Chapter XVI
Designing Antiphishing Education

James W. Ragucci
Syracuse University, USA

Stefan A. Robila
Montclair State University, USA

ABSTRACT

Fraudulent e-mails, known as phishing attacks, have brought chaos across the digital world causing billions of dollars of damage. These attacks are known for their ability to exploit the human aspect of a computer system by pretending to originate from a source trusted by the victim. While technology defenses have been setup for protection, people are still succumbing to these attacks at alarming rates. Therefore, educational techniques must implement to strengthen the human factor of security. We propose the use of a phishing IQ test that when used in classroom setting can help users build experience needed to identify phishing e-mail during their daily routine.

INTRODUCTION

Phishing is generally described as sending computer users messages claiming to originate from a legitimate entity and attempting to lead the user to provide private information that will be further used for identity theft (“Phishing,” 2006). While the nature of the message (and the purported originating entity) varies from with each individual attack, one can notice that the entities continue to diversify and that the sole number of such attacks is staggering. A brief review of phishing related news for the first seven days of November 2006 in chronological order is shown in Figure 1. Such bleak reality is shared by professional reports that suggest that the number of reported phishing at-
Designing Antiphishing Education


Faced with an increasing threat, software companies, federal agencies, financial and commercial institutions and internet service providers have increased their antiphishing efforts. Statistics are now being compiled monthly monitoring the threat level, and repositories of phishing events have been created (and are publicly available). As the variety of phishing techniques increase, more defense tools/methods are developed. In recent versions of the internet browsers, ‘anti-phishing’ filters are provided (an application component that checks the website against a list of known phishing sites) (Microsoft, 2006). Log-in procedures have been revamped by requiring multi-step authentication and changing challenge-response pairs (Schechter, Dhamija, Ozment, & Fischer, 2007). Despite all this effort from the IT world, people continue to fall victim to phishing tactics. It is therefore necessary to improve upon previous methods of education to help protect an increasingly vulnerable population. Thus, we present an educational method that can be used to help teach users how to protect themselves from phishing associated identity theft. To better understand how to identify a phishing attack, people need to learn how and why phishing works. Hence, it is imperative to show the reasons phishing is so successful as well as why it has become one of the top cyber threats of the new millennium. With this knowledge people should be able to see their own mistakes in phishing identification and be able to reduce the problem.

In the following, we start by providing a survey of the ‘state of the art’ in phishing. Next, we describe the current phishing education strategies we developed and implemented. The educational method includes phishing detection tests, as well as an education session that starts by defining the threat and builds that knowledge into means for phish identification. The education module has been already administered to approximately 120 undergraduate students at Montclair State University. Survey results indicate an increased awareness of the issue and an increased ability to detect phishing attempts.

IDENTIFYING THE THREAT

The Diversity in Phishing

The increase in phishing attacks and their diversity can be explained by several factors. First, more and more of the day to day human activities are done online, therefore increasing the number of opportunities for accