7-18-2019

Antecedents and Outcome of Deficient Self-Regulation in Unknown Wireless Networks Use Context: An Exploratory Study

Emmanuel Wusuhon Yanibo Ayaburi
The University of Texas Rio Grande Valley

James Wairimu
The University of Texas Rio Grande Valley

Francis K. Andoh-Baidoo
The University of Texas Rio Grande Valley

Recommended Citation

Ayaburi, E.W., Wairimu, J. & Andoh-Baidoo, F.K. Antecedents and Outcome of Deficient Self-Regulation in Unknown Wireless Networks Use Context: An Exploratory Study. Inf Syst Front 21, 1213–1229 (2019). https://doi.org/10.1007/s10796-019-09942-w

Antecedents and Outcome of Deficient Self-regulation in Unknown Wireless Networks Use Context: An Exploratory Study

Emmanuel W. Ayaburi, James Wairimu and Francis Kofi Andoh-Baidoo*

Department of Information Systems, The University of Texas Rio Grande Valley, Edinburg, TX, USA

*Correspondence:
Francis Kofi Andoh-Baidoo, Ph.D.
The University of Texas Rio Grande Valley
Department of Information Systems
e-mail: francis.andohbaidoo@utrgv.edu

Abstract Wireless networks are becoming the norm in the society, where hotspots afford users access to the internet through mobile devices. Unknown wireless networks, open public networks with unknown identity, pose threats as hackers can gain unauthorized access to users' private information stored in their mobile devices. Despite the imminent dangers, individuals continue to use these networks. This study explicates a self-regulation theory to investigate the antecedents of deficient self-regulation (DSR) and its effects on habitual use of technology. We posit that both habit cues and information security experiential factors influence DSR, leading to habitual use of unknown wireless networks. The results show that perceived attachment, perceptions on privacy risk, and information security self-efficacy significantly influence DSR, which subsequently influences habitual use unknown wireless networks. This study contributes to the literature on self-regulatory theory, privacy, and provides implications for managers in dealing with vulnerabilities posed by employees using private or corporate mobile devices on unknown wireless network.

Keywords: Habits, Cues, Security, Privacy, Unknown Wireless Networks, Deficient self-regulation

Antecedents and Outcome of Deficient Self-regulation in Unknown Wireless Networks Use Context: An Exploratory Study

1 Introduction

Unknown wi-fi networks are open public networks whose identity are unsure/unfamiliar (Cisco 2018; Gast 2002). Anecdotal evidence suggests that individuals frequently use unknown wireless networks to connect to the internet through their portable computing devices. For example, individuals in an automatic fashion with little cognitive involvement allow their smartphone to connect to any available wireless network. Alternatively, there are individuals who regularly make effort to consciously check their Facebook account for newsfeeds. Such desires could lead to addictive behaviors (van Deursen et al. 2015). The use of open public wireless networks creates security issues for most organizations that promote the use of bring-your-own-device (BYOD). Nevertheless, little theory-driven investigation has been carried out in this regard. The growth in wireless fidelity (Wi-Fi) hotspots is bound to be positively influenced by the increased ubiquitous computing in the form of portable computing devices, and the increased internet penetration on the global scale (MarketWatch 2018). On the one hand, wireless networks typically located in high traffic areas including coffee shops and transport terminals, offer several advantages over wired networks including; flexibility, mobility, and lower connectivity costs (Cisco 2018; Gast 2002). However, wireless network users are faced with privacy and security risks as these networks are assumed to be less secure relative to wired networks (Sombatruang et al. 2016). In the process of using these networks, users are exposed to vulnerabilities including; loss of personal information such as credit card details, emails, and security credentials relayed by individuals over these networks (Kaspersky Lab 2018).

Some prior studies aimed at understanding the factors that influence wireless network use have employed cost-benefit analysis and have found that, individuals' behavior over public networks usage is salient in their exposure to information security risk (Choi and Carpenter 2013; Sombatruang et al. 2016). Identity theft and other catastrophic consequences that result from compromise of personal devices do not deter individuals from using wireless networks that have no trusted security. Wi-fi authentication, a process of ensuring that the right people are authorized for access, provides a means to ascertain the truth about a network's identity and provide a sense of comfort about who operates or is on the network. However, some rogue networks have setup to obtain personal information during authentication of unsuspecting users (EFF 2018; Kindberg et al. 2009).

The regular use of wireless network connectivity have led to several negative outcomes such as addictive smartphone usage, unregulated internet and Facebook use (LaRose et al. 2003; Gökçearslan et al. 2016; Lee et al. 2016). Most of these studies have investigated unregulated technology use by employing Self-regulatory theory (SRT) as the basis and investigated deficient self-regulation (DSR) as a predictor of negative outcomes. SRT suggests that human behavior is based on cognitions formed before undertaking an action (Bandura 1991). Few studies have conclusively explicated factors that lead to DSR in the use of technology. DSR is an individuals' loss of behavior control, such that one is unable to judge their actions, and behavior patterns (Bandura 1991; LaRose et al. 2003). SRT is associated with formation of habits that are motivated by prior behavior (Lee and Perry 2004). Some prior studies have investigated habit formation in the use of technology (Vance et al. 2012; van Deursen et al. 2015). Habitual use of systems that may be the outcome of unregulated systems use, can be considered a composite concept comprising automatically (unconscious) and routine (conscious) systems use (Ersche et al. 2017). SRT may offer new insights into why individuals continue to use unknown wireless networks despite the dangers involved and the constant education/encouragement to use security measures such as VPN and SSL to avoid disclosure of personal information on these networks (Dolly 2018; Kaspersky 2018). Accordingly, we pose the following overarching research question:

What explains individuals' self-regulation and habitual use of technology in the context of unknown wireless networks?

To investigate our inquiry, we develop a conceptual model explicating the antecedents and consequences of DSR and test our model using survey data from 476 wireless network users. We contribute to both theory and practice. For theory, we have extended the SRT in the unknown wireless network use context by providing the antecedents and negative outcomes of the DSR model. Prior relevant studies have studied SRT antecedents and outcomes separately, but both are yet to be incorporated in a single study for a comprehensive explication of SRT. The nomological network of the DSR model developed in this study indicates that, although habitual use of technology consists of conceptually two distinct dimensions – automatic and routine use, the two dimensions may be operationally identical. Additionally, the results show that different cues and experiential factors that are predictors of habitual systems use vary on their influence on the development of individuals' DSR. For practice, the result with respect to habitual use have implications for managers who are tasked with protecting and promoting safe use of network by designing mechanism that are targeted to users. The rest of the paper is as follows; next we discuss the theoretical foundations and background literature. Next, we develop our conceptual model based on SRT and discuss the collection and analysis

of data. The finial sections present the results, discusses the implications of the results, and the contributions of the results to research and practice.

2 Background Literature

Wireless Network Use

Wireless networks provide easy and flexibility access of services such as; online banking, social networking, emails, and instant messaging (Gast 2002; Klasnja et al. 2009). Wireless networks are however faced with security challenges that users seem to ignore or are rather not aware of as prior studies have reported increased use of unknown wireless network. (Aime et al. 2007). Wireless networks have been facing a constant threat from hackers despite the encryption standards developed and enforced over the years (Olufon et al. 2014). Over nine million people succumb to identity theft from credit card information, and other bank transactions conducted over wireless networks (CBS 2010). Extensive research has been carried out on the vulnerabilities of wireless network connections (Aime et al. 2007; Noor and Hassan 2013; Cho et al. 2012; Balachandran et al. 2005) and the losses that users suffer from these connections (CBS 2010; Schlesinger 2016; Finjan Mobile 2018). To understand individual's continued usage of the wireless networks, a utility-based approach has often been used with mixed results. For example, in a 150 hour long experiment on public wireless network connection and follow up interviews, Sambamurthy et al. (2003), reported that individuals who connected to the experiment's Wi-Fi network were not motivated by utility value as predicted. Most people were aware of risk exposure, but still decided to connect to the network using personal information. In a related study, Klasnja et al. (2009) report that most users are neither aware nor concerned about the privacy risks they are exposed to when connecting to wireless networks. Such individuals assume that the connections were secure. Such users are thus, susceptible to suffering breaches as some hackers create fake hotspots to gain access to private devices. Although these studies show reasons why users are likely to connect to wireless networks, not much is known about the rationale behind the decision-making process in the context of unknown wireless network use. The goal of this study is to identify behavioral factors that lead users to connecting to unknown wireless network.

We explore behavioral factors that influence continued use of unknown networks despite the risks posed. Although not widely explored in the information systems literature, few studies have attempted to investigate self-regulatory theory in terms of its deficiency and the effects it has on human behavior in information technology (IT) usage. Deficiency in self-regulatory is described as the loss of self-control, such that one is unable to judge their actions, and behavior patterns (Bandura 1991; LaRose et al. 2003). Such states result in individuals lacking a self-evaluation mechanism that leads to habits and behavior automaticity. We employ SRT perspective to understand

predictors and consequence of unregulated portable computing device use in the context of unknown wireless networks.

