# Improved User Security Through Graphical Feedback

Justice Juraschek
Computer Science and Engineering
Taylor University
Upland, Indiana
jjurasch@cse.taylor.edu

Dannie M. Stanley
Computer Science and Engineering
Taylor University
Upland, Indiana
ds@cse.taylor.edu

## ABSTRACT

A plethora of methods of being secure are available to end-users, yet there is a lack of adoption of said methods. We argue that one of the primary reasons for this is the absence of proper feedback within security-sensitive situations. We believe that a graphical representation of security-related consequences can positively influence security-sensitive user decisions.

To test this hypothesis, we created two versions of an interactive fiction time-management game. One version had a graphical representation of security-related consequences while the other did not. The game consists of a series of decisions with some of those decisions are security-sensitive. The overt objective of the game is to complete a todo-list within time constraints. The participants were split between two groups: one that received the graphic and one that did not. The analysis found that no real change occurred in spite of the differences between game versions. On average, three out of eight of the security-related questions were answered in a secure manner.

We conclude that while our findings did not support our hypothesis, the experiment needs to be repeated with several factors changed in order to receive conclusive results. We believe the test needs to be run with more participants, more in-game security-sensitive scenarios, repeated in-game security-sensitive scenarios, a more naturally motivating graphical aid, and for a longer duration.

## 1. INTRODUCTION

End users are placed in potentially security compromising situations every day of their lives [5]. In those situations, end users typically do not see an element of risk and are unmotivated to use the protective tools given to them by society [5]. This could be detrimental in a variety of scenarios, especially in a missions-based environment. The manner in which a missionary's security is handled has the possibility of leading to life or death situations.

A survey was conducted by the National Cyber Security AOL in 2004 that discovered two thirds of end users had not updated their antivirus software within the past week of the survey [5]. They also determined that close to seventy-two percent of end users' firewalls were not properly configured [5]. This demonstrates that the technology and software tools that are needed to stay secure are within the hands of the typical end user, but are regularly not used.

End users often operate technology with false mental models (folk models) which have the possibility to lead to flawed decision making [4]. End users then make security-compromising decisions through practicing these folk models in their day-to-day lives [4].

Folk models are not created by chance. They are formed through a combination of poor human behavior and lack of proper feedback from the security tools end users have been given [5]. When very minimal feedback is given in a potentially security compromising situation, it leads to ineffective and incorrect security practices taking place [6]. Without proper feedback, learning from consequences is hindered and less secure actions are adopted by the end user [5].

In our experiment, we attempt to achieve three main goals. Our first goal is to reduce the number of insecure actions that end users take. Our second goal is to expand end users' mental models of security situations. Our third goal is to increase the feedback given in security situations. Our method of reaching these goals is by creating a graphical representation of security-related consequences.

In Isaac Lipkus' study, end users' risk aversion was increased when presented with graphical figures [3]. Potential risks are also better communicated and easier to understand when presented in a graphical format [3].

Our hypothesis is that a graphical representation of security-related consequences can positively influence security-sensitive user decisions. We use interactive fiction to test our hypothesis. Through game play end users make a series of decisions. Some of the decisions are security-sensitive.

In the following work, we further define the issues that are currently present in end user's mental models. We continue by stating the observations made in our direct analysis of the problem and the detailed findings of our user test. Finally, we conclude with our final recommendations based off of the results of those findings.

## 2. PROBLEM

### 2.1 Users and Security

We found four main problems in end user's perception on security. First, end users are not aware of the risks associ-

ACM ISBN 978-1-4503-2138-9.
DOI: 10.1145/1235

ated with common computing activities. Second, end users make security-sensitive choices with insufficient knowledge and improper mental models. Third, often the secure choice is an encumbrance to the end user's primary goal. Lastly, often end users perceive no consequence for non-secure decisions because of insufficient feedback.

## 2.2 The Problem with Security User Tests

Because security is rarely a primary goal of the end user, it is seldom given attention to in their day-to-day lives [2]. The main instance when security is considered is when something is mis-functioning or lacking from it [2].

Many times end users are not motivated to take protective actions toward their security [2]. When an investigator presents outside motivation for an end user to complete security related tasks, he or she may be adding bias into the evaluation [2]. This bias causes the participant to pay more close attention to security than they would in a normal situation [2]. All of this is what makes performing a security-related study difficult.

