Location Based Services and the Health Belief Model Based Investigation of Student Intentions and Behaviors

Completed Research

Gregory Schymik, PhD
Grand Valley State University
schymikg@gvsu.edu

Jie Du, PhD
Grand Valley State University
dujie@gvsu.edu

Andrew Kalafut, PhD
Grand Valley State University
kalafuta@gvsu.edu

Abstract

This research aims to understand the information security and privacy perceptions and behaviors of undergraduate students at one midwestern public, master's granting university regarding their use of built-in location-based services (LBS) in mobile devices. We surveyed students in an introductory computing course about their use of such services. The eight factors of the Health Belief Model are used as the basis for survey questions: LBS behavior, perceived barriers to practice, self-efficacy, cues to action, prior security experience, perceived vulnerability, perceived benefits, and perceived severity. Perceived severity, barriers to entry, and perceived benefits were found to have a significant impact on students' LBS security behaviors. This study provides a foundation upon which further investigation into security behaviors related to the use of LBS can be based. The findings and implications for researchers and educators are discussed.

Keywords

Location based services security, health belief model, survey

Introduction

Mobile phone users' locations are very likely being tracked in ways the authors of this proceeding believe most would find rather disturbing. The New York Times recently reported that "At least 75 companies receive anonymous, precise location data from apps whose users enable location services to get local news and weather or other information" and that, while this data has been anonymized, individuals, through their use of location based services (LBS) on mobile devices, can be easily tracked with incredible precision: accurate to within a few yards and updated thousands of times a day in some cases (Valentino-DeVries et al. 2018). Without reading privacy policies in detail, many users simply do not realize that allowing an app to use the device's GPS to help it find a gas station in which to fill their tank could also be allowing the app to use that data to track industry trends or that the publisher of the app might even be selling their data to data aggregators. The authors of the article found that it was not difficult to identify specific individuals in a database to which they were granted access and interviewed some of those individuals. The subjects interviewed were surprised and concerned when they were shown the detailed information these companies have recorded about their activities[1]. This data can be used in nefarious ways. In one reported case, the location of a person's bedroom inside their home was known by an intruder (not simply the address of the home, the location of the bedroom) (Huddleston 2018).

[1] The interactive version of this article might be an eye-opening experience for many people: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

Thankfully, Apple and Google have provided instructions on how we can manage our location settings on their devices (Fowler 2018). The question is: are people concerned enough about the privacy risks they face from using LBS that they would take action to protect themselves from that risk, and is there some explanatory link between their reported behaviors and their concerns? To be more specific, we ask the following research question: What drives people to take preventive action to protect themselves from the risks associated with the use of location based services (LBS)?

In the pursuit of an answer to that question, we have surveyed students in an introductory computing course at a major midwestern public, master's granting university. This paper starts with a discussion of research into LBS usage and then focuses on the adoption of preventive behaviors and the health belief model. A description of the research model and methodology we applied to help answer our research question follows. Finally, it concludes with a presentation of the results and a discussion of their implications.

Literature Review

Location Services and Privacy

There has been a substantial amount of research published recently regarding the use of location based services and the impact privacy concerns might have on LBS usage. Much of this research has focused on Technology Acceptance Model (TAM)-based, inquiries into the drivers of LBS usage and most have added a factor associated with privacy risk or trust to variations of TAM-based models (Jang and Lee 2018; Mao and Zhang 2013; Palos-Sanchez et al. 2017; Zhou 2015). Others have added similar privacy and trust factors to variations of the more up-to-date TAM-based theory: the Unified Theory of Acceptance and Use of Technology (UTAUT) (Yun et al. 2013; Zhou 2013) to examine usage intention. Much of this research has found that privacy concerns and trust do have an impact on the adoption of LBS.