Self-regulatory Theory

Self-regulatory theory (SRT) is drawn from social cognitive theory to explain human behavior based on cognitions formed prior to undertaking an action (Bandura 1991). SRT has been used to investigate many individual behavioral actions including gambling (Haagsma et al. 2013), microblogging (Wang et al. 2015), internet use (Caplan 2010) and smartphone use (Gökçearslan et al. 2016). SRT influences the development of standards of behavior among individuals which lead to the formation of habits (Lee and Perry 2004). Individual self-monitoring, behavior judgement, and behavioral reactions are key components of SRT (Bandura (1991). While individual self-monitoring occurs when individuals observe situations and thoughts that may affect their habitual behavior, behavior judgement motivates individuals to repeat or control behaviors. The nature of self-monitoring and behavior judgement influences an individual's behavioral reactions.

Self-regulation influences individuals' cognitive bias (Barber et al. 2009) or the ability to multitask (Uzun and Kilis 2019). SRT has been used as the framework to investigate various negative behavioral outcomes. Prior literature employing SRT to understand individuals' impulsive behavior suggest that individuals with low self-regulation easily develop habits such as addictive texting or excessive mobile communication (Bayer, Dal Cin, et al. 2016). Studies on SRT in IT context focus on understanding individuals' deficiency in self-regulation (DSR) that lead to negative outcomes including; compulsive internet use (Caplan 2010; LaRose et al. 2003), gaming (Haagsma et al. 2013), mobile phone addiction (Gökçearslan et al. 2016; Soror et al. 2015; Soror et al. 2012; van Deursen et al. 2015), and addictive use of social networking sites (SNS) (Lee et al. 2016). Antecedents of DSR include boredom (Eastin et al. 2007; Soror et al. 2012), anxiety (Soror et al. 2012), self-efficacy (LaRose et al. 2003), and need for social interaction (Caplan 2010). Boredom is a mental state that makes an individual avoid self-reflections on actions being undertaken (Soror et al. 2012). Boredom limits an individual's willpower to avoid actions that lead to negative behavior. Increase in boredom has been thought to be a result of ubiquitous computing as individuals remain often connected to the internet. On the other hand, social interaction anxiety could lead to individual isolation (Lee et al. 2016). Withdrawals would lead to engaging in in-person activities that bring individuals relief. The need for social connectedness drive individuals to seek emotional satisfaction from their social relationship (van Deursen et al. 2015). Individuals may stay connected online to maintain their social ties as a way to strengthen their social connection. The

preceding factors that influence DSR provide the explanatory basis for SRT to understand the habitual use of technology with special focus on wireless networks. Habits are driven by either conscious or unconscious motivation for the individual (Ersche et al. 2017). Prior to developing our research model, we discuss in detail the dimensions of habits.

Habit

Habits such as uncontrolled use of mobile phones (van Deursen et al. 2015) and SNS (Polites et al. 2018) are some negative outcomes of DSR. Habits are routines or automatic behaviors that are formed in reaction to stimuli (Anderson et al. 2016; Sokolov 1963). Routine behaviors are familiar actions that are done regularly while automatic behaviors are actions that are not deliberate but conscious effort is made to control (Ersche et al. 2017). Once the cues that trigger a habitual behavior no longer exist, conscious effort may be made to discontinue routine behavior. For example, an individual who is used to keeping their Facebook status active may have a high likelihood of not only keeping their wireless connectivity automatic to any available wireless network, but also routinely put their phone on charge when they wake up in the morning. On the other hand, an individual who likes to watch movies at the airport while waiting to board their next flight, would actively seek to connect to the strongest Wi-Fi to stream the movie. Habits development is a complex process during which the brain compares stored mental model against an incoming stimulus resulting in either sensitization or habituation (Grooves 1970). When the stimuli result in an action leading to a gratifying reward, the brain will respond by habituating. Habit has been identified as a stumbling block to learning or behavioral change such that excessive stimulus response leads to compulsive disorders (Anderson et al. 2016; Gillan et al. 2016). Excessive habituation, thus, leads to disregard of cues that might be important. The habit loop, as shown in Figure 1 posits that the habituation process is initiated by cues that lead to routines, and rewards prompting individuals to repeat the process (Richardson 2018). The feedback enforcement results when an individual is satisfied by a routine triggered by an environmental cue (Richardson 2018). Thus, it can be inferred from the habit loop that individuals are likely to engage in repetitive behaviors to achieve satisfaction, resulting in habituation.

Habits as automatic actions require neither planning nor prior organization as they occur in response to strong stimulus responses without the need for effort or control, while habits as routine actions are frequent behaviors motivated by intrinsic (material) and extrinsic (mental) cues (Ersche et al. 2017). As portrayed in the habit loop, feedback enforcement results in repetition of past behavior that satisfies these cues. Habits may turn to be maladaptive behaviors when individual traits are triggered cues (Wood and Neal 2007). We posit that habitual use of unknown wireless networks may stimulated traits such as social interaction anxiety (hereafter referred to as anxiety), social connectedness (hereafter referred to as connectedness), and attachment. In addition to the cues, communication and experience of dangers drive habitual behaviors

including texting while driving (Bayer and Campbell 2012). Individual habits positively increase security vulnerabilities and self-efficacy in intentions to comply with IS security policies (Vance et al. 2012). We argue (see model development) that these experiential factors such as privacy risk and self-efficacy in security would influence the repetitive use of unknown networks. We incorporate these experiential factors in the modified habit loop as shown in Figure 1.

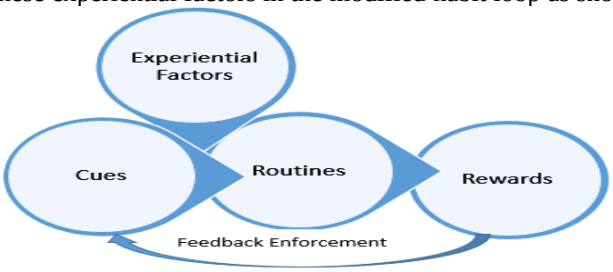

Figure 1. Modified Habit Loop with Experiential Factors

3 Research Model and Hypotheses Development

Based on the preceding theoretical discussions, we develop our research model as shown in Figure 1. In a deficient self-regulatory framework, we contend that individual internal traits, habit cues, influence DSR, leading to habitual use of unknown wireless networks. Prior security studies posit that individuals are weary of their information security but still engage in risky behaviors (Xu et al. 2013). Example of such risky behavior include using unknown wireless networks that have no confirmed security. As individuals continue to engage in behaviors that expose them to information security and privacy risks, a deficient self-regulatory mechanism serves as an appropriate framework for explaining these risky behaviors. It is arguable that individuals may exercise much self-control of their behaviors, but cues exist that limit their self-regulation. Once a habit is formed, rationality is blocked, and individuals result to automatic/routine behavior caused by repeated actions/cues (Gillan et al. 2016).

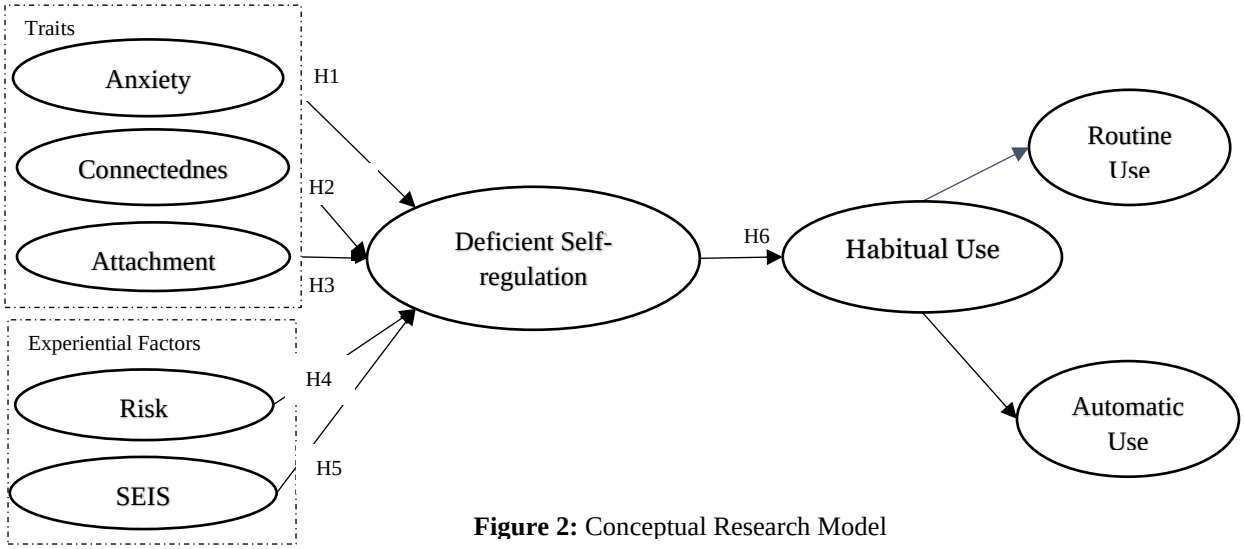

Figure 2: Conceptual Research Model

Traits and Hypothesis

We postulate that psychological antecedent factors of social interaction anxiety, social connectedness and attachment to digital presence or artifact act as stimuli/cues to trigger uncontrolled use of unknown wireless networks. Individuals with habits of connecting to unknown wireless networks may not realize their actions since they may be controlled by stimuli. Such stimuli have been explored in addiction studies where, individuals become attached to digital devices that lead to risky behaviors such as texting while driving (Turner and Turner 2013), or compulsive use of digital media (Khang et al. 2013).

