Chapter 1

Introduction

Phishing is a kind of attack in which criminals use spoofed emails and fraudulent web sites to trick people into giving up personal information. Victims perceive these emails as associated with a trusted brand, while in reality they are the work of con artists interested in identity theft [57].

Phishing is a widespread problem that is impacting both business and consumers. In May 2009, MessageLabs estimated that 0.41% of the 3.3 billion emails going through their system each day were phishing emails [87]. Microsoft Research recently estimated that 0.4% of email recipients are victimized by phishing attacks [36]. The annual cost to consumers and businesses due to phishing in the US alone is estimated to be between $350 million and $2 billion [43, 92].

To reduce the damage due to phishing, stakeholders have implemented their own countermeasures: major web browsers have built-in filters (e.g. [10], [46], [90]), Internet service providers filter suspicious phishing emails, law enforcement officers find and prosecute phishers, and US government agencies and corporations now educate consumers on phishing.

Phishing scams have also evolved, sometimes at a faster pace than countermeasures. Phishers launch attacks on specific groups (e.g. users of social networking sites) through multiple channels (e.g. phone, instant messaging), and phishing toolkits and compromised credentials are readily available for sale at low prices on Internet black markets [38]. Sophisticated phishing schemes such as man-in-the-middle attacks and malware are becoming more frequent [62].

As the battle against phishing continues, many questions remain about where stakeholders should place their efforts to achieve effective prevention, speedy detection, and fast action. Do

stakeholders have sufficient incentives to act? What should be the top priorities for the anti-phishing community?

1.1 Thesis statement

This dissertation aims to provide insights in answering the objectives raised above through four studies.

> **This thesis presents recommendations about how to better fight phishing; these recommendations are informed by empirical data on the effectiveness of current approaches as well as systematic analyses of stakeholder interests and the phishing life cycle. Semi-structured expert interviews were used to rank and prioritize the recommendations. In addition, we used case studies on the effectiveness of web browser anti-phishing toolbars and anti-phishing education to provide empirical data for our analysis.**

The centerpiece of the thesis is an expert analysis of phishing countermeasures. 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. Experts discussed technical countermeasures, education, and law enforcement, which led to eight key findings and 18 recommendations to improve phishing countermeasures.

One of the findings from the expert analysis is that experts think education and awareness are important. However, not all experts agree on the effectiveness of end-user security education. To investigate this issue further, we conducted two in-depth studies. Firstly, we studied phishing susceptibility with a role-play survey administered to 1000 users of Mechanical Turk. This studies showed different demographic factors' impact on phishing susceptibility. In the second study, we designed and evaluated Anti-Phishing Phil, an online game that teaches users good habits to help them avoid phishing attacks.

Another key area where experts commented on is the strategic position of browsers. Several experts noted that organizations are conservative about filtering and warning about phish because they are worried about false positives. To investigate this further, we studied the effectiveness of popular phishing tools that are used by major web browsers.

1.2 Thesis contribution

This thesis is both timely and needed to reduce the negative consequences of semantic attacks on society. The education component of this research can potentially help reduce the increasing number of people who fall for phishing and other semantic attacks, the policy recommendations from this research could help government and various stakeholders to better prioritize their resources and manage their risks to fight for phishing and other semantic attacks. This thesis work builds on existing knowledge in the fields of computer security and privacy, human computer interaction, and economics, and adds to the literature with the following contributions.

1. We designed and evaluated Anti-Phishing Phil, an online game that teaches users good habits to help them avoid semantic attacks. People trained with Anti-phishing Phil were much better at distinguishing phishing website and legitimate websites, and retain their knowledge after one week. The Anti-Phishing Phil game has been played over 110,000 times world-wide and is being commercialized by Wombat Security Technologies. This research showed that computer users can be trained to make better online trust decisions if the training materials are presented in a fun and interactive manner and grounded in learning science principles.

2. We conducted semi-structured interviews with 31 anti-phishing experts from academia, law enforcement, and industry on phishing countermeasures. Our analysis led to eight key findings and 18 recommendations to improve phishing countermeasures.

3. We studied the effectiveness of popular phishing tools that is used by major web browsers. 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. We recommend toolbars vendors use heuristics to complement blacklists to speed up phishing detection.

4. We studied demographics and phishing susceptibility with an role play survey administered to 1001 users of Mechanical Turk. This research is the first study that studied demographics factors contributing to susceptibility to semantic attacks. We also demonstrated the successful use of mechanical turk to conduct online experiments.

1.3 Outline of the thesis

The next chapter introduces the fundamentals of phishing attacks and some of the related work that builds the foundation for the thesis; Chapter 3 discusses the expert interviews study in depth, and presents the key findings and recommendations; Chapter 4 discussed our study on the effectiveness of popular phishing tools that is used by major web browsers; Chapter 5 described the design and evaluation of Anti-Phishing Phil, an online game that teaches users good habits to help them avoid phishing attacks; Chapter 6 discussed the role-play survey conducted with mechanical turk users to study demographics and phishing susceptibility. Finally, Chapter 7 presents conclusions from this thesis work and offers recommendations for public policy makers.