Health Belief Model

As noted above, much research has focused on the drivers of LBS usage while mentioning privacy risk as a factor but it appears that few researchers have attempted to investigate what drives people to adopt preventive behaviors that can reduce or eliminate the risks associated with LBS. The findings that privacy concerns and trust appear to impact LBS adoption lead us to wonder what drives the adoption of preventive behaviors regarding LBS usage. The Health Belief Model (HBM) was first developed in the 1950s as an expectancy-value model that explains preventive health behaviors (Rosenstock 1974). Preventive healthcare behaviors refer to behaviors that will lessen the effects of diseases, such as vaccination, diet and exercise. According to the HBM, a person's attitude towards preventive health behaviors is a function of the perceived likelihood of outcomes associated with the behaviors and the expected value of those outcomes. The perceived likelihood depends on two beliefs, the perceived susceptibility and perceived severity of the illness. The expected value of the health behavior is determined by the perceived benefits and perceived barriers to performing the preventive health behavior. Three other variables, self-efficacy, cues to action, and general health orientation were included into the HBM a decade after the HBM was first introduced in an attempt to better explain the adoption of preventive health behaviors (Janz 1984).

In computer security, protective security behavior refers to behaviors that will lessen the effects of security incidents. Given the common ground between adopting preventive health behaviors and practicing protective security countermeasures, the HBM has been widely applied to study security behaviors in the information systems domain, including the use of email (Ng et al. 2009), the adoption of computer security software (Claar et al. 2013), and how to prevent unauthorized access to computers (Williams et al. 2014). Schymik and Du (2017) summarizes their findings.

Research Model and Hypotheses

This research represents a portion of a broader examination of the HBM and its usage to help explain information security and privacy behaviors and adopts a research model used in prior HBM research on email security behavior (Schymik and Du 2017). The dependent variable in the research model is self-

reported behavior related to the use of location based services. Seven independent variables (IVs) are derived from the original HBM core constructs, including the perceived benefits of performing email security behavior (BEN), the perceived barriers to entry of performing LBS behavior (BAR), the subject's self-efficacy to carry out LBS security behaviors (EFF), the perceived vulnerability to LBS-based security incidents (VUL), the cues to action regarding LBS security behavior (CUE), the subjects' prior experience with LBS-related security issues (EXP), and the perceived severity of LBS-related security incidents (SEV). The first model we analyze uses all seven of the constructs as main-effects IVs.

Construct Name	*Label*	*Definition*
LBS Security Behavior	BEH	An individual's self-reported behavior regarding using and securing location based services (LBS)
Perceived Benefits	BEN	An individual's beliefs of the value of a behavior to reduce the risk of a security incident
Perceived Barriers	BAR	An individual's own evaluation of the obstacles in the way of adopting a new behavior
Self-Efficacy	EFF	The belief in an individual's own ability to do something
Perceived Vulnerability	VUL	The personal risk or susceptibility of contracting a condition
Cues to Action	CUE	Events, things, or people that move people to change their behavior
Prior Experience	EXP	An individual's previous experience with LBS behaviors
Perceived Severity	SEV	An individual's belief about the seriousness or severity of a security incident

Table 1 - The Core Constructs in the Research Model

In a second version of the model, we follow previous email-related HBM research and model the prior experience (EXP) and the perceived severity (SEV) constructs as moderating variables that magnify or reduce the effects of the other IVs on self-reported LBS behavior (BEH). Table 1 defines the eight core HBM constructs and Figure 1 presents a combination of the direct effects and interactions models explored in this research. The instrument was adopted from prior literature and adapted to the context of LBS security.

Main-effects Hypotheses

We propose the following main-effects model hypotheses:

- H1 – Perceived benefits (BEN) of practicing LBS security behaviors are positively related to LBS security behaviors.
- H2 – Perceived barriers (BAR) to practicing LBS security behaviors are negatively related to LBS security behaviors.
- H3 – Self-efficacy (EFF) is positively related to LBS security behaviors.
- H4 – Perceived vulnerability (VUL) to LBS-related security incidents is positively related to LBS security behaviors.
- H5 – Cues to action (CUE) are positively related to LBS security behaviors.
- H6 – Prior experience (EXP) with LBS-related security issues is positively related to LBS security behaviors.
- H7 – Perceived severity (SEV) of LBS-related security issues is positively related to LBS security behaviors.

