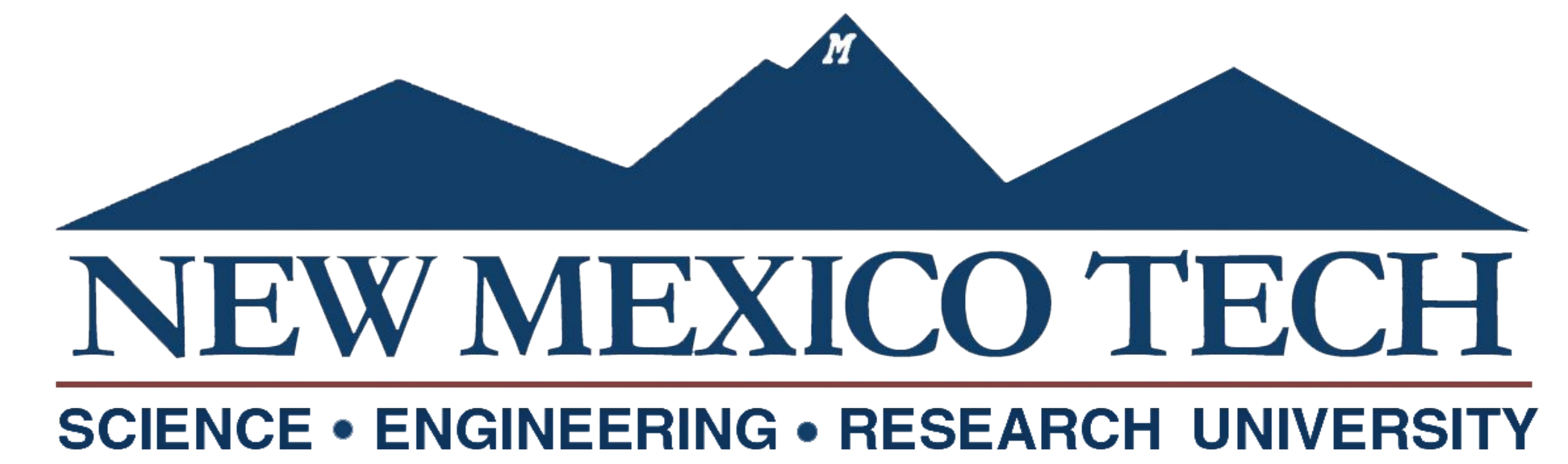




National
Science
Foundation
CNS-1757945

Behavior Control-Based Approach to Influencing User's Cyber Security Actions

Vincent Lombardi¹, Sarah Ortiz², Dongwan Shin³



Computer Science, Gonzaga University¹, Computer Science, Willamette University², Computer Science and Engineering, New Mexico Tech³

Introduction

The most vulnerable part of any system is the user. This is due to the fact that social engineering is the easiest and most effective way to break into any system. Not necessarily because the user is incompetent or not intelligent, but because they may be unaware of the risks they face and the consequences of not protecting themselves or their data. Because user's are the most vulnerable part of the system, it is not only in the best interests of companies to secure user behavior, it is also in the user's interest to secure their own behavior because their data is also at risk.

Knowing that user's are at risk how can we influence their behavior to more positive cyber security actions? In this project, we addressed that question in two ways. First, we developed an application, CyberAware, for both Android and Apple mobile OS's. The goal of this application is to provide real time information to the user about cybersecurity issues around them and provide warnings based off of their application usage, location, and network connections. Second, we conducted a survey to test our research model, which is adapted from The Theory of Planned Behavior, includes Macovei Octav-Ionut's addition of "Awareness" in the model, and adds in the portion of Context-Based Information. The goal of the model is to determine if context-based information is a strong determinant for user's awareness which in turn determines their intent to protect themselves and their cybersecurity behavior.

Hypotheses

- ❖ 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 of cybersecurity has a positive influence on their intention to protect themselves from cyber attacks.
- ❖ Hypothesis 3: Users' awareness of the consequence and the need of cybersecurity has a positive influence on users' cybersecurity behavior.
- ❖ Hypothesis 4: Users' context-based information has a positive influence on users' awareness of the consequence and the need of cybersecurity.

