protection motivation theory form the framework to develop our Online Addiction Security Behavior (OASB) theory in this study.

4.3.1. Dual-System Theory

The idea that different mechanisms in the human brain can motivate or inhibit a behavior has a long history in cognitive, personality and social psychology studies (Epstein 1998, Strack and Deutsch 2004, Hofmann et al. 2009). Dual-system theory indicates two separate but interactive neural systems in the brain which determine whether we pursue or avoid a behavior (Bechara et al. 2006, Hofman et al. 2009). The first system is the impulsive (or reflexive) system of the brain and the second system is the avoiding (or controlling) system. System 1 generates motivations and incentives to engage in the behavior. System 2 analyzes the behavior and determines if the behavior is rational and matches the individual's goals (Hofman et al. 2009, Turel and Bechara 2016).

For a given behavior, the two-brain systems conflict about engaging or inhibiting the behavior. The relative strength of the activity triggered by the impulsive versus the controlling systems determines which system prevails (Strack and Deutsch 2004).

The dual-system theory has been applied in the study of problematic and risky behaviors such as gambling, drinking, smoking, overeating and problematic use of OSNs (Evans 2008, Everitt et al. 2008, Turel and Qahri-Saremi 2016). In problematic behaviors, dual-system theory explains the composition of disorder-specific strong impulsive system and weak controlling system (Wiers et al. 2013). In other words, an excessive impulsive system causes deficits in making decision (Bechara 2005, Hofmann et al. 2009) which can be identified as mental disorders in the forms of addictive and problematic behaviors (Turel and Qahri-Saremi 2016). Given conceptual similarities among OSN addiction and the other types of addiction and problematic behaviors, the dual-system theory is a sufficient theory for analyzing OSN addiction.

Recently many dual-system models have been applied to explain conscious/unconscious and addictive behaviors as special cases within general dual-system models (Tiffany 1990, Deutsch and Strack 2006, Bechara 2005, Wiers et al. 2012). Prior works have used different range of cognitive, emotional and behavioral factors to demonstrate and measure the two systems (Hofmann et al. 2009, Fries and Hofmann 2009, Soror et al. 2015). Collins and Lapp's proposed factors to represent System 1 and System 2 in the study of problematic use of alcohol consumption. Later, these factors were applied in problematic use of OSNs and excessive use of mobile social network sites (Turel and Qahri-Saremi 2016, Cao et al. 2018). Collins and Lapp's proposed difficulty of controlling alcohol use as the imbalance between cognitive-emotional preoccupation (System 1) and cognitive-behavioral control (System 2). For the sake of eliminating confusion, we call System1 as cognitive-emotional preoccupation and System 2 as behavioral control.

4.3.2. Protection Motivation Theory

Protection motivation theory (PMT) was first introduced by Roger (1975). It explains the effect of fear appeal on motivating health-related behavior. This theory has been applied in other areas to study environmental, security, political and protection issues threats (Floyd et al. 2000, Anderson and Agarwal 2010). In IS, PMT and technology threat avoidance theory (TTAT) (Liang and Xue 2009) are used extensively in security research and protective behaviors (Floyd et al. 2000, Liang and Xue 2009). These theories have been used in a number of security studies, including security behavior of employees and home computer users (Workman 2008, Anderson and Agarwal, 2010) and information security policy compliance (Herath and Rao, 2009, Vance et al. 2012). PMT

provides an understanding of changing attitudes and behavior in the face of threats (Floy et al. 2000).

PMT defines how people cope with a threat based on two appraisals: Threat appraisal and coping appraisal. Threat appraisal consists of two constructs: Perceived susceptibility and perceived severity. Perceived susceptibility is defined as "individual's subjective probability that a malicious IT will negatively affect him or her" (Liang and Xue 2009, p 80). Perceived severity is defined as "the extent to which an individual perceived the negative consequences caused by the malicious IT are severe" (Liang and Xue 2009, p 80). The two constructs of threat appraisal show the individuals' perceptions of threat. Coping appraisal includes two constructs: perceived self-efficacy and perceived response efficacy. Perceived self-efficacy refers to "users' confidence in taking the safeguarding measure" (Liang and Xue 2010, p 399). Perceived response efficacy refers to "the subjective of a safeguarding measure regarding how effectively it can be applied to avoid IT threat" (Liang and Xue 2010, p 399). PMT explains that an individual appraises a threat by his/her perception of the threat's severity, susceptibility to the threat and likelihood of being affected. After assessing the threat, self-efficacy and the efficacy of the recommended response are evaluated by the individual in order to avoid or reduce the threat. These four constructs evaluate individual's protective behavior.

Since addiction is associated with an "overactive appetite system" (Lang et al. 2005), it may influence an individual's security perceptions. Therefore, in this study we use the extended PMT applied to online security behaviors by (Chen and Zahedi 2016) to see the outcomes of security perceptions and coping behaviors of individuals. We focus on key security perceptions introduced by PMT and its extensions and examine how users' levels of addiction affect their security behavior by distorting these perceptions.

Extended PMT proposes three coping behaviors including: taking protective action, seeking help and limiting use. Taking action refers to applying protective tools, seeking help refers to individuals' efforts to find proper information and advice to deal with threats, and limiting use refers to avoiding uses of the system. Since our research focus is on OSN addicted individuals and the concept of limiting use is in contrast with addiction, we will not include it as a coping behavior in our model. Therefore, we considered taking action and seeking help as two coping behaviors in this study. We study whether perceptions and beliefs distorted by OSN addiction affect the security perception and protective behavior of individual users in OSN.

4.4. Model Conceptualization

In this research, we synthesize dual-system theory and extended PMT to build OASB theory. We theorized about online security behavior of OSN addicts, arguing that OSN addicts have different security perceptions and coping efficacies. Our conceptualization model consists of the following constructs: cognitive-emotional preoccupation, behavioral-control, OSN addiction, perceived security threats, perceived coping efficacy and security behavior. Figure 4.1 demonstrates our OASB model.

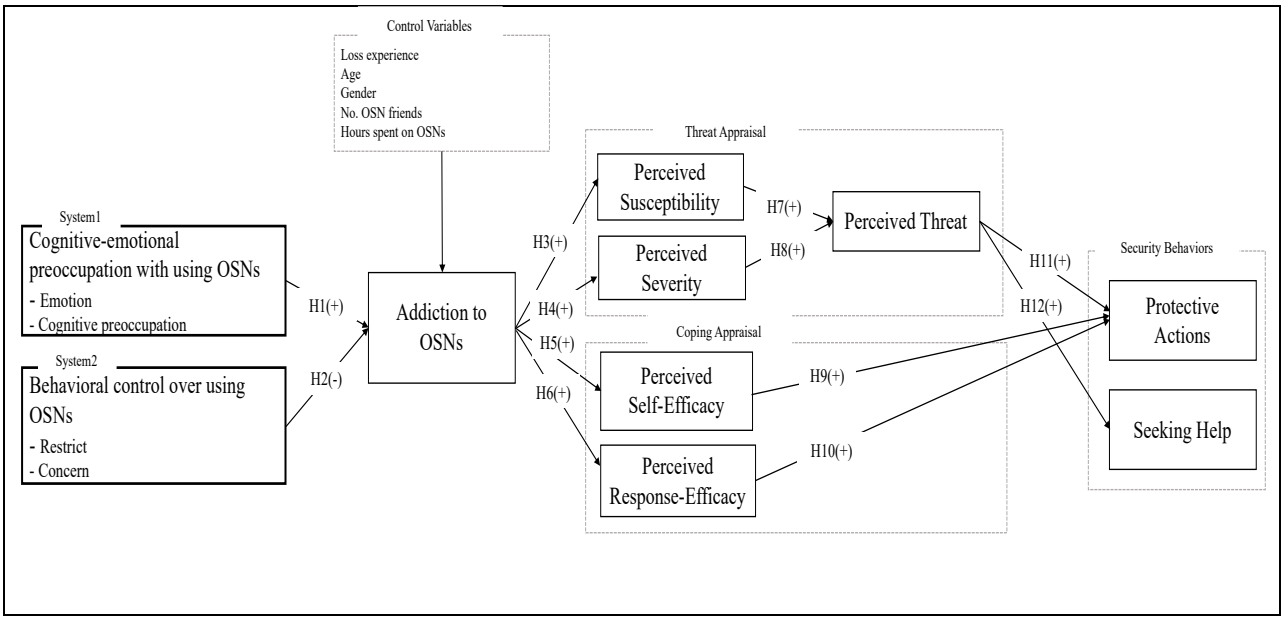


Figure 4.1. Online Addiction Security Behavior (OASB) Model

4.5. Hypotheses

Drawing on dual-system theory, we argue that OSN addiction is the result of high cognitive-emotional preoccupation with using OSN. The cognitive-emotional preoccupation with a behavior refers to obsession thoughts to persist in the behavior despite of its negative consequences (Fillmore 2001, Hoffman et al. 2009). Cognitive-emotional preoccupation with a behavior[5] is the base of impulsivity about the behavior (Collins and Lapp 1992). Impulses toward a behavior bolster an individual's thought to engage in the behavior and develop a

[5] Cognitive-emotional preoccupation with a behavior is the result of activation of certain associative clusters in long-term memory by the stimulus. Associative clusters have been formed gradually by temporal coactivation of the external stimulus, emotional impressive reactions and behavioral schema related to those reactions (Strack and Deutsch 2004, Hofmann et al. 2009). After forming such associative clusters in one's long term memory, any stimulant cue can activate the associative cluster and we can see strong incitement in terms of preoccupation of feeling and thoughts with the behavior.

motivational condition which is hard to resist and causes problematic behavior (Hoffman et al. 2009, Turel and Qahre-Saremi 2016). Prior research indicates that cognitive-emotional preoccupation is one of the main symptoms of problematic internet and OSN use (Shapira et al. 2003, Haagsma et al. 2013, Zheng and Lee 2016, Turel and Qahre-Saremi 2016). The presence of high cognitive-emotional preoccupation clearly explains the link between internet use and its adverse outcome (Caplan 2010). Moreover, in OSN, excessive levels of preoccupation with OSNs use generate motivations for people to use these platforms and creates strong thoughts and emotional dependency on the OSNs (Turel and Qahre-Saremi 2016). Therefore, more thinking about OSN can insist potent motivation to use it despite of its risky and problematic consequences. Extending this finding to the context of OSN addiction, we assert that cognitive-emotional preoccupation with using OSNs develops urges for people to use OSNs which are difficult to resist and provides the basis for addiction to OSNs.

> ***Hypothesis 1.*** *There is a positive association between individuals' cognitive-emotional preoccupation with using OSNs and their addiction to OSNs.*

Considering dual-system theory, we argue that after activation of the cognitive-emotional preoccupation with using OSN, the behavioral control restrains the impulses the effect of preoccupying thoughts on the behavior. Behavioral control refers to an individual's capacity to restrain, discontinue or change impulsive thoughts and behaviors to reduce the preoccupying thoughts and thus limit problematic behaviors (Tangney et al. 2004, Hofmann and Kotabe 2012). Behavioral control depends on two factors: 1) the individual's level of awareness and concern about the impulses and 2) the strength of the individual's willpower to deal with the impulses and their consequences (Hofmann and Kotabe 2012). Moreover, controlling the impulses and negative outcomes depends on the amount of conflicts among one's perceived possibility of

adverse consequences of the behavior, one's long-term goals and the level of motivation to avoid any negative outcomes of the behavior (Wood and Bechara 2014, Turel and Qahri-Saremi 2016). Individuals with strong behavioral control are highly motivated to and have the ability to overcome impulsive thoughts, so they can achieve their life goals (Wood and Bechara 2014) and mitigate problematic behaviors (Collins and Lapps 1992, Turel and Qahri-Saremi 2016). Therefore, acting based on long-term goals requires behavioral control to overcome impulsive behavior. However, behavioral control is challenging for addicts.

Addictive individuals seldom consider long-term goals and act based on the impulsive system rather than controlling system. Prior research has found that there is a negative association between individuals' behavioral control and their motivation to smoke, drink alcohol and gamble (Colling and Lapp 1992, Hoffmann et al. 2009). Moreover, the literature on OSN use shows that having low behavioral control over use of OSNs leads to problems on using OSNs and as a result causes problem in the social, psychological, family, work and academic performance of individuals (Turel and Qahri-Saremi 2016, Zheng and Lee 2016). Consequently, we argue that behavioral control over use of OSN improves individuals' capacity to control using OSN and prevent the addictive behavior. Hence:

> ***Hypothesis 2.*** *There is a negative association between individuals' behavioral control over use of OSNs and their addiction to OSNs.*

In the study of security perception of addicted individuals, we argue that the extent of perceived susceptibility to online security threats is associated on the level of the individual's addiction to OSN. One of the main symptoms of addiction is the persistence of the behavior despite recurrent psychological or physical problems caused by it (Goldstein 2001, Koob and Le Moal 2006). Addicted individuals rely strongly on their emotions to make decisions (Beck 1976, Damasio

1994). Repeated addictive behavior by a vulnerable individual alters his brain at the molecular level, which makes it difficult for the individual to avoid the behavior (Kendler et al. 2000, Hyman and Malenka 2001, Hofmann et al. 2009). Addicted individuals engage in the risky behavior in order to maximize their enjoyment (Turel et al. 2011). They irrationally expose themselves to risks associated with the behavior despite being aware of them (Hyman and Malenka 2001). Recent research shows that high-risk groups know the risks and damages associated with their high-risk behavior and their vulnerabilities to those risks (Cohn et al. 1995, Gerrard et al. 1996). Therefore, they have a high level of perceived susceptibility to their behavior. Thus, we argue that in OSN, addicted individuals are more impacted by their perception of sustainability. Hence:

> ***Hypothesis 3.*** *There is a positive association between individual users' addiction to OSN and their perceived threat susceptibility.*

We argue that the extent of perceived severity to security threats is associated by individuals' level of addiction to OSNs. Research on crime and addictive behaviors shows that the extent of harm and hazard in the addictive behavior is not significantly associated with reduction in the level of doing the behavior (Pogarsky 2002, Yu et al. 2006). Addicted individuals are often aware of and experience the harmful aspects of their addiction (Robinson and Berridge 2003, Moore and Gullone 1996). However, they tend to pursue their addictive behavior regardless of their previous severe experiences and punishments (MacCoun 1993). Powell et al. (1999) argue that in gambling, risk-taking is positively related to the degree of addiction. Highly addicted individuals experience more damages associated with the behavior and still are reluctant to discontinue the behavior. Based on such findings, we posit that there is a positive association between OSN addiction and perceived severity. Hence:

Hypothesis 4. *There is a positive association between individual users' addiction to OSN and their perceived threat severity.*

We argue that OSN addiction can increase an individual's self-efficacy to overcome online security threats. Self-efficacy is defined as ''the conviction that one can successfully execute the behavior required to produce the outcomes" (Bandura 1977, p. 193). Self-efficacy affects individuals' choice, their level of effort, their perseverance in the face of difficult problems and the psychological situations they experience (Bandura 1990, Maisto et al., 2000). Perceived self-efficacy is essential to sustain coping behaviors (Kadden and Litt 2011). It is the degree to which the individual believes he/she can cope with the threat and prevent the negative consequences of the threat (Bandura 1997). In the absence of self-efficacy, individuals cannot manage a situation properly despite their awareness and having the required skills. Researchers have shown strong relationship between self-efficacy and behaviors such as drug and alcohol consumption, smoking, uncontrolled sexual activity and gambling (Bandura 1990, Dolan et al. 2008, Hodgins et al. 2004, Kadden and Litt 2011). Individuals with proper skills and strong coping efficacy have more confidence to mobilize the required efforts to inhibit the high-risk situation for addictive behaviors (Bandura 1986). Therefore, in the context of OSN, we argue that those with high level of addiction to OSNs have more self-efficacy.

Hypothesis 5. *There is a positive association between individual users' addiction to OSN and their perceived security self-efficacy.*

We argue that OSN addiction may increase an individual's belief toward response efficacy. Response efficacy refers to the perception of effectiveness of recommended responses to a threat. A decision about adopting the recommended coping responses depends on one's beliefs about the effectiveness of the coping response to avoid the harm and also one's ability to perform the

response (Floyd et al. 2000). In the context of OSNs, recommended responses consist of security settings and antivirus programs. Individuals mostly rely on available security settings at the platform levels and outsource the possible risks to the platforms. Accordingly, compulsive and unthoughtful use of OSNs shows higher confidence of individual users on power of security tools in OSNs. We argue that OSN addicts have a high response efficacy to overcome online security threats. Hence:

> ***Hypothesis 6.*** *There is a positive association between individual users' addiction to OSN and their perceived response-efficacy.*

The second set of hypotheses are modeled by Chen and Zahedi (2016), to study individuals' online security perceptions and coping behaviors dealing with online security threat. The hypotheses and their rationales are outlined in Table 4.1.

Table 4.1. Model Hypotheses Adapted from Chen and Zahedi (2016)

Hypotheses (H)	Rationale
H7. There is a positive association between individual users' perceived threat susceptibility to online threat and their perceived threat.	Based on TTAT, perceived threat involves two constructs: perceived severity and perceived susceptibility. Perceived threats are impacted by these two constructs (Liang and Xue 2009). In the context of addiction, perceived threat is a function of the individuals' susceptibility and severity perceptions about the threats (Baker et al. 2004).
H8. There is a positive association between individual users' perceived threat severity of online threat and their perceived threat.	
H9. There is a positive association between individual users' perceived threat to online threat and taking protective actions.	Based on TTAT, perceived threat activates decision about taking protective actions to deal with threats (Liang and Xue 2009). In the context of addiction, decision to take protective actions is a positive function of perceived threat (Floyd et al. 2000).
H10. There is a positive association between individual users' perceived threat and seeking help.	Seeking help is a popular coping strategy to deal with threats. People seek information and advice about the threat before making any decision (Newell and Simon 1972). In the context of addiction (e.g. drinking problems) individuals who are fearing to be or become addicted have more tendency toward seeking help (Jordan and Oei 1989). Moreover, physical harm and adverse personal and social outcomes have been determined as the main factors for requesting help (Hingson et al 1982, Thom 1986).

H11. There is a positive association between individual users' perceived security response efficacy and taking protective actions.	One source of coping abilities is related to protective tools and safeguarding measures. Response efficacy can motivate individuals to take protective behaviors (Woon et al. 2005, Anderson and Agarwal 2010, Liang and Xue 2010). The more confidence about effectiveness of protection tools brings more motivations to adopt them (Liang and Xue 2010). In the area of addiction research, especially smoking and drinking alcohol, there is a positive relation between response efficacy and taking protective and adaptive behaviors. With regard to smoking behavior, individuals with high response efficacy have greater expectations for avoid adverse effects by stopping the behavior (Greening 1997). In the case of cigarette smoking, effectiveness of coping response has positive effect on adopting preventive health behavior (Maddux and Rogers 1982).
H12. There is a positive association between individual users' perceived security self- efficacy and taking protective actions	One source of coping abilities is working on self. Self-efficacy is an important determinant of taking protective actions. Individuals with a high level of self-efficacy are more motivated to use protective actions. In addictive behaviors (e.g. smoking), high self-efficacy to resist cigarette offers is associated with high protective actions toward declining smoking (Thrul et al. 2013).