Interactions Model Hypotheses

In a second model exploring interaction effects, we combine the Ng et al. (2009) and Claar and Johnson (2010) HBM model variations and hypothesize that the subjects' prior experience with LBS-related security issues (EXP) and their perception of the severity of LBS security-related issues (SEV) are moderating variables. The health belief model implies several psychosocial variables (age, education) as moderators (Rosenstock 1974). Since our subject population is fairly homogeneous and falls in a narrow

age range (90% are between the ages of 19 and 26), and the vast majority are first- or second-year undergraduate students, we do not include these psycho-social variables in our analysis.

Experience as a Moderator

We hypothesize that subjects' prior experience with LBS-related information security attacks would have a moderating effect on the other main-effects IVs. Claar and Johnson (2010) suggested this interaction in their research without explanation. We suggest that those who have had security issues related to LBS usage in the past would be influenced by those experiences in ways that would impact the likelihood of any individual model construct effecting their behaviors. To be more specific, we suggest that: a subject who has experienced LBS-related information security problems would probably more easily see the value of being diligent with LBS usage (EXPxBEN), be expected to have a reduced focus on the difficulty of performing the appropriate preventative actions (EXPxBAR), give less weight to any perception of LBS self-efficacy (EXPxEFF), have a better, or more realistic understanding of their vulnerability to LBS-related security issues (EXPxVUL), have a higher appreciation for the cues to action they might have seen (EXPxCUE), and have a better understanding of the severity of LBS-related security incidents (EXPxSEV). We state the following hypotheses regarding the moderating effects of a subject's prior experience with LBS-related information security incidents:

- H6a – Prior experience with LBS-related security incidents increases the positive effect of perceived benefits on LBS security behaviors (EXPxBEN).
- H6b – Prior experience with LBS-related security incidents reduces the negative effect of barriers to practice on LBS security behaviors (EXPxBAR).
- H6c – Prior Experience with LBS-related security incidents reduces the positive effect of self-efficacy on LBS-related security behaviors (EXPxEFF).
- H6d – Prior experience with LBS-related security incidents increases the positive effect of perceived vulnerability on LBS security behaviors (EXPxVUL).
- H6e – Prior experience with LBS-related security incidents increases the positive effect of cues to action on LBS security behaviors (EXPxCUE).
- H6f – Prior experience with LBS-related security incidents increases the positive effect of perceived severity on LBS security behaviors (EXPxSEV).

