Improving Security Behavior Through Better Security Message Comprehension: fMRI and Eye-Tracking Insights

Anthony Vance, Jeffrey L. Jenkins, Bonnie Brinton Anderson, C. Brock Kirwan and Daniel Bjornn

Abstract Security warnings are critical to help users make contextual security decisions. Unfortunately, users find these warnings hard to understand, and they routinely expose themselves to unintended risks as a result. Although it is straightforward to determine when users fail to understand a warning, it is more difficult to pinpoint *why* this happens. The goal of this research is to use eye tracking and fMRI to step through the building blocks of comprehension—attention, semantics, syntax, and pragmatics—for SSL and other common security warnings. Through this process, we will identify ways to design security warnings to be more easily understood.

Keywords NeuroIS · Eye-tracking · fMRI · Comprehension
Security messages

1 Introduction

Users routinely disregard protective messages such as software security warnings [2, 3]. One reason for the ineffectiveness of warnings is the mismatch between security concerns and security behavior. For example, individuals' stated security concerns have been found to be inconsistent with their subsequent behavior in response to

A. Vance
Temple University, Philadelphia, PA, USA
e-mail: anthony@vance.name

J. L. Jenkins · B. B. Anderson (✉) · C. Brock Kirwan · D. Bjornn
Brigham Young University, Provo, UT, USA
e-mail: bonnie_anderson@byu.edu

J. L. Jenkins
e-mail: jeffrey_jenkins@byu.edu

C. Brock Kirwan
e-mail: kirwan@byu.edu

D. Bjornn
e-mail: dbjornn@byu.edu

© Springer Nature Switzerland AG 2019

F. D. Davis et al. (eds.), *Information Systems and Neuroscience*,
Lecture Notes in Information Systems and Organisation 29,
https://doi.org/10.1007/978-3-030-01087-4_2

security warnings [11]. These empirical results confirm those of Crossler et al. [5], who called for research that explains the discrepancy between security intentions and behaviors.

One important factor contributing to the disconnect between security concerns and actual behavior is the lack of comprehension. For example, in the case of security warnings, although users may intend to behave securely, they may not comprehend a security warning, which may in turn lead them to make a choice that unintentionally exposes themselves to security risks.

Past research on comprehension of security warnings has highlighted the difficulty users have in understanding security warnings. Felt et al. [6] tested several iterations of text and design for SSL warnings in Google Chrome. They found that users routinely had difficulty determining the threat source and data risk, even after designing interventions to improve comprehension.

However, comprehension is not a binary event, but rather involves interrelated stages that lead to understanding. These stages include [9]:

1. Attention—focused mental resources on a certain object.
2. Semantics—the meaning of individual words and simple phrases.
3. Syntax—the structure of sentences that creates relationships between words.
4. Pragmatics—the application of past experience and knowledge to infer meaning.

The research objectives of this study are to: (1) use eye tracking, fMRI, and users' behavioral responses, through a series of complementary experiments, to determine failures at each of the above stages of comprehension for security warnings. Through this process, we will (2) identify ways to design security warnings to improve comprehension at each stage.

2 Planned Research and Expected Outcomes

2.1 Past Research on Comprehension of Security Warnings

Poor comprehension of security warnings is a common finding in the human–computer interaction literature. For example, researchers found that Android users paid attention to app permissions during installation only 17% of the time, and only 3% of users could correctly answer comprehension questions about permissions they saw [7]. Similarly, in a later study they found that users comprehended the threat source of SSL warnings in Chrome only 37.7% of the time, and comprehended even less what data was at risk. By changing the warning design based on recommendations from warning literature, they improved threat source comprehension nearly 12%. However, the design was not able to improve the comprehension of the risk to data [6].

We build on this past literature by applying behavioral information security to better understand and improve users' security behaviors [1]. Based on our findings, we expect to be able to determine more precisely where and why warning comprehension breaks down both from a neural and behavioral perspective. This will, in turn, allow us to create guidelines to improve comprehension in security warnings.

Previous work on comprehension using eye tracking found that more complex sentence structures result in poorer comprehension. For example, participants who read sentences with confusing ("ambiguous") syntax had poorer ability to answer simple questions about the sentences correctly compared to similar sentences that were changed slightly to be less confusing ("disambiguated"). Specifically, comprehension accuracy decreased by 15–38% when syntax was complex. This impaired comprehension was paired with significantly more re-reading of the ambiguous sentences (27–60% more time spent re-reading). In summary, not only does complex syntax impair comprehension, but re-reading is a reliable indicator of this impairment [4].