4.6. Methodology and Results

4.6.1. Data Collection

The data was collected using the survey method. Students in a large Midwest university recruited three people from their family or friends to participate in the online survey and receive extra course credit as an incentive. From 1134 requested survey links, 827 responses were collected. The response rate was 73 percent. Sixty-three of respondents who do not use OSNs were excluded from the data set, resulting in a total of 764 responses. Validity of responses was done by removing any observations in which 1) most of the questions were not answered and 2) total

spent time of answering the questions was less than the minimum required time as determined with the pilot test (5 minutes).

After validating responses, we had 691 usable responses. The mean age was 32.3, with 26 percent of respondents above 45 years old and 74 percent at or below 45 years. The demographic results of our data set are reported in Table 4.2. In addition, we asked the respondents to state how many hours a day they spent on OSNs and their approximate number of friends in OSNs. The respondents spent on average 3 hours a day on OSNs and had about 1000 friends in OSNs. Moreover, respondents were active on about 3.04 of the popular OSNs such as Twitter (38%), Facebook (81%), Instagram (64%), Snapchat (66%) and Pinterest (24%). The results are reported in Table 4.3.

Table 4.2. Participants' Demographic Information (n=691)

Profile Variables	Mean	STD
Age	32.30	14.13
Education*	3.15	1.10
Employment **	3.26	0.94
Gender	**Female (%)**	**Male (%)**
	62%	38%
*Education scales: 1 = Middle school diploma; 2 = High school graduate; 3 = Undergraduate students; 4 = Undergraduate degree; 5 = Master's degree; 6 = Doctoral degree.		
**Employment scales: 1 = Retired/Unemployed not looking for work; 2 = Unemployed looking for work; 3 = Employed part time in college; 4 = Employed full time.		

Table 4.3. Participants' OSN Information (n=691)

Profile Variables	Mean	STD
Hours spent on OSNs per day	2.70	2.25
Number of friends in OSNs	966.48	1449.21
Number of active OSNs per person	3.04	1.40

4.6.2. Measurement Development

Measurements items for the constructs of OASB model were adopted from the relevant literatures. The scale for cognitive-emotional preoccupation with using OSNs and Behavioral control were developed based Collins and Lapp's research (1992) and contextualized for

problematic use of OSN by (Turel and Qahri-Saremi 2016). Cognitive-emotional preoccupation using OSN addiction consists of two sub-dimensions: emotion and cognitive preoccupation. "Emotion" refers to avoiding or limiting negative emotions by using OSNs. "Cognitive preoccupation" refers to being distracted by continuous thought about using OSNs. Behavioral control over use of OSN consists of two sub-dimensions: restrict and concern. "Restrict" refers to attempting to inhibit the use of OSNs. "Concern" refers to having concerns about using OSNs and making decision to decrease their use. The scale of OSN addiction was developed based on technology addiction research (Charlton et al. 2007, Turel and Serenko 2012). We also adopted Chen and Zahedi (2016) instruments for measuring the extended PMT constructs. All the items were evaluated and refined based on a pilot test consisting of eight participants. Based on the feedback, minor revisions were done on the instrument. Appendix E reports the construct definitions and key references. Appendix F reports all the items for each construct.

4.7. Data Analysis and Results

We assessed the reliability and validity of the constructs. According to Table 4.4, the Cronbach Alpha value of each construct is greater than the threshold value of .70, the composite factor reliability (CFR) value of each construct is greater than the recommended value of .70, and the average variance extracted (AVE) value of each construct is greater than the recommended value of .50 (Chin 1998). Therefore, there is a proper construct reliability.

We assessed convergent and discriminant validity by using exploratory factor analyses. First, as Table 4.5 shows, all items are loaded adequately in their corresponding latent variable.

Items have higher self-loading and there is no cross loading. Second, based on the results in Table 4.6, the square root of AVE for each construct was higher than the correlation values with other constructs. Hence, the results confirm satisfactory convergent and discriminant validity (Fornell and Larcker 1981). Appendix F reports factor loadings and t-values for the items in the measurement model as well.

We applied MPLUS with the mean-adjusted maximum likelihood method for estimating the measurement model and testing the hypotheses. Table 4.7 reports the fit indices of the measurement model. The results illustrate acceptable fit with SRMR<= .10, RMSEA<=.05 and significant CFI .96 (Hu and Bentler 1999). Therefore, there is a valid model fit.

Table 4.4. Reliability Checks

Constructs	Cronbach Alpha	CFR	AVE
OSN Addiction	0.91	0.93	0.72
Emotion	0.83	0.87	0.69
Cognitive	0.81	0.76	0.78
Concern	0.75	0.80	0.81
Restrict	0.82	0.83	0.79
Susceptibility	0.83	0.88	0.71
Severity	0.89	0.92	0.78
Perceived threat	0.92	0.95	0.87
Self-efficacy	0.82	0.87	0.69
Response efficacy	0.92	0.93	0.81
Protective action	0.89	0.91	0.77
Seeking help	0.88	0.91	0.77

Notes: CFR=composite factor reliability, AVE=average variance extracted

Table 4.5. Exploratory Factor Analysis

		Constructs			
Level 1	***Items***	*1*	*2*	*3*	*4*
Emotion	emo1	**0.84**	0.16	0.08	0.23
	emo2	**0.77**	0.13	0.12	0.20
	emo3	**0.87**	0.12	0.11	0.10
Cognitive	cog1	0.38	0.12	0.13	**0.77**
	cog2	0.15	0.31	0.14	**0.80**
Concern	con1	0.12	0.25	**0.86**	0.11
	con2	0.15	0.36	**0.77**	0.15
Restrict	res1	0.08	**0.83**	0.23	0.20
	res2	0.27	**0.77**	0.18	0.19

	res3	0.11	**0.77**	0.34	0.12
Cumulative variance explained		0.23	**0.46**	0.62	0.77
Level 2	***Items***	***1***		***2***	
OSN Addiction	ad1	**0.86**		0.14	
	ad2	**0.88**		0.13	
	ad3	**0.85**		0.15	
	ad4	**0.78**		0.30	
	ad5	**0.85**		0.13	
Loss experienced	lsa1	0.14		**0.79**	
	lsa2	0.18		**0.89**	
	lsa3	0.16		**0.86**	
Cumulative variance explained		0.46		0.75	
Level 3	**Items**	**1**		**2**	
Susceptibility	sus1	0.24		**0.86**	
	sus2	0.23		**0.83**	
	sus3	0.14		**0.83**	
Severity	sev1	**0.83**		0.26	
	sev2	**0.91**		0.16	
	sev3	**0.91**		0.22	
Cumulative variance explained		0.41		0.79	
Level 3	***Items***	***1***	***2***	***3***	
Self-efficacy	self1	0.05	0.17	**0.87**	
	self2	-0.05	0.17	**0.87**	
	sclf3	-0.03	0.32	**0.73**	
Response efficacy	ref1	0.03	**0.90**	0.19	
	ref2	0.02	**0.90**	0.22	
	ref3	-0.05	**0.89**	0.26	
Perceived threat	sc1	**0.93**	0.00	-0.02	
	sc2	**0.95**	0.00	0.01	
	sc3	**0.92**	0.00	-0.02	
Cumulative variance explained		0.29	0.58	0.82	
Level 4	***Items***	***1***	***2***		
Protective actions	act1	0.31	**0.84**		
	act2	0.23	**0.89**		
	act3	0.15	**0.90**		
Seeking help	sh1	**0.89**	0.23		
	sh2	**0.84**	0.21		
	sh3	**0.90**	0.21		
Cumulative variance explained		0.41	0.82		

Table 4.6. Correlations Matrix, AVE, Means, and Standard Deviations of Constructs

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	Mean	std
1.Susceptibility	**0.84**																	4.36	2.60
2.Severity	0.03	**0.88**																5.03	2.93
3.Perceived threat	0.39	0.57	**0.93**															4.19	2.91
4.Self-efficacy	-0.01	-0.02	-0.02	**0.83**														6.65	2.53
5.Response efficacy	0.00	0.00	0.00	0.00	**0.90**													6.61	2.17
6.Seeking help	0.12	0.17	0.31	-0.01	0.00	**0.87**												4.25	2.74
7.Protective Actions	0.08	0.12	0.22	0.29	0.19	0.45	**0.88**											5.46	2.45
8.Emotion	0.08	0.12	0.10	-0.07	0.01	0.03	0.00	**0.83**										4.20	2.98
9.Cognitive	0.11	0.16	0.13	-0.09	0.02	0.04	0.01	0.64	**0.89**									3.37	2.61
10.Concern	0.06	0.10	0.08	-0.06	0.01	0.02	0.00	0.35	0.46	**0.90**								4.54	2.84
11.Restrict	0.08	0.13	0.10	-0.07	0.01	0.03	0.00	0.46	0.60	0.80	**0.89**							4.31	2.72
12.OSN Addiction	0.13	0.20	0.16	-0.11	0.02	0.05	0.01	0.62	0.82	0.49	0.64	**0.85**						3.22	2.85
13.Loss Experienced	0.05	0.08	0.07	-0.05	0.01	0.02	0.00	0.26	0.34	0.27	0.35	0.42	**0.92**					2.05	2.59
14.Gender	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02	0.00	na				1.63	0.50
15.Age	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	-0.02	0.00	0.06	na			32.30	14.13
16.OSN spent hours	0.02	0.03	0.03	-0.02	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.17	0.00	0.10	0.05	na		2.70	2.25
17.OSN #of friends	0.01	0.02	0.02	-0.01	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.11	0.00	0.01	0.00	0.35	na	966.48	1449.21

Notes: The boldface values on the diagonal are the square roots of AVEs. na = Single item variable

Table 4.7. Fit Indices

Fit Index	Measurement Model	OASB Model
Normed chi square	1.76	2.57
CFI	0.96	0.91
TLI	0.96	0.91
RMSEA	0.03	0.04
SRMR	0.04	0.10

4.7.1. The OASB Model Estimation

Figure 4.2 shows the OASB model estimation results. The model has R^2 of .84, hence explaining 84% of variation in OSN addiction. The estimated path coefficients and their levels of significance show that all hypotheses were supported except for H2, H5 and H6. Our results show that perceived susceptibility and perceived severity have significant and positive relationships with perceived threat. The association between protective actions and both perceived self-efficacy and perceived response efficacy are positively significant. Moreover, perceived threat has positive and significant relationships with protective action and seeking

help. Therefore, H7, H8, H9, H10, H11 and H12 adapted from (Chen and Zahedi 2016) were all supported. The results indicated that System 1, manifested in cognitive-emotional preoccupation with using OSN had a significant positive association with OSN addiction (H1: .82, p<.001), providing support for H1. OSN addiction had a significant positive association with perceived severity (H3: .13, p<.001) and perceived susceptibility (H4: .20, p<.001), providing support for H3 and H4. H5 was supported in reverse and there is significant negative association between OSN addiction and self-efficacy (-.11, p<.01). Therefore, that result shows that those who are more addicted to OSN have low self-efficacy.

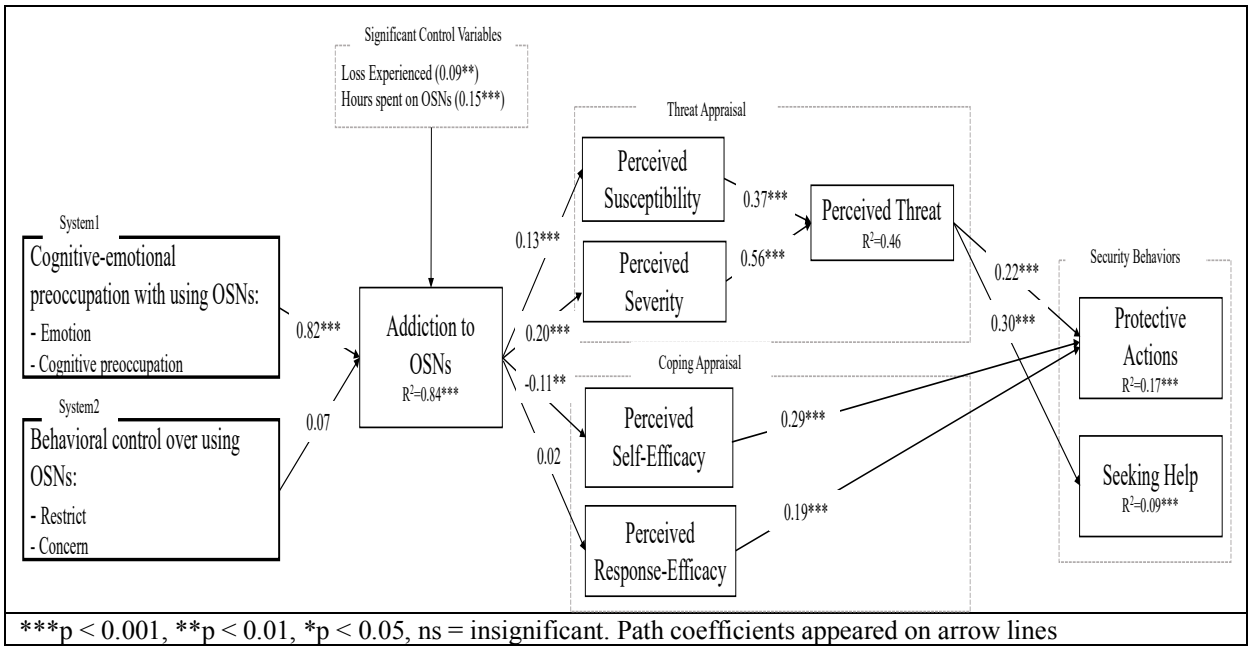


Figure 4.2. Results of the Model Estimation

We included age, gender, hours spent on OSNs, number of friends in OSNs and loss experienced using OSNs as control variables for OSN addiction. Both losses experienced, and hours spent on OSN had positive associations with addiction to OSN, showing that people who experienced loss due to online threats are more addicted and that spend more hours on OSN. The path coefficients and p-values are summarized in Table 4.8.

Table 4.8. Detailed Results of Tested Hypotheses and Control Variables

Tested Hypotheses and Paths	Path coefficients	Conclusions
H1. Cognitive-emotional preoccupation with using OSN → OSN Addiction	0.82 ($p<0.001$)	H1 is supported
H2. Behavioral control → OSN Addiction	0.07 ($p=0.12$)	H2 is not supported
H3. OSN addiction → Perceived Susceptibility	0.13 ($p<0.001$)	H3 is supported
H4. OSN addiction → Perceived Severity	0.20 ($p<0.001$)	H4 is supported
H5. OSN addiction → Perceived Self-efficacy	-0.11 ($p<0.01$)	H5 is supported in reverse
H6. OSN addiction → Perceived Response Efficacy	0.02 ($p=0.58$)	H6 is not supported
H7. Perceived Susceptibility → Perceived Threat	0.37 ($p<0.001$)	H7 is supported
H8. Perceived Severity → Perceived Threat	0.56 ($p<0.001$)	H8 is supported
H9. Perceived Self-efficacy → Protective Actions	0.29 ($p<0.001$)	H9 is supported
H10. Perceived Response Efficacy → Protective Actions	0.19 ($p<0.001$)	H10 is supported
H11. Perceived Threat → Protective Actions	0.22 ($p<0.001$)	H11 is supported
H12. Perceived Threat → Seeking Help		H12 is supported
Control Variables		
Loss Experienced → OSN Addiction	0.09 ($p<0.01$)	Yes
Age → OSN Addiction	-0.02 ($p=0.29$)	No
Gender → OSN Addiction	0.00 ($p=0.92$)	No
Number of OSN friends → OSN Addiction	0.05 ($p=0.06$)	No
Hours Spent on OSNs → OSN Addiction	0.15 ($p<001$)	Yes

4.8. Discussion

The aim of this study was to examine a theoretical model to describe the etiology of OSN addiction and its impact on individuals' security perceptions and behavior. Addiction distorts the rational thinking process. Distorted rationality biases individuals' perception about the behavior causing the addiction and leads to persistence of the behavior regardless of the past experiences and problems caused by that behavior. Similar to other addictive behaviors, it is reasonable to study OSN addiction as distorted decision making which is rooted in the conflicts within the impulsive and controlling mental systems. A theoretical perspective that considers impulsive, irrational and problematic use behaviors is required to understand OSN addiction. However, prior research has shown that addiction conveys dependency and loss of control for individuals, which causes them to experience failure and damage from the behavior. While previous studies

examined the consequences of OSN addiction, they rarely indicated the relationships between OSN addiction and security behavior with biased perception toward the artifact. Based on the concept of security perception in the presence of a threatened event, we adopted a well-founded theory known as Protection Motivation Theory (PMT). Thus, we developed a research model based on dual-system theory and extended PMT that included seeking help as a coping behaviors when one confronts perceived online security threats. In particular, our model builds on prior research on addiction and shows a multifaceted perspective of the relation between OSN addiction and individuals' security perceptions to online threats. The main outcomes of the research model are summarized below.

First, results of this study indicate that dual-system theory is a proper theory to explain the mechanism for developing addictive use of OSN. Using dual-system theory, this study showed that OSN addiction is induced by a strong impulsive system. Impulsive system in this study was shown by cognitive-emotional preoccupation with using OSN. Data analysis reveals that emotional and cognitive preoccupations explain a large amount of the variance (84%) in OSN addiction. Data analysis results imply that a high level of cognitive-emotional preoccupation with using OSNs drives OSN addiction. Contrary to our hypothesis, the controlling system which manifested by controlling behavior over using OSN does not have a significant relation to OSN addiction.

Second, results show that extended PMT can explain the role of OSN addiction in individuals' security perception and behavior. We found that an addiction to OSN affects the individual's perception of two appraisals (threat appraisal and coping appraisal) for taking protective actions and seeking help. In terms of threat appraisal, our finding demonstrates that OSN addicts believe they are more susceptible to online security attacks and the consequences of

the threats would be more harmful and severe for them. These results imply that OSN addicts are aware of their weakness and confirm that their behavior is problematic and has severe outcomes for them but still have dependency and loss of control about it. These results are in line with the prior research that shows the most critical aspect of addiction is the persistence and repetition of performing the behavior to which they are addicted to, despite its negative consequences (Cohn et al. 1995, Greenfield and Rogers 1999, Hyman and Malenka 2001). Also, the results are consistent with the findings that OSNs users take higher security risks to enjoy the benefits of these platforms (Govani and Pashley 2005) and consider security as a second goal (Dhamija et al. 2006).

In terms of coping appraisals, contrary to our hypothesis, results show that OSN addicts have low security self-efficacy when facing online threats and do not believe they are capable of overcoming with the threats by taking protective actions and using security tools. In particular, while higher OSN addiction can improve the individual's perceived ability to use OSN, that perception may not be enough to deal with the negative security threat consequences increased OSN use. In other words, the compulsion to use OSN leaves OSN addicts feel unprepared to deal with security threats that may result from their addition.