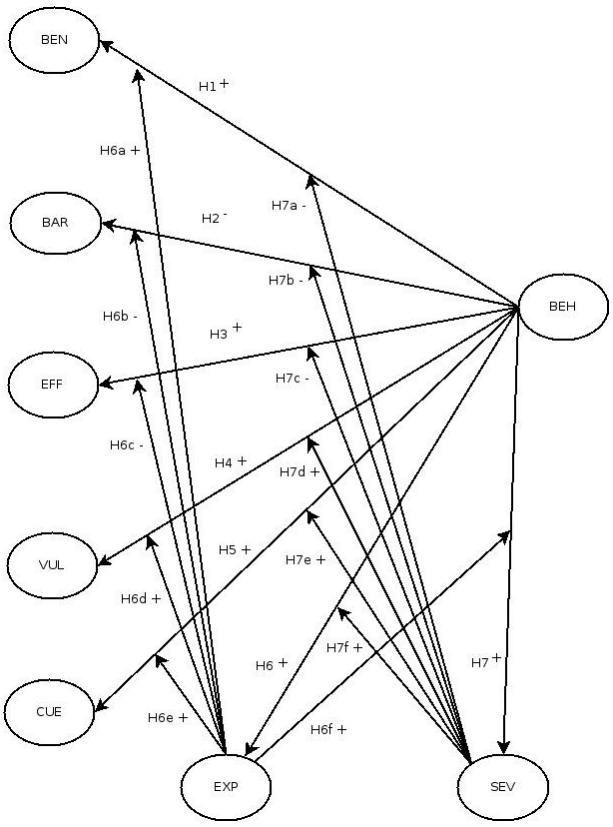

Figure 1 - Main Effects and Interactions Models

Severity as a Moderator

Ng et al. (2009) relied on expectancy-value theory, protection motivation theory, and health belief model literature to hypothesize that perceived severity would have a moderating effect on the other IVs in the model. Based on their efforts, we hypothesize that perceived severity will have an influence on the remaining independent variables and state the following factor-specific hypotheses.

- H7a – Perceived severity of any LBS-related security incidents reduces the positive effect of perceived benefits on LBS security behaviors (SEVxBEN).
- H7b – Perceived severity of any LBS-related security incidents reduces the negative effect of barriers to practice on LBS security behaviors (SEVxBAR).

- H7c – Perceived severity of any LBS-related security incidents reduces the positive effect of self-efficacy on LBS security behaviors (SEVxEFF).
- H7d – Perceived severity of any LBS-related security incidents increases the positive effect of perceived vulnerability on LBS security behaviors (SEVxVUL).
- H7e – Perceived severity of any LBS-related security incidents increases the positive effect of cues to action on LBS security behaviors (SEVxCUE).
- H7f – Perceived severity of any LBS-related security incidents increases the positive effect of prior experience on LBS security behaviors (SEVxEXP)

Methodology

Electronic questionnaires containing 34 questions were sent to 779 undergraduate students from an introductory computing course through the school's Blackboard course management system. The Blackboard system allows the students to submit responses anonymously. Participants who responded were automatically entered in a drawing for one of four gift cards (iTunes or a local coffee shop). Except for the age and gender questions, all questions on the survey focused on the eight constructs and are anchored on 5-point Likert scales. 148 students responded ultimately resulting in 140 usable survey response sets representing an 18 percent response rate.

Survey Development

The survey questions used for each construct were derived from three difference sources. Questions used to measure BEH, CUE, and EXP were derived from those used in Claar and Johnson (2012). Those used to measure BEN and VUL were sourced from Ng et al. (2009). BAR and EFF questions were derived from a combination of those two resources. SEV questions were derived from a combination of those used by NG et al. (2009) and from sources cited on the Consumer Health Informatics Research Resource at the National Institutes of Health (Logan et al. 2019): Champion (1984), Moss-Morris et al. (2002), and Figueiras and Alves (2007). Space limitations prevent the listing of the questions in this proceeding. Please contact the authors to obtain a copy of the survey questions. The items in the survey focused on eight constructs including seven IVs and one dependent variable. All items are anchored on 5-point Likert scales. The scales for three BEH questions were inverted in order to keep the scores consistent for the factor. High scores in the BEH questions indicate better behavior.

Construct	*Item*	*Factor loadings*	*Cronbach Alpha*
BEH			0.715
	BEH1	.606	
	BEH3	.898	
	BEH4	.516	
BAR			0.787
	BAR1	.805	
	BAR2	.822	
	BAR3	.618	
EFF			0.873
	EFF1	.652	
	EFF2	.947	
	EFF3	.865	
CUE			0.742
	CUE1	.791	
	CUE2	.757	
VUL			0.807
	VUL1	.920	
	VUL2	.666	
	VUL3	.717	
BEN12			0.815
	BEN1	.641	
	BEN2	.970	
BEN34			0.7 87
	BEN3	.619	
	BEN4	.898	
SEV			0.816
	SEV1	.713	
	SEV2	.802	
	SEV3	.790	
	SEV4	.574	

Table 2 - Factor Loadings and Chronbach Alpha

Data Analysis

We conducted a three-step analysis to examine the effects of the independent variable constructs on the LBS-based security behavior dependent variable (BEH). First, an exploratory factor analysis was done to extract the factors (latent variables) to validate our model constructs. Second, a multiple regression analysis was conducted using the SPSS calculated factor scores. The dependent variable was regressed on the seven IVs to determine the main effects (Model 1). We then added the

moderating variables, perceived severity (SEV) and prior experience (EXP) were added into the regression model to examine the interaction effects of those IVs (Model 2).

