Behavior Control-Based Approach to Influencing User's Cybersecurity Actions Using Mobile News App

Vincent Lombardi
Gonzaga University
Spokane, USA
vlombardi@zagmail.gonzaga.edu

Sarah Ortiz
Willamette University
Salem, USA
sarahqortiz23@gmail.com

Jen Phifer
New Mexico Tech
Soccorro, USA
jen.phifer@nmt.edu

Tomas Cerny
Baylor University
Waco, USA
tomas_cerny@baylor.edu

Dongwan Shin
New Mexico Tech
Soccorro, USA
dongwan.shin@nmt.edu

ABSTRACT

In this paper, we propose that the theory of planned behavior (TPB) with the additional factors of awareness and context-based information can be used to positively influence users' cybersecurity behavior. A research model based on TPB is developed and validated using a user study. As a proof-of-concept, we developed a mobile cybersecurity news app that incorporates context-based information such as location, search history, and usage information of other mobile apps into its article recommendations and warning notifications to address user awareness better. Through a survey of 100 participants, the proposed research model was validated, and it was confirmed that context-based information positively influences users' awareness in cybersecurity.

ACM Reference Format:
Vincent Lombardi, Sarah Ortiz, Jen Phifer, Tomas Cerny, and Dongwan Shin. 2021. Behavior Control-Based Approach to Influencing User's Cybersecurity Actions Using Mobile News App. In *Proceedings of ACM SAC Conference (SAC'21).* ACM, New York, NY, USA, Article 4, 4 pages. https://doi.org/10.1145/3412841.3442103

1 INTRODUCTION

The growing number of online users, diversity of devices, and easier access to the Internet provide great opportunities for cyber attackers, and users are becoming aware of the potential consequences of cyber attacks. According to the Identity Theft Resource Center 2018 report, "hacking was the most common form of a data breach in 2018, totaling 482 data breaches and exposing 16 million (16,698,248) consumer records" [1]. Of the data breaches caused by hacking, phishing was the most common approach to breaking into the system. The phishing attack, a type of semantic attacks [17], is also becoming harder to detect as hackers become more sophisticated. The lack of a user's ability to detect and recognize phishing attempts has a direct negative impact on companies and the online community as it poses a risk to everyone's private data.

The intricacy and sophistication of semantic attacks tend to make users the most vulnerable part in securing computer systems, and understanding their mental model of information processing could help mitigate the vulnerability. According to a recent work [9], a security application whose main feature was enhanced with an analysis of user behaviors based on reasoned action approach (RAA) [2] could help users make more informed decisions in cybersecurity. Importantly, the study which was focused on developing and validating a mental model based on RAA with a new additional component called *Awareness* concluded that the user awareness impacts the cybersecurity behavior of the user. In this paper, we extended the prior work in such a way that users can be influenced and thus better prepared for cybersecurity-related actions with their *context*-based information. For that purpose, we proposed a model adapted from the theory of planned behavior (TPB) [3] with the additional factors of awareness and context-based information. Through a user study, the proposed model was validated, and it was confirmed that context-based information positively influences users' awareness in cybersecurity. In addition, this paper discussed as a proof-of-concept implementation a mobile cybersecurity news application called *CyberAware* that incorporates context-based information such as location, search history, and usage information of other mobile applications into its article recommendations and warning notifications to address user awareness better.

2 THEORY OF PLANNED BEHAVIOR

Icek Ajzen introduced the Theory of Planned Behavior (TPB) in 1985, building off of the Reasoned Action Approach (RAA) with the added variable of "perceived behavioral control" [3]. RAA supposes that a person's intention is a precursor to their behavior, and their subjective norms and attitudes directly influence their behavioral intention. The added "perceived behavioral control" to TPB refers to a person's belief in their ability to perform a task or behavior. The "perceived behavioral control" directly impacts a person's intention to perform a behavior, meaning if they have a low "perceived behavior control," they are less likely to intend to perform the behavior, making them less likely to do the behavior. For example, suppose they do not believe that they can accurately identify a phishing

SAC'21, March 22-26, 2021, Virtual Event, South Korea

ACM ISBN 978-1-4503-8104-8/21/03…$15.00
https://doi.org/10.1145/3412841.3442103

attempt. In that case, they are less likely to intend to identify a phishing attempt, and then they will not try to identify a phishing attempt. In TPB, the main factors that affect intention are their subjective norms, attitude, and their perceived behavioral control, and the added perceived behavioral control allows for behavior predictions in scenarios where people may not have the control or ability to perform certain tasks [4].