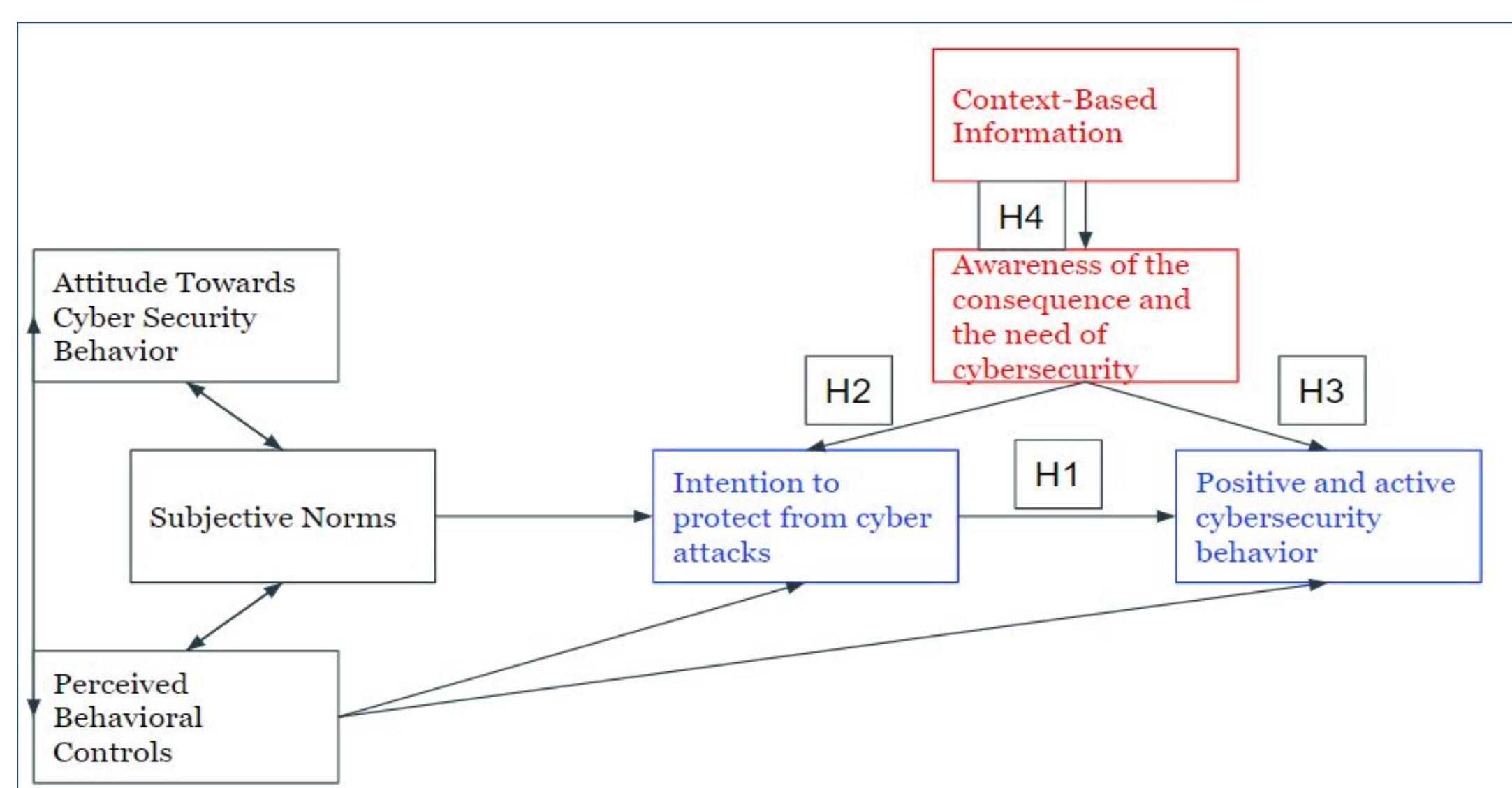


Figure 1: Planned Behavior Model with Awareness and Context-Based Information. Hypotheses located where they fit in the model following the order given above.

Implementation

- ❖ News Source:
 - News API: Free online API with 30,000+ sources.
 - Used 19 sources that had cybernews or a tech focus: ABC News, CNN, BBC, Bloomberg, Crypto Coins News, Fox News, Google News, Tech Crunch, Tech Radar, NYT, The Verge, and Wired.
- ❖ Notifications:
 - Article Recommendation Notifications:
 - Based off of user's search history and interests to determine which articles they might be interested in as seen in Figure 2.
 - Warning Notifications:
 - Using APNS and FireBase send notifications when users are accessing separate applications or when connecting to insecure networks as seen in Figure 3.