2.2 Description of Project and Expected Outcomes

To achieve our research objectives, we will record eye tracking data to step through the stages of comprehension (see Fig. 1). Comparable to code debugging, we will work through the different stages of comprehension to determine where comprehension is impeded. We will then improve warning designs to increase attention, ensure clear semantic and syntactic understanding, and promote pragmatic cognition. For example, at the level of attention, use of symbols or animation may help to improve overall attention. Similarly, semantic understanding may be improved through use of more familiar terms, or increased word frequency. By examining each stage individually, we expect to improve comprehension overall.

Eye tracking is an ideal tool for measuring the moment-by-moment allocation of attention. It is also used in psychology and linguistics to explore how people understand written language and to measure comprehension difficulty. For instance, words that are less familiar or unexpected (semantics) are looked at longer, and complex or confusing sentences (syntax) are re-read more often than are simple sentences [10]. In contrast to eye tracking, fMRI can provide information about the underlying neural and cognitive operations in attentional, semantic, and syntactic processing [8].

2.3 Hypotheses

We propose an eye-tracking experiment that examines the influence of syntax on users' comprehension of warnings. We will examine whether changing the syntax of the warning, to place the focus on different aspects of the warning, influences the likelihood of a data security breach. In addition to the usual focus on the attacker or

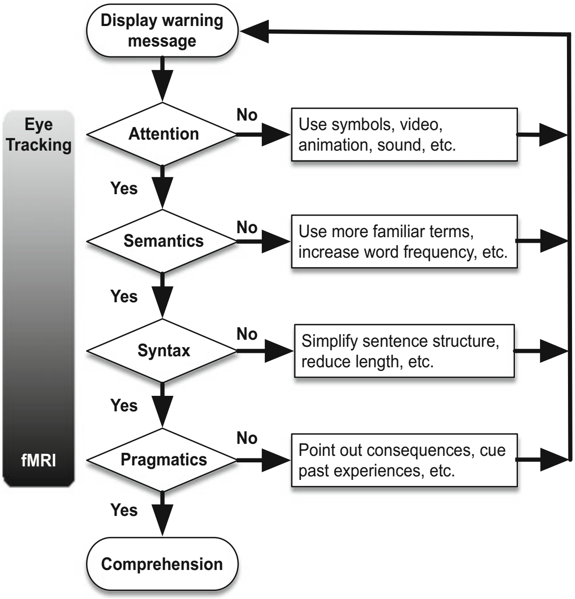
Display warning message
Eye Tracking
fMRI
Attention
No
Use symbols, video, animation, sound, etc.
Yes
Semantics
No
Use more familiar terms, increase word frequency, etc.
Yes
Syntax
No
Simplify sentence structure, reduce length, etc.
Yes
Pragmatics
No
Point out consequences, cue past experiences, etc.
Yes
Comprehension

Fig. 1 Evaluating warnings at different stages of comprehension using eye tracking and fMRI

the target website, we will also include a condition where the syntax of the warning shifts the focus to the consequences of ignoring the warning. We hypothesize that:

> Hypothesis 1—changing the focus of the warning will result in significant differences in comprehension as evidenced by a significant difference in the number of regressions (i.e., rereading) across warning focus.

Eye movement regressions are often used as a non-conscious measure of reading comprehension. As such, they may be more sensitive to subtle differences in comprehension between the different warning focus conditions in our experiment. Additionally, syntax changes should result in differences in overt comprehension as measured by performance on post hoc comprehension questions. We hypothesize that:

> Hypothesis 2—eye regressions in turn will significantly predict whether participants correctly understand the warnings as measured by performance on a post hoc comprehension quiz.

3 Eye Tracking Pilot Study

3.1 Participants and Stimuli

A total of 43 college-age individuals (14 male, 29 female) participated in the study. Five participants were not able to fully participate because an accurate calibration was not obtained. Removing these five participants left the sample with 38 individuals (14 male, 24 female). Participants were given course credit for participating in the study.

Warnings were created by sampling four warning types from the Google Chrome browser and the Apple Safari browser, namely malware, phishing, SSL, and unwanted software. The text for the warnings was then manipulated by changing the subject, verb, and object of the statement. For example, warnings from Chrome focus on the attacker as the subject of the statement. An example of this focus can be seen from the SSL warning text, "Attackers might be trying to steal your information from expired.badssl.com (for example, passwords, messages, or credit cards)." Warnings from Safari focus on the website as the subject of the statement. Chrome warning text was manipulated to change the focus to the website and Safari warning text was manipulated to change the focus to the attacker.

Along with the focus on the attacker and the website, a third text condition focused on the potential consequences of ignoring the warning. For example, the chrome SSL warning could be changed to, "Your information from expired.badssl.com (for example, passwords, messages, or credit cards) might be stolen if you visit it." Text from Chrome and Safari warnings were manipulated to fit this design.