TPB has been used to test the user's intention to perform certain tasks to mitigate cybersecurity risks in the past. For instance, there were TPB-based studies that measured participants' intention to use anti-malware [16] and participants' intention to comply with information security policies [5]. In addition, additional variables to TPB were suggested to be more capable of accurately predicting the user's intention to predict positive cybersecurity behaviors. For instance, 16 additional variables were added to TPB to more accurately predict the intention of workers to comply with the information security policy [15]. However, our proposed approach is different from these modified models since we identified and incorporated the unique variable of the context-based information that has a positive impact on both user intention and user behavior.

3 OUR APPROACH

3.1 The Research Model

Based on and extended from TPB, our research model has seven variables, as shown in Figure 1. The model has attitude, subjective norms, perceived behavioral control, intention, behavior, awareness, and *context-based information*. The first five variables were unchanged from TPB, while the last two variables (in red colored font) were added for our research purpose. The *impact* relationship between the variables are depicted by a line with an arrow (unidirectional or bi-directional). For instance, behavior is impacted by the intention to perform the behavior and is also impacted by the perceived behavior control over the action in both TPB and our proposed model. The strongest relationship between variables is typically the relationship between intention and behavior. The additional variable of context-based information should increase the amount of awareness a person has due to using the knowledge that is relevant to their experience and surroundings. Using context to make information more relevant to people has been shown to improve their knowledge of the subject more than non-contextual information in [7].

3.2 Hypotheses

In order to test whether the newly added components (awareness and context-based information) impact behavior in cybersecurity, we developed four hypotheses as follows:

- *Hypothesis 1: Users' intention to protect themselves from cyber-attacks has a positive influence on users' cybersecurity behavior.*
- *Hypothesis 2: Users' awareness of the consequence and the need for cybersecurity has a positive influence on their intention to protect themselves from cyber-attacks.*
- *Hypothesis 3: Users' awareness of the consequence and the need for cybersecurity has a positive influence on users' cybersecurity behavior.*

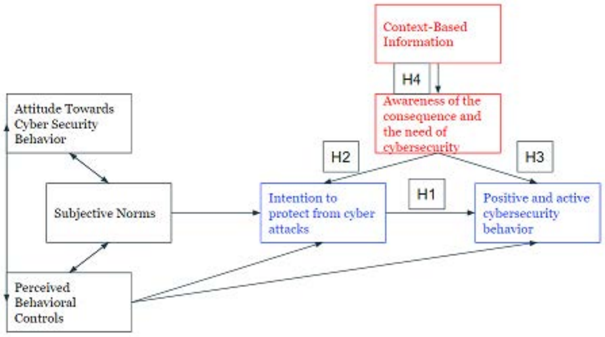

Context-Based Information
H4
Awareness of the consequence and the need of cybersecurity
Attitude Towards Cyber Security Behavior
H2
H3
Subjective Norms
Intention to protect from cyber attacks
H1
Positive and active cybersecurity behavior
Perceived Behavioral Controls

Figure 1: Proposed Research Model with Labeled Hypotheses.

- *Hypothesis 4: Users' context-based information has a positive influence on users' awareness of the consequence and the need for cybersecurity.*

The hypotheses developed are depicted in Figure 1, along with the model elements that they are concerning. Note that we did not develop hypotheses associated with other model elements such as attitude, subjective norm, and perceived behavioral control, due to the fact that there existed prior research that developed and tested their relationship [13] and those variables were not the main focus of our research.

4 OUR USER STUDY

The survey was conducted on Amazon Mechanical Turk, where 100 individuals participated in the survey during August of 2019. Of the participants 52 were identified as male and 48 identified as female. The average age of the participants was 35 years old. Over half of the participants reported being moderately familiar with topics of cybersecurity. From these 100 participants, 34 were removed as outliers. The remaining 66 participant's answers were analyzed using Microsoft Excel and IBM SPSS Statistics, and the model fit was tested using warpPLS 6.0 [11].