Exploratory Factor Analysis (EFA)

The initial factor analysis failed to complete after 25 iterations due to a communality issue. No factors were extracted. After taking a careful look at the data, we found that the three items in the EXP construct are highly correlated which caused the extracting process to terminate without extracting any factors. We removed EXP1 from the data set to resolve the communality issue because it had the highest correlations with the other items in the construct ($r = .849$, $p < .01$ with EXP2 and $r = .734$, $p < .01$ with EXP3) (Field 2013).

We reran the EFA with EXP1 removed from the dataset seeking eight factors. We set 0.5 as the factor loading threshold based on the size of our data set (Hair, Tatham, Anderson, & Black, 1998). Three rounds were run before we arrived at a set of factors loading at 0.5 or above. In the first run, eight survey questions (BEH2, EFF4, CUE3, CUE4, EXP2, EXP3, SEV5, and SEV6) having a factor loading lower than 0.5 were removed from further consideration. An additional survey question (SEV7) was removed in the second round.

The results of the final round of EFA resulted in eight factors being extracted from the data: BEH, SEV, EFF, VUL, BAR, BEN12, BEN34, and CUE. Note that the combination of resolving the communality issue and the EFA resulted in the removal of the experience (EXP) factor from the original proposed model. The EFA also resulted in the splitting of the original benefits factor (BEN) into two factors: BEN12, and BEN34. Both of these unexpected results will be addressed in the discussion section later in this paper.

Construct Validity and Reliability

We further examined internal consistency to test the interrelatedness of the data. To evaluate the reliability of the data, Cronbach Alpha coefficients were calculated for each latent variable. The acceptable value of Cronbach Alpha should be at least 0.70 (Nunnally and Berstein 1994). Table 2 summarizes the factor loadings and Cronbach Alpha values for each item. The factor loadings for all items are greater 0.5 and the Cronbach Alpha values for all factors are greater than 0.7.

Results

We conducted a two-step regression analysis to examine the effects of the IVs on the DV (BEH).

1. A multiple regression analysis was conducted using the SPSS calculated factor scores. The dependent variable was regressed on the six IVs (EXP was removed due to low factor loadings) to determine the main effects (Model 1).
2. The moderating variables, perceived severity was added into the regression model to examine the interaction effects of those IVs (Model 2).

We found that in the main model, SEV, BAR, and BEN34 are three significant determinants of our subjects' location service security behaviors (Table 3).

We found that in the interaction model, three factors (SEV, BAR and SEVxBEN12) are significant factors that impact our subjects' location service behaviors (see Table 3).

We also tested the model fit by gender (Table 3) and found that in the main model, BAR and SEV are two significant determinants in both gender groups. The significance level of BAR is higher in the female group compared to the male group. In the interaction model, BAR and SEV are two significant determinants for our female subjects' location behaviors. SEV has a significant influence on EFF, VUL, BAR, BEN12, and BEN34 in the male group. These substantial differences might be caused by the extremely unbalanced data set (25% male vs 75% female) but they do suggest that gender differences in LBS behaviors might exist. This warrants further exploration in the future.