Social Interaction Anxiety is a state that individuals experience when they are in doubt of their ability to impress other people (Schlenker and Leary 1982). Anxiety causes individuals to avoid social interactions due to fear of being scrutinized if they fail to impress others. Individuals with high social interaction anxiety may avoid direct face-to-face or social relations and have preference for online communication (King et al. 2013) due to less negative evaluations, and the ability to enhance self-presentation on online platforms such as Facebook (McCord et al. 2014). Participation in online communities poses strict requirement on network connection compelling individuals with high social interaction anxiety to connect to any available network disregarding security risks. Anxiety can cause individuals to be self-deficient in controlling unwanted behaviors such as unregulated use of technology. Soror et al. (2012) found that anxiety leads to DSR in unregulated mobile phone use. In the context of wireless network use, we expect that, anxiety can cause individuals to be deficient in their ability to self-regulate their decision or desire to use unknown wireless network irrespective of their awareness of the dangers to such technologies. Thus, we present our first hypothesis as;

H1: Social interaction anxiety will positively influence deficient self-regulation in the use of unknown wireless networks.

Social connectedness is a psychological sense of belonging and involvement with a social group that yields comfort to an individual (Hagerty et al. 1993; Lee et al. 2001). Individuals feel bored when they are not socially connected. Boredom leads to DSR in technology use in several contexts including workplace communication technology (Eastin et al. 2007) and mobile phone use (Soror et al. 2012). Poor physical social network has been linked to failure in controlling the compulsive use of the internet (Bayer, Campbell, et al. 2016; McIntyre et al. 2015), as internet use provides channels for individuals to stay connected to their social group (Lee et al. 2001). Social connectedness has been portrayed as a functional behavior that has its origins from past behavioral patterns (Hagerty et al. 1993).

Maintaining close contact with a social group has not only become a social norm, but a habit (Bayer, Campbell, et al. 2016). People with low social connectedness have the tendency to avoid boredom by constantly connecting online to their social network. It is expected that high desire among such individuals to connect to their social group lead to cognitive overload that deplete the needed resources to control the use of unknown wireless network. Therefore, we posit that;

H2: Social connectedness will positively influence deficient self-regulatory in the use of unknown wireless networks.

Perceived Attachment, in the context of information technology, refers to the affective bond a user shares with digital artifacts (Turner and Turner 2013). A bond may be formed out of continued interaction over time. For instance, strong desire for digital presence lead frequent smartphone users to habitually operate their phones while driving (Bayer, Campbell, et al. 2016). The urge for continual use of phones acts as a stimulant that triggers habitual behavior of engaging in risky behavior of texting while driving. Attachment to mobile phones drives individuals to connect to Wi-Fi as most of the applications on mobile devices are useful only when the device is connected to the internet (Fullwood et al. 2017). Failure to control the compulsive use of these functions has resulted in phone addiction (Khang et al. 2013; Salehan and Negahban 2013). Individuals with high perceived attachment would seek to stay connected to internet through wireless networks to enjoy functionalities such as connecting to Facebook, listening to music, and texting even when situations such as battery life threatens their continued connection without paying attention to the damages that unknown networks may pose (Fullwood et al. 2017). Taken together, we present the following hypothesis.

H3: Attachment to online presence positively influence deficient self-regulatory in the use of unknown wireless networks.

Experiential factors and Hypothesis

Individuals experiences, negative or positive, will influence the level of repeated actions. Prior exposure affects the desire to control behavior that may put individuals' information at risk. Two key experiential factors – perceived privacy risk and self-efficacy in Information security- are considered in this study. Our justification for the integration of the two experiential factors and DSR is that theoretical studies on self-regulation and motivation found self-efficacy and risk as antecedents to loss of control (Khang et al. 2013). For instance, Khang et al. (2013) found that self-esteem, a reflection of an individual's self-efficacy, to be highly correlated with addictive use of digital media.

In this study context, we expect that self-efficacy in information security will influence individuals uncontrolled use of wireless networks. Also, Vance et al. (2012) argued and found support for risk as key motivation or deterrence coping mechanism when they appraise a threat. In the context of using unknown wireless network where there is high likelihood compromising individuals' privacy, we argue that perception or experience of risk has an impact on uncontrolled use of devices. Thus, in addition to the above stimuli or psychological cues, we also explore experiential factors of privacy and self-efficacy in information security as antecedents to DSR of vulnerable behaviors, which in this study is the use of unknown wireless network. This is because most users express concerns about their privacy when using wireless network (Norton 2017). Individuals' experience has been demonstrated to affect their privacy behavior when using information technologies (Smith et al. 1996). Prior research employing cost-benefit perspective such as privacy calculus suggests that privacy risk negatively affects individual information disclosure on technological platforms (Smith et al. 2011). Habituation Theory posits that the rewards from the habitual actions influence cues and routines which could depend on the individual's ability and concerns; these relationships have been empirically studied in terms of the individual's use of online presence to engage with others (Xu et al. 2013).Next, we develop arguments for our conjecture that privacy risk and self-efficacy is related to DSR.

Privacy risk in the context of wireless network use, reflects the loss an individual anticipates from disclosure of their personal information over unknown wireless networks. There is a general consensus in the literature that individuals with high perception of risk for their privacy are more averse to personal information disclosure behaviors (Xu et al. 2013). The exposure of personal information put users at risk of threats such as identity theft and financial loss when credit card details are exposed. Thus, an individual's privacy risk perception will influence how they control vulnerable behavior such as the use of unknown network where they have less control in the privacy of their personal information. We expect that such risk concerns would cause individuals to self-regulate the vulnerable behavior of using unknown wireless networks. Therefore,

> H4: Information privacy risk perception will negatively influence deficient self-regulation in the use of unknown networks.

Self-efficacy in our study security refers to individual's belief in self-protection mechanisms against threats from unknown wireless networks. We draw this definition from the information security domain where self-efficacy is defined as, "belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability" (Rhee et al. 2009, p. 818). Individuals with such belief have

been found to have a high propensity of engaging in risky behavior such as personal information disclosure in social networks sites (Chen and Chen 2015). Such users are aware of privacy threats but see them as less harmful since they perceive to have adequate skills to counter them. A public Wi-Fi usage study reported that 92% of the respondents exuded confidence in the safety of their personal information over public networks and engaged in activities that led to disclosure of personal information (Norton 2017). We argue that such users ignore warnings on the dangers of using personal information due to their belief on their ability to protect their information. We posit that such users will not take time to self-regulate their behaviors related to the unwanted behavior of using unknown wireless networks. Thus,

H5: Perception of Self-Efficacy in Information System Security positively influence deficient self-regulation of the use of unknown wireless networks.

Second-order Habitual Use Construct and Hypothesis

The two dimensions of the habits described in the previous sections provide conceptual understanding of the two closely related facets of habitual use of technology. However, we conceptualize the habit as a second order construct with the two first-order factors as its reflective indicators because; (1) previous research has found them to be highly correlated (Ersche et al. 2017), (2) prior studies on habits have operationalized the construct as one (Anderson et al. 2016; Sokolov 1963) and (3) both dimensions are rooted on the same concept of cognitive involvement (Ersche et al. 2017). Formulation of habit as a second order construct eliminates any potential multicollinearity problems. We therefore argue that, both dimension of habit will be affected in the same manner by DSR.

