Expert and Non-expert Viewing Patterns When Seeking Security Cues

Suzanne Lien
Computer Science & Engineering
Santa Clara University
Santa Clara, California 95051 USA
slien@scu.edu

Abstract
Identity theft is responsible for the loss of billions of dollars worldwide, and a significant component of modern identity theft is online fraud. The security cues found in web browsers are meant to alert users to potential online threats, yet they are largely ineffective in this regard. However, technical expertise is a known mitigating factor in computer crime. We use eyetracking equipment to analyze computer experts and non-experts, as they use popular social media websites, to explore possible behavioral reasons for the failure of web browser security cues. We hope the results of our research can be used to inform the design of more usable security cues.

Introduction

In the past, computer crimes used to be a small, local problem perpetrated by the few, petty thieves. However, in recent years it has revolutionized to become a more globalized problem with massive economic costs. In 2006 alone, it was reported that the annual loss from identity theft is $2.8 billion [3,5]. With such an enormous amount of money lost to online crimes, our security on the web becomes increasingly important. One way a security risk is relayed to internet users is through web browser security indicators.

Security indicators exist to notify people when they may be in a malicious virtual locale, at risk of compromise. However, computer users are often unaware of these cues [1,4,6,8,9]. And even if they are aware of them, many people are unsure about how to interpret them, bringing into question their effectiveness.

Because previous studies have shown that people studying in technical fields are less susceptible to computer crimes [2,6,9], we want to determine what these experts are looking at in order to identify a website as malicious. Are they looking at the security cues provided by the web browser or using implicit knowledge, noticing things like misspellings on the webpage or the lack of ads? The goal of our experiment is not to determine whether experts and non-experts are able to successfully identify malicious websites. Instead, we are only interested in comparing the viewing behaviors of experts and novices to see if they are making use of security indicators. Where do people look as they browse the web and login to online accounts?

By determining the current viewing behaviors of experts and non-experts with regards to security indicators, we will have a clearer idea of what needs to be done to make security cues more usable. If we find that even experts are not utilizing security cues, this informs us that their design needs to be modified. If we find that experts are making use of web browser security

indicators while non-experts do not, this informs us that the design of security cues needs to be improved and made more usable for novices.

To determine the current usage of security cues, we will ask experts and non-experts to complete a series of tasks on social media websites as we collect eyetracking data. After completing the tasks, participants will be given a survey to self-report their use of security cues.

In this paper, we will begin with a discussion of related work, and then talk about our methodology. In the end, we will present our findings, conclusions, and possible directions for future work.

Related Work

Many studies have explored the effectiveness of current security cues.

In April 2006, a study was conducted to test the effectiveness of security toolbars in preventing phishing attacks [9]. Participants were asked to use security toolbars to identify malicious phishing websites. Despite being told to make use of the toolbar, many of their participants failed to do so. Even when the toolbar alerted warnings, participants explained them away when the website appeared to be legitimate. Ultimately, the researchers found that security toolbars were ineffective.

In another study done in February 2007, researchers tested people's attention to web browser security cues by removing them and observing whether participants continued to enter their passwords for their online banking accounts [4]. They found that after removing HTTPS indicators and site-authentication images, the majority of their participants still continued to enter their personal information.

Whalen and Inkpen conducted another study using eyetracking to determine people's attention to and use of visual security cues [7]. They found that while the lock icon is commonly viewed, few people click on it to review the security information in detail.

From all of these previous studies, it has been shown that security indicators are often not used. When they are used, they have done little to indicate to the users when they may be in a compromised setting.

A study done in April 2005 at Indiana University Bloomington has shown that there is a correlation between technical knowledge and the ability to detect phish [2]. In the study, researchers sent a fake phishing email to university students. Researchers found that students studying in technology-related fields were least likely to fall for phish; of all the students in technology-related majors, 0% fell for the attack in a controlled setting and 36% fell for it in the social setting.

If technical expertise is a mitigating factor in being able to determine phish, how exactly are these experts coming to their conclusions? What are they looking at that indicates to them that something is malicious? While previous studies have shown that people generally have made little use of security indicators, no previous study has explicitly compared experts' and non-experts' information seeking behaviors and use of security cues.

Study Design

Since we want to test people's attention to security cues, we will ask our participants to carry out common online tasks while we track their gazes. Participants will be using a website we created that gives task instructions in a random order. The tasks are: posting a comment on LiveJournal,

adding a friend on Facebook from a Yahoo! Mail address book, sharing an item from Amazon, sharing and commenting on a CNN story, logging into a Yahoo! Mail account using single sign-on, and rating a movie on Rotten Tomatoes. These tasks will be done either through Facebook Connect, or Twitter and OpenID.