Moreover, this negative relation may imply that there is a similarity between perceived inability of OSN addicts to deal with security threats and their inabilities to discontinue using the system. Prior studies found that addicted individuals have less ability to discontinue the addictive behaviors despite their awareness about the associated problems. Having awareness about the problems and perceived low ability to stop the behavior denotes low self-efficacy (Turel 2015). This finding, however, is consistent with studies indicating that addiction reduces individuals' self-efficacy to resist the behavior (Eiser et al. 1978, Walton et al. 2003, Kadden and Litt 2011).

Recent research also shows that IT and OSN addicts have low self-efficacy to decrease their use of the system (Turel et al. 2014, Vaghefi and Qahri-Saremi 2017).

Furthermore, our finding did not support the relationship between OSN addiction and perceived response efficacy. One explanation for this lack of significance is that OSN addicts may not attempt to take protective actions and explore the potency of various security tools and procedures due to their perception of low self-efficacy in dealing with threats and the fear that protective actions may limit the scope of their OSN activities. This avoidance of taking security protective actions may leave them ignorant about security protective actions and tools, and unable to judge the response efficacy of such actions.

While recent studies focused on OSN addiction and its negative consequences, we need more research on that analyses the security behavior of OSN addicts and their perceptions to deal with online threats. Hence, this study has significant theoretical and practical implications.

4.9. Implications

This section reports the theoretical and practical implications of this work.

4.9.1. Theoretical Implications

This research makes a number of contributions to theory and research. First, we developed the Online addiction & security behaviors (OASB) theory by synthesizing dual-system theory and extended protection motivation theory (extended PMT) to study the online security behavior of OSN addicts. Our theory-based model is the first attempt to study perceptions of online security threats and coping efficacies for individuals with a psychological dependency to OSNs. This

model sets the ground for researchers to expand studies on the online security behaviors of online addicts.

Second, this study contributes by showing that the emotional impulsive system of the mind can be as an antecedent in studying OSN addiction. OSN addiction can be explained by the impulsive system of the human mind. Our findings show that OSN addiction manifests when an emotional-cognitive preoccupation with using OSN is high.

Third, this work has contribution in studying security threat perceptions of OSN addicts. Our work shows that OSN addicts have impulsivity toward the OSNs and as a result cannot protect themselves from being victimized by security threats. In fact, they suffer high levels of damages from these threats.

Fourth, another contribution of this study is showing how helpless OSN addicts are to cope with security threats. Our results show OSN addicts do not have enough self-coping efficacy to counter with online security threats. This finding is a dark side of OSN addiction which should draw the attention of IS researchers. Fifth, this study confirms extended PMT in the context of OSN addiction. While the extended PMT has been studied in the literature, investigating security perceptions and behavior in the context of OSN addiction is a new aspect of the research. Our work indicates that OSN addiction has an impact on both security threat perception and coping capability. Therefore, any study of online security perceptions and coping efficacies needs to consider individuals' dependence on the behavior.

4.9.2. Practical Implications

From practical standpoint, our research offers several implications for individual users and OSN providers. First, based on the literature, OSN addiction creates mental and emotional problems

for individuals. A person becomes addicted to OSNs to escape from stress, depression, loneliness and negative feelings (Griffith et al. 2014, Xu and Tan 2012). Individuals having low self-esteem use these platforms as a means to be approved by others (Valkerburg et al. 2006, Kuss and Griffith 2011). OSN addicts also engage in social networking to distract themselves from over thinking and detach from their own feelings (Andreassen 2015). However, OSN addicts are unable to stop using OSNs. Limiting use of OSNs may bring them anxiety, depression, mood swings, poor self-esteem, jealousy and unhappiness (Thadani et al. 2011, Andreassen 2015, Krasnova et al. 2015, Lowry et al. 2016). Our findings reveal that OSN addicts have strong impulsive cognitive-emotional preoccupation with the system. We propose that having awareness of the negative consequences of OSN addiction may persuade individuals to control and reduce their use of OSN. Individuals should learn about ways to control their impulsive system and limit the cues that lead to increasing their preoccupation, but that strategy may not be sufficient. As a result, OSN addiction should be considered a mental health problem that requires medical treatment to help OSN addicts.

Second, Individuals with proper knowledge about threat perception, security self-efficacy and effectiveness of countermeasures will be more encouraged to protect themselves from online security threats (Liang and Xue 2010). This study supports the worthiness of security awareness, education and training for OSN use. Individuals' awareness about using OSNs impact their security perceptions and coping capabilities.

Third, public awareness campaigns and security awareness programs should consider the popularity of OSNs, the increasing number of OSN addicts, and their perceptions of security, then hold workshops and events to enhance the knowledge of individuals about using OSNs and decreases their level of losses from it.

Fourth, while time spent on online social networks can provide financial benefits for the platforms, our study shows that higher levels of addiction to OSN can negatively impact on individuals' security capabilities. Our study shows that OSN administrators should consider additional security protections for individuals with high frequency of using OSN platforms. Fifth, for organizations that adopt social network platforms inside their IT infrastructure to increase the level of knowledge sharing and communications among employees, having high reliance on OSN platforms may reduce their level of security awareness, which can lead to organizational security breaches. It is important for organizations to develop comprehensive policies that cover the level of permitted usage and the amount of information to be shared in these platforms. Additionally, they can conduct various training sessions to educate users about possible security flaws.

4.10. Limitations and Future Research

This study had several limitations that can be considered in future research. First, our respondents are popular OSNs active users without any limitation on the type of OSN or the devices they use to connect to OSNs. Individuals using different OSNs may have various view about security. Sometimes addiction to a behavior causes other addictive or problematic behavior. For example, individuals who use smartphones to log into their OSN accounts can become addicted to the smartphones, which can affect OSN addiction or vice versa.

Second, in this study we consider age, gender, time spent on OSNs, number of friends and loss experienced as variables when studying security perceptions of OSN addicted users. Future research may broaden the model by considering additional variables in different contexts

(societal and individuals' characteristics) to see how these variables can fully or partially mediate the impact of OSN addiction on online security perceptions and behaviors. Moreover, different mental and psychological conditions of individuals can be considered in the future research.

Third, we test the model on a sample of all OSN users without any limitations in their characteristics and demographic attributes. Since young people are more at risk of being addicted to social networks, future studies should focus on online security behavior for young people. In addition, researchers can study the security behavior of other online technology addictions to see any similarities between OSN addiction and other online addictions in terms of security perceptions and coping capabilities.

REFERENCES

Abdullah, S., & Wu, X. (2011, November). An epidemic model for news spreading on twitter. In *2011 IEEE 23rd international conference on tools with artificial intelligence* (pp. 163-169). IEEE.

Adali, S., Escriva, R., Goldberg, M. K., Hayvanovych, M., Magdon-Ismail, M., Szymanski, B. K., ... & Williams, G. (2010, May). Measuring behavioral trust in social networks. In *2010 IEEE International Conference on Intelligence and Security Informatics* (pp. 150-152). IEEE.

Adar, E., & Adamic, L. A. (2005, September). Tracking information epidemics in blogspace. In *Proceedings of the 2005 IEEE/WIC/ACM international conference on web intelligence* (pp. 207-214). IEEE Computer Society.

Adger, W. N. (2006). Vulnerability. *Global environmental change*, *16*(3), 268-281.

Adler, P. S., & Kwon, S. W. (2002). Social capital: Prospects for a new concept. *Academy of management review*, *27*(1), 17-40.

Adler, P. S., & Kwon, S. W. (2000). Social capital: The good, the bad, and the ugly. *Knowledge and social capital*, *89*.

Aladwani, A. M., & Almarzouq, M. (2016). Understanding compulsive social media use: The premise of complementing self-conceptions mismatch with technology. *Computers in Human Behavior*, *60*, 575-581.

Albert, R., Jeong, H., & Barabási, A. L. (2000). Error and attack tolerance of complex networks. *nature*, *406*(6794), 378.

Albrecht, U., Kirschner, N. E., & Grüsser, S. M. (2007). Diagnostic instruments for behavioural addiction: an overview. *GMS Psycho-Social Medicine*, *4*.

Algarni, A., Xu, Y., & Chan, T. (2015). Susceptibility to social engineering in social networking sites: The case of Facebook.

Almaatouq, A., Shmueli, E., Nouh, M., Alabdulkareem, A., Singh, V. K., Alsaleh, M., ... & Alfaris, A. (2016). If it looks like a spammer and behaves like a spammer, it must be a spammer: analysis and detection of microblogging spam accounts. *International Journal of Information Security*, *15*(5), 475-491.

Althaus, C. L. (2014). Estimating the reproduction number of Ebola virus (EBOV) during the 2014 outbreak in West Africa. *PLoS currents*, *6*.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643.

Anderson, R. M., & May, R. M. (1992). *Infectious diseases of humans: dynamics and control*. Oxford university press.

Andreassen, C. S. (2015). Online social network site addiction: A comprehensive review. *Current Addiction Reports*, *2*(2), 175-184.

Andreassen, C. S., Torsheim, T., & Pallesen, S. (2014). Predictors of use of social network sites at work-a specific type of cyberloafing. *Journal of Computer-Mediated Communication*, *19*(4), 906-921.

Andreassen, C. S., Torsheim, T., Brunborg, G. S., & Pallesen, S. (2012). Development of a Facebook addiction scale. *Psychological reports*, *110*(2), 501-517.

Andreassen, C. S. & Pallesen, S. (2014). Social network site addiction-an overview. *Current pharmaceutical design*, *20*(25), 4053-4061.

Aral, S., & Walker, D. (2014). Tie strength, embeddedness, and social influence: A large-scale networked experiment. *Management Science*, *60*(6), 1352-1370.

Bailey, N. T. (1975). *The mathematical theory of infectious diseases and its applications* (No. 2nd ediition). Charles Griffin & Company Ltd 5a Crendon Street, High Wycombe, Bucks HP13 6LE..

Baker, T. B., Piper, M. E., McCarthy, D. E., Majeskie, M. R., & Fiore, M. C. (2004). Addiction motivation reformulated: an affective processing model of negative reinforcement. *Psychological review*, *111*(1), 33.

Bakshy, Eytan, Itamar Rosenn, Cameron Marlow, and Lada Adamic. "The role of social networks in information diffusion." In *Proceedings of the 21st international conference on World Wide Web*, pp. 519-528. ACM, 2012.

Balakrishnan, V., & Shamim, A. (2013). Malaysian Facebookers: Motives and addictive behaviours unraveled. *Computers in Human Behavior*, *29*(4), 1342-1349.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2), 191.

Bandura, A. (1986). Fearful expectations and avoidant actions as coeffects of perceived self-inefficacy.

Bandura, A. (1990). Perceived self-efficacy in the exercise of control over AIDS infection. *Evaluation and program planning*, *13*(1), 9-17.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. Macmillan.

Bapna, R., Gupta, A., Rice, S., & Sundararajan, A. (2017). Trust and the Strength of Ties in Online Social Networks: An Exploratory Field Experiment. *MIS Quarterly*, *41*(1), 115-130.

Barabasi, A. L. (2003). Linked: How everything is connected to everything else and what it means.

Barker, V. (2009). Older adolescents' motivations for social network site use: The influence of gender, group identity, and collective self-esteem. *Cyberpsychology & behavior*, *12*(2), 209-213.

Bauckhage, C. (2011, July). Insights into internet memes. In *Fifth International AAAI Conference on Weblogs and Social Media*.

Baumeister, R. F. (2002). Yielding to temptation: Self-control failure, impulsive purchasing, and consumer behavior. *Journal of consumer Research*, *28*(4), 670-676.

Bechara, A. (2005). Decision making, impulse control and loss of willpower to resist drugs: a neurocognitive perspective. *Nature neuroscience*, *8*(11), 1458.

Bechara, A., Noel, X., & Crone, E. A. (2006). Loss of willpower: Abnormal neural mechanisms of impulse control and decision making in addiction. *Handbook of implicit cognition and addiction*, *1*, 215-232.

Beck, A. T. (1979). *Cognitive therapy and the emotional disorders*. Penguin.

Bell, D. C., Atkinson, J. S., & Carlson, J. W. (1999). Centrality measures for disease transmission networks. *Social networks*, *21*(1), 1-21.

Benbasat, I., & Wang, W. (2005). Trust in and adoption of online recommendation agents. *Journal of the association for information systems*, *6*(3), 4.

Benevenuto, F., Magno, G., Rodrigues, T., Almeida, V., & Detecting Spammers on Twitter," in Collaboration. (2010). electronic messaging, anti-abuse and spam conference (CEAS), vol. 6. *Redmond, Washington, July*.

Bernroider, E. W., Krumay, B., & Margiol, S. (2014). Not without my smartphone! Impacts of smartphone addiction on smartphone usage. ACIS.

Blondel, V. D., Guillaume, J. L., Lambiotte, R., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of statistical mechanics: theory and experiment*, *2008*(10), P10008.

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature*, *489*(7415), 295.

Borgatti, S. P., Jones, C., & Everett, M. G. (1998). Network measures of social capital. *Connections*, *21*(2), 27-36.

Borgatti, S. P., Mehra, A., Brass, D. J., & Labianca, G. (2009). Network analysis in the social sciences. *science*, *323*(5916), 892-895.

Brady, S. S., Dolcini, M. M., Harper, G. W., & Pollack, L. M. (2009). Supportive friendships moderate the association between stressful life events and sexual risk taking among African American adolescents. *Health Psychology*, *28*(2), 238.

Brechwald, W. A., & Prinstein, M. J. (2011). Beyond homophily: A decade of advances in understanding peer influence processes. *Journal of Research on Adolescence*, *21*(1), 166-179.

Brown, J. J., & Reingen, P. H. (1987). Social ties and word-of-mouth referral behavior. *Journal of Consumer research*, *14*(3), 350-362.

Burnside, C., Eichenbaum, M., & Rebelo, S. (2016). Understanding booms and busts in housing markets. *Journal of Political Economy*, *124*(4), 1088-1147.

Burt, R. S. (1984). Network items and the general social survey. *Social networks*, *6*(4), 293-339.

Burt, R. S. (1987). Social contagion and innovation: Cohesion versus structural equivalence. *American journal of Sociology*, *92*(6), 1287-1335.

Burt R. S. (1992) *Structural holes*. Harvard University Press, Cambridge.

Burt, R. S. (2009). *Structural holes: The social structure of competition*. Harvard university press.

Cao, X., Masood, A., Luqman, A., & Ali, A. (2018). Excessive use of mobile social networking sites and poor academic performance: Antecedents and consequences from stressor-strain-outcome perspective. *Computers in Human Behavior*, *85*, 163-174.

Caplan, S. E. (2010). Theory and measurement of generalized problematic Internet use: A two-step approach. *Computers in Human Behavior, 26*(5), 1089-1097.

Cha, M., Haddadi, H., Benevenuto, F., & Gummadi, K. P. (2010, May). Measuring user influence in twitter: The million follower fallacy. In *fourth international AAAI conference on weblogs and social media*.

Cha, M., Mislove, A., & Gummadi, K. P. (2009, April). A measurement-driven analysis of information propagation in the flickr social network. In *Proceedings of the 18th international conference on World wide web* (pp. 721-730). ACM.

Chan, T. K., Cheung, C. M., Lee, Z. W., & Neben, T. (2015, January). Why do I keep checking my Facebook? The role of urge in the excessive use of social networking sites. In *2015 48th Hawaii International Conference on System Sciences*(pp. 314-323). IEEE.

Charlton, J. P., & Danforth, I. D. (2007). Distinguishing addiction and high engagement in the context of online game playing. *Computers in Human Behavior, 23*(3), 1531-1548.

Chen, D., Lü, L., Shang, M. S., Zhang, Y. C., & Zhou, T. (2012). Identifying influential nodes in complex networks. *Physica a: Statistical mechanics and its applications*, *391*(4), 1777-1787.

Chen, H. T., & Kim, Y. (2013). Problematic use of social network sites: The interactive relationship between gratifications sought and privacy concerns. *Cyberpsychology, Behavior, and Social Networking*, *16*(11), 806-812.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *Mis Quarterly, 40*(1), 205-222.

Cheng, J. J., Liu, Y., Shen, B., & Yuan, W. G. (2013). An epidemic model of rumor diffusion in OSNs. *The European Physical Journal B, 86*(1), 1-7.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, *295*(2), 295-336.

Chow, W. S., & Chan, L. S. (2008). Social network, social trust and shared goals in organizational knowledge sharing. *Information & management*, *45*(7), 458-465.

Chowell, G., Fenimore, P. W., Castillo-Garsow, M. A., & Castillo-Chavez, C. (2003). SARS outbreaks in Ontario, Hong Kong and Singapore: the role of diagnosis and isolation as a control mechanism. *Journal of theoretical biology, 224*(1), 1-8.

Chowell, G., Hengartner, N. W., Castillo-Chavez, C., Fenimore, P. W., & Hyman, J. M. (2004). The basic reproductive number of Ebola and the effects of public health measures: the cases of Congo and Uganda. *Journal of Theoretical Biology, 229*(1), 119-126.

Christley, R. M., Pinchbeck, G. L., Bowers, R. G., Clancy, D., French, N. P., Bennett, R., & Turner, J. (2005). Infection in social networks: using network analysis to identify high-risk individuals. *American journal of epidemiology, 162*(10), 1024-1031.

Chua, A. (2002). The influence of social interaction on knowledge creation. *Journal of Intellectual Capital, 3*(4), 375-392.

Cohn, L. D., Macfarlane, S., Yanez, C., & Imai, W. K. (1995). Risk-perception: differences between adolescents and adults. *Health Psychology*, *14*(3), 217.

Coleman, J. S. (1988). Social capital in the creation of human capital. *American journal of sociology*, *94*, S95-S120.

Coleman, J. S. (1990). *Foundations of social theory.* Harvard University Press.

Collins, R. L., & Lapp, W. M. (1992). The Temptation and Restraint Inventory for measuring drinking restraint. *British Journal of Addiction, 87*(4), 625-633.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. *Journal of applied psychology, 92*(4), 909.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189-211.

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J., & Rovira, E. (2012, January). The influences of social networks on phishing vulnerability. In *2012 45th Hawaii International Conference on System Sciences* (pp. 2366-2373). IEEE.

Damasio, A. R. (1994). Descartes' error: Emotion, rationality and the human brain.

Danon, L., Ford, A. P., House, T., Jewell, C. P., Keeling, M. J., Roberts, G. O., ... & Vernon, M. C. (2011). Networks and the epidemiology of infectious disease. *Interdisciplinary perspectives on infectious diseases*, *2011*.

Davis, R. A. (2001). A cognitive-behavioral model of pathological Internet use. *Computers in human behavior*, *17*(2), 187-195.

Dess, G. G., & Shaw, J. D. (2001). Voluntary turnover, social capital, and organizational performance. *Academy of Management Review, 26*(3), 446-456.