The four warning types (i.e., malware, phishing, SSL, and unwanted software) for two browsers (i.e., Chrome and Safari) across three different conditions (i.e., attacker focus, consequence focus, and site focus) provided 24 different warnings. All references to a specific website were changed to "this website" for ease of presentation.

The warning text was overlaid onto a mock warning image for each trial. Warning titles were created from the standard text from the warning type for each browser (e.g., "Your connection is not private" for the Chrome SSL warning and "This Connection Is Not Private" for the Safari SSL warning).

3.2 Task

Participants viewed each warning one at a time on the computer screen and then answered a question. Each trial began with a drift check, which required participants to look at a circle on the top left part of the screen and press the spacebar to continue. The warning was then presented and participants read the warning and pressed the spacebar when they were ready to continue. The last part of each trial was the comprehension question which asked, "If this were a real threat and I ignored this warning, an attacker could," and then presented four answer options. Each of the answer options corresponded to a warning type:

- Phishing—"Trick me into installing malicious software or disclose personal information"
- Malware—"Install a dangerous program on my computer that could steal my information or delete my data"
- SSL—"See anything I send or receive from the website"

- Unwanted Software—“Install software that displays ads on my computer or makes changes to my browser”.

The answer options were presented in a random order for each trial. The full task consisted of 24 trials. The eye tracker was calibrated before the start of the task and after every 6 trials. Warnings were presented in a random order for each participant.

3.3 Planned Analysis

The results of this experiment will be analyzed by examining the behavioral and eye tracking measures of comprehension. For the behavioral analyses, we will calculate the proportions correct for warning type and warning focus separately. Repeated measures ANOVA tests will be run to test these factors individually in order to ensure a large enough number of trials for each bin.

For hypothesis 1, we will test whether warning focus predicts the number of regressions (i.e., rereading the text) by entering the total number of regressions for each trial as a dependent variable into a linear regression model with an independent variable of warning focus. For hypothesis 2, we will test whether the number of regressions predict accuracy on the comprehension test by entering trial accuracy as a dependent variable into a linear regression model with an independent variable of the total number of regressions in the trial. We will also use comprehension of other, non-security, messages and warnings for a comparison. Our post-study survey will contain the standard demographic, education and computer experience, as well as security risk questions, big five personality traits, and general risk propensity profile.

4 Conclusion

Users often respond inappropriately to security warnings. A significant factor in this failure is users’ difficulty in comprehending warnings. The insights expected to be gained from this research have the potential to inform the design and evaluation of warnings that more effectively help users to respond to security threats, enhancing the information security of individuals and organizations.

References

1. Anderson, B.B., Kirwan, C.B., Jenkins, J.L., Eargle, D., Howard, S., Vance, A.: How polymorphic warnings reduce habituation in the brain: insights from an fMRI study. In Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI) ACM, Seoul, South Korea (2015)

2. Anderson, B.B., Vance, A., Kirwan, C.B., Eargle, D., Jenkins, J.L.: How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. Eur. J. Inf. Syst. **25**(4), 364–390 (2016)
3. Bravo-Lillo, C., Komanduri, S., Cranor, L.F., Reeder, R.W., Sleeper, M., Downs, J., Schechter, S.: Your attention please: designing security-decision uis to make genuine risks harder to ignore. In Proceedings of the Ninth Symposium on Usable Privacy and Security ACM, Newcastle, United Kingdom, pp. 1–12 (2013)
4. Christianson, K., Luke, S.G., Hussey, E.K., Wochna, K.L.: Why reread? Evidence from garden-path and local coherence structures. Q. J. Exp. Psychol. **70**(7), 1380–1405 (2017)
5. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Comput. Secur. **32**(1), 90–101 (2013)
6. Felt, A.P., Ainslie, A., Reeder, R.W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., Grimes, J.: Improving ssl warnings: comprehension and adherence. In Proceedings of the Conference on Human Factors in Computing Systems (2015)
7. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: user attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security ACM, pp. 3:1–3:14 (2012)
8. Keller, T.A., Carpenter, P.A., Just, M.A.: The neural bases of sentence comprehension: a fMRI examination of syntactic and lexical processing. Cereb. Cortex **11**(3), 223–237 (2001)
9. Rayner, K.: Eye movements in reading and information processing: 20 years of research. Psychol. Bull. **124**(3), 372–422 (1998)
10. Rayner, K.: Eye movements and attention in reading, scene perception, and visual search. Q. J. Exp. Psychol. **62**(8), 1457–1506 (2009)
11. Vance, A., Anderson, B.B., Kirwan, C.B., Eargle, D.: Using measures of risk perception to predict information security behavior: insights from electroencephalography (eeg). J. Assoc. Inf. Syst. **15**(10), 679–722 (2014)