To ensure the security cues are consistent from one participant to another, we chose to have our participants carry out these tasks using Firefox v4.0 on a Windows 7 platform as these seem to be more commonly used. As our participants are logging in, they will use fake accounts we have created for the purpose of our experiment so that their personal information will not be compromised.

Prior to and upon completion of the tasks, we will run a calibration to check to see if participants are looking where we think they are looking. After the eyetracking experiment, participants will be asked to fill out a questionnaire and a survey. The questionnaire asks participants whether or not they completed a certain task. If they chose not to complete a task, we asked them to give a reason why they did not do so. The survey is used to collect demographic information as well as self-reported usage of security cues.

Participants

Experts were recruited from Indiana University's School of Informatics and Computer Science graduate programs. Non-experts will be recruited from a pool of voluntary participants from the local Farmer's Market in Bloomington, Indiana.

A compensation of $15 for taking part in the experiment was given. Participants were paid $1 for each task they complete, up to $7 for a total of seven tasks. Upon completion of the after-experiment survey, participants were paid the remaining $8.

Expected Results

Since the data analysis has not yet been finished, there are no results to present. We expect to find that our experts' gazes will heavily concentrate in several key security areas. We also expect their viewing behaviors will follow a particular pattern. Meanwhile, we anticipate that our novices may glance at one or two security cues, but generally will have a random viewing pattern.

Limitations

Although we hope that our results will closely represent true experts and non-experts, there are a few factors we have to consider when presenting our results.

The use of fake login accounts does not simulate a real situation as there are no real risks. As a result, the viewing behaviors we observe may not reflect participants' usual viewing pattern. Also, some participants may be unfamiliar with our selected web browser and platform, so their observed viewing behavior may not accurately reflect their normal viewing behaviors; they may not recognize that particular browser's security cues.

Further, because the data analysis takes such a long time to do for each participant (typically around 8 hours, sometimes more), we lack the ability to run analysis on a large group of people, which leads to a lack of statistical power. Although this may be unacceptable to most

research done in informatics and computing, the standard number of participants required for a publishable eyetracking study is typically 12 participants.

Discussion and Future Work

Although we do not have results yet, running through the experiment with real participants revealed some changes we may need to make in our future experiments.

While running our experiments, I realized that many of our users are not familiar with the social media sites we asked them to use. As a result, many people had trouble carrying out the tasks we asked of them. This may be a potential problem that will need to be addressed as our participants may be too occupied with our tasks that they are not employing their usual viewing patterns.

While working on the data analysis, I realized that many of our participants' eyes were half-closed, which made accurately finding the pupil locations difficult. This was because the laptops we used were much lower in height than our participants' direct horizontal line of vision. Since their head movements were restricted with a chin rest, this resulted in our participants having to turn their gaze downwards in order to complete the tasks we asked of them. For future experiments, it would be a good idea to elevate the laptops so that the screen is directly in our participants' line of vision so their eyes will remain open during the majority of the experiment.

Also, adjusting the scene camera so that the monitor is straight may help capture the corners better when we do our analysis.

Acknowledgements

I would like to thank my mentors, Timothy Kelley and L Jean Camp, for looking over initial drafts of my paper. My summer research experience was sponsored by the Distributed Research Experiences for Undergraduates (DREU) program supported by the Computing Research Association for Women (CRA-W). Without this sponsorship, my involvement in this project would not have been possible.

References

1. Downs, J.S., Holbrook, M., and Cranor, L.F. *Behavioral response to phishing risk.* ACM Press, New York, New York, USA, 2007.
2. Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. Social phishing. *Communications of the ACM 50*, 10 (2007), 94-100.
3. Moore, T., Clayton, R., and Anderson, R. The Economics of Online Crime. *Journal of Economic Perspectives 23*, 3 (2009), 3-20.
4. Schechter, S.E., Dhamija, R., Ozment, A., and Fischer, I. The Emperor's New Security Indicators. *Security and Privacy, IEEE Symposium on 0*, (2007), 51-65.
5. Science and Technology Committee. Personal Internet Security. *5th Report of Session 2006-2007*, House of Lords (2007), 121.
6. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., and Downs, J. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of

interventions. *Proceedings of the 28th international conference on Human factors in computing systems*, ACM (2010), 373–382.
7. Whalen, T. Gathering evidence: use of visual security cues in web browsers. *Proceedings of Graphics Interface 2005*, (2005), 137-144.
8. Wright, R.T. and Marett, K. The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems 27*, 1 (2010), 273-303.
9. Wu, M., Miller, R.C., and Garfinkel, S.L. Do Security Toolbars Actually Prevent Phishing Attacks? *World Wide Web Internet And Web Information Systems*, (2006), 601-610.