Deutsch, R., & Strack, F. (2006). Reflective and impulsive determinants of addictive behavior. *Handbook of implicit cognition and addiction*, *16*, 45-57.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). ACM.

Diekmann, O., Dietz, K., & Heesterbeek, J. A. P. (1991). The basic reproduction ratio for sexually transmitted diseases: I. Theoretical considerations. *Mathematical biosciences, 107*(2), 325-339.

Dolan, S. L., Martin, R. A., & Rohsenow, D. J. (2008). Self-efficacy for cocaine abstinence: Pretreatment correlates and relationship to outcomes. *Addictive behaviors, 33*(5), 675-688.

Dormann, C. F., Elith, J., Bacher, S., Buchmann, C., Carl, G., Carré, G., ... & Münkemüller, T. (2013). Collinearity: a review of methods to deal with it and a simulation study evaluating their performance. *Ecography*, *36*(1), 27-46.

Egele, M., Stringhini, G., Kruegel, C., & Vigna, G. (2013, February). Compa: Detecting compromised accounts on social networks. In *NDSS*.

Eakin, H., & Luers, A. L. (2006). Assessing the vulnerability of social-environmental systems. *Annu. Rev. Environ. Resour.*, *31*, 365-394.

Easley, D., & Kleinberg, J. (2010). *Networks, crowds, and markets* (Vol. 8). Cambridge: Cambridge university press.

Eastin, M. S., & LaRose, R. (2000). Internet self-efficacy and the psychology of the digital divide. *Journal of computer-mediated communication, 6*(1), JCMC611.

Ebbinghaus, H. (1964). *Memory: Acontribution to experimental psychology*. Dover.

Eirinaki, M., Singh Monga, S. P., & Sundaram, S. (2012). Identification of influential social networkers. *International Journal of Web Based Communities*, *8*(2), 136.

Eiser, J. R., Sutton, S. R., & Wober, M. (1978). "Consonant" and "dissonant" smokers and the self-attribution of addiction. *Addictive Behaviors*, *3*(2), 99-106.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of OSN sites. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168.

Elphinston, R. A., & Noller, P. (2011). Time to face it! Facebook intrusion and the implications for romantic jealousy and relationship satisfaction. *Cyberpsychology, Behavior, and Social Networking*, *14*(11), 631-635.

Enrique, E. (2010). Addiction to new technologies and to online social networking in young people: A new challenge. *Adicciones*, *22*(2).

Epstein, S. (1998). Cognitive-experiential self-theory. In *Advanced personality* (pp. 211-238). Springer, Boston, MA.

Erchul WP, Raven BH (1997). Social power in school consultation: a contemporary view of French and Raven's bases of power model. *Journal of School Psychology 35*(2):137–171.

Euster, P., Guerraoui, R., Kermarrec, A. M., & Maussoulie, L. (2004). From epidemics to distributed computing. *IEEE Computer, 37*(5), 60-67.

Evans, J. S. B. (2008). Dual-processing accounts of reasoning, judgment, and social cognition. Annu. Rev. *Psychol., 59*, 255-278.

Everitt, B. J., Belin, D., Economidou, D., Pelloux, Y., Dalley, J. W., & Robbins, T. W. (2008). Neural mechanisms underlying the vulnerability to develop compulsive drug-seeking habits and addiction. *Philosophical Transactions of the Royal Society of London B: Biological Sciences, 363*(1507), 3125-3135.

Faghani, M. R., & Saidi, H. (2009, October). Malware propagation in online social networks. In *2009 4th International Conference on Malicious and Unwanted Software (MALWARE)* (pp. 8-14). IEEE.

Fang, X., & Hu, P. J. (2016). Top persuader prediction for social networks. *MIS Quarterly, Forthcoming*.

Faraj, S., Kudaravalli, S., & Wasko, M. (2015). Leading collaboration in online communities. *MIS Quarterly, 39*(2).

Fenichel, M. (2010). Facebook Addiction Disorder (FAD)-A New Challenge?. *Fenichel. com Site Map. http://www. fenichel. com/facebook/(accessed April 12, 2012)*.

Fiegerman, S. (2012). Twitter now has more than 200 million monthly active users. *Finn, S. and E. Mustafaraj (2012). Real-Time Filtering for Pulsing Public Opinion in Social*.

Fillmore, M. T., Rush, C. R., Kelly, T. H., & Hays, L. (2001). Triazolam impairs inhibitory control of behavior in humans. *Experimental and Clinical Psychopharmacology*, *9*(4), 363.

Finlayson, T. J., Le, B., Smith, A., Bowles, K., Cribbin, M., Miles, I., ... & DiNenno, E. (2011). HIV risk, prevention, and testing behaviors among men who have sex with men–National HIV Behavioral Surveillance System, 21 US cities, United States, 2008. *MMWR Surveill Summ*, *60*(14), 1-34.

Fleizach, C., Liljenstam, M., Johansson, P., Voelker, G. M., & Mehes, A. (2007, November). Can you infect me now?: malware propagation in mobile phone networks. In *Proceedings of the 2007 ACM workshop on Recurring malcode* (pp. 61-68). ACM.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology, 30*(2), 407-429.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 39*-50.

Franceschi-Bicchierai, L. (2016). Another day, another hack: 117 million LinkedIn emails and passwords. *Vice Motherboard.*

Freeman, L. C. (1979). Centrality in social networks conceptual clarification. *Social networks, 1*(3), 215-239.

Friese, M., & Hofmann, W. (2009). Control me or I will control you: Impulses, trait self-control, and the guidance of behavior. *Journal of Research in Personality, 43*(5), 795-805.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983-988.

Gao, H., Hu, J., Huang, T., Wang, J., & Chen, Y. (2011). Security issues in OSNs. Internet Computing, *IEEE, 15*(4), 56-63.

Garriss, Scott, Michael Kaminsky, Michael J. Freedman, Brad Karp, David Mazières, and Haifeng Yu. "RE: Reliable Email." In *NSDI*, vol. 6, pp. 22-22. 2006.

Gerrard, M., Gibbons, F. X., Benthin, A. C., & Hessling, R. M. (1996). A longitudinal study of the reciprocal nature of risk behaviors and cognitions in adolescents: what you do shapes what you think, and vice versa. *Health psychology*, *15*(5), 344.

Gino, F., Schweitzer, M. E., Mead, N. L., & Ariely, D. (2011). Unable to resist temptation: How self-control depletion promotes unethical behavior. *Organizational Behavior and Human Decision Processes, 115*(2), 191-203.

Goldenberg J, Han S, Lehmann D, Hong J (2009). The role of hubs in the adoption process. *Journal of Marketing 73*(2):1–13

Goldstein, A. (2001). *Addiction: From biology to drug policy*. Oxford University Press.

Govani, T., & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. *unpublished paper presented at the "Privacy Poster Fair" at the Carnegie Mellon University School of Library and Information Science*, *9*, 1-17.

Grant, J. E., Potenza, M. N., Weinstein, A., & Gorelick, D. A. (2010). Introduction to behavioral addictions. *The American journal of drug and alcohol abuse, 36*(5), 233-241.

Gray, E., Seigneur, J. M., Chen, Y., & Jensen, C. (2003, May). Trust propagation in small worlds. In *International conference on trust management* (pp. 239-254). Springer, Berlin, Heidelberg.

Greenfield, T. K., & Rogers, J. D. (1999). Alcoholic beverage choice, risk perception and self-reported drunk driving: effects of measurement on risk analysis. *Addiction, 94*(11), 1735-1743.

Greening, L. (1997). Adolescents' Cognitive Appraisals of Cigarette Smoking: An Application of the Protection Motivation Theory 1. *Journal of Applied Social Psychology*, *27*(22), 1972-1985.

Grier, C., Thomas, K., Paxson, V., & Zhang, M. (2010, October). @ spam: the underground on 140 characters or less. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 27-37). ACM.

Griffin, C., & Brooks, R. (2006). A note on the spread of worms in scale-free networks. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, *36*(1), 198-202.

Griffiths, M. (1999). Internet addiction: fact or fiction?. *The Psychologist*.

Griffiths, M. (2005). A 'components' model of addiction within a biopsychosocial framework. *Journal of Substance use, 10*(4), 191-197.

Griffiths, M. D. (2010). The role of context in online gaming excess and addiction: Some case study evidence. *International Journal of Mental Health and Addiction*, *8*(1), 119-125.

Griffiths, M. D., Kuss, D. J., & Demetrovics, Z. (2014). Social networking addiction: An overview of preliminary findings. *In Behavioral addictions* (pp. 119-141).

Griffiths, M., & Parke, A. (2008). Internet gambling. In *Encyclopedia of Internet Technologies and Applications* (pp. 228-234). IGI Global.

Gross, R., & Acquisti, A. (2005, November). Information revelation and privacy in OSNs. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society* (pp. 71-80). ACM.

Gruhl, D., Guha, R., Liben-Nowell, D., & Tomkins, A. (2004, May). Information diffusion through blogspace. In *Proceedings of the 13th international conference on World Wide Web* (pp. 491-501). ACM.

Gu, B., Konana, P., Raghunathan, R., & Chen, H. M. (2014). Research note—The allure of homophily in social media: Evidence from investor responses on virtual communities. *Information Systems Research, 25*(3), 604-617.

Gul, F., & Pesendorfer, W. (2004). Self-control and the theory of consumption. *Econometrica, 72*(1), 119-158.

Gulati, R. (1995). Does familiarity breed trust? The implications of repeated ties for contractual choice in alliances. *Academy of management journal*, *38*(1), 85-112.

Guo, H., Cheng, H. K., & Kelley, K. (2016). Impact of network structure on malware propagation: a growth curve perspective. *Journal of Management Information Systems*, *33*(1), 296-325.

Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI global.

Haagsma, M. C., Caplan, S. E., Peters, O., & Pieterse, M. E. (2013). A cognitive-behavioral model of problematic online gaming in adolescents aged 12–22 years. *Computers in human behavior, 29*(1), 202-209.

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and Facebook. *arXiv preprint arXiv:1301.7643.*

Han, X., Wang, L., Crespi, N., Park, S., & Cuevas, Á. (2015). Alike people, alike interests? Inferring interest similarity in online social networks. *Decision Support Systems, 69*, 92-106.

Hatfield, D. (1984). Trust in Advertising. Does it Apply to Vitamin Supplements. *American Council on Science and Health*, *5*(1).

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, *14*(2), 171-180.

Heesterbeek, J. A. P. (2002). A brief history of R 0 and a recipe for its calculation. *Acta biotheoretica, 50*(3), 189-204.

Heesterbeek, J. A. P., & Dietz, K. (1996). The concept of Ro in epidemic theory. *Statistica Neerlandica, 50*(1), 89-110.

Heffernan, J. M., Smith, R. J., & Wahl, L. M. (2005). Perspectives on the basic reproductive ratio. *Journal of the Royal Society Interface, 2*(4), 281-293.

Heidemann, J., Klier, M., & Probst, F. (2010). Identifying key users in online social networks: A pagerank based approach.

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.

Hidi, S. (2006). Interest: A unique motivational variable. *Educational research review, 1*(2), 69-82.

Hill, A. N., & Longini, I. M. (2003). The critical vaccination fraction for heterogeneous epidemic models. *Mathematical biosciences, 181*(1), 85-106.

Hingson, R., Mangione, T., Meyers, A., & Scotch, N. (1982). Seeking help for drinking problems; a study in the Boston Metropolitan Area. *Journal of Studies on Alcohol*, *43*(3), 273-288.

Hinz O, Skiera B, Barrot C, Becker JU (2011) Seeding strategies for viral marketing: an empirical comparison. *Journal of Marketing 75*(6):55–71

Hodgins, D., Peden, N., & Makarchuk, K. (2004). Self-efficacy in pathological gambling treatment outcome: Development of a gambling abstinence self-efficacy scale (GASS). *International Gambling Studies, 4*(2), 99-108.

Hoffman, B. R., Monge, P. R., Chou, C. P., & Valente, T. W. (2007). Perceived peer influence and peer selection on adolescent smoking. *Addictive Behaviors*, *32*(8), 1546-1554.

Hofmann, W., Deutsch, R., Lancaster, K., & Banaji, M. R. (2010). Cooling the heat of temptation: Mental self-control and the automatic evaluation of tempting stimuli. *European Journal of Social Psychology*, *40*(1), 17-25.

Hofmann, W., & Kotabe, H. (2012). A general model of preventive and interventive self-control. *Social and Personality Psychology Compass*, *6*(10), 707-722.

Hofmann, W., Friese, M., & Strack, F. (2009). Impulse and self-control from a dual-systems perspective. *Perspectives on Psychological Science, 4*(2), 162-176.

Holmes, K. K., Mardh, P.A., Sparling, P. F. and Wiesner, P. J. (1990). Sexually transmitted diseases. 2nd ed. McGraw-Hill, New York;

Hu, Li-tze, and Peter M. Bentler. "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives." *Structural equation modeling: a multidisciplinary journal* 6, no. 1 (1999): 1-55.

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, *31*(4), 6-48.

Huang, G. C., Unger, J. B., Soto, D., Fujimoto, K., Pentz, M. A., Jordan-Marsh, M., & Valente, T. W. (2014). Peer influences: the impact of online and offline friendship networks on adolescent smoking and alcohol use. *Journal of Adolescent Health, 54*(5), 508-514.

Huberman, B. A., Romero, D. M., & Wu, F. (2009). Crowdsourcing, attention and productivity. *Journal of Information Science, 35*(6), 758-765.

Hyman, S. E., & Malenka, R. C. (2001). Addiction and the brain: the neurobiology of compulsion and its persistence. *Nature reviews neuroscience, 2*(10), 695.

Inkpen, A. C., & Tsang, E. W. (2005). Social capital, networks, and knowledge transfer. *Academy of management review, 30*(1), 146-165.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011, July). Reverse social engineering attacks in online social networks. In *International conference on detection of intrusions and malware, and vulnerability assessment* (pp. 55-74). Springer, Berlin, Heidelberg.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. K. (2007, February). What instills trust? a qualitative study of phishing. In *International Conference on Financial Cryptography and Data Security* (pp. 356-361). Springer, Berlin, Heidelberg.

Jadack, R. A., Fresia, A., Rompalo, A. M., & Zenilman, J. (1997). Reasons for not using condoms of clients at urban sexually transmitted diseases clinics. *Sexually Transmitted Diseases*, *24*(7), 402-408.

James, W. (1983). *Talks to Teachers on Psychology and to Students on Some of Life's Ideals* (Vol. 12). Harvard University Press.

Jeger, M. J., Pautasso, M., Holdenrieder, O., & Shaw, M. W. (2007). Modelling disease spread and control in networks: implications for plant sciences. *New Phytologist, 174*(2), 279-297.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 549-566.

Jordan, C. M., & Oei, T. P. (1989). Help-seeking behaviour in problem drinkers: a review. *British Journal of Addiction*, *84*(9), 979-988.

Kadden, R. M., & Litt, M. D. (2011). The role of self-efficacy in the treatment of substance use disorders. *Addictive behaviors, 36*(12), 1120-1126.

Kahneman, D., & Tversky, A. (2013). Prospect theory: An analysis of decision under risk. In *Handbook of the fundamentals of financial decision making: Part I* (pp. 99-127).

Kane, G. C., Alavi, M., Labianca, G. J., & Borgatti, S. P. (2014). Whar's different about social media networks? A framework and research agenda. *MIS Quarterly*, 38(1).

Karaiskos, D., Tzavellas, E., Balta, G., & Paparrigopoulos, T. (2010). P02-232-Social network addiction: a new clinical disorder?. *European Psychiatry*, *25*, 855.

Karyotis, V., & Khouzani, M. H. R. (2016). *Malware diffusion models for modern complex networks: theory and applications*. Morgan Kaufmann.

Kaspersky Labs (2009), Kaspersky Security Bulletin: Malware Evolution, available at: http://www.kaspersky.com/ news?id = 207575761.

Katz E, Lazarsfeld PF (1955) *Personal influence: the part played by people in the flow of mass communications*. Glencoe, IL: Free Press.

Kawachi, K. (2008). Deterministic models for rumor transmission. *Nonlinear analysis: Real world applications, 9*(5), 1989-2028.

Keeling, M. J. (1999). The effects of local spatial structure on epidemiological invasions. *Proceedings of the Royal Society of London B: Biological Sciences, 266*(1421), 859-867.

Kendler, K. S., Karkowski, L. M., Neale, M. C., & Prescott, C. A. (2000). Illicit psychoactive substance use, heavy use, abuse, and dependence in a US population-based sample of male twins. *Archives of general psychiatry, 57*(3), 261-269.

Khelil, A., Becker, C., Tian, J., & Rothermel, K. (2002, September). An epidemic model for information diffusion in MANETs. In *Proceedings of the 5th ACM international workshop on Modeling analysis and simulation of wireless and mobile systems* (pp. 54-60). ACM.

Kim ES, Han SS (2009) An analytical way to find influencers on social networks and validate their effects in disseminating social games. In: Proc international conference on advances in social network analysis and mining, Athens, pp 41–46.

Kirschner, P. A., & Karpinski, A. C. (2010). Facebook® and academic performance. *Computers in human behavior*, *26*(6), 1237-1245.

Kiss, C., & Bichler, M. (2008). Identification of influencers—measuring influence in customer networks. *Decision Support Systems*, *46*(1), 233-253.

Kivelä, M., Pan, R. K., Kaski, K., Kertész, J., Saramäki, J., & Karsai, M. (2012). Multiscale analysis of spreading in a large communication network. Journal of Statistical Mechanics: Theory and Experiment, 2012(03), P03005.

Klovdahl, A. S. (1985). Social networks and the spread of infectious diseases: the AIDS example. Social science & medicine, 21(11), 1203-1216.

Koc, M., & Gulyagci, S. (2013). Facebook addiction among Turkish college students: The role of psychological health, demographic, and usage characteristics. *Cyberpsychology, Behavior, and Social Networking*, *16*(4), 279-284.

Koob, G. F., & Le Moal, M. (2006). What is addiction. *Neurobiology of Addiction. Koob GF, Le Moal M (eds), Elsevier/Academic Press, Amsterdam/Boston*, 1-22.

Krasnova, H., Widjaja, T., Buxmann, P., Wenninger, H., & Benbasat, I. (2015). Research note—why following friends can hurt you: an exploratory investigation of the effects of envy on social networking sites among college-age users. *Information systems research*, *26*(3), 585-605.

Kretzschmar, M., & Morris, M. (1996). Measures of concurrency in networks and the spread of infectious disease. *Mathematical biosciences, 133*(2), 165-195.

Kuss, D. J., & Griffiths, M. D. (2011). Online social networking and addiction—a review of the psychological literature. *International journal of environmental research and public health, 8*(9), 3528-3552.

Kwak, H., Lee, C., Park, H., & Moon, S. (2010, April). What is Twitter, a social network or a news media?. In *Proceedings of the 19th international conference on World wide web* (pp. 591-600). ACM.