SRT posits that some human behaviors are predicted by prior cognition formed by the individual (Bandura 1991). Prior research has identified DSR as a key determinant of compulsive behavioral intention or altitude (Soror et al. 2015; Soror et al. 2012). For example, some addictive behaviors such as texting while driving results from conscious text pattern developed by the individual (Gökçearslan et al. 2016). The repeated technology use from stored patterns in the individual's mind causes the individual to ignore potential harm from such actions. Uncontrolled internet use, gaming or mobile phone use, examples of negative outcomes, may be attributed to the individuals' DSR (LaRose et al. 2003; Haagsma et al. 2013; Soror et al. 2015). We expect that DSR will have more effect on individual's external locus of control than intrinsic cues. Loss of external locus of control has been found to influence compulsive use of communication technology (Lee et al. 2014). Having encountered a stimulus such as the notification of the presence of wireless network, some individuals connect to the wireless network consciously. Some individuals exhibit

such behaviors regularly and consistently. Failing to control the edge to frequently use unknown wireless network so as not to appear distant from the world may be the result of DSR. This is because individuals with little control or regulation of their technology use may develop psychological dependence which has been confirmed about micro bloggers (Wang et al. 2015). We consider DSR as an important influence on individuals' conscious/unconscious use of wireless network regularly. Based on the preceding we hypothesize that:

H6: Deficiency in self-regulation in the use of unknown networks positively influence habitual use of unknown networks.

4 Methodology

To empirically test the hypotheses and evaluate the proposed model, data was collected using a survey instrument. This methodology was selected to measure perception on the construct of interest of individuals who have used unknown open wireless network. The sub-sections that follow describe the sample and measures employed for the study.

Sample and Measurement Items

Participants for this study were drawn from a diverse sample in a survey conducted over Amazon Mechanical Turk (Buhrmester et al. 2011). Five hundred complete responses were collected out of which 24 answers were eliminated as respondents stated that they have never used unknown wireless networks before, resulting in a final sample of 476 consisting of 300 males (63%), and 176 females (37%) and average age range from 25 to 35 years. A large proportion of the respondents had a bachelor's degree (60.7%), and some with college (22.7%), whereas 15.3% had a graduate degree. Respondents were asked to indicate the activities that they carried out over unknown wireless networks. In a word count analysis shown in figure 3, most of the activities are browsing, WhatsApp messaging, checking and sending emails, and social media use on Facebook and YouTube. The measurement items used were adopted from prior studies (Ersche et al. 2017; Lee et al. 2001; Lee and Robbins 1995; Xu et al. 2013; Chen and Chen 2015; Rhee et al. 2009). Table 2 shows the operationalization and sources of the constructs in this study.

Table 1: Demographic Statistics

		N (%)			**N (%)**
Gender	Male	300(63%)	Education	High school or less	6(1.3%)
	Female	176(37%)		Some college	108(22.7%)
Age	<25	94 (19.7%)		Bachelor's degree	289(60.7%)
	25 - 35	252(52.9%)		Graduate	73(15.3%)
	36 - 45	74(15.5%)			

	>45	56(11.8%)

Figure 3: Word Cloud of major activities on wireless network

Table 2. Construct definition

Construct	Definition	Reference
Deficient Self-Regulation (D.S.R)	loss of self-control, such that one is unable to judge their actions, and behavior patterns of using the internet	(Lee and Perry 2004)
Automatic Use of Unknown Wireless Network (AWU)	The degree to which an individual repeatedly uses unknown wireless networks unconsciously.	(Ersche et al. 2017)
Routine Use of Unknown Wireless Network (RWU)	The degree to which an individual regularly uses unknown wireless networks consciously	(Ersche et al. 2017)
Social Connectedness	Users' subjective sense of closeness or belonging, and continual sense of connection to a wider social world.	(Lee et al. 2001; Lee and Robbins 1995)
Attachment (SC)	The degree of perceived sense of affection for online presence.	(Weller et al. 2013)
Social Interaction Anxiety (SI)	The degree of excessive fear of social situations or interactions with others, and of being evaluated or scrutinized by other people.	(Schlenker and Leary 1982)
Perceived Risk (PR)	The amount of loss an individual anticipates because of disclosure of their personal information online.	(Xu et al. 2013)
Self-Efficacy in Information System (SEIS)	The belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability.	(Chen and Chen 2015; Rhee et al. 2009)

Data Analysis and Results

For data analysis, we follow a two-step process; measurement model assessment and structural model testing, in the analysis of our data. We used SmartPLS software for our structural model testing, due to its versatility to sample sizes (Ringle et al. 2014) where, we apply Partial Least Squares technique due to its effectiveness in cause-and-effect modelling and the exploratory nature of our study (Hair et al. 2012).

Measurement model

The measurement model was first analyzed to ensure psychometric properties of validity, reliability, and common method bias. Convergent validity and discriminant validity tests were performed to test for accuracy of the measurement items. Majority of the items above loaded 0.6 except for ATT5 and PR3 loading 0.52 and 0.54 respectively. Each construct was measured with multiple other items well above 0.6. This shows that the items were indicative of the respective constructs they represent. Thus, our measurement items were deemed to have sound convergent validity. As shown in Table 3, reliability is confirmed as composite reliability (CR) values for all factors were above the recommended 0.7 value threshold, indicating item consistency and scale reliability (Hair et al. 2012). The variance explained (AVE) is above the satisfactory threshold of 0.5, confirming convergent validity (Hair et al. 2012). For the discriminant validity, the square root of the AVE (off diagonal) should be greater than the inter-factor correlations (Hulland 1999), which is confirmed in Table 2. Additionally, items loadings were found to be at least 0.2 greater than their cross loadings (see Appendix II).

To examine the extent of threat from common method bias, Harman's single factor test was conducted (Podsakoff et al. 2003). Common method bias is considered an issue when one single factor accounts for the majority of the covariance among the variables (Podsakoff et al. 2003). All items were loaded onto a single factor in an exploratory factor analysis without rotation. The test showed that the factor that accounted for the largest variance extracted is 31.25%, suggesting that common method bias was not a threat to the study. We conducted model robustness checks for multicollinearity. VIF values of attachment (1.23), privacy risk (1.07), SEIS (1.03), social interaction anxiety (1.93), social connectedness (1.984), DISR (1.00) were at satisfactory levels and well below the recommended maximum threshold of 5 (Hair et al. 2012). Thus, multicollinearity was not a problem in the study.

Table 3: Results of CFA Analysis

	CR	***α***	**Items**	**Loadings**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1. Social Interaction Anxiety	.938	.923	SIA1	0.69	**.828**							
			SIA2	0.68								
			SIA3	0.60								

			SIA4	0.71								
			SIA5	0.75								
			SIA6	0.81								
			SIA7	0.83								
2. Attachment	.915	.875	ATT1	0.82	.352	**.853**						
			ATT2	0.84								
			ATT3	0.80								
			ATT4	0.64								
			ATT5	0.52								
3. Automatic-Use	.925	.878	AU1	0.82	.374	.346	**.896**					
			AU2	0.86								
			AU3	0.82								
4. Social Connectedness	.963	.953	SC1	0.87	.670	.390	.468	**.900**				
			SC2	0.87								
			SC3	0.90								
			SC4	0.77								
			SC5	0.82								
			SC6	0.79								
5. D.S.R	.753	.569	DR1	0.85	.346	.583	.416	.299	**.713**			
			DR2	0.75								
			DR3	0.67								
6. Privacy Risk	.907	.867	PR1	0.76	.140	.146	-.125	-.029	.218	**.842**		
			PR2	0.75								
			PR3	0.54								
			PR4	0.69								
7. Routine Use	.958	.935	RU1	0.89	.335	.417	.725	.451	.400	-.070	**.941**	
			RU2	0.92								
			RU3	0.83								
8. SEIS	.921	.888	SEIS1	0.89	.142	.119	.198	.111	-.104	.067	.275	**.863**
			SEIS2	0.89								
			SEIS3	0.77								
			SEIS4	0.62								

Note: CR= Composite Reliability; **α=** Cronbach Alpha; **D.S.R** = Deficient Self- Regulation; Bolded diagonal are Square root of Average Variance Extracted

From our measurement model analysis, we empirically validated our conceptualization of habit as consisting of two first-order factors; automatic and routine use. As shown in Table 3, the two first-order factors were found to be highly correlated (0.725) with each other. Following (Son and Kim 2008), we set up a second-order factor model in which routine and automatic use are viewed as reflective indicators of the second-order construct of habitual use. The second order factor model is preferred over the first-order factor model because it presents more parsimonious model.

Structural Model

In the assessment of the explanatory power, our model accounted for 19% variance in explaining individuals' habitual use of unknown wireless networks respectively. Additionally, the antecedents in the study explain about 38% of the variance in DSR. The results of hypotheses testing indicate that H1 is not supported ($p > 0.05$; $t = 1.04$; $\beta = 0.06$), showing that individuals, preference for online social interaction does not necessarily lead to the development

of DSR. Additionally, individuals with high social connections do not have DSR according to our results, thus H2 is not supported (*p > 0.05; t= 0.09; β= 0.01*). Support for H3 was shown in our model, where individuals with high attachment to online presence are likely to be deficient in self-regulating technology (*p < 0.05; t=10.51; β= 0.45*), Support for H4 was shown in our model (p<0.05; t= 5.57; β= -0.25) where, privacy risk negatively leads to DSR.

