Tracking users' fixations when evaluating the validity of a web site

A. Xiong, R. Proctor, W.-L. Zou and N. Li, USA

ABSTRACT: Phishing refers to attacks over the Internet that often proceed in the following manner. An unsolicited email is sent by the deceiver posing as a legitimate party, with the intent of getting the user to click on a link that leads to a fraudulent webpage. This webpage mimics the authentic one of a reputable organization and requests personal information such as passwords and credit card numbers from the user. If the phishing attack is successful, that personal information can then be used for various illegal activities by the perpetrator. The most reliable sign of a phishing website may be that its domain name is incorrect in the address bar. In recognition of this, all major web browsers now use domain highlighting, that is, the domain name is shown in bold font. Domain highlighting is based on the assumption that users will attend to the address bar and that they will be able to distinguish legitimate from illegitimate domain names. We previously found little evidence for the effectiveness of domain highlighting, even when participants were directed to look at the address bar, in a study with many participants conducted online through Mechanical Turk. The present study was conducted in a laboratory setting that allowed us to have better control over the viewing conditions and measure the parts of the display at which the users looked. We conducted a laboratory experiment to assess whether directing users to attend to the address bar and the use of domain highlighting assist them at detecting fraudulent webpages. An Eyelink 1000plus eye tracker was used to monitor participants' gaze patterns throughout the experiment. 48 participants were recruited from an undergraduate subject pool; half had been phished previously and half had not. They were required to evaluate the trustworthiness of webpages (half authentic and half fraudulent) in two trial blocks. In the first block, participants were instructed to judge the webpage's legitimacy by any information on the page. In the second block, they were directed specifically to look at the address bar. Whether or not the domain name was highlighted in the address bar was manipulated between subjects. Results confirmed that the participants could differentiate the legitimate and fraudulent webpages to a significant extent. Participants rarely looked at the address bar during the trial block in which they were not directed to the address bar. The percentage of time spent looking at the address bar increased significantly when the participants were directed to look at it. The number of fixations on the address bar also increased, with both measures indicating that more attention was allocated to the address bar when it was emphasized. When participants were directed to look at the address bar, correct decisions were improved slightly for fraudulent webpages ("unsafe") but not for the authentic ones ("safe"). Domain highlighting had little influence even when participants were directed to look at the address bar, suggesting that participants do not rely on the domain name for their decisions about webpage legitimacy. Without the general knowledge of domain names and specific knowledge about particular domain names, domain highlighting will not be effective.