

Look Sharp! How Eye Tracking and Memory Explain Susceptibility to Phishing

Ian Jones ian.reed.jones@gmail.com ij222
Thomas Kelly thomasqkelly@gmail.com thomasqk
Jeff Penovich jspenovich88@gmail.com pjeffres

Dr. Anthony Vance Information Systems Department, Marriott School of Management
Dr. Bonnie Anderson Information Systems Department, Marriott School of Management

Project Purpose

The goal of this project is to understand how human memory, as measured by eye movements, affects individuals' susceptibility to phishing email attacks.

Project Importance

Phishing has become a major attack vector for hackers and cost victims \$687 million in the first half of 2012 alone [1]. Additionally, despite technical solutions to defend against this threat, reports show that phishing attacks are increasing. There is therefore a pressing need to understand why individuals continue to fall victim to phishing, and how such attacks can be prevented.

In this proposal, we argue that the cognitive neuroscience of memory provides a useful lens through which to study the problem of phishing. A commonly reported finding from the field of memory is the *eye movement-based memory effect* (EMM), the phenomenon of people paying less visual attention to images that have been previously viewed [2]. We aim to show in this paper that this effect holds in the context of email processing, and that the eye movement-based memory effect is a significant contributing factor to individuals' susceptibility to phishing.

We propose an experimental design that uses a memory task involving simulated phishing emails, and measures individuals' behavioral responses and eye tracking data in response to our phishing manipulations. We further propose to show how training can be designed to help individuals overcome the EMM effect and become less prone to phishing attacks.

Proposal

To better understand cognitive processes, many researchers have turned to the methodology of eye tracking. Eye tracking monitors the eye movements of an individual, gauging important variables such as time spent on each area of an image, number of times an area was visited, and pupil dilation as an index of emotional response. These eye-movements allow researchers to better measure conscious and unconscious processes and may be used as an indirect measure of memory [3]. Memory researchers have found that subjects pay significantly less attention to an image they thought to have seen previously, and that attention decreases further for each repeated viewing [2].

We hypothesize that the EMM effect will apply to phishing emails in that attackers create phishing emails to be similar to legitimate emails regularly viewed by individuals [1]. We hypothesize that because an individual receives legitimate emails from a familiar source, they are less likely to scrutinize a phishing email fabricated to be similar to the legitimate email. In this way, our memory and the EMM effect work against our ability spot telltale signs of phishing attacks.

In a pilot experimentation for this proposal, eye tracking data was gathered using a Tobii T120 eye tracker (see Figure 1). Preliminary data includes "heat map" images, which show how intensely the email messages were scrutinized, with warmer colors indicating higher intensity (see Figure 2 below). These heat maps suggest that, in accordance with the EMM effect, participants gazed much less intently on an image in just the second time it was shown. These heat maps also suggest that the EMM effect may play a major role in susceptibility to phishing.

Our next steps are to fully analyze the pilot data, refine experimental design, collect primary data, and further analyze how the EMM effect influences individuals' susceptibility to phishing. In this way, we hope to find ways people can overcome the EMM effect and become less susceptible to phishing.



Figure 1: A Tobii T120 Eye tracker

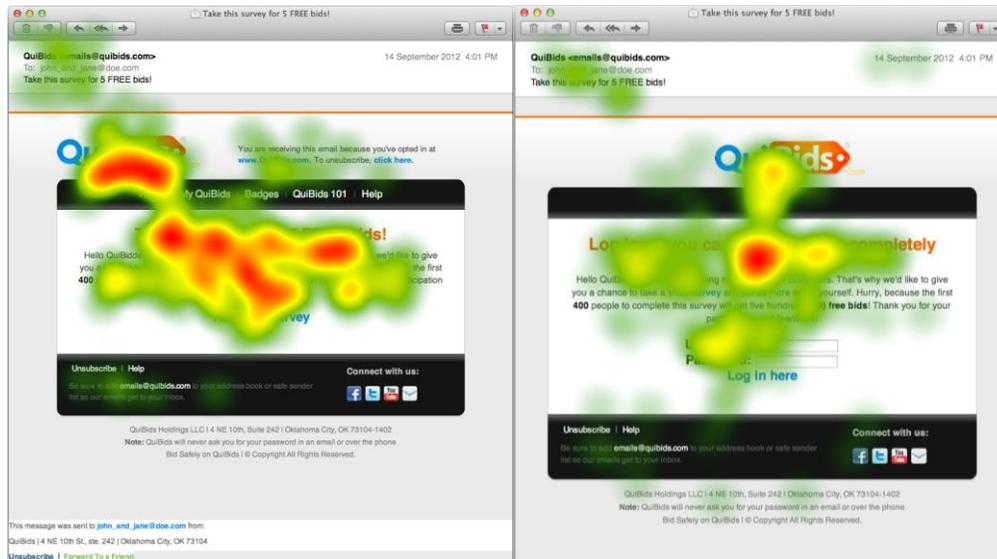


Figure 2. Heat maps of the original email (left) compared with the manipulated phishing email (right). These show that much less attention (in red) is paid to the phishing email, despite it being manipulated.

Anticipated Academic Outcome

We expect our research to have at least two academic outcomes. We will:

1. Submit and present our research at the 2014 Association for Information Systems Conference International Conference for Information Systems, a leading IS conference.
2. Submit a journal article to *Information Systems Research*, a premier IS journal.

Qualifications

Dr. Anthony Vance is as an assistant professor of IS in the Marriott School of Management. He has published work on information security in *MIS Quarterly* and other premier journals.

Dr. Bonnie Anderson is an associate professor of IS. She has worked and coauthored with students on mentored research for the past 10 years.

Ian Jones is an IS undergraduate in the Marriott School of Management. He has worked with Dr. Vance as a teaching assistant in an information security course.

Thomas Kelly is an IS undergraduate in the Marriott School of Management. He is seeking a PhD in IS with an emphasis in information security.

Jeff Penovich is an IS undergraduate in the Marriott School of Management. He currently works for the BYU IT audit department, documenting and enhancing security/risk procedures.

Project Timetable

Nov 2013	Analyze pilot data and refine experimental design
Dec–Jan 2013	Collect and analyze primary data collection for approximately 100 subjects
Feb–Mar 2014	Write and submit conference paper to AMCIS 2014
Apr–Aug 2014	Write and submit research paper to <i>Information Systems Research</i>

Scholarly Sources

- [1] Kessem, L. 2012. "Phishing in Season: A Look at Online Fraud in 2012," *RSA: Speaking of Security*, accessed online at <http://blogs.rsa.com/phishing-in-season-a-look-at-online-fraud-in-2012/>, 10/29/2013.
- [2] Hannula, D. E., and Ranganath, C. 2009. "The eyes have it: hippocampal activity predicts expression of memory in eye movements," *Neuron*, (63:5), pp. 592-599.
- [3] Smith, C. N., Hopkins, R. O., and Squire, L. R. 2006. "Experience-Dependent Eye Movements, Awareness, and Hippocampus-Dependent Memory," *The Journal of Neuroscience*, (26:44), pp. 11304-11312.