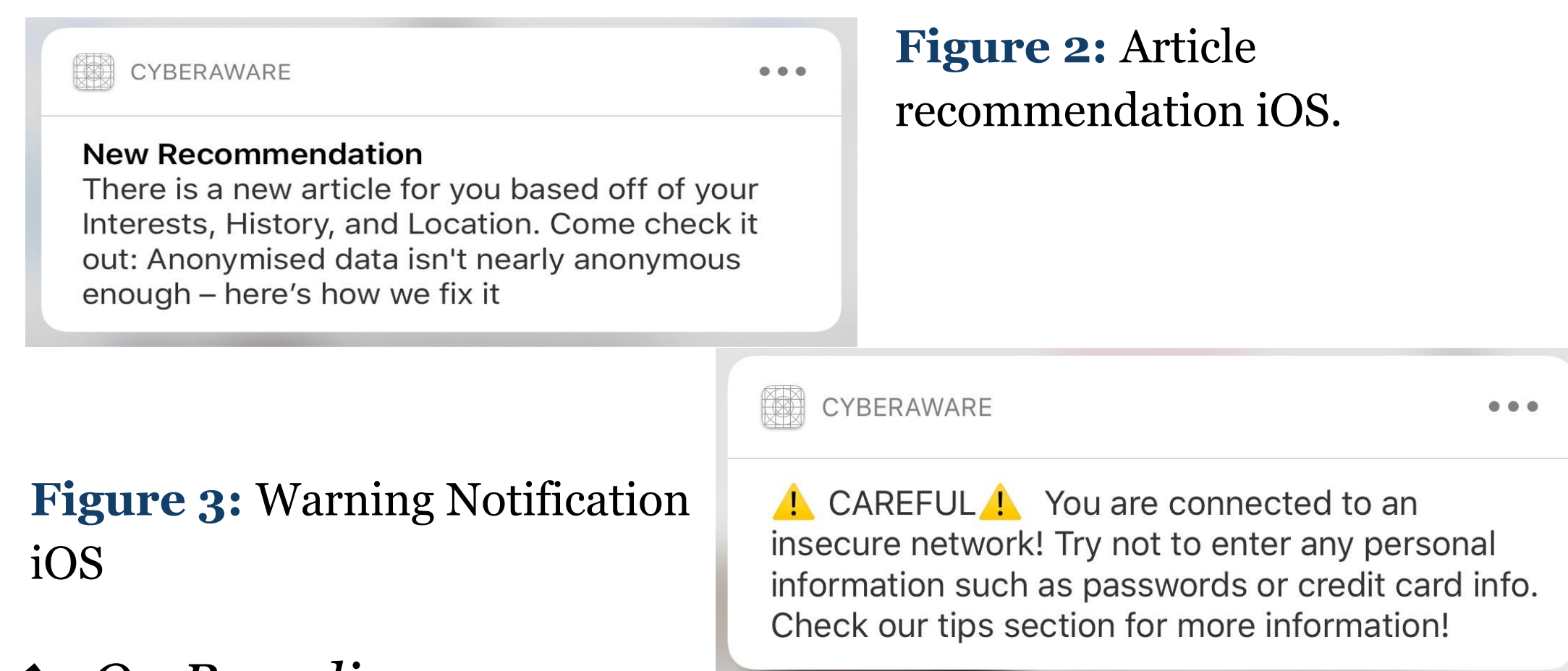


Figure 3: Warning Notification iOS

- ❖ On Boarding:
 - The Onboarding process collects user information to use for recommendations and progress tracking as seen in Figure 4.



Figure 4: Figures a-b are the Android onboarding process and c-e are the iOS onboarding process.

- ❖ Main Application:
 - Includes a main news feed, personalized news feed, CyberTips section, the ability to save articles, and customizable settings as seen in Figure 5.