Lampel, J., & Bhalla, A. (2007). The role of status seeking in online communities: Giving the gift of experience. *Journal of Computer-Mediated Communication, 12*(2), 434-455.

Lang, A., Shin, M., & Lee, S. (2005). Sensation seeking, motivation, and substance use: A dual system approach. *Media Psychology, 7*(1), 1-29.

LaRose, R., Lin, C. A., & Eastin, M. S. (2003). Unregulated Internet usage: Addiction, habit, or deficient self-regulation?. *Media Psychology, 5*(3), 225-253.

Lazarsfeld, P. F., & Merton, R. K. (1954). Friendship as a social process: A substantive and methodological analysis. *Freedom and control in modern society*, *18*(1), 18-66.

Leibnitz, K., Hoßfeld, T., Wakamiya, N., & Murata, M. (2006, March). On pollution in eDonkey-like peer-to-peer file-sharing networks. In *13th GI/ITG Conference-Measuring, Modelling and Evaluation of Computer and Communication Systems* (pp. 1-18). VDE.

Lerman, K., & Ghosh, R. (2010, May). Information contagion: An empirical study of the spread of news on digg and twitter social networks. In *Fourth International AAAI Conference on Weblogs and Social Media*.

Leskovec, J., Adamic, L. A., & Huberman, B. A. (2007). The dynamics of viral marketing. *ACM Transactions on the Web (TWEB)*, *1*(1), 5.

Leskovec, J., McGlohon, M., Faloutsos, C., Glance, N., & Hurst, M. (2007, April). Patterns of cascading behavior in large blog graphs. In *Proceedings of the 2007 SIAM international conference on data mining* (pp. 551-556). Society for Industrial and Applied Mathematics.

Levin, D. Z., & Cross, R. (2004). The strength of weak ties you can trust: The mediating role of trust in effective knowledge transfer. *Management science*, *50*(11), 1477-1490.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces, 63*, 967–985.

Li, H., Cheng, X., & Liu, J. (2014). Understanding video sharing propagation in social networks: Measurement and analysis. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 10*(4), 33.

Li, M., Cao, N., Yu, S., & Lou, W. (2011, April). Findu: Privacy-preserving personal profile matching in mobile social networks. In *INFOCOM, 2011 Proceedings IEEE* (pp. 2435-2443). IEEE.

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

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394.

Lin, N. (1999). Building a network theory of social capital. *Connections, 22*(1), 28-51.

Lin, N. (2002). *Social capital: A theory of social structure and action* (Vol. 19). Cambridge university press.

Lipsitch, M., Cohen, T., Cooper, B., Robins, J. M., Ma, S., James, L., ... & Fisman, D. (2003). Transmission dynamics and control of severe acute respiratory syndrome. *Science, 300*(5627), 1966-1970.

Liu, H., & Maes, P. (2005). Interestmap: Harvesting social network profiles for recommendations. *Beyond Personalization-IUI*, *56*.

Lowry, P. B., Zhang, J., Wang, C., & Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning model. *Information Systems Research*, *27*(4), 962-986.

Lü, L., Zhang, Y. C., Yeung, C. H., & Zhou, T. (2011). Leaders in social networks, the delicious case. *PloS one, 6*(6), e21202.

Luscombe, B. (2009). Social norms. Facebook and divorce. *Time*, *173*(24), 93.

MacCoun, R. J. (1993). Drugs and the law: a psychological analysis of drug prohibition. *Psychological bulletin, 113*(3), 497.

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.

Maisto, S. A., Connors, G. J., & Zywiak, W. H. (2000). Alcohol treatment changes in coping skills, self-efficacy, and levels of alcohol use and related problems 1 year following treatment initiation. *Psychology of Addictive Behaviors, 14*(3), 257.

Mansfield-Devine, S. (2008). Anti-social networking: exploiting the trusting environment of Web 2.0. *Network Security*, *2008*(11), 4-7.

Marsden, P. V. (1987). Core discussion networks of Americans. *American sociological review*, 122-131.

Mashable. Twitter now has more than 200 million monthly active users http://mashable.com/2012/12/ 18/twitter-200-million-active-users/.

May, R. M., & Anderson, R. M. (1987). COMMENTARY~ Transmission dynamics of HIV infection. *Nature*, 326, 137.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review, 20*(3), 709-734.

McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual review of sociology, 27*(1), 415-444.

Meena, P. S., Mittal, P. K., & Solanki, R. K. (2012). Problematic use of social networking sites among urban school going teenagers. *Industrial Psychiatry Journal*, *21*(2), 94.

Mehroof, M., & Griffith, M. (2010). D.(2010). Online gaming addiction: The role of sensation seeking, Self control, Neuroticism, Aggression, State anxiety, And trait anxiety. *Journal Cyberpsychology, Behavior, and Social Networking*, *13*(3).

Menard, S. (2002). *Applied logistic regression analysis* (Vol. 106). Sage.

Meyers, L. A., Pourbohloul, B., Newman, M. E., Skowronski, D. M., & Brunham, R. C. (2005). Network theory and SARS: predicting outbreak diversity. *Journal of theoretical biology, 232*(1), 71-81.

Miller, D. T. (1999). The norm of self-interest. *American Psychologist, 54*(12), 1053.

Miller, D. T., & Ratner, R. K. (1998). The disparity between the actual and assumed power of self-interest. *Journal of personality and social psychology, 74*(1), 53.

Mills, C. E., Robins, J. M., & Lipsitch, M. (2004). Transmissibility of 1918 pandemic influenza. *Nature, 432*(7019), 904-906.

Mislove A, Viswanath B, Gummadi KP, Druschel P (2010, February) You are who you know: inferring user profiles in online social networks. In *Proceedings of the third ACM international conference on Web search and data mining* (pp. 251-260) ACM.

Mislove, A., Marcon, M., Gummadi, K. P., Druschel, P., & Bhattacharjee, B. (2007, October). Measurement and analysis of OSNs. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement* (pp. 29-42). ACM.

Modic, D., & Lea, S. E. (2012). How neurotic are scam victims, really? The big five and Internet scams. *The Big Five and Internet Scams (September 10, 2012)*.

Moore, C., & Newman, M. E. (2000). Epidemics and percolation in small-world networks. *Physical Review E, 61*(5), 5678.

Moore, S., & Gullone, E. (1996). Predicting adolescent risk behavior using a personalized cost-benefit analysis. *Journal of youth and adolescence, 25*(3), 343-359.

Moorman, C., Deshpande, R., & Zaltman, G. (1993). Factors affecting trust in market research relationships. *Journal of marketing*, *57*(1), 81-101.

Moorman, C., Zaltman, G., & Deshpande, R. (1992). Relationships between providers and users of market research: the dynamics of trust within and between organizations. *Journal of marketing research*, *29*(3), 314-328.

Morris, M., & Kretzschmar, M. (1995). Concurrent partnerships and transmission dynamics in networks. *Social Networks*, *17*(3-4), 299-318.

Morris, R. (1994). Computerized content analysis in management research: A demonstration of advantages & limitations. *Journal of Management*, *20*(4), 903-931.

Muise, A., Christofides, E., & Desmarais, S. (2009). More information than you ever wanted: Does Facebook bring out the green-eyed monster of jealousy?. *CyberPsychology & behavior*, *12*(4), 441-444.

Mukandavire, Z., Gumel, A. B., Garira, W., & Tchuenche, J. M. (2009). Mathematical analysis of a model for HIV-malaria co-infection.

Myers, S. A., Zhu, C., & Leskovec, J. (2012, August). Information diffusion and external influence in networks. In *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 33-41). ACM.

Myers, S., & Leskovec, J. (2010). On the convexity of latent social network inference. In *Advances in Neural Information Processing Systems* (pp. 1741-1749).

Nahapiet, J., & Ghoshal, S. (1998). Social capital, intellectual capital, and the organizational advantage. *Academy of management review, 23*(2), 242-266.

Nahl, D., & Meer, M. P. (1997). User-centered assessment of two Web browsers: Errors, perceived self-efficacy, and success. In *Proceedings of the ASIST Annual Meeting* (Vol. 34, pp. 89-97).

Neter, J., Wasserman, W., & Kutner, M. H. (1989). Applied linear regression models.

Newell, A., & Simon, H. A. (1972). *Human problem solving* (Vol. 104, No. 9). Englewood Cliffs, NJ: Prentice-Hall.

Newman, M. E. (2002). Spread of epidemic disease on networks. *Physical review E, 66*(1), 016128.

Noyes, A. (2007). Biggest threat to Internet could be a massive virtual blackout. *National Journal's Technology Daily*.

Orford, J. (2001). *Excessive appetites: A psychological view of addictions.* John Wiley & Sons Ltd.

Pastor-Satorras, R., & Vespignani, A. (2001). Epidemic spreading in scale-free networks. *Physical review letters, 86*(14), 3200.

Pei, S., Muchnik, L., Andrade Jr, J. S., Zheng, Z., & Makse, H. A. (2014). Searching for superspreaders of information in real-world social media. *Scientific reports*, *4*, 5547.

Pierson, J. (2012). Online privacy in social media: a conceptual exploration of empowerment and vulnerability. *Communications & Strategies*, (88), 99-120.

Piquero, A., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice quarterly*, *13*(3), 481-510.

Pogarsky, G. (2002). Identifying "deterrable" offenders: Implications for research on deterrence. *Justice Quarterly, 19*(3), 431-452.

Powell, J., Hardoon, K., Derevensky, J. L., & Gupta, R. (1999). Gambling and risk-taking behavior among university students. *Substance Use & Misuse, 34*(8), 1167-1184.

Probst, F., Grosswiele, L., & Pfleger, R. (2013). Who will lead and who will follow: Identifying Influential Users in Online Social Networks. *Business & Information Systems Engineering, 5*(3), 179-193.

Putnam, R. D. (1995). Bowling alone: America's declining social capital. *Journal of democracy, 6*(1), 65-78.

Ratner, R. K., & Miller, D. T. (2001). The norm of self-interest and its effects on social action. *Journal of personality and social psychology, 81*(1), 5.

Ren, W. H. (1999). Self-efficacy and the search for government information: A study of small-business executives. *Reference & User Services Quarterly*, 283-291.

Riley, S., Fraser, C., Donnelly, C. A., Ghani, A. C., Abu-Raddad, L. J., Hedley, A. J., ... & Chau, P. (2003). Transmission dynamics of the etiological agent of SARS in Hong Kong: impact of public health interventions. *Science, 300*(5627), 1961-1966.

Riolo, C. S., Koopman, J. S., & Chick, S. E. (2001). Methods and measures for the description of epidemiologic contact networks. *Journal of Urban Health*, *78*(3), 446-457.

Rizzo, A., Frasca, M., & Porfiri, M. (2014). Effect of individual behavior on epidemic spreading in activity-driven networks. *Physical Review E, 90*(4), 042801.

Robinson, T. E., & Berridge, K. C. (2003). Addiction. *Annual Review of Psychology, 54*, 25-53.

Rodriguez, M. G., Leskovec, J., Balduzzi, D., & Schölkopf, B. (2014). Uncovering the structure and temporal dynamics of information propagation. *Network Science, 2*(1), 26-65.

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

Romero, D. M., Meeder, B., & Kleinberg, J. (2011, March). Differences in the mechanics of information diffusion across topics: idioms, political hashtags, and complex contagion on twitter. In *Proceedings of the 20th international conference on World wide web* (pp. 695-704). ACM.

Rosenstein, A. W., & Grant, A. E. (1997). Reconceptualizing the role of habit: A new model of television audience activity. *Journal of Broadcasting & electronic media*, *41*(3), 324-344.

Rothenberg, R. B., Potterat, J. J., Woodhouse, D. E., Darrow, W. W., Muth, S. Q., & Klovdahl, A. S. (1995). Choosing a centrality measure: epidemiologic correlates in the Colorado Springs study of social networks. *Social Networks, 17*(3), 273-297.

Rothenberg, R. B., Potterat, J. J., Woodhouse, D. E., Muth, S. Q., Darrow, W. W., & Klovdahl, A. S. (1998). Social network dynamics and HIV transmission. *Aids, 12*(12), 1529-1536.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust 1. *Journal of personality*, *35*(4), 651-665.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review, 23*(3), 393-404.

Ryan, T., Chester, A., Reece, J., & Xenos, S. (2014). The uses and abuses of Facebook: A review of Facebook addiction.

Salton, G., & McGill, M. J. (1983). *Introduction to modern information retrieval.* McGraw Hill.

Sanzgiri, A., Hughes, A., & Upadhyaya, S. (2013, September). Analysis of malware propagation in twitter. In *2013 IEEE 32nd International Symposium on Reliable Distributed Systems* (pp. 195-204). IEEE.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), 122-131.

Schneier, B. (2000). Semantic network attacks. *Communications of the ACM*, *43*(12), 168-168.

Schröder-Butterfill, E., & Marianti, R. (2006). A framework for understanding old-age vulnerabilities. *Ageing & Society*, *26*(1), 9-35.

Scott, J. (2000). Rational choice theory. Understanding contemporary society: theories of the present. *International Encyclopedia of Social Sciences*, *2*, 126-138.

Seibert, S. E., Kraimer, M. L., & Liden, R. C. (2001). A social capital theory of career success. *Academy of management journal, 44*(2), 219-237.

Shah, D., & Zaman, T. (2011). Rumors in a network: Who's the culprit?. *IEEE Transactions on information theory, 57*(8), 5163-5181.

Sharif Vaghefi, M. (2018). Online Social Networks' Investigations of Individuals' Healthy and Unhealthy Lifestyle Behaviors and Social Factors Influencing Them—Three Essays.

Shapira, N. A., Lessig, M. C., Goldsmith, T. D., Szabo, S. T., Lazoritz, M., Gold, M. S., & Stein, D. J. (2003). Problematic internet use: proposed classification and diagnostic criteria. *Depression and anxiety, 17*(4), 207-216.

Shaw, L. H., & Gant, L. M. (2004). In defense of the Internet: The relationship between Internet communication and depression, loneliness, self-esteem, and perceived social support. *Internet Research*, *28*(3).

Sherchan, W., Nepal, S., & Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys (CSUR), 45*(4), 47.

Shi, Z., Rui, H., and Whinston, A.B. (2014). Content Sharing in a Social Broadcasting Environment: Evidence from Twitter. *MIS Quarterly 38*(1), pp. 123-142.

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers, 22*(5), 428-438.

Shirley, M. D., & Rushton, S. P. (2005). The impacts of network topology on disease spread. *Ecological Complexity, 2*(3), 287-299.

Shive, S. (2010). An epidemic model of investor behavior. *Journal of Financial and Quantitative Analysis*, *45*(1), 169-198.

Shtatland, E. S., & Shtatland, T. (2008). Early detection of epidemic outbreaks and financial bubbles using autoregressive models with structural changes. *Proceedings of the NESUG, 21*.

Simon-Morton, B., & Farhat, T. (2010). Recent finding on peer group influences on adolescent substance use. *J Prim Prev*, *31*, 191-298.

Soror, A. A., Hammer, B. I., Steelman, Z. R., Davis, F. D., & Limayem, M. M. (2015). Good habits gone bad: Explaining negative consequences associated with the use of mobile phones from a dual-systems perspective. *Information Systems Journal, 25*(4), 403-427.

Spraggins, A. (2009). *Problematic use of online social networking sites for college students: Prevalence, predictors, and association with well-being*. Gainesville, FL: University of Florida.

Staples, D. S., Hulland, J. S., & Higgins, C. A. (1999). A self-efficacy theory explanation for the management of remote workers in virtual organizations. *Organization Science, 10*(6), 758-776.

Strack, F., & Deutsch, R. (2004). Reflective and impulsive determinants of social behavior. *Personality and social psychology review, 8*(3), 220-247.

Suh, B., Hong, L., Pirolli, P., & Chi, E. H. (2010, August). Want to be retweeted? large scale analytics on factors impacting retweet in twitter network. In *Social computing (socialcom), 2010 IEEE second international conference on* (pp. 177-184). IEEE.

Sun, E., Rosenn, I., Marlow, C. A., & Lento, T. M. (2009, March). Gesundheit! modeling contagion through facebook news feed. In *Third international AAAI conference on weblogs and social media*.

Sussman, S., Lisha, N., & Griffiths, M. (2011). Prevalence of the addictions: a problem of the majority or the minority?. *Evaluation & the health professions, 34*(1), 3-56.

Sutton, S. (1987). Social-psychological Approaches to Understanding Addictive Behaviours: attitude-behaviour and decision-making models. *British Journal of Addiction*, *82*(4), 355-370.

Tang, J., Gao, H., Hu, X., & Liu, H. (2013, February). Exploiting homophily effect for trust prediction. In *Proceedings of the sixth ACM international conference on Web search and data mining* (pp. 53-62). ACM.

Tangney, J. P., Baumeister, R. F., & Boone, A. L. (2004). High self-control predicts good adjustment, less pathology, better grades, and interpersonal success. *Journal of personality*, *72*(2), 271-324.

Thadani, D. R., & Cheung, C. M. (2011, January). Online social network dependency: Theoretical development and testing of competing models. In *2011 44th Hawaii International Conference on System Sciences* (pp. 1-9). IEEE.

Thrul, J., Stemmler, M., Bühler, A., & Kuntsche, E. (2013). Adolescents' protection motivation and smoking behaviour. *Health education research*, *28*(4), 683-691.

Tiffany, S. T. (1990). A cognitive model of drug urges and drug-use behavior: role of automatic and nonautomatic processes. *Psychological review, 97*(2), 147.

Tobin, D. L., Holroyd, K. A., Reynolds, R. V., & Wigal, J. K. (1989). The hierarchical factor structure of the Coping Strategies Inventory. Cognitive therapy and research, 13(4), 343-361.

Tokunaga, R. S. (2011). Social networking site or social surveillance site? Understanding the use of interpersonal electronic surveillance in romantic relationships. *Computers in Human Behavior*, *27*(2), 705-713.

Thom, B. (1986). Sex differences in help-seeking for alcohol problems–1. The barriers to help-seeking. *British Journal of Addiction*, *81*(6), 777-788.

Trucco, E. M., Colder, C. R., & Wieczorek, W. F. (2011). Vulnerability to peer influence: A moderated mediation study of early adolescent alcohol use initiation. *Addictive behaviors*, *36*(7), 729-736.

Tsai, W., & Ghoshal, S. (1998). Social capital and value creation: The role of intrafirm networks. *Academy of management Journal, 41*(4), 464-476.

Tsukayama, H. (2013). Twitter turns 7: Users send over 400 million tweets per day. Washington Post. March 21. https://www.washingtonpost.com/business/technology/twitter-turns-7-users-send-over-400-million-tweets-per-day/2013/03/21/2925ef60-9222-11e2-bdea-e32ad90da239_story.html

Turel, O. (2015). Quitting the use of a habituated hedonic information system: a theoretical model and empirical examination of Facebook users. *European Journal of Information Systems*, *24*(4), 431-446.