The survey questionnaires were designed to test the four hypotheses, which pertain to *Context-Based Information*, *Awareness of the Consequences and the Need of Cybersecurity*, *Intention to Protect from Cyberattacks*, and *Positive and Active Cybersecurity Behavior*, as shown in Figure 1. Each of these four was measured using six statements that address the area of interest. Each of the statements was measured using a 5 point Likert Scale: 1- Strongly Agree, 2 - Agree, 3 - Neutral, 4 - Disagree, 5 - Strongly Disagree. The four items of our research model are:

- **Contextual Based Information** refers to information based on the user's location, frequency of mobile application usage, and wireless network connections.
- **User's awareness** of the consequences and need for cybersecurity pertains to two separate factors. The first is aimed at assessing the user's knowledge of the risks they face online. The statements focus on a specific threat vector: WiFi networks, phishing attacks, and shoulder surfing. The second is

aimed at their awareness of current cybersecurity services and their ability to customize these content.

- **User's intention** to protect themselves from cyber-attacks is measured in two different directions. The first being the intention to protect one's personal or work data. These statements were adapted from Soderlund and Ohman's work on Intentions in Consumer Research [10]. The second is the intention to use cybersecurity software and respond to information given from the software.
- **User's Behavior** that is positive and active towards cybersecurity is measured in two areas of interest. First, the area of positive cybersecurity behavior will mitigate their risks online by choosing not to engage in poor cybersecurity practices. The second is an active behavior towards cybersecurity where a user will seek cybersecurity software, then listen and respond to any warnings received by the software.

4.1 Analysis

After outliers were removed from the data set, the reverse coded questions were renumbered to reflect the response accurately. Reliability analysis tests were conducted to test the overall consistency of those research questionnaires in each of the areas. We used the Cronbach's Alpha and Composite Reliability (CR) for the reliability and validity testing, as shown in Table 1. The Cronbach's Alpha for Intention and Awareness are above the acceptable > 0.7 [12]. Behavior is a bit lower but still within the range of acceptability of > 0.6 given by Haris et. all [8]. The Context construct has the lowest Cronbach's Alpha of .495, which is below the acceptable values.

Table 1: Reliability and Validity

Categories	***Cronbach's Alpha***	***Composite Reliability***
Context	0.495	0.724
Awareness	0.745	0.832
Intention	0.837	0.880
Behavior	0.641	0.811

CR is another measure of reliability in addition to Cronbach's Alpha, and its measurements were calculated using SPSS factor analysis with a Varimax rotation and an extracted Eigenvalue of 0.9. All of the CR values are within the acceptable range of > 0.7, and thus showing the internal consistency of our measurement.

4.2 Results

For the purpose of testing our hypotheses, we used the structural equation modeling (SEM) approach. A SEM model was constructed using warpPLS 6.0, as shown in Figure 2, and it was processed using the bootstrap resampling for 100 iterations. Each oval in the model corresponds to the element in our research model: *Context* is Context-Based Information, *Aware* is Awareness of the consequence and need of cybersecurity, *Intent* is Intention to protect from cyber attacks, and *Behavior* is Positive and Active cybersecurity behavior. As shown in Figure 2, there is a statistically significant ($p < .01$) relationship between Context-Based Information and Awareness, Awareness and Intention, and Intention and Behavior with path coefficients of $\beta = 0.54$, $\beta = 0.70$, and $\beta = 0.50$. These results validate our hypotheses (Hypothesis 1, 2, and 4). However, there is a statistically insignificant relationship ($p = .11$) between Awareness and Behavior, which invalidates Hypothesis 3. There could be several possible reasons for this, including a small sample size and a less number of statements (6 instead of 10) than SEM is recommended to have. The effect of context on awareness has $R^2 = 0.29$ or 29% of the variance of user's cybersecurity awareness, which is statistically significant. The effect on intent by awareness has $R^2 = 0.49$ or 49%, which is also significant. The user's cybersecurity behavior also has $R^2 = 0.49$, which is determined by intent and awareness.

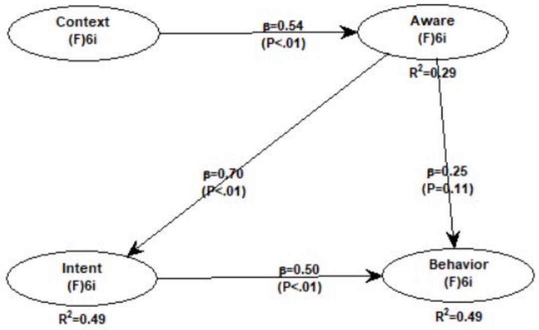


Figure 2: SEM Model for testing our hypotheses. Created with warpPLS 6.0.