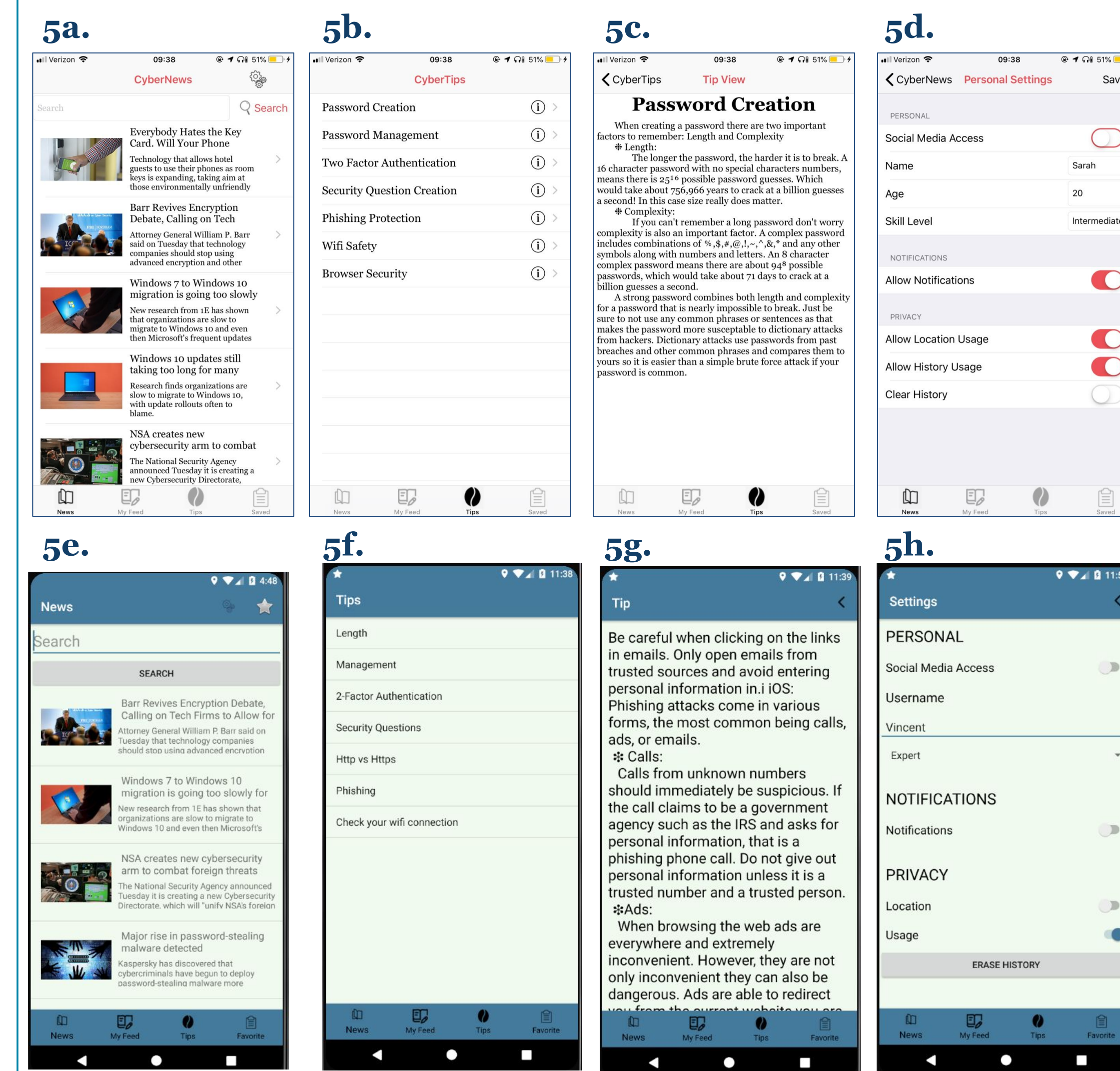


Figure 5: Figures a-d show the iOS application's a) Main Feed, b) CyberTips, c) Tip View, d) Settings. E-h show the Android application's e) Main Feed, f) CyberTips, g) Tip View, h) Settings.

Testing

- ❖ Survey:
 - Using Amazon Mechanical Turk we surveyed 100 people to test the four hypotheses in Figure 1.
 - Context Based Information.
 - Awareness of the consequence and need of cybersecurity.
 - Intention to protect from cyber attacks.
 - Behavior that is active and positive towards cybersecurity.
 - Participant information:
 - Of the one hundred participants 52% were male and 48% were female.
 - The average age of the participants was 35 years old.
 - More than half reported to be moderately familiar with cybersecurity.
 - The survey was separated into four categories based off of the hypotheses.
 - Each category had six questions and responses were measured on a Likert scale.

Results

Out of the 100 participants thirty four were marked as outliers and removed. From this we used the 66 participants data to fit our model seen in Figure 6. There is a statistically significant ($p < .01$) relationship between Context-Based Information and Awareness, Awareness and Intention, and Intention and Behavior. Therefore, Hypotheses 1,2, and 4 are accepted. Hypothesis 3 is rejected because the relationship between Awareness and Behavior is statistically insignificant ($p = .11$).

