Expert and Non-expert Viewing Patterns When Seeking Security Cues

Suzanne Lien
Santa Clara University

Timothy Kelley
Indiana University, Bloomington

L Jean Camp
Indiana University, Bloomington

1. Introduction

Phishing scams cost people millions of dollars worldwide. While they may be difficult to recognize, previous studies have found that technical knowledge helps reduce the risk [5,7]. What enables computer experts to identify malicious websites that novices are not able to identify? Are they looking at the security cues provided by the web browser, or are they simply using implicit knowledge? In our study, we will use eye-tracking to identify exactly where experts and non-experts are looking when they are browsing the web. No other study has explicitly compared experts and novices and only a few studies have made use of eye-trackers.

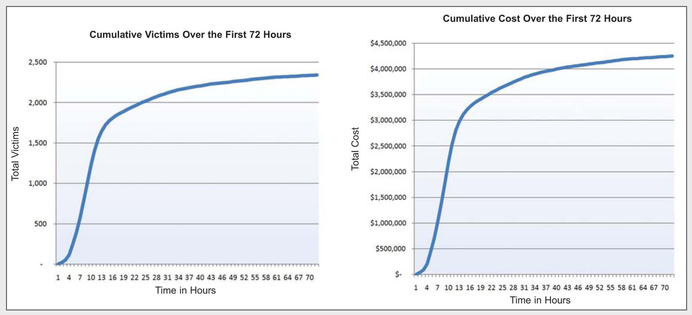
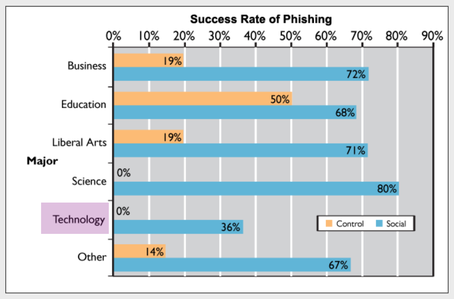


Image taken from a Cyveillance Report [3]

Graph shows the estimated cost of phishing over time for one attack. With more phishing scams, costs will accumulate to an even greater extent.



Shows the success rate of a simulated phishing attack. We can see that those who are studying in technical fields are less likely to fall for phish.

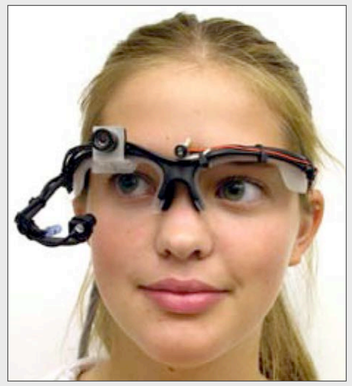
Image taken from Jagatic [5]

2. Goals

- Examine differences in information-seeking behaviors of experts and non-experts through eye-tracking.
- Evaluate differences between actual eye movements and self-reported evaluation.
- Create a training program in order to increase technical knowledge of non-experts.

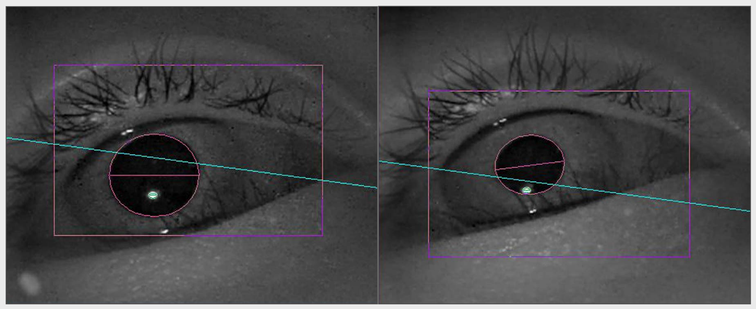
3. Methodology

- Participants will be asked to perform a series of randomly ordered tasks on the web as we record the movement of one of their eyes.
- After taking part in the eye-tracking experiment, participants will be asked to complete a survey.
- To analyze our data, we plan to create heap maps to see where people are looking.



Images taken from Babcock [2]

Images of what the eye-tracker looks like.



Images of a part of the data analysis process

We are using the ExpertEyes application to analyze the movement of people's eyes by finding the location of the pupils and cornea reflections.

4. Expected Results

We anticipate experts' viewing patterns will heavily concentrate in several key security areas. Meanwhile, we expect non-experts may glance at one or two security cues, but generally will have a random viewing pattern.

5. Limitations

While we hope that our results will closely represent the true population, there are several limitations to our study.

- Fake log-in accounts do not simulate a real situation as there are no real risks.
- Unfamiliarity with our selected web browser and computer system does not accurately reflect the participant's usual viewing pattern as they may not recognize that particular browser's security cues.
- Restricted ability to run data analysis for a large group of people leads to a lack of statistical power.

6. References

1.Asgharpour F, Liu D, Camp LJ: Mental models of computer security risks. *Workshop on the Economics of Information Security* 2007.
2.Babcock, J.S. and Pelz, J.B. Building a lightweight eyetracking headgear, ETRA 2004: Eye Tracking Research and Applications Symposium. (2004), 109-113.
3.Cyveillance. *The Cost of Phishing : Understanding the True Cost Dynamics Behind Phishing Attacks, A Cyveillance Report*. 2008.
4.Downs JS, Holbrook M, Cranor LF: *Behavioral response to phishing risk*. New York, New York, USA: ACM Press; 2007:37-44.
5.Jagatic TN, Johnson NA, Jakobsson M, Menczer F: Social phishing. *Communications of the ACM* 2007, 50:94-100.
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.Wu M, Miller RC, Garfinkel SL: Do Security Toolbars Actually Prevent Phishing Attacks? *World Wide Web Internet And Web Information Systems* 2006:601-610.

Acknowledgements: Tom Busey, Brandi Emerick, Silvia Figueira, Samiha Mourad, Computing Research Association for Women (CRA-W)