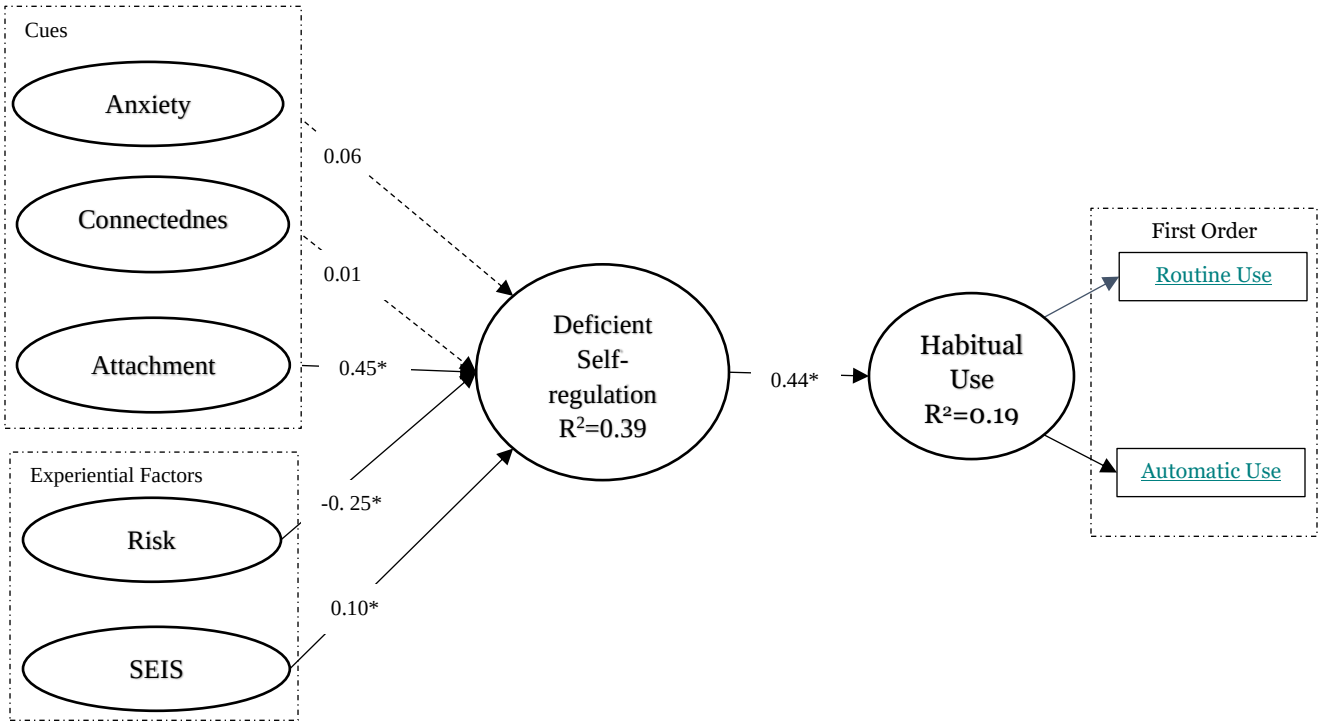

Figure 4: Research model with results

The relationship between Self-efficacy and DSR was also supported in our model (p < 0.05; t=2.31; β= 0.10). The analysis of data demonstrate support for the relationship between DSR and habitual use of unknown networks, supporting H6 (p < 0.05; t=12.03; β= 0.44).

5 Discussion and Conclusion

Use of wireless networks afford an opportunity to explore the boundaries of individual self-regulations and habitual behavior. Therefore, in this study we explore the antecedents and consequences of DSR in the context of the use of unknown wireless networks. DSR is when an individual fails to control the desire to give up a goal or behavior (Sayette and Kasey 2004). The results of this study suggest that DSR is a good predictor of individuals' habit (routine and automatic) of using technology especially in the context of wireless network use. That is, when it is difficult for

an individual to go for a day without using the internet or cut back on their use of online connectivity, it may result in conscious or unconscious habitual use of technology such as wireless network. This may explain why the number of individuals using such network is showing no downward trends even for sensitive activities such as banking despite increased awareness of threats exposure on unknown wireless networks. This implies that, when individuals are presented with a stimuli or cue, they may take an action without employing any cognitive effort in making such a decision. For example, when an individual gets a notification about the availability of wireless network, they may instantly connect their phones without analyzing their environment or investigating the operators of the network. Such individuals are exhibiting automatic use of technology. On the other hand, there are individuals who regularly seek to use technology and would make conscious effort to stay connected. For instance, a frequent traveler may always seek to use airport wireless network to accomplish task that require network connectivity. Such a conscious and regular use of airport wireless constitute routine use of technology. This confirms that active or passive psychological involvement plays an important role in decision-making. However, individuals' sensitivity to the risks that emanate from their actions can be severely impacted by habitual behaviors (Gillan et al. 2016). Some individuals may not consider the trade-off between the cost and benefits of using technology such as unknown wireless networks. Surprisingly, only attachment to portable computing devices, prompts the developments of low elf-control. This is consistent with prior literature that show gratification from the use of evolving portable computing technologies that increases the desire to remain connected to one's social groups or friends results in the development of attachment to portable computing devices (Anderson et al. 2016; Hampton et al. 2009).

We argue in research model development how some non-risk psychological factors act as cues to influence individuals' uncontrolled use of technology. The result of the effect of perceived attachment is consistent with prior behavioral research where attachment leads to individuals failing to control their urge not to use their phone while driving (Weller et al. 2013). Social media and psychology literature suggest that, social connectedness portrays relationships that individuals share with others (Hagerty et al. 1993). Individuals with low social relations seek greater social connection to the world around them. We postulate that, the greater the need to connect with the world around would drive uncontrolled desire to use wireless networks including unknown wireless networks. The results of our analysis with respect to this argument were unexpected. Future research would further explore this outcome. One possible explanation could be that, individuals in need of social connections may be craving for physical contact and therefore seek alternatives to virtual worlds as they seek to expand their social network.

Individuals with anxiety avoid face-to-face interactions in favor of online interactions where perceived judgement is limited (King et al. 2013; Lee and Stapinski 2012; Prizant-Passal et al. 2016). It is expected that such individuals would have uncontrolled urge to connect to the nearest wireless network even when they are unfamiliar with the network. Our results show that, this may not always be the case. Individual's anxiety may act as causation because of the need to avoid frustration from unfulfilled anxious situations. DSR depends on lack of awareness, or attention (LaRose 2010). An individual who has social interaction anxiety may attempt to control their interactions. Such individuals will exercise some control in the desire to use unknown wireless networks to stay connected to the activities they like to engage with.

The test of experiential factors suggests that as individual's perception of privacy risk increases, such individual will control their urge to use technology. However, individuals' degree of their perception of their ability to protect their computing technology would have a significant effect on controlling the urge to use portable computing technologies. The confirmation of the effect of privacy risk and security self-efficacy supports the role of trust that individuals have about protections of sensitive data.

Based on self-control theory, we stated that individuals with low self-control cannot resist temptation when an opportunity presents itself and therefore are expected to engage in risky behaviors such as automatic or routine use of unknown wireless networks. Our findings with respect to the relationship between DSR and habit is consistent with prior literature that shows that self-control is a strong predictor of deviant behavior (Pratt and Cullen 2000). In the software piracy context, individuals' inability to exercise self-control has been found to be significantly related to software piracy (Higgins and Makin 2004). Deficiency in self-regulation require minimal cognitive processing and shorter response time, therefore increases the likelihood of consciously or unconsciously connecting to wireless network habitually. This is because an individuals who does not control their use of portable computing device may transition to uncontrol use with repeated use of wireless network (LaRose 2010).

Theoretical Implications

We built and tested a theoretical model that predicts the antecedents and outcome of DSR. In the context of wi-fi and portable computing technology use, we identified the following variables as DSR antecedents: attachment, privacy risk and self-efficacy in information system. Prior literature primarily focused on the unconscious patterns developed in using technology (Anderson et al. 2016; Sokolov 1963). However, little is known about the factors that

influence individual's conscious development of patterns in the use of technology. We contribute to behavioral information systems security research by adopting and demonstrating that habitual use of technology is critical in explaining why individuals repetitively engage in unregulated use of technology such as risky wireless network usage behaviors. DSR is critical in the development of psychological dependence in portable computing devices. Our work makes an initial effort in differentiating the two routes to developing habitual use of technology; but did not statistically separate these two routes, we offer a new basis for future investigation of the nomological network of DSR. This insight could encourage researchers to explore the two dimensions of habits in other contexts and expand the understanding of other problematic use of technology.

Additionally, the results of the study show that privacy risk and self-efficacy in information systems affects how individuals use risky technologies. An example of risky use of technology is the routine and automatic connection to unknown wireless networks. This outcome complements prior research outcomes on privacy risk perception as a complex phenomenon that should be studied from multiple perspective (Smith et al. 2011). The findings of the study compliment prior utility-based studies that investigated individuals' behavior of connecting to unsecure Wi-Fi despite awareness of risks associated with such networks (Sombatruang et al. 2016).