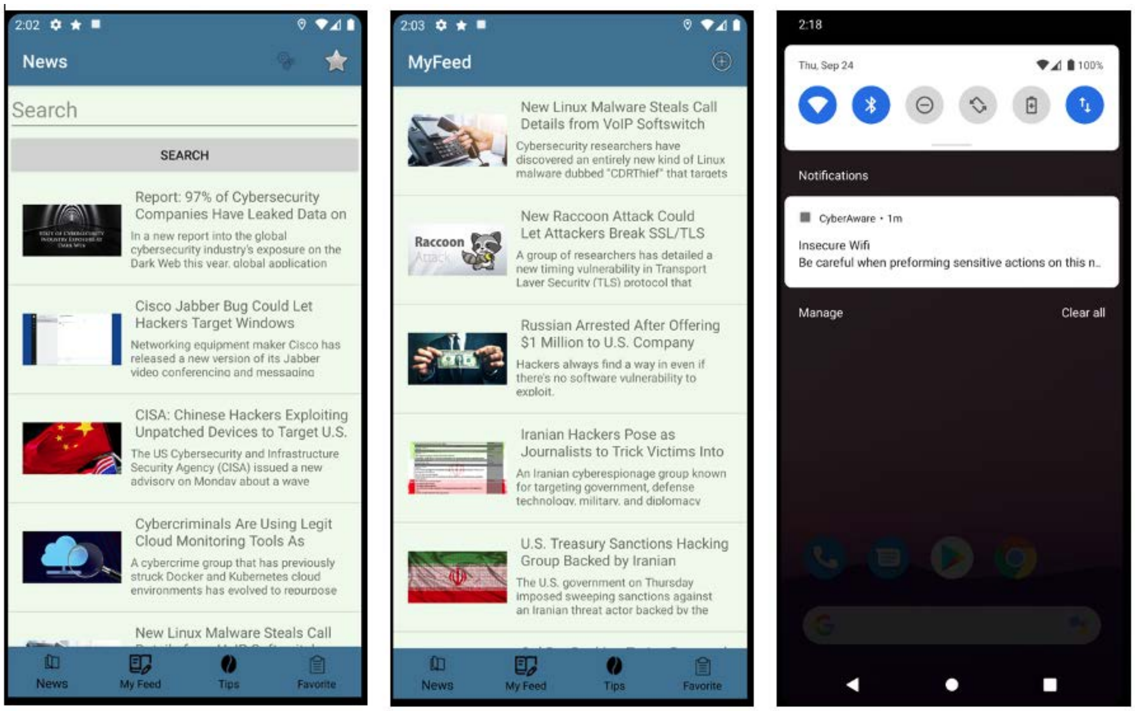
Using warpPLS, the model was tested for the fit and quality indices were calculated to show how relevant and effective the model is. The test results show that the Hypotheses 1,2, and 4 are validated and the addition of Context-Based Information to our proposed model can predict an increase in Awareness and can influence users' behavior through impacting users' intent.

5 CYBERAWARE

As a proof-of-concept, a mobile app, called *CyberAware*, which could provide users with both effective warnings and relevant cybersecurity information was developed. This mobile news app incorporates context-based information such as user location, search history, and usage information of other mobile apps into its article recommendations and warning notifications to address user awareness better. We believe that a mobile app is the most effective outlet for this purpose since mobile devices are widely available and people are almost always carrying their mobile devices with them. *CyberAware* was developed on Android OS, as shown in Figure 3.

6 DISCUSSION AND CONCLUSION

In this paper, we presented an approach based on the Theory of Planned Behavior (TPB) to study how to persuade users to be more engaged in cybersecurity, thereby helping them make better cybersecurity decisions when they need to be made. A research model extended from TPB with the additional factors of Awareness and



Report: 97% of Cybersecurity Companies Have Leaked Data on

In a new report into the global cybersecurity industry's exposure on the Dark Web this year, global application

Cisco Jabber Bug Could Let Hackers Target Windows

Networking equipment maker Cisco has released a new version of its Jabber video conferencing and messaging

CISA: Chinese Hackers Exploiting Unpatched Devices to Target U.S.

The US Cybersecurity and Infrastructure Security Agency (CISA) issued a new advisory on Monday about a wave

Cybercriminals Are Using Legit Cloud Monitoring Tools As

A cybercrime group that has previously struck Docker and Kubernetes cloud environments has evolved to repurpose

New Linux Malware Steals Call

New Linux Malware Steals Call Details from VoIP Softswitch

Cybersecurity researchers have discovered an entirely new kind of Linux malware dubbed "CDRThief" that targets

New Raccoon Attack Could Let Attackers Break SSL/TLS

A group of researchers has detailed a new timing vulnerability in Transport Layer Security (TLS) protocol that

Russian Arrested After Offering $1 Million to U.S. Company

Hackers always find a way in even if there's no software vulnerability to exploit.