# 3. APPROACH

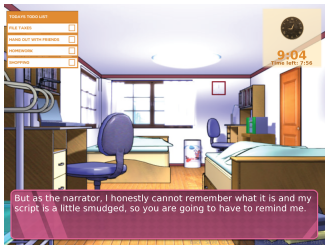


**Figure 1: Experiment Without Security Graphic**

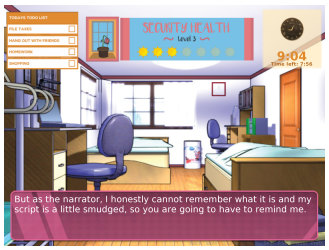


**Figure 2: Experiment With Security Graphic**

We chose interactive fiction as our medium for the following experimentation. It allows the participants to put themselves into the story given with a minimal amount of role-play being involved [1]. It also provides a controlled situation for data to be gathered. If designed correctly, a game can provide consistent situations across all participants with little variance between sessions.

We presented the game to the participants as a time management game. Not telling the participants the underlying purpose of the experiment was in an effort to remove bias from our results. We therefore omitted terminology associated with security as being the main purpose of the game and experiment.

We had a population of fourteen college-aged students take part in the study. The participants were split into two groups. One group of users played a version of the game with the inclusion of a graphical representation of security-related consequences. A second group played a version of the game without the graphical representation. The overt objective of the game is to complete a to-do list within time-constraints.

# 4. RESULTS

We summarize the most significant results of the interactive fiction game user test given to the participants. The data gathered from our research did not support our hypothesis. Minimal change was present between the two groups. On average, participants answered three out of the eight security-sensitive situations present within the interactive fiction game in a secure manner. This does not aide in proving our hypothesis, but it does demonstrate the depth of the problems we proposed.

# 5. FUTURE WORK

To receive more conclusive results, we recommend performing the experiment again with several factors changed. First, increase the number of participants. Our current sample size of fourteen students is too small to formulate accurate results. Second, repeat in-game security-sensitive scenarios. Due to this not being present in our past experiment, any evidence of the participants learning from our graphic was not seen. Lack of repeated in-game security-sensitive scenarios impacted our results the most. Third, create a more naturally motivating graphical aid. The flower graphic did not accurately capture the participants' attention or demonstrate risk. Fourth, increase game duration to more closely simulate real life. More results could be gathered and more conclusive results could be achieved. Lastly, add more in-game security-sensitive scenarios. A wider range of security-sensitive situations are present in day-to-day life than were able to be included in our first experiment. This would provide more realistic results.

# 6. CONCLUSION

Our initial experiment did not prove our hypothesis. The graphic appeared to have had no effect on the participants and their security-sensitive decision making process. In order to receive conclusive results, the experiment should be performed again with more participants, more in-game security-sensitive scenarios, repeated in-game security-sensitive scenarios, a more naturally motivating graphical aid, and for a longer duration.

# 7. ACKNOWLEDGEMENTS

We thank FMUS for the financial support for this project. The contents of this publication are the sole responsibility of the authors.

# 8. REFERENCES

[1] Ignacio X Domínguez, Rogelio E Cardona-Rivera, James K Vance, and David L Roberts. The Mimesis Effect: The Effect of Roles on Player Choice in Interactive Narrative Role-Playing Games. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 3438–3449, 2016.

[2] Serge Egelman, Jennifer King, Robert C Miller, Nick Ragouzis, and Erika Shehan. Security user studies: methodologies and best practices. *Proceedings of ACM CHI 2007 Conference on Human Factors in Computing Systems*, 2:2833–2836, 2007.

[3] I M Lipkus and J G Hollands. The visual communication of risk. *Journal of the National Cancer Institute. Monographs*, 27701(25):149–63, 1999.

[4] Rick Wash and Emilee Rader. Influencing Mental Models of Security: A Research Agenda. *Proceedings of the 2011 workshop on New security paradigms - NSPW '11*, pages 57–66, 2011.

[5] Ryan West. The Psychology of Security. *Commun. ACM*, 51(4):34–40, apr 2008.

[6] Alma Whitten and J.D. Tyger. Why Johnny Can ' t Encrypt : A Usability Evaluation of PGP 5.0 University of California Understanding the problem. *the 8th USENIX Security Symposium*, 1999.