Practical Implications

Our study and research findings also offer several practical implications to managers. First, our work indicates that the influence of lack of control in the urge to use technology on individuals' habitual behaviors is two-fold, where conscious decisions lead to routine use, whereas unconscious decisions result in automatic use of technology. Therefore, if managers want to decrease the negative effects of DSR, they should treat these distinct group of users differently. We also compliment prior research (Weber and Rudman 2018) in addressing the risk associated with BYOD by highlighting that managers should go beyond providing employees with security skills to raising the privacy issues related with using their personal devices or corporate mobile devices on wireless networks. For example, for routine use, increase awareness or outright denial of services would be appropriate solution to address security and privacy concerns regarding the habitual use of technology including wireless networks. However, for automatic use, a reminder on digital devices to warn users may be most useful. Second, our empirical results also indicate that individuals who perceive a higher level of privacy risk tend to control their urge to regulate their use of technology while their security efficacy did not impact that urge. Despite the warnings, individuals continue to connect

and engage in activities that make them vulnerable in unsecure public wireless networks. Public Wi-Fi use is expected to expand globally in the future, and in North America, wireless networks use is predicted to grow up to 99% by 2021 as a result of growth in mobile devices use (Cisco 2017). In a wireless risks report by Norton (2017), 55% of respondents interviewed posited that they would do anything possible to voluntarily get a strong Wi-Fi signal, including disclosure of personal information for authorization to use these unverifiable networks. Majority of these users exuded confidence in the safety of their personal information over public networks and would usually engage in sensitive activities such as using banking services that expose them to personal information disclosure (Norton 2017). To contain any negative effect of habitual use of technology, managers may aim to educate individuals to exert effort to control their desire to use unfamiliar technology such as the use of unknown wireless network.

Conclusion

The current study explores the nomological network of DSR in the context of technology use. We collected data from users of unknown wireless network to validate our proposed model. Our empirical findings validate the predictive role of cues such as attachment along with experiential factors such as privacy risk and self-efficacy in information systems as good predictors of DSR in technology use. When using apps in their mobile devices on wireless network, users' information is at risk of being intercepted by hackers (Norton 2018). For example, in a spyware campaign report, EFF (2018) stated that 'Dark Carakal', a spyware that emanated from Lebanon had remotely infiltrated individuals in over 21 countries through mobile devices majority of which are connected to Wi-Fi hotspots, resulting in loss of personal data such as call recordings, text messages, and photos. Victims of these breaches suffer huge resource loss in the recovery process. These trends are exacerbated by the emergence of Internet of Things (IoT) that require constant internet connectivity, notwithstanding the huge amount of data that they handle, opening research areas in privacy and security research (Sicari et al. 2016). Additionally, our analysis shows that DSR leads to two distinct outcomes namely routine and automatic use of technology. Despite these outcomes, our study is not without limitations. We did not test disposition factors, such as suspicion, and traits such as conscientiousness in this study. Testing these dispositional factors along with factors examined in this study would contribute to strengthening the study. Future research should explore the interactive effect of cues and experiential factors on DSR. Methodologically, we only examined the presence of common method bias using Harman's single factor approach in this study. Future study should employ other techniques such as the Marker variable or unmeasured latent method construct to increase the validity of the results obtained in this study.

Our study contributes to the literature on self-regulation theory by explicating predictors and consequences of DSR. We also contribute to the habitual use of technology by proposing and validating its multidimensional view. We provide managers with strategies to understand and control for employees who are likely to use company or personal devices on unknown wireless network by treating the two groups of habitual users as distinct and implement different strategies to promote responsible use of technology.

References

Aime, M., Calandriello, G., & Lioy, A. (2007). Dependability in Wireless Networks: Can We Rely on WiFi? *IEEE Security and Privacy Magazine*, *5*(1), 23–29.

Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J. L., & Eargle, D. (2016). From Warning to Wallpaper: Why the Brain Habituates to Security Warnings and What Can Be Done About It. *Journal of Management Information Systems*, *33*(3), 713–743.

Bandura, A. (1991). Social Cognitive Theory of Self-Regulation. *Organizational Behavior and Human Decision Processes*, (50), 248–287.

Barber, L. K., Munz, D. C., Bagsby, P. G., & Grawitch, M. J. (2009). When does time perspective matter? Self-control as a moderator between time perspective and academic achievement. *Personality and Individual Differences*, *46*(2), 250–253.

Bayer, J. B., Campbell, S. W., & Ling, R. (2016). Connection Cues: Activating the Norms and Habits of Social Connectedness: Connection Cues. *Communication Theory*, *26*(2), 128–149.

Bayer, J. B., Dal Cin, S., Campbell, S. W., & Panek, E. (2016). Consciousness and Self-Regulation in Mobile Communication: Consciousness in Mobile Communication. *Human Communication Research*, *42*(1), 71–97.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data? *Perspectives on Psychological Science*, *6*(1), 3–5.

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

CBS. (2010). Dangers of Free Public Wifi. https://www.cbsnews.com/news/dangers-of-free-public-wifi/. Accessed 15 March 2018

Chen, H.-T., & Chen, W. (2015). Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 13–19.

Choi, H. S., & Carpenter, D. (2013). Connecting to Unknown Wi-Fi Hotspots - A Risk Taking Perspective, 10.

Cisco. (2017). Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–202, 35.

Cisco. (2018). Five Reasons to Go Wireless. *Cisco*. https://www.cisco.com/c/en/us/solutions/small-business/resource-center/work-anywhere/why-go-wireless.html. Accessed 25 April 2018

Dolly, J. (2018). Why you should never, ever connect to public WiFi | CSO Online. https://www.csoonline.com/article/3246984/wi-fi/why-you-should-never-ever-connect-to-public-wifi.html. Accessed 5 April 2018

Eastin, M. S., Glynn, C. J., & Griffiths, R. P. (2007). Psychology of Communication Technology Use in the Workplace. *CyberPsychology & Behavior*, *10*(3), 436–443.

EFF. (2018). Dark carakal: Cyber-espionage at a Global Scale. *Lookout*. https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf. Accessed 5 April 2018

Ersche, K. D., Lim, T.-V., Ward, L. H. E., Robbins, T. W., & Stochl, J. (2017). Creature of Habit: A self-report measure of habitual routines and automatic tendencies in everyday life. *Personality and Individual Differences*, *116*, 73–85.

Finjan Mobile. (2018). The Dangers of Using Unsecured Wi-Fi | How Bad is it, Really? https://www.finjanmobile.com/the-dangers-of-using-unsecured-wi-fi/. Accessed 29 March 2018

Fullwood, C., Quinn, S., Kaye, L. K., & Redding, C. (2017). My virtual friend: A qualitative analysis of the attitudes and experiences of Smartphone users: Implications for Smartphone attachment. *Computers in Human Behavior*, *75*, 347–355.

Gast, M. S. (2002). *802.11 Wireless Networks: the definitive guide: [creating and administering Wireless Networks]* (1. ed.). Beijing: O'Reilly.

Gillan, C. M., Robbins, T. W., Sahakian, B. J., van den Heuvel, O. A., & van Wingen, G. (2016). The role of habit in compulsivity. *European Neuropsychopharmacology*, *26*(5), 828–840.

Gökçearslan, Ş., Mumcu, F. K., Haşlaman, T., & Çevik, Y. D. (2016). Modelling smartphone addiction: The role of smartphone usage, self-regulation, general self-efficacy and cyberloafing in university students. *Computers in Human Behavior*, *63*, 639–649.

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

Hagerty, B. M. K., Lynch-Sauer, J., Patusky, K. L., & Bouwsema, M. (1993). An Emerging Theory of Human Relatedness. *Image: the Journal of Nursing Scholarship*, *25*(4), 291–296.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, *40*(3), 414–433.

Hampton, K. N., Livio, O., & Sessions Goulet, L. (2009). The Social Life of Wireless Urban Spaces: Internet Use, Social Networks, and the Public Realm. *Journal of Communication*, *60*(4), 701–722.

Higgins, G. E., & Makin, D. A. (2004). Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy?, *2*(2), 1–22.

Hulland. (1999). Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. *Strategic Management Journal*, *20*(2), 195–204.

Kaspersky. (2016). Public WiFi Risks and what you can do about it | Kaspersky Lab US. https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks. Accessed 15 April 2018

Khang, H., Kim, J. K., & Kim, Y. (2013). Self-traits and motivations as antecedents of digital media flow and addiction: The Internet, mobile phones, and video games. *Computers in Human Behavior*, *29*(6), 2416–2424.

Kindberg, T., Bevan, C., O'Neill, E., Mitchell, J., Grimmett, J., & Woodgate, D. (2009). Authenticating Ubiquitous Services: A Study of Wireless Hotspot Access, 12.