	Model 1			*Model 2*		
Factors	Main Effects Coefficient			Main + Interactions Coefficient		
	Combined	Male	Female	Combined	Male	Female
SEV	***.374	**.501	**.301	***.322	-.169	*.233
EFF	.171	.026	.134	.127	-.074	.136
VUL	-.023	-.131	-.002	-.022	.019	-.025
BAR	***-.373	*-.390	***-.370	***-.396	-.216	**-.331
BEN12	.000	.192	-.101	-.023	-.007	-.069
BEN34	*-.194	-.251	-.105	-.168	.126	-.099
CUE	-.048	.007	-.007	.050	.391	.109
SEVxEFF				-.035	*.418	-.192
SEVxVUL				.047	*.791	-.098
SEVxBAR				-.023	**-.804	.065
SEVxBEN12				*.245	*.547	.211
SEVxBEN34				-.072	*-.433	.002
SEVxCUE				.069	.110	.102
R^2	.248	.431	.203	.312	.743	.292
Adjusted R^2	.208	.284	.145	.241	.584	.191

Table 3 - Regression Results

Discussion

Subjects' responses indicate that SEV, BAR and BEN34 are significant determinants of BEH. Supporting H7 and H2 while contradicting H1. The contradiction of H1 will be discussed in detail a little later in this section but it seems to indicate that, while students believe that being careful about LBS usage is effective in preventing LBS-related security incidents, they still use LBS on a regular basis.

Support for H7 indicates that students who believe that LBS-related incidents can have severe effects take care when using, or do not use LBS.

Support for H2 indicates that students who believe that there are substantial barriers to protecting themselves from the impact of LBS-related security incidents will not put in the effort required to protect themselves from potential LBS-related security incidents.

Construct Removal

It should be noted that two different steps in our analysis efforts led to the removal of the EXP construct from our initially hypothesized model. This drove us to examine the data set in more detail in an attempt to understand potential causes of this result. We found that the majority of responses for all three questions were NEVER (EXP1 – 61.4%, EXP2 – 75.0, EXP3 – 58.6%). If we add in the RARELY responses, we see that at least 77.9% of our survey respondents had little or no experience with LBS-related security issues (EXP1 – 82.1%, EXP2 – 80.0%, EXP3 – 77.9%). This explains the multi-collinearity in the data and raises two points about LBS-bases security research. First, LBS-related incidents might be rare while the second is a question about the usefulness of our population sample: students. The idea that younger generations tend to be heavier users of social media apps and services

than do the older generations might actually discount the latter concern and provide support for the first point: that these incidents might be rare and therefore this factor might not be appropriate when researching beliefs and intentions related to LBS-based security behaviors. In any case, because they happen so rarely in our sample population, they are not a factor with our limited and fairly homogeneous sample.

Splitting a Model Construct

Our analysis also resulted in the splitting of the perceived benefits factor (BEN) into two separate factors (BEN12, BEN34) based on the EFA results. A simple look at the questions gives insight into why this may have been necessary (Table 4). The first two items relate to the perceived benefits from awareness of the issues surrounding LBS use while the second two focus on the benefits of preventive behavior. Given these differences, it seems at least logical that the perceived benefits factor needs to be split. Another argument might be that students perceived the second set of questions as questions about their behavior instead of their perceptions about potential behavior. A third argument could be related to the notion that people might believe that the benefits of using LBS outweigh the risks associated with it. If this is the case, being aware of LBS based settings and being on the alert for LBS related risk (BEN1 and BEN2) are not likely to be clear drivers of usage or avoidance of LBS without taking the benefits/risks understanding into account. BEN3 and BEN4 could be indicators of user confidence in which might explain why the BEN34 construct was found to be a significant driver of usage of LBS, contradicting our hypothesis that BEN34 would be a significant driver of avoiding LBS. The question as to how people perceive the benefits and risks of LBS usage is one that should be explored in the future.

Contradicting a Hypothesis

The regression coefficient on BEN34 is negative in both the main effects and interactions models (significant only in the main effects model). BEN12's coefficient is negative or zero in the models and is not statistically significant in either model.

Item	*Question*
BEH1	I post photos to online services/websites with geotagging/location data embedded.
BEN1	Being on the alert for geotagging or location tracking is effective in preventing geotagging or location tracking problems.
BEN2	Being aware of/managing geotagging/location tracking settings is effective in preventing geotagging/location tracking problems
BEN3	Disabling geotagging/location services when you don't need them is effective in preventing geotagging or location tracking problems.
BEN4	Exercising care when using location services is effective in preventing geotagging or location tracking.