Iranian Hackers Pose as Journalists to Trick Victims Into

An Iranian cyberespionage group known for targeting government, defense technology, military, and diplomacy

U.S. Treasury Sanctions Hacking Group Backed by Iranian

The U.S. government on Thursday imposed sweeping sanctions against an Iranian threat actor backed by the

CyberAware • 1m

Insecure Wifi

Be careful when preforming sensitive actions on this n...

Figure 3: CyberAware: Main News Feed (leftmost), Personal News Fees - with *Cryptography* and *Malware* as topics selected (center), and Notification when connected to a non-whitelisted, public WiFi (rightmost)

Context-Based Information was proposed and validated, along with hypotheses that show the new variable of Context-Based Information is a good determinant for users' awareness of the consequence and need of cybersecurity.

This research is by no mean complete. The result of this research clearly shows that there is a positive, indirect link between Context-Based Information and Behavior. More importantly, it shows that Context-Based Information has a strong influence on Awareness and can be used as a way to educate users on cybersecurity issues more effectively. Our immediate future work will focus on diversifying context-based information so that users can get more personalized and engaging learning experiences from *CyberAware*. We also plan to have a user study to test the efficacy and effectiveness of the mobile app.

ACKNOWLEDGEMENT

This work was partially supported at the Secure Computing Laboratory at New Mexico Tech by the grants from the National Science Foundation (1757945, 1833630).

REFERENCES

[1] 2018 End of Year Data Breach Report (pp. 1-17, Rep.). (2019). San Diego, CA: Identity Theft Resource Center.

[2] Fishbein, M. Ajzen, I. (2010). Predicting and changing behavior: The Reasoned Action Approach. New York: Taylor Francis.

[3] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211.

[4] Ajzen, Icek. (2012). The theory of planned behavior. 10.4135/9781446249215.n22.

[5] Brown, D. A. (2017). Examining the Behavioral Intentions of Individuals Compliance with Information Security Policies. Walden University ScholarWorks. Retrieved August 3, 2019.

[6] Fornell, C., and Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research (18:1), pp. 39-50.

[7] Gutwill-Wise, J. P. (2001). The Impact of Active and Context-Based Learning in Introductory Chemistry Courses: An Early Evaluation of the Modular Approach [Abstract]. Journal of Chemical Education. Retrieved August 7, 2019.

[8] Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis: Pearson College Division.

[9] Liljestrand, I., Gonzales, M., & Shin, D. (n.d.). Developing a Mental Model for use in the Context of Cyber Security.

[10] Magnus Soderlund and Niclas Ohman (2005) ,"Intentions Are Plural: Towards a Multidimensional View of Intentions in Consumer Research", in E - European Advances in Consumer Research Volume 7, eds. Karin M. Ekstrom and Helene Brembeck, Goteborg, Sweden : Association for Consumer Research, Pages: 410-416.

[11] Ned Knock. 2018. WarpPLS User Manual: Version 6.0. (August 2018).

[12] Nunnally, J. C. (1978). Psychometric theory: New York : McGraw-Hill, c1978. 2d ed.

[13] Octav-Ionut, Macovei. (2015). Applying the Theory of Planned Behavior in Predicting Pro- environmental Behaviour: The Case of Energy Conservation. Acta Universitatis Danubius. íconomica. 11. 15-32.

[14] Pham, K. (n.d.). PushNotification [Computer software]. Retrieved from https://github.com/onmyway133/PushNotifications

[15] Sommestad, Teodor & Karlz©n, Henrik & Hallberg, Jonas. (2017). The Theory of Planned Behavior and Information Security Policy Compliance. Journal of Computer Information Systems. 1-10. 10.1080/08874417.2017.1368421.

[16] Vafaei-Zadeh, A., Thurasamy, R. and Hanifah, H. (2018), "Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior", Kybernetes, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/K-05-2018-0226

[17] Schneier, Bruce. (2000) "Semantic attacks: The third wave of network attacks," CryptoGram Newsletter.

[18] M. Wu, R. C. Miller, and S. L. Garfinkel. (2006), "Do security toolbars actually prevent phishing attacks?," In Proceedings of the SIGCHI conference on Human Factors in computing systems, CHI '06, pages 601–610, New York, NY, USA, ACM.