King, A. L. S., Valença, A. M., Silva, A. C. O., Baczynski, T., Carvalho, M. R., & Nardi, A. E. (2013). Nomophobia: Dependency on virtual environments or social phobia? *Computers in Human Behavior*, *29*(1), 140–144.

Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. (2009). "When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday Wi-Fi Use, 10.

LaRose, R. (2010). The Problem of Media Habits. *Communication Theory*, *20*(2), 194–222.

LaRose, R., Lin, C. A., & Eastin, M. S. (2003). Unregulated Internet Usage: Addiction, Habit, or DSR? *Media Psychology*, *5*(3), 225–253.

Lee, B. W., & Stapinski, L. A. (2012). Seeking safety on the internet: Relationship between social anxiety and problematic internet use. *Journal of Anxiety Disorders*, *26*(1), 197–205.

Lee, K. C., & Perry, S. D. (2004). Student Instant Message Use in a Ubiquitous Computing Environment: Effects of DSR. *Journal of Broadcasting & Electronic Media*, *48*(3), 399–420.

Lee, R. M., Draper, M., & Lee, S. (2001). Social Connectedness, Dysfunctional Interpersonal Behaviors, and Psychological Distress: Testing a Mediator Model, 9.

Lee, R. M., & Robbins, S. B. (1995). Measuring belongingness: The social connectedness and the social assurance scales. *Journal of counseling psychology*, *42*(2), 232.

Lee, Y.-K., Chang, C.-T., Lin, Y., & Cheng, Z.-H. (2014). The dark side of smartphone usage: Psychological traits, compulsive behavior and technostress. *Computers in Human Behavior*, *31*, 373–383.

Lee, Z. W. Y., Cheung, C. M. K., & Chan, T. K. H. (2016). Technology-Mediated Self-Regulation: An Implication for Preventing Online Gaming Addiction. *International Conference on Information Systems*, 10.

MarketWatch. (2018). Global Wi-Fi hotspot Market Growth Expected to be Driven by Increasing Use of Mobile Devices and Smartphones Coupled with Growing Internet Penetration Across the Globe - MarketWatch. https://www.marketwatch.com/story/global-wi-fi-hotspot-market-growth-expected-to-be-driven-by-increasing-use-of-mobile-devices-and-smartphones-coupled-with-growing-internet-penetration-across-the-globe-2018-02-21. Accessed 15 March 2018

McCord, B., Rodebaugh, T. L., & Levinson, C. A. (2014). Facebook: Social uses and anxiety. *Computers in Human Behavior*, *34*, 23–27.

McIntyre, E., Wiener, K. K. K., & Saliba, A. J. (2015). Compulsive Internet use and relations between social connectedness, and introversion. *Computers in Human Behavior*, *48*, 569–574.

Norton. 2017. “Norton Wi-Fi Risk Report.” (https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf, accessed April 5, 2018).

Norton. (2018). The Personal Impact of Cybercrime. https://us.norton.com/internetsecurity-emerging-threats-personal-impact-cybercrime.html. Accessed 25 April 2018

Olufon, T., Campbell, C. E.-A., Hole, S., Radhakrishnan, K., & Sedigh, A. (2014). Mitigating External Threats in Wireless Local Area Networks. *International Journal of Communication Networks and Information Security*, *6*(3), 18.

Oulasvirta, A., Rattenbury, T., Ma, L., & Raita, E. (2012). Habits make smartphone use more pervasive. *Personal and Ubiquitous Computing*, *16*(1), 105–114.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

Polites, G. L., Serrano, C., Thatcher, J. B., & Matthews, K. (2018). Understanding social networking site (SNS) identity from a dual systems perspective: an investigation of the dark side of SNS use. *European Journal of Information Systems*, *27*(5), 600–621.

Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology*, *38*(3), 931–964.

Prizant-Passal, S., Shechner, T., & Aderka, I. M. (2016). Social anxiety and internet use – A meta-analysis: What do we know? What are we missing? *Computers in Human Behavior*, *62*, 221–229.

Przybylski, A. K., & Weinstein, N. (2013). Can you connect with me now? How the presence of mobile communication technology influences face-to-face conversation quality. *Journal of Social and Personal Relationships*, *30*(3), 237–246.

Public WiFi Risks and what you can do about it | Kaspersky Lab US. (2018). https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks. Accessed 15 April 2018

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826.

Richardson, J. (2018). The New Science of Habit Formation and Change. *Fire Uo Today*. http://fireuptoday.com/the-new-science-of-habit-formation-and-change/. Accessed 15 April 2018

Ringle, C. M., Da Silva, D., & Bido, D. D. S. (2014). Structural Equation Modeling with the Smartpls. *Revista Brasileira de Marketing*, *13*(02), 56–73.

Salehan, M., & Negahban, A. (2013). Social networking on smartphones: When mobile phones become addictive. *Computers in Human Behavior*, *29*(6), 2632–2639.

Sambamurthy, Bharadwaj, & Grover. (2003). Shaping Agility through Digital Options: Reconceptualizing the Role of Information Technology in Contemporary Firms. *MIS Quarterly*, *27*(2), 237.

Sayette, M. A., & Kasey, G. M. (2004). *Self-regulatory failure and addiction* (Vol. 2). Handbook of self-regulation: Research, theory, and applications.

Schlenker, B. R., & Leary, M. R. (1982). Social Anxiety and Self-Presentation: A Conceptualization and Model. *Social Anxiety*, 29.

Schlesinger, J. (2016). Most people unaware of the risks of using public Wi-Fi. https://www.cnbc.com/2016/06/28/most-people-unaware-of-the-risks-of-using-public-wi-fi.html. Accessed 29 March 2018

Sicari, S., Cappiello, C., De Pellegrini, F., Miorandi, D., & Coen-Porisini, A. (2016). A security-and quality-aware system architecture for Internet of Things. *Information Systems Frontiers*, *18*(4), 665–677.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989 -1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167–196.

Sokolov, E. N. (1963). Higher Nervous Functions: The Orienting Reflex. *Annual Review of Physiology*, *25*(1), 545–580.

Sombatruang, N., Sasse, M. A., & Baddeley, M. (2016). Why do people use unsecure public wi-fi?: an investigation of behaviour and factors driving decisions (pp. 61–72). ACM Press.

Son, & Kim. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. *MIS Quarterly*, *32*(3), 503.

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: Good habits gone bad. *Information Systems Journal*, *25*(4), 403–427.

Soror, A. A., Steelman, Z. R., & Limayem, M. (2012). Discipline Yourself Before Life Disciplines You: DSR and Mobile Phone Unregulated Use. In *2012 45th Hawaii International Conference on System Sciences* (pp. 849–858).

Turner, P., & Turner, S. (2013). Emotional and aesthetic attachment to digital artefacts. *Cognition, Technology & Work*, *15*(4), 403–414.

Uzun, A. M., & Kilis, S. (2019). Does persistent involvement in media and technology lead to lower academic performance? Evaluating media and technology use in relation to multitasking, self-regulation and academic performance. *Computers in Human Behavior*, *90*, 196–203.

van Deursen, A. J. A. M., Bolle, C. L., Hegner, S. M., & Kommers, P. A. M. (2015). Modeling habitual and addictive smartphone behavior. *Computers in Human Behavior*, *45*, 411–420.

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.

Wang, C., Lee, M. K. O., & Hua, Z. (2015). A theory of social media dependence: Evidence from microblog users. *Decision Support Systems*, *69*, 40–49.

Weber, L., & Rudman, R. J. (2018). Addressing the Incremental Risks Associated with Adopting Bring Your Own Device. *Open Access*, *11*(1), 13.

Weller, J. A., Shackleford, C., Dieckmann, N., & Slovic, P. (2013). Possession attachment predicts cell phone use while driving. *Health Psychology*, *32*(4), 379–387.

Wood, W., & Neal, D. T. (2007). A new look at habits and the habit-goal interface. *Psychological Review*, *114*(4), 843–863.

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research*, *13*(2), 151–168.