Table 4 - Perceived Benefits Survey Items

This negative coefficient contradicts our hypothesis that perceived benefits of practicing LBS security behaviors would, essentially, prevent usage of LBS (H1). This seems to imply that the more the subjects agree that you can protect yourself in these situations, the more they use the services. A more detailed look at the survey responses supports this idea: there is a significant, negative relationship between BEN3 and BEH1 ($r = -.140$, $p < .05$, see Table 4 for the survey questions). This correlation tells us that the more subjects believe that disabling LBS can effectively prevent LBS-related security issues, the more they post photos "with geotagging/location data embedded". While they believe disabling LBS features would be a good behavior, they do not disable them. They must feel that the risk does not outweigh the benefit or they simply do not believe that using LBS is a risky behavior. This might be why EFA suggested we eliminate the experience factor (EXP) from the model. This might also be impacted by whatever caused BEH2 ("I purposely avoid situations where I believe location information may be recorded") to be dropped during EFA for not loading high enough on any one factor. Could this be an indicator that

students find it difficult to disable LBS, or won't invest the time to disable LBS on their devices? The fact that perceived barriers to entry (BAR) is a significant factor in reported behaviors might support that idea.

One other argument that could be made about the contradictory results in re H1 is that the subjects do not understand location based services. The population of students sampled had completed the introduction to computing course the semester before participating in the survey. This course includes discussions of location based services so we expect these subject to have a basic understanding of the concept.

Limitations

There are two limitations that must be acknowledge regarding this research. The first is the obviously limited sample population. While an argument can be made that this is an entirely appropriate sample given this generations widespread use of multi-media driven (photographs and videos) social media, the authors must admit that an examination of a broader and more diverse population could add more detail and significance to the findings. The second is that, while the survey was built from prior surveys in IT security and healthcare, some of the issues with factor loadings could be caused by weaknesses in the survey itself.

Implications for Research, Education, and Practice

There are at least two implications of these findings for the research community. First, the notion that students appear to believe that LBS-related incidents can have severe impacts but still use LBS is an intriguing one and should be explored. Why do people ignore that type of risk? What do they understand about it? Is there something bigger in social media usage that drives people to ignore the associated risks? The limited number of significant factors in the model could be an indicator that better models are needed, particularly since this paucity of significant factors can be seen across several applications of the HBM in IT security and privacy research (Claar et al. 2013; Ng et al. 2009; Schymik and Du 2017). In general, more research into preventive IT security and privacy behaviors is certainly warranted.

Implications for education focus around getting students more exposure to the concept of LBS. General Education courses intended to introduce computing in general or IT security and privacy to students can add more specifically focused sections to their curricula that clearly define LBS and provide specific detail on its usage and configuration could help students better understand the risk that our results indicate they appear to be ignoring. Similar concerns exist regarding training in professional environments as it is not hard to imagine how LBS-related incidents can impact the workplace in certain scenarios.

Conclusion

A survey was developed based on the HBM and conducted at a public university to understand students' intentions and behaviors when using location-based services (LBS) on their mobile devices. Perceived severity, barriers to entry, and perceived benefits were found to have a significant impact on students' LBS security behaviors.

Understanding people's intentions and behaviors when using mobile technology is a first step towards the goal of providing effective education and policies on security and privacy related to the use of such technologies. This study sheds light on how educators and IT organizations can better educate students and professionals on how to protect their security and privacy when using LBS.

References

Champion, V. L. 1984 "Instrument Development for Health Belief Model Constructs," *Advances in Nursing Science* (6:3), pp.73-85.

Claar, C. L., and Johnson, J. 2010. "Analyzing the Adoption of Computer Security Utilizing the Health Belief Model," *Issues in Information Systems* (11:1), pp. 286-291.