Turel, O., & Bechara, A. (2016). A triadic reflective-impulsive-interoceptive awareness model of general and impulsive information system use: behavioral tests of neuro-cognitive theory. *Frontiers in psychology, 7*, 601.

Turel, O., & Qahri-Saremi, H. (2016). Problematic use of social networking sites: antecedents and consequence from a dual-system theory perspective. *Journal of Management Information Systems, 33*(4), 1087-1116.

Turel, O., & Serenko, A. (2010). Is mobile email addiction overlooked?. *Communications of the ACM*, *53*(5), 41-43.

Turel, O., & Serenko, A. (2012). The benefits and dangers of enjoyment with social networking websites. *European Journal of Information Systems, 21*(5), 512-528.

Turel, O., Serenko, A., & Giles, P. (2011). Integrating technology addiction and use: An empirical investigation of online auction users. *MIS Quarterly, 35*(4), 1043-1062.

Utz, S. (2015). The function of self-disclosure on social network sites: Not only intimate, but also positive and entertaining self-disclosures increase the feeling of connection. Computers in *Human Behavior, 45*, 1-10.

Vaghefi, I., & Qahri-Saremi, H. (2017). From IT addiction to discontinued use: A cognitive dissonance perspective. In *Proceedings of the 50st Hawaii International Conference on System Sciences*.

Valente, T. W., Unger, J. B., & Johnson, C. A. (2005). Do popular students smoke? The association between popularity and smoking among middle school students. *Journal of Adolescent Health*, *37*(4), 323-329.

Valkenburg, P. M., Peter, J., & Schouten, A. P. (2006). Friend networking sites and their relationship to adolescents' well-being and social self-esteem. *CyberPsychology & Behavior*, *9*(5), 584-590.

Valenzuela, S., Arriagada, A., & Scherman, A. (2014). Facebook, Twitter, and youth engagement: A quasi-experimental study of social media use and protest behavior using propensity score matching. *International Journal of Communication*, *8*, 25.

Van den Bulte, C., & Joshi, Y. V. (2007). New product diffusion with influentials and imitators. *Marketing science*, *26*(3), 400-421.

Van den Bulte, C., & Wuyts, S. H. K. (2007). Social networks in marketing. *MSI Relevant Knowledge Series*.

Van den Eijnden, R. J., Lemmens, J. S., & Valkenburg, P. M. (2016). The social media disorder scale. *Computers in Human Behavior, 61*, 478-487.

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.

Ver Steeg, G., Ghosh, R., & Lerman, K. (2011, July). What stops social epidemics?. In *Fifth International AAAI Conference on Weblogs and Social Media*.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586.

Viswanath, B., Mislove, A., Cha, M., & Gummadi, K. P. (2009, August). On the evolution of user interaction in facebook. In *Proceedings of the 2nd ACM workshop on OSNs* (pp. 37-42). ACM.

Viswanathan, V., & Jain, V. (2013). A dual-system approach to understanding "generation Y" decision making. *Journal of consumer marketing, 30*(6), 484-492.

Wald, R., Khoshgoftaar, T. M., Napolitano, A., & Sumner, C. (2013, August). Predicting susceptibility to social bots on twitter. In *Information Reuse and Integration (IRI), 2013 IEEE 14th International Conference on* (pp. 6-13). IEEE.

Wallinga, J., & Teunis, P. (2004). Different epidemic curves for severe acute respiratory syndrome reveal similar impacts of control measures. *American Journal of Epidemiology, 160*(6), 509-516.

Walton, M. A., Blow, F. C., Bingham, C. R., & Chermack, S. T. (2003). Individual and social/environmental predictors of alcohol and drug use 2 years following substance abuse treatment. *Addictive Behaviors, 28*(4), 627-642.

Wang, Q., Lin, Z., Jin, Y., Cheng, S., & Yang, T. (2015). ESIS: emotion-based spreader–ignorant–stifler model for information diffusion. *Knowledge-Based Systems, 81*, 46-55.

Wang, Y., Chakrabarti, D., Wang, C., & Faloutsos, C. (2003, October). Epidemic spreading in real networks: An eigenvalue viewpoint. In *Reliable Distributed Systems, 2003. Proceedings. 22nd International Symposium on* (pp. 25-34). IEEE.

Wang, Z. Wen, H. Tong, C.-Y. Lin, C. Song, and A.-L. Barabasi. 2011. Information spreading in context. In *Proceedings of the 20th International Conference on World Wide Web (WWW'11)*. 735–744

Washington Post. Twitter turns 7: Users send over 400 million tweets per day. http://articles.washingtonpost.com/2013-03-21/ business/37889387_1_tweets-jack-dorsey-twitter.

Wasko, M. M., & Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*, 35-57.

Watts, D. J., & Dodds, P. S. (2007). Influentials, networks, and public opinion formation. *Journal of consumer research*, *34*(4), 441-458.

Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world'networks. *nature, 393*(6684), 440-442.

Webb, T. L., Sniehotta, F. F., & Michie, S. (2010). Using theories of behaviour change to inform interventions for addictive behaviours. *Addiction*, *105*(11), 1879-1892.

Weimann, G., Tustin, D. H., Van Vuuren, D., & Joubert, J. P. R. (2007). Looking for opinion leaders: Traditional vs. modern measures in traditional societies. *International Journal of Public Opinion Research*, *19*(2), 173-190.

Weng, J., Lim, E. P., Jiang, J., & He, Q. (2010, February). Twitterrank: finding topic-sensitive influential twitterers. In *Proceedings of the third ACM international conference on Web search and data mining* (pp. 261-270). ACM.

West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2009). The weakest link: A psychological perspective on why users make poor security decisions. In *Social and Human elements of information security: Emerging Trends and countermeasures* (pp. 43-60). IGI Global.

Wiers, R. W., Gladwin, T. E., Hofmann, W., Salemink, E., & Ridderinkhof, K. R. (2013). Cognitive bias modification and cognitive control training in addiction and related psychopathology: Mechanisms, clinical perspectives, and ways forward. *Clinical Psychological Science, 1*(2), 192-212.

Wilcox, K., & Stephen, A. T. (2012). Are close friends the enemy? Online social networks, self-esteem, and self-control. *Journal of Consumer research, 40*(1), 90-103.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, 1-20.

Wilson, C., Boe, B., Sala, A., Puttaswamy, K. P., & Zhao, B. Y. (2009, April). User interactions in social networks and their implications. In *Proceedings of the 4th ACM European conference on Computer systems* (pp. 205-218). Acm.

Winter, F., & Kataria, M. (2013). You are who your friends are: An experiment on trust and homophily in friendship networks. Retrieved May 15, 2015, from http://dx.doi.org/

10.2139/ssrn.2347536

Wolniczak, I., Cáceres-DelAguila, J. A., Palma-Ardiles, G., Arroyo, K. J., Solís-Visscher, R., Paredes-Yauri, S., ... & Bernabe-Ortiz, A. (2013). Association between Facebook dependence and poor sleep quality: a study in a sample of undergraduate students in Peru. *PloS one*, *8*(3), e59087.

Woo, J., & Chen, H. (2016). Epidemic model for information diffusion in web forums: experiments in marketing exchange and political dialog. *SpringerPlus, 5*(1), 66.

Woo, J., Son, J., & Chen, H. (2011, July). An SIR model for violent topic diffusion in social media. In *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics* (pp. 15-19). IEEE.

Wood, S. M., & Bechara, A. (2014). The neuroscience of dual (and triple) systems in decision making.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 proceedings*, 31.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674.

Wu, F., Huberman, B. A., Adamic, L. A., & Tyler, J. R. (2004). Information flow in social groups. *Physica A: Statistical Mechanics and its Applications, 337*(1), 327-335.

Wu, A. M., Cheung, V. I., Ku, L., & Hung, E. P. (2013). Psychological risk factors of addiction to social networking sites among Chinese smartphone users. *Journal of behavioral addictions*, *2*(3), 160-166.

Wu, S., Hofman, J. M., Mason, W. A., & Watts, D. J. (2011, March). Who says what to whom on twitter. In *Proceedings of the 20th international conference on World wide web* (pp. 705-714). ACM.

Xiong, F., Liu, Y., Zhang, Z. J., Zhu, J., & Zhang, Y. (2012). An information diffusion model based on retweeting mechanism for online social media. *Physics Letters A, 376*(30), 2103-2108.

Xu, H., & Tan, B. C. (2012). Why do I keep checking Facebook: Effects of message characteristics on the formation of social network services addiction.

Xu, Y. C., Zhang, C., Xue, L., & Yeo, L. L. (2008). Product adoption in OSN. *ICIS 2008 Proceedings*, 200.

Yan, G., Chen, G., Eidenbenz, S., & Li, N. (2011, March). Malware propagation in OSNs: nature, dynamics, and defense implications. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 196-206). ACM.

Yang, C., Harkreader, R. C., & Gu, G. (2011, January). Die free or live hard? empirical evaluation and new design for fighting evolving twitter spammers. In *Recent Advances in Intrusion Detection* (pp. 318-337). Springer Berlin Heidelberg.

Yellowlees, P. M., & Marks, S. (2007). Problematic Internet use or Internet addiction?. *Computers in human behavior, 23*(3), 1447-1453.

Young, K. S. (1998). Internet addiction: The emergence of a new clinical disorder. *Cyberpsychology & behavior, 1*(3), 237-244.

Young, K., Pistner, M., O'MARA, J. A. M. E. S., & Buchanan, J. (1999). Cyber disorders: The mental health concern for the new millennium. *CyberPsychology & Behavior*, *2*(5), 475-479.

Yu, J., Evans, P. C., & Clark, L. P. (2006). Alcohol addiction and perceived sanction risks: Deterring drinking drivers. Journal of Criminal Justice, 34(2), 165-174.

Zafarani, R., Abbasi, M. A., & Liu, H. (2014). *Social media mining: an introduction*. Cambridge University Press.

Zanette, D. H. (2002). Dynamics of rumor propagation on small-world networks. *Physical review E, 65*(4), 041908.

Zangerle, E., & Specht, G. (2014, March). Sorry, I was hacked: a classification of compromised twitter accounts. In *Proceedings of the 29th Annual ACM Symposium on Applied Computing* (pp. 587-593). ACM.

Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: challenges and opportunities. *IEEE network, 24*(4).

Zhao, L., Wang, J., Chen, Y., Wang, Q., Cheng, J., & Cui, H. (2012). SIHR rumor spreading model in social networks. *Physica A: Statistical Mechanics and its Applications, 391*(7), 2444-2453.

Zhao, L., Wang, Q., Cheng, J., Chen, Y., Wang, J., & Huang, W. (2011). Rumor spreading model with consideration of forgetting mechanism: A case of online blogging LiveJournal. *Physica A: Statistical Mechanics and its Applications, 390*(13), 2619-2625.

Zheng, X., & Lee, M. K. (2016). Excessive use of mobile social networking sites: Negative consequences on individuals. *Computers in Human Behavior, 65*, 65-76.

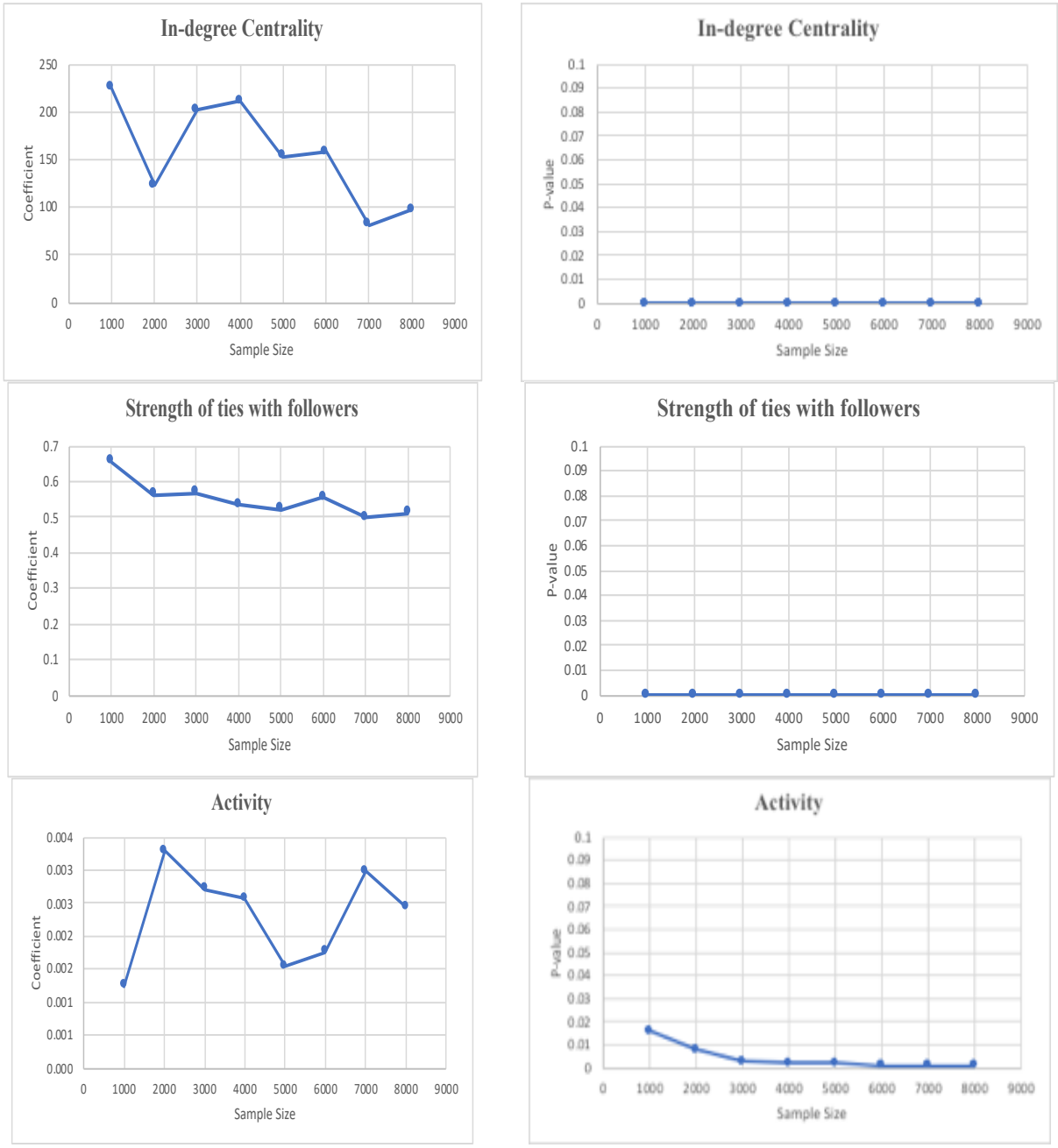
Zou, C. C., Gong, W., & Towsley, D. (2002, November). Code red worm propagation modeling and analysis. In *Proceedings of the 9th ACM conference on Computer and communications security* (pp. 138-147). ACM.

Zou, C. C., Towsley, D., & Gong, W. (2004, October). Email worm modeling and defense. In *Proceedings. 13th International Conference on Computer Communications and Networks (IEEE Cat. No. 04EX969)* (pp. 409-414). IEEE.

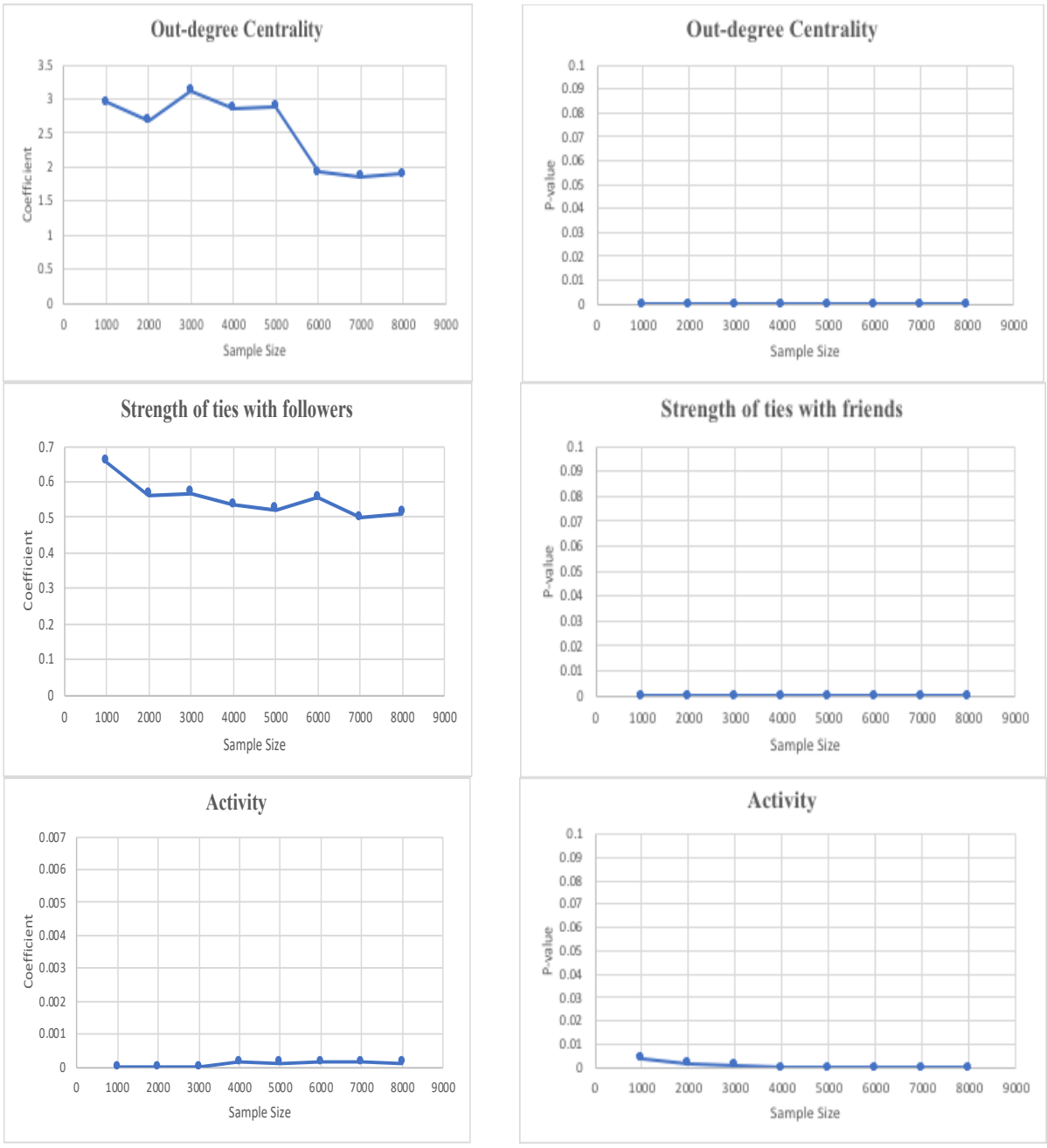
APPENDICES

Appendix A: Robustness Check with Smaller Samples Sizes for Essay1

The coefficients and p-values of the factors in the model for 8 different sample sizes are reported below.