Appendix I: Survey Items

Gender:
[ ] Male
[ ] Female

Age:
[ ] 25 and below
[ ] 26 - 30
[ ] 31 – 35
[ ] 36 – 40
[ ] 41 – 45
[ ] 46 – 50
[ ] 51 – 55
[ ] above 55

Education:
[ ] High school or less
[ ] Some college
[ ] Undergraduate/bachelor's degree
[ ] Graduate

Have you ever connected to a wi-fi or wireless network you do not know are not sure who operates it?? [ ] Yes [ ] No

How often have you connected to such wi-fi? Very often [ ] **Often** [ ] **Sometimes**[ ] **Rarely** [ ] **Never** [ ]

Which of the following activities do you perform while connected to unknown network?
Banking [ ] **Emails** [ ] **Facebook** [ ] **Instagram[ ] Twitter**[ ] **News** [ ]

Routine Use (Ersche et al. 2017)

	Measurement Items	Strongly Disagree			Neutral			Strongly Agree
RU1	I regularly connect to the next available unknown wireless network	1	2	3	4	5	6	7
RU2	I frequently use unknown wireless network connections	1	2	3	4	5	6	7
RUI3	I tend to use unacquainted wireless network connections to browse the internet.	1	2	3	4	5	6	7

Automatic Use (Ersche et al. 2017)

	Measurement Items	Strongly Disagree			Neutral			Strongly Agree
AU1	I unconsciously connect to next available unknown wireless networks	1	2	3	4	5	6	7
AU2	I often connect to unknown wireless networks without being aware of it	1	2	3	4	5	6	7
AU3	It is difficult to resist connecting my device to unknown wireless network	1	2	3	4	5	6	7

Deficient Internet Self-regulation (Kevin C. Lee & Stephen D. Perry 2004)

	Measurement Items	Strongly Disagree			Neutral			Strongly Agree
DR1	It would be difficult for me to go for a day without using the Internet	1	2	3	4	5	6	7
DR2	Time seems to pass more quickly when I am using the Internet	1	2	3	4	5	6	7
DR3	1 have tried to cut back on my Internet use, but I can't seem to do it	1	2	3	4	5	6	7

Privacy Risk (Xu et al. 2013)

	Measurement Items	Strongly Disagree			Neutral			Strongly Agree
PR1	In general, it would be risky to give personal information online	1	2	3	4	5	6	7
PR2	There would be high potential for privacy loss associated with giving personal information online	1	2	3	4	5	6	7
PR3	Personal information could be inappropriately used by online platforms	1	2	3	4	5	6	7
PR4	Providing online platforms with my personal information could lead to many unexpected problems	1	2	3	4	5	6	7

Self-Efficacy in information Security (Chen and Chen 2015)

	Measurement Items	Strongly Disagree			Neutral			Strongly Agree
SEIS1	I feel confident detecting viruses on my smartphone, tablet or IPad	1	2	3	4	5	6	7
SEIS2	I feel confident getting rid of any spyware on my smartphone, tablet or IPad	1	2	3	4	5	6	7
SEIS3	I feel confident setting the security level on the browser when surfing the net on my smartphone, tablet or IPad	1	2	3	4	5	6	7
SEIS4	I feel confident protecting my personal information when connecting to unknown wireless networks	1	2	3	4	5	6	7

Social Interactions Anxiety (Lee, Chang, Lin, & Cheng, 2014)

	Measurement Items	Strongly Disagree			Neutral			Strongly Agree
SIA1	I often feel nervous even in casual get-togethers	1	2	3	4	5	6	7
SIA2	I get nervous when I must talk to a teacher or a boss	1	2	3	4	5	6	7
SIA3	I sometimes feel tense when talking to people of my own gender if I don't know them very well	1	2	3	4	5	6	7
SIA4	I would be nervous if I was being interviewed for a job	1	2	3	4	5	6	7
SIA5	In general, I am a shy person	1	2	3	4	5	6	7
SIA6	I often feel nervous when calling someone I don't know very well on the telephone	1	2	3	4	5	6	7
SIA7	I get nervous when I speak to someone in a position of authority	1	2	3	4	5	6	7

Social Connectedness: (Lee, & Robbins, 1995)

	Measurement Items	Strongly Disagree			Neutral			Strongly Agree
SC1	I feel disconnected from the world around me	1	2	3	4	5	6	7
SC2	Even around people I know, I don't feel that I really belong	1	2	3	4	5	6	7
SC3	I feel so distant from people when not connected to them in some way	1	2	3	4	5	6	7
SC4	I have no sense of togetherness with my peers	1	2	3	4	5	6	7
SC5	I don't feel related to anyone unless when connected to them in some way	1	2	3	4	5	6	7
SC6	I catch myself losing all sense of connectedness with society	1	2	3	4	5	6	7
SC7	I don't feel I interact with anyone or any group unless when connected to them in some way	1	2	3	4	5	6	7

Attachment (Weller, Shackleford, Dieckmann, & Slovic, 2013)

	Measurement Items	Strongly Disagree			Neutral			Strongly Agree
ATT1	I would feel uncomfortable if I didn't have my smartphone, tablet or IPad for a long period of time	1	2	3	4	5	6	7
ATT2	I would feel lost if I didn't have my smartphone, tablet or IPad	1	2	3	4	5	6	7
ATT3	I would feel detached from my friends if I didn't have my smartphone, tablet or IPad	1	2	3	4	5	6	7
ATT4	I feel momentarily distressed if I realize that I can't connect my smartphone, tablet or IPad to the internet while I am out and about	1	2	3	4	5	6	7
ATT4	I would rather lose my wallet than my smartphone, tablet or IPad	1	2	3	4	5	6	7

Appendix II: Cross Loadings

	AWU	Attachment	Connectedness	Habit	RWU	Risk	SEIS	DSR	Anxiety
ATT1	0.241	0.895	0.371	0.292	0.281	0.267	0.188	0.517	0.399
ATT2	0.331	0.908	0.377	0.366	0.322	0.263	0.195	0.548	0.396
ATT3	0.357	0.844	0.428	0.418	0.388	0.114	0.179	0.437	0.319
ATT4	0.278	0.708	0.333	0.352	0.351	0.041	0.073	0.310	0.291
AU1	0.912	0.302	0.373	0.811	0.531	-0.031	0.222	0.436	0.270
AU1	0.912	0.302	0.373	0.811	0.531	-0.031	0.222	0.436	0.270
AU2	0.925	0.296	0.427	0.836	0.563	-0.010	0.232	0.442	0.342
AU2	0.925	0.296	0.427	0.836	0.563	-0.010	0.232	0.442	0.342
AU3	0.874	0.364	0.395	0.784	0.518	0.064	0.184	0.494	0.338
AU3	0.874	0.364	0.395	0.784	0.518	0.064	0.184	0.494	0.338
DR1	0.322	0.497	0.133	0.258	0.135	0.409	0.200	0.853	0.260
DR2	0.310	0.390	0.091	0.233	0.100	0.432	0.241	0.829	0.208
DR3	0.586	0.465	0.397	0.550	0.393	0.124	0.157	0.787	0.326
PR1	-0.022	0.112	-0.009	-0.046	-0.061	0.748	0.100	0.180	0.158
PR2	-0.058	0.127	-0.044	-0.066	-0.060	0.672	0.084	0.122	0.143
PR3	0.052	0.232	0.024	0.017	-0.024	0.901	0.208	0.454	0.184
PR4	-0.057	0.135	0.028	-0.035	-0.006	0.666	0.025	0.126	0.141
RU1	0.559	0.333	0.362	0.825	0.922	-0.111	0.206	0.201	0.285
RU1	0.559	0.333	0.362	0.825	0.922	-0.111	0.206	0.201	0.285
RU2	0.542	0.321	0.370	0.826	0.939	-0.049	0.195	0.204	0.312
RU2	0.542	0.321	0.370	0.826	0.939	-0.049	0.195	0.204	0.312
RU3	0.542	0.418	0.386	0.807	0.902	0.044	0.238	0.334	0.306
RU3	0.542	0.418	0.386	0.807	0.902	0.044	0.238	0.334	0.306
SC1	0.333	0.320	0.826	0.386	0.358	-0.079	0.091	0.124	0.592
SC2	0.339	0.322	0.836	0.361	0.306	-0.059	0.072	0.150	0.588
SC3	0.348	0.359	0.870	0.382	0.333	-0.025	0.124	0.174	0.604
SC4	0.405	0.429	0.898	0.431	0.363	0.064	0.156	0.286	0.584
SC5	0.435	0.418	0.908	0.460	0.385	0.015	0.175	0.260	0.577
SC6	0.413	0.426	0.913	0.439	0.370	0.042	0.192	0.287	0.616
SEIS1	0.208	0.153	0.127	0.223	0.190	0.168	0.924	0.235	0.176
SEIS2	0.219	0.217	0.185	0.261	0.248	0.176	0.925	0.251	0.226
SEIS3	0.174	0.170	0.119	0.174	0.136	0.154	0.843	0.174	0.179
SEIS4	0.252	0.080	0.144	0.294	0.273	0.031	0.651	0.062	0.179
SIA1	0.330	0.211	0.545	0.354	0.303	-0.047	0.174	0.146	0.723
SIA2	0.356	0.248	0.506	0.376	0.316	0.004	0.127	0.163	0.758
SIA3	0.397	0.250	0.533	0.401	0.319	0.021	0.173	0.194	0.697
SIA4	0.197	0.424	0.438	0.205	0.167	0.388	0.165	0.385	0.798
SIA5	0.258	0.305	0.557	0.271	0.225	0.177	0.252	0.253	0.782

SIA6	0.249	0.361	0.579	0.290	0.268	0.168	0.181	0.266	0.834
SIA7	0.249	0.364	0.563	0.305	0.296	0.122	0.113	0.218	0.821