Claar, C. L. and Johnson, J. 2012. "Analyzing Home PC Security Adoption Behavior," *Journal of Computer Information Systems* (52:4), pp.20-29.

Claar, C. L., Shields, R. C., Rawlinson, D., and Lupton, R. 2013. "College Student Home Computer Security Adoption," *Issues in Information Systems* (14:2), pp. 139-148.

Field, A. 2013. *Discovering Statistics Using Ibm Spss Statistics, 4th Ed.* Sage Publications Ltd.

Figueiras, M. J. and Alves, N. C. 2007. "Lay perceptions of serious illnesses: An adapted version of the Revised Illness Perception Questionnaire (IPQ-R) for healthy people," *Psychology and Health 22*, pp.143-158.

Fowler, B. 2018. "How to Turn Off Location Services on Your Smartphone." *Consumer Reports* Retrieved January 17, 2019, from https://www.consumerreports.org/privacy/how-to-turn-off-location-services-on-your-smartphone/

Huddleston, J. 2018. "Are You Sharing Your Location on Social Media?" Retrieved January 11, 2019, from http://www.wbrc.com/2018/09/07/are-you-sharing-your-location-social-media/

Jang, S., and Lee, C. 2018. "The Impact of Location-Based Service Factors on Usage Intentions for Technology Acceptance: The Moderating Effect of Innovativeness," *Sustainability* (10:6).

Janz, N. B., MH. 1984. "The Health Belief Model: A Decade Later," *Health Education Quaterly*), pp. 1-48.

Logan, R., Hensel, B., and Leshner, G. 2019. "Chihr - Consumer Health Informatics Research Resource." Retrieved January 17, 2019, from https://chirr.nlm.nih.gov/index.php

Mao, E., and Zhang, J. 2013. "The Role of Privacy in The Adoption of Location-Based Services," *Journal of Information Privacy & Security* (9:2), pp. 40-59.

Moss-Morris, R., Weinman, J., Petrie, K. J., Horne, R., Cameron, L. D. & Buick, D. 2002. "The revised illness perception questionnaire (IPQ-R)," Psychology and Health 17, pp.1-16.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:4), pp. 815-825.

Nunnally, J., and Berstein, L. 1994. *Psychometric Theory*. New York: McGraw-Hill Higher Ed.

Palos-Sanchez, P. R., Hernandez-Nogollon, J. M., and Campon-Cerro, A. M. 2017. "The Behavioral Response to Location Based Services: An Examination of the Influence of Social and Environmental Benefits, and Privacy," *Sustainability* (9:11).

Rosenstock, I. M. 1974. "The Health Belief Model and Preventive Health Behavior," *Health Education Monographs* (2:4), pp. 354-386.

Schymik, G., and Du, J. 2017. "Student Intentions and Behaviors Related to Email Security: An Application of the Health Belief Model," *The Conference on Information Systems Applied Research*, Austin, Texas, USA.

Valentino-DeVries, J., Singer, N., Keller, M. H., and Krolik, A. 2018. "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret." Retrieved Januеary 11, 2019, from https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

Williams, C., Wynn, D., Madupalli, R., Karahanna, E., and K. Duncan, B. 2014. "Explaining Users' Security Behaviors with the Security Belief Model," *Journal of Organizational and End User Computing* (26:3), pp. 23-46.

Yun, H., Han, D., and Lee, C. 2013. "Understanding the Use of Location-Based Service Applications: Do Privacy Concerns Matter?," *Journal of Electronic Commerce Research* (14:3), pp. 215-230.

Zhou, T. 2013. "Understanding User Adoption of Location-Based Services from a Dual Perspective of Enablers and Inhibitors," *Information Systems Frontiers* (17:2), pp. 413-422.

Zhou, T. 2015. "Understanding User Adoption of Location-Based Services from a Dual Perspective of Enablers and Inhibitors," *Information Systems Frontiers* (17), pp. 413-422.