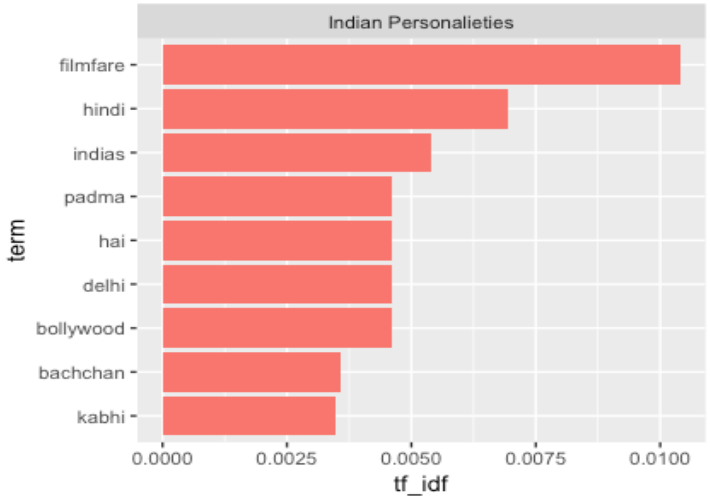


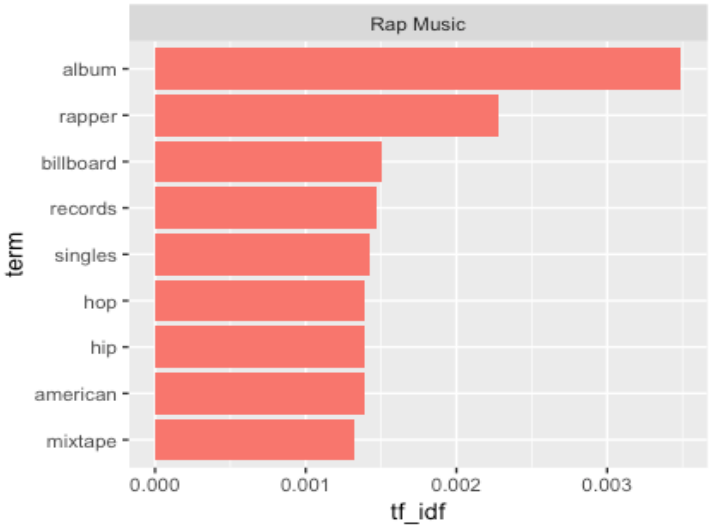
Robustness Check for Propagation Efficacy with Smaller Sample Sizes

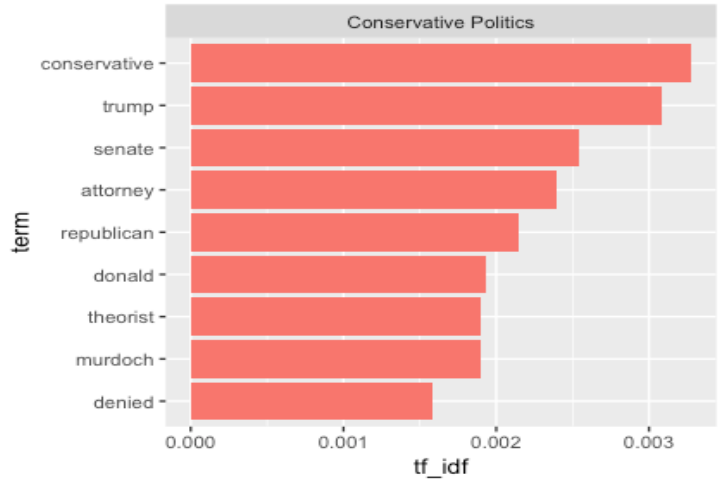


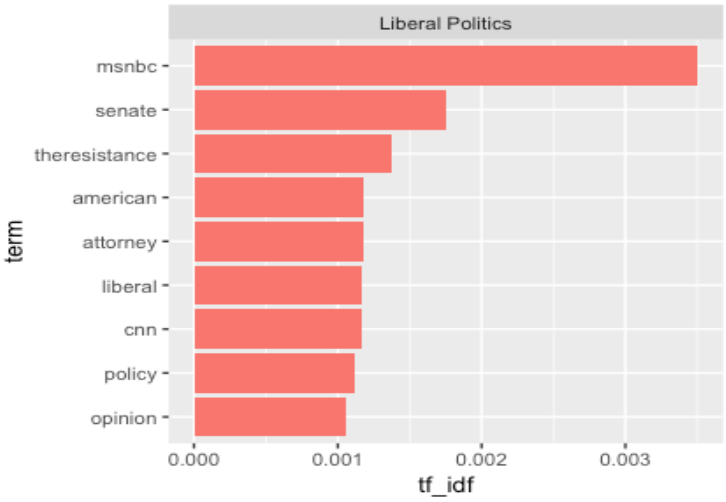
Robustness Check for Threat Vulnerability with Smaller Sample Sizes

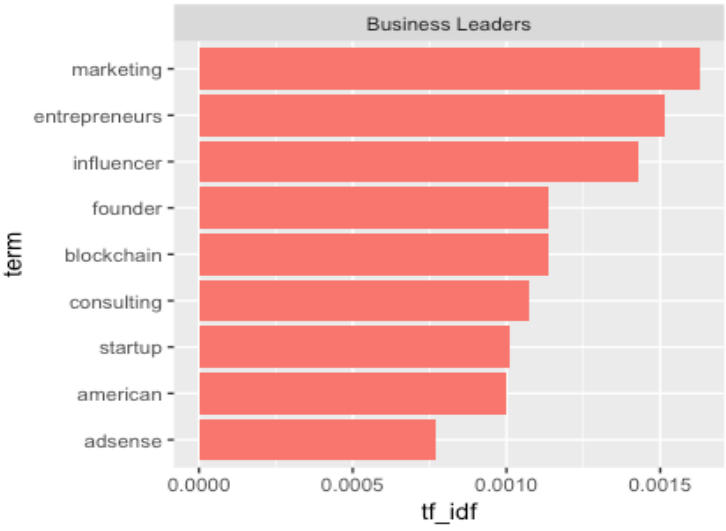
Appendix B: High Frequency Key words for each Community of Interest

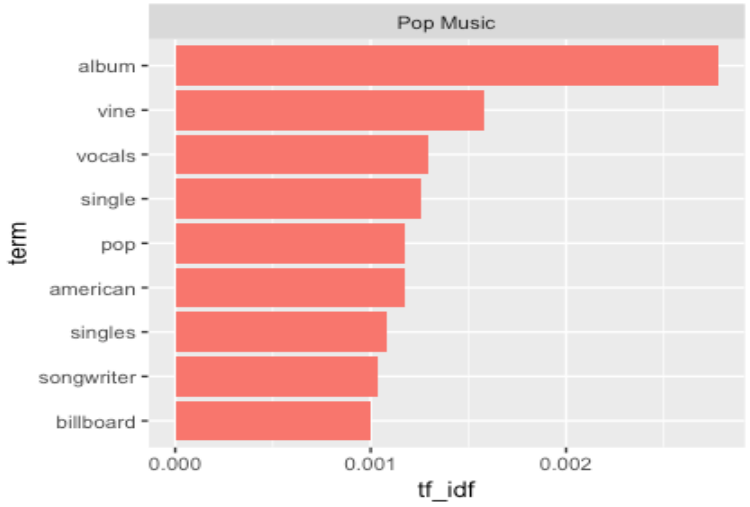


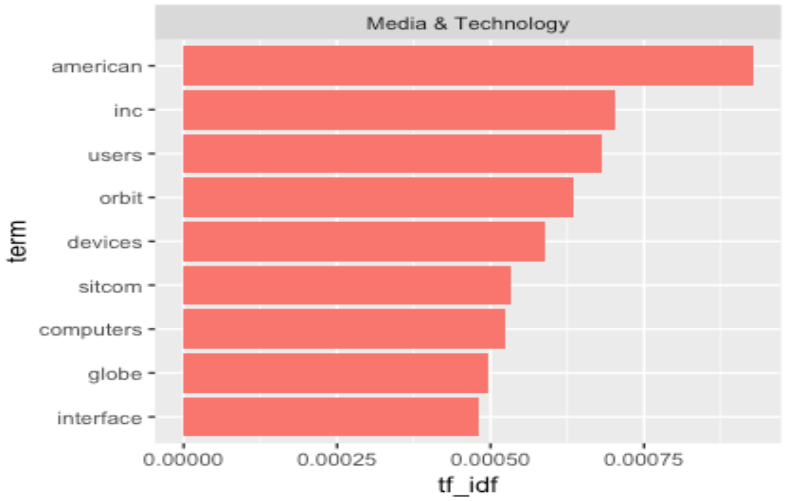


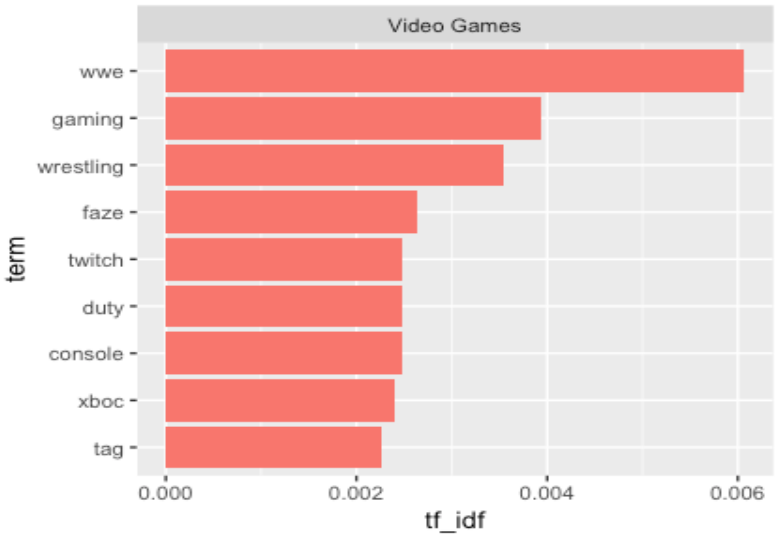

Conservative Politics
conservative
trump
senate
attorney
republican
donald
theorist
murdoch
denied
term
0.000
0.001
0.002
0.003
tf_idf


Liberal Politics
msnbc
senate
theresistance
american
attorney
liberal
cnn
policy
opinion
term
0.000
0.001
0.002
0.003
tf_idf


Business Leaders
marketing
entrepreneurs
influencer
founder
blockchain
consulting
startup
american
adsense
term
0.0000
0.0005
0.0010
0.0015
tf_idf


Pop Music
album
vine
vocals
single
pop
american
singles
songwriter
billboard
term
0.000
0.001
0.002
tf_idf


Media & Technology
american
inc
users
orbit
devices
sitcom
computers
globe
interface
term
0.00000
0.00025
0.00050
0.00075
tf_idf

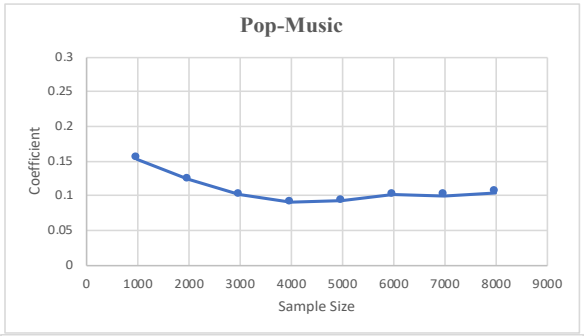

Video Games
wwe
gaming
wrestling
faze
twitch
duty
console
xboc
tag
term
0.000
0.002
0.004
0.006
tf_idf

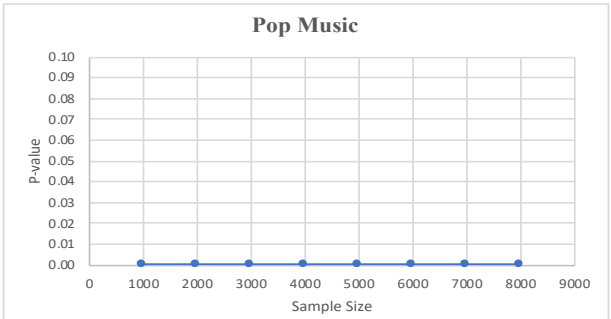
Appendix C: Variable Correlations

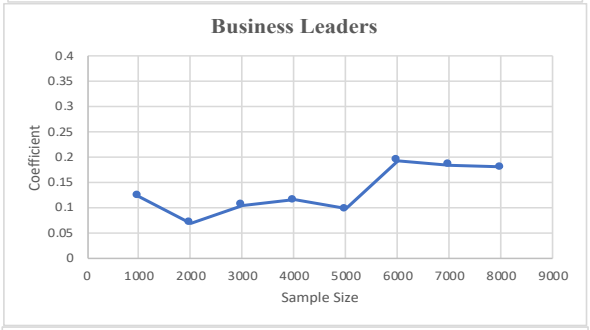
	1	2	3	4	5	6	7	8	9	10	11	12
1.Indian Personalities	1											
2.Rap Music	-0.03**	1										
3.Conservative Politics	0.06***	0.05***	1									
4. Business Leaders	0.02	0.11***	0.22***	1								
5.Liberal Politics	0.07***	0.10***	0.27***	0.22***	1							
6.Pop Musis	-0.01	0.24***	0.01	0.08***	0.02*	1						
7.Media & Technology	0.12***	0.37***	0.25***	0.24***	0.48***	0.43***	1					
8.Video Games	0.01	0.20***	0.02	0.05***	0	0.20***	0.27***	1				
9.Ave. Similarity	0.01	0.04***	0.01	0.05***	0.04***	0.07***	0.05***	0.03**	1			
10. Strength of Ties	-0.06***	-0.05***	0.05***	0.20***	0.04***	-0.12***	-0.09***	-0.10***	0.38***	1		
11.Out-degree Centrality	0.02*	0.05***	0.12***	0.38***	0.10***	0.05***	0.12***	0.02	0.04***	0.09***	1	
12.Activity	0	0.01	0.07***	0.07***	0.05***	-0.05***	-0.04***	-0.06***	0	0.15***	0.06***	1
13. Threat Vulnerability	0.02	0.04***	0.16***	0.35***	0.28***	0.04***	0.09***	0.03**	0.27***	0.25***	0.44***	0.13*

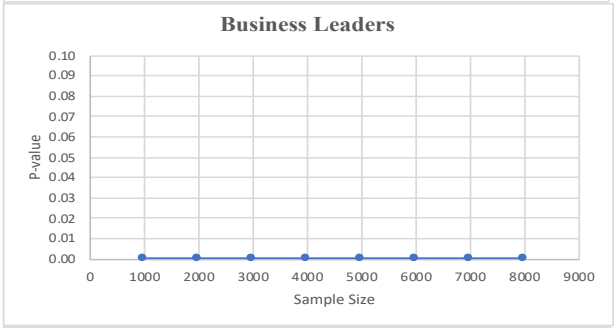
Appendix D: Robustness Check with Smaller Samples Sizes for Essay2

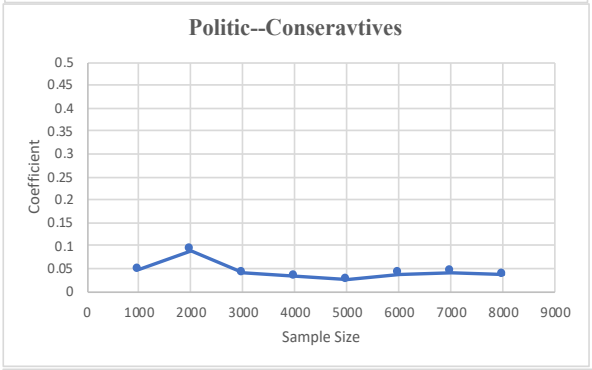
The coefficients and p-values of the factors in the model for 8 different sample sizes are reported below.

