ABSTRACT

Phishing is a kind of attack in which criminals use spoofed emails and fraudulent web sites to trick people into giving up personal information. This thesis looks at the phishing problem holistically by examining various stakeholders and their countermeasures, and by surveying experts' opinions about the current and future threats and the kinds of countermeasures that should be put in place. It composed of four studies.

In the first study, we conducted semi-structured interviews with 31 anti-phishing experts from academia, law enforcement, and industry. We surveyed experts' opinions about the current and future of phishing threats and the kind of countermeasures that should be put in place. Our analysis led to eight key findings and 18 recommendations to improve phishing countermeasures. In the second study, we study the effectiveness of popular phishing tools that are used by major web browsers. We used fresh phish that were less than 30 minutes old to conduct two tests on eight anti-phishing toolbars. We found blacklists were ineffective when protecting users initially. The tools that uses heuristics to complement blacklists caught significantly more phish than blacklist-only tools with very low false positives. In the third study, we describe the design and evaluation of Anti-Phishing Phil, an online game that teaches users good habits to help them avoid phishing attacks. We used learning science principles to design and iteratively refine the game. We evaluated Anti-Phishing Phil through laboratory and real-world experiments. These experiments showed that people trained with Anti-Phishing Phil were much better at detecting phishing websites, and they retain knowledge after one week. In the fourth and final study we present our results of a roleplay survey instrument administered to 1001 online survey respondents to study both the relationship between demographics and phishing susceptibility, and the effectiveness of several anti-phishing educational materials. Our results suggest that women are more susceptible than men to phishing

and participants between the ages of 18 and 25 are more susceptible to phishing than other age groups. We explain these demographic factors through a mediation analysis. Educational materials reduced users tendency to enter information into phishing webpages by 40% percent; however, some of the educational materials we tested also slightly decreased participants tendency to click on legitimate links.