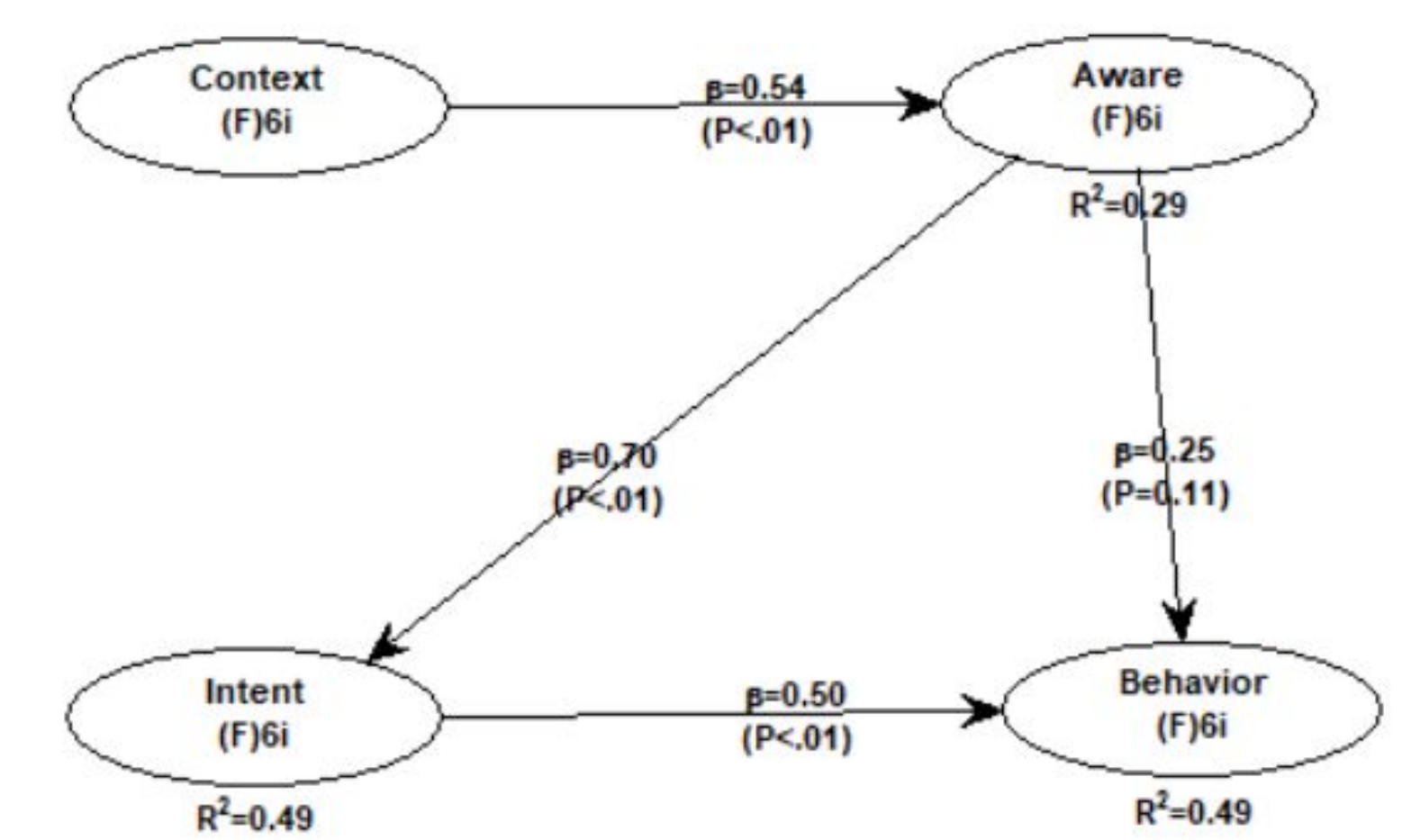


Figure 6: Behavior Model with statistical significance.

Conclusion and Future Work

Given that hypotheses 1, 2, and 4 are statistically significant they are accepted. Therefore, we can conclude that our addition of Context-Based Information to the model is an accurate determinant for user's Awareness. The relationship from Awareness to Intention and Intention to Behavior shows that the user's awareness can have an indirect, positive influence on their cyber security behavior. The application developed works as a proof of concept to demonstrate how Context-Based Information can be implemented in a mobile application.

Future work for this project includes fully implementing the application, conducting a user study testing the effectiveness of the application, publishing the application to the Apple and Google Stores, and conducting a more refined survey for further model testing.

References

- ❖ Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.
- ❖ Liljestrand, I., Gonzales, M., & Shin, D. (n.d.). Developing a Mental Model for use in the Context of Cyber Security.
- ❖ Octav-Ionut, Macovei. (2015). Applying the Theory of Planned Behavior in Predicting Pro- environmental Behaviour: The Case of Energy Conservation. *Acta Universitatis Danubius. Œconomica*. 11. 15-32.

Contact Information

1. Vincent Lombardi, vhl2@live.com
2. Sarah Ortiz, sarahqortiz23@gmail.com
3. Dongwan Shin, dongwan.shin@nmt.edu

This work is supported by the National Science Foundation under grant no. CNS-1757945