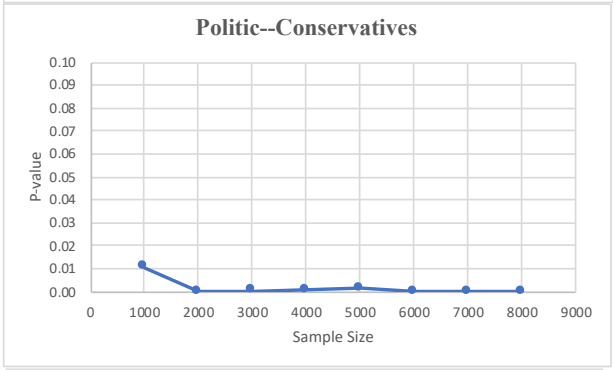


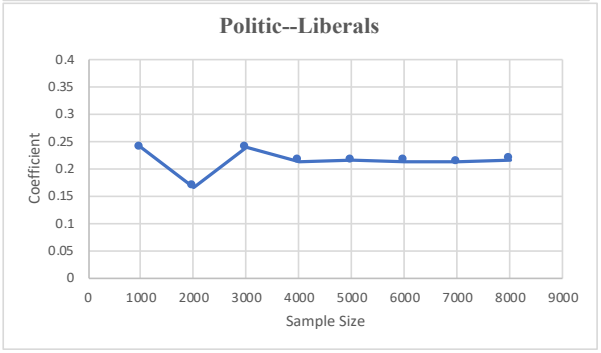


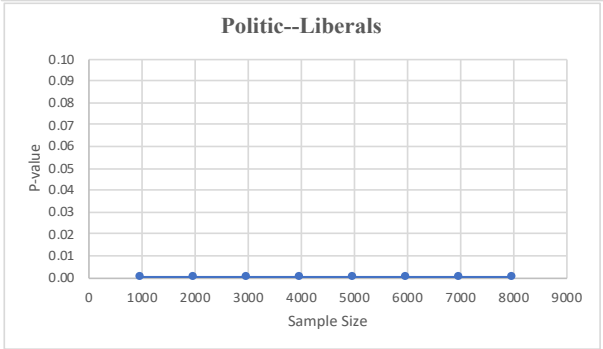


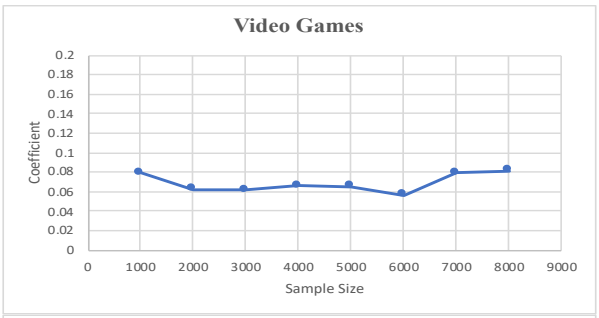


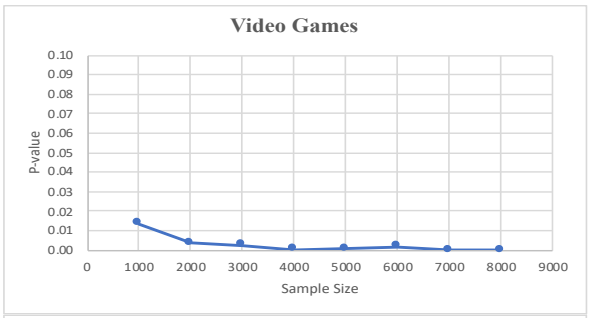


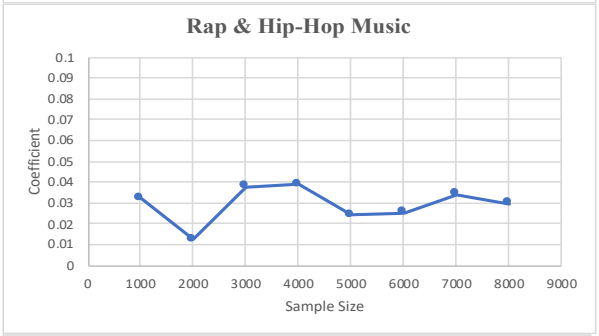


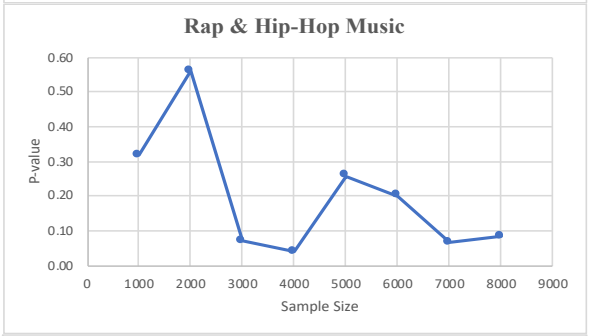


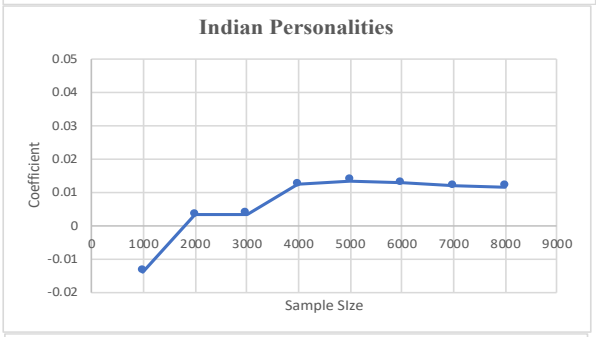


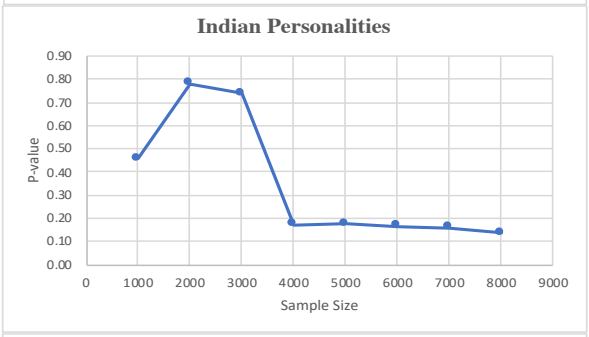

Video Games
Coefficient
Sample Size

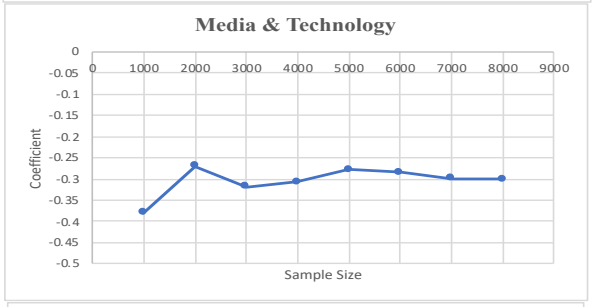

Video Games
P-value
Sample Size

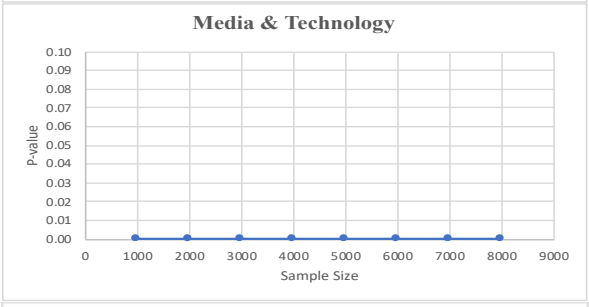

Rap & Hip-Hop Music
Coefficient
Sample Size

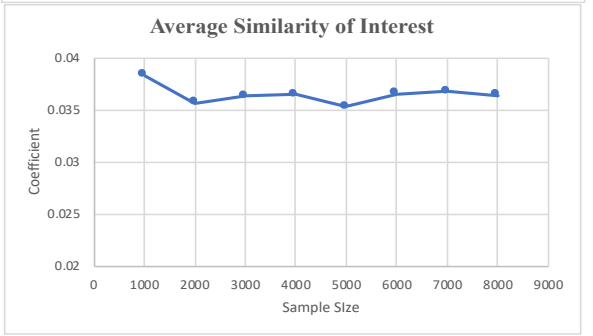

Rap & Hip-Hop Music
P-value
Sample Size

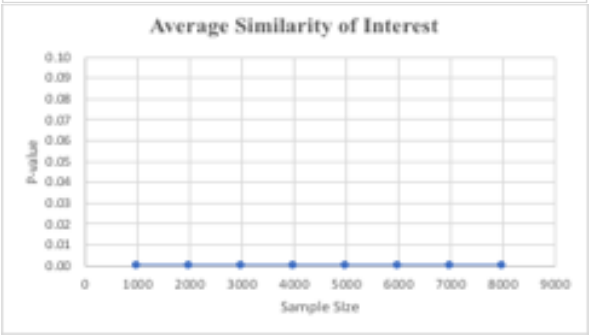

Indian Personalities
Coefficient
Sample SIze

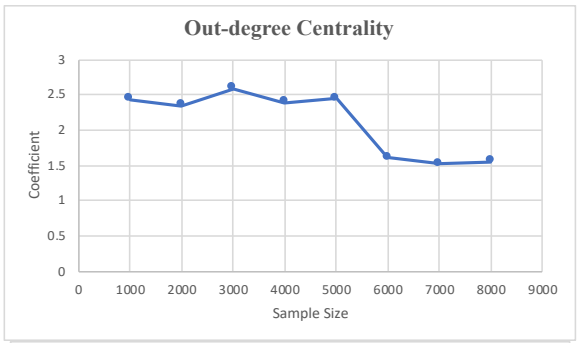

Indian Personalities
P-value
Sample Size

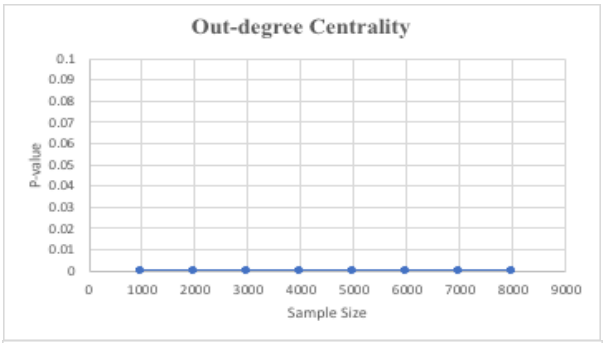

Media & Technology
Coefficient
Sample Size

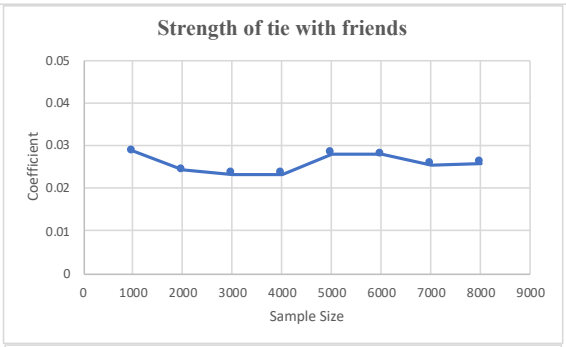

Media & Technology
P-value
Sample Size

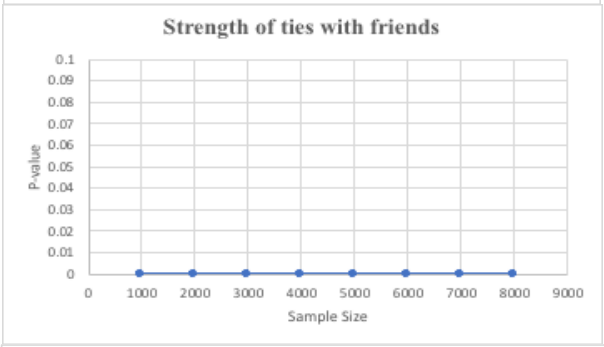

Average Similarity of Interest
Coefficient
Sample SIze

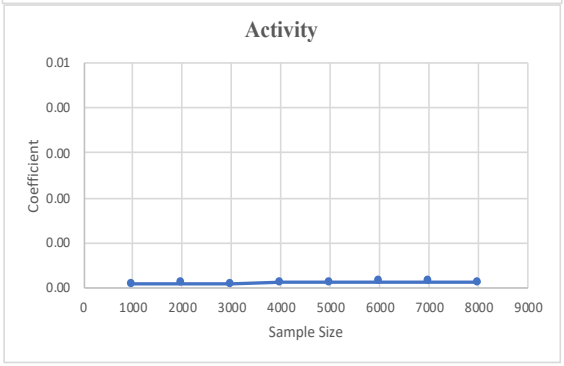

Average Similarity of Interest
P-value
Sample Size

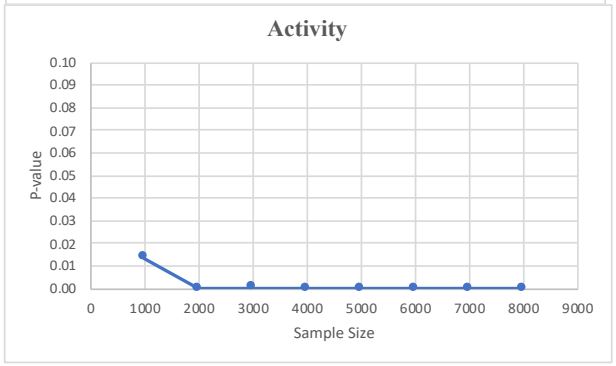












Robustness Check for Threat Vulnerability with Smaller Sample Sizes

Appendix E: Constructs, Definitions, and Key References

Constructs	Definitions	Key References
Cognitive-emotional preoccupation with using an OSN	Obsession thoughts to persist a behavior despite of their negative consequences	Fillmore 2001, Hoffman et al. 2009
Behavioral control	Individual users' abilities to inhibit or change impulsive behavior to reduce problematic behaviors	Tangney et al. 2004, Hofmann and Kotabe 2012
Perceived susceptibility	Individual users' perception about the degree of vulnerability to online security attacks	Rogers 1975, Liang and Xue 2009, Chen and Zahedi 2016
Perceived severity	Individual users' perception about the significance or seriousness of harm caused by online security attacks	Liang and Xue 2009, Chen and Zahedi 2016
Perceived threat	Individual users' degree of fear about online security attacks.	Liang and Xue 2009, Chen and Zahedi 2016
Perceived self-efficacy	Individual users' perception about their ability to take protective measures to deal with online security attacks	Liang and Xue 2009, Chen and Zahedi 2016
Perceived response efficacy	Individual users' perception about the effectiveness of protect against online security attacks	Liang and Xue 2009,2010, Chen and Zahedi 2016
Protective actions	Individual users' protective countermeasures to reduce risk of online security attacks	Tobin 1989, Chen and Zahedi 2016
Seeking help	Individual users' interaction with others in seeking assistance in dealing with online security threats	Liang and Xue 2009,2010, Chen and Zahedi 2016

Appendix F: Survey Instrument

Construct	Item Name	Item
Emotion		My craving to use social networks when I feel:
	emo1	anxious is (none/very high)
	emo2	lonely is (none/very high)
	emo3	nervous is (none/very high)
Cognitive		Considering the extent of my preoccupation with social networks:
	cog1	The amount of time I think about the social networks is (none/very high)
	cog2	The extent to which my thoughts about social networks interfere with my daily activities is (none/very high)
Concern		Considering my concerns about my use of social networks:
	con1	The extent to which negative news about social networks increases my concerns about limiting my use is (none/very high)
	con2	The extent to which seeing other people using social networks reminds me of the need to control my use of them (none/very high)
Restrict		Considering restricting my use of social networks:
	res1	The extent of my attempts to reduce my hours of using social networks is (none/very high)
	res2	My guilt feeling about too much use of social networks is (none/very high)
	res3	My avoidance of social networks to address my concerns about using them is (none/very high)
OSN addiction		Considering the level of my addiction to social networks,
	ad1	The extent to which social networks make me neglect important things (none/very high)
	ad2	The extent to which my checking social networks interferes with my social, school, work and other activities (none/very high)
	ad3	The extent to which I get inadequate rest because of using social networks is (none/very high)
	ad4	The level of my agitation/anxiety/distress when I cannot use social networks is (none/very high)
	ad5	My lack of control over the number of times I check social networks is (none/very high)
Susceptibility		When it comes to the possibility of getting security attacks, I believe that:
	sus1	My risks of getting security attacks are (none/very high)
	sus2	The likelihood that I would be a target of security attacks is
	sus3	The extent of my vulnerability to security attacks is (none/very high)
Severity		When it comes to severity of security attacks, if I encounter social networks security attacks:
	sev1	The consequences of security attacks for me is (none/very high)
	sev2	The seriousness of security attacks for me is (none/very high)
	sev3	The significance of security attacks for me is (none/very high)
Self-efficacy		When it comes to my ability to take protective actions against security attacks, I believe that:
	self1	My knowledge for taking preventive actions is (none/very high)
	self2	My ability to seek advice from others about how to take protective actions is (none/very high)
	self3	My level of access to people who can help me is (none/very high)
Response efficacy		When it comes to the effectiveness of protective actions against security attacks, I believe that:
	ref1	The chance of stopping security attacks by taking protective actions is (none/very high)
	ref2	The likelihood to avoid security attacks by taking protective actions is (none/very high)

	ref3	My confidence in effectiveness of protective actions is (none/very high)
Perceived threat		When it comes to my feelings and concerns about security attacks:
	sc1	My fear of exposure to security attacks is (none/very high)
	sc2	My worry about security attacks is (none/very high)
	sc3	My anxiety about potential loss due to security attacks is (none/very high)
Protective action		My actions to protect me against security attacks can be characterized as:
	act1	no actions at all/frequent taken actions
	act2	no plan at all/well-planned
	act3	no precautions at all/many precautions
Seeking help		When it comes to increasing my knowledge about security attacks, I believe that:
	sh1	The extent of my asking for help has been (none/very high)
	sh2	The extent of my seeking professional advice has been (none/very high)
	sh3	The extent of my seeking support from others has been (none/very high)
Loss Experienced		The extent of your losses you have experienced due to the above security attacks has been:
	lsa1	Financial (Monetary Loss) (none/very high)
	lsa2	Time and effort spent to solve the problems (none/very high)
	lsa3	Psychological (tension, stress, anxiety) (none/very high)

Appendix G: Standardized Factor Loading in the Measurement Model

Constructs	Items	Loading	t-Value
Emotion	emo1	0.87	45.93
	emo2	0.70	31.14
	emo3	0.82	49.40
Cognitive	cog1	0.79	44.67
	cog2	0.87	57.99
Concern	con1	0.74	28.31
	con2	0.81	33.08
Restrict	res1	0.78	34.18
	res2	0.80	41.28
	res3	0.77	36.81
OSN addiction	adc1	0.82	45.68
	adc2	0.85	65.42
	adc3	0.80	42.99
	adc4	0.77	43.14
	adc5	0.81	47.40
Susceptibility	sus1	0.90	50.51
	sus2	0.77	31.26
	sus3	0.70	28.82
Severity	sev1	0.79	40.41
	sev2	0.88	58.20
	sev3	0.92	76.70
Self-efficacy	self1	0.84	29.79
	self2	0.82	39.17
	self3	0.67	23.27
Response efficacy	ref1	0.88	49.23
	ref2	0.90	56.85
	ref3	0.89	60.83
Perceived threat	sc1	0.87	61.91
	sc2	0.93	75.27
	sc3	0.85	58.77
Protective actions	act1	0.83	38.75
	act2	0.87	51.13
	act3	0.83	35.62
Seeking help	sh1	0.89	55.93
	sh2	0.76	33.94
	sh3	0.91	64.65
Loss experienced	lsa1	0.64	26.34
	lsa2	0.91	52.26
	lsa3	0.82	37.75

CURRICULUM VITAE

NESHAT BEHESHTI

EDUCATION

2014-2019 **Ph.D. Candidate: Information Systems Management**
University of Wisconsin – Milwaukee (Lubar School of Business)

- Recipient of Fitzsimonds Doctoral Scholarship (2018-2019)
- Recipient of Sheldon B. Lubar Doctoral Scholarship (2017-2018)
- Recipient of Sheldon B. Lubar Doctoral Scholarship (2016-2017)
- Recipient of Sheldon B. Lubar Doctoral Scholarship (2015-2016)
- Recipient of Info-Metrics Graduate Student Fellowship Award-American University (2015)

2008-2010 **Master of Science: Industrial Engineering**
K.N.Toosi University of Technology – Tehran

2004-2008 **Bachelor of Science: Pure Mathematics**
Amirkabir University of Technology (Tehran Polytechnic) – Tehran

- Recipient of Distinguished Graduate Student Mention Award

WORK HISTORY

09/2008 to 05/2010 **Graduate Assistant**
K.N.Toosi University of Technology – Tehran

- Teaching Assistant for Statistical Quality Control
- Teaching Assistant for Statistics
- Teaching Programming Software of MATLAB

09/2014 to Current **Graduate Assistant**
University of Wisconsin-Milwaukee

- Research Assistant
- Teaching Assistant for Introduction to Information Technology
- Course Instructor for Global Information Technology Management

PUBLICATIONS

Refereed Journals

Beheshti, N., Racine, J. S., & Soofi, E. S. (2019). "Information measures of kernel estimation". *Econometric Reviews*, *38*(1), 47-68.

Vaghefi MS, Sharifvaghefi M, **Beheshti N** (2014). "A Pricing Model for Group-Buying Auction Based on Customers' Waiting-time". *Marketing Letters* 25(4) 425-434.

Conference Papers

Beheshti N., Racine J., Soofi E. "Bayesian Updating of Dirichlet Process Prior Via Kernel Estimate". *(2015) Annual Meeting-INFORMS.*

Beheshti N., Shahriari H., (2010) "Determination of A Linear Regression Model Using Combined Simulated Annealing and stepwise Regression Methods". *The 2nd International Conference on Operation Research (ICOR) 2010.*

Beheshti N., Shahriari H., (2010) "Determination Linear Regression Model Using Simulated Annealing". *The 7th International Industrial Engineering Conference-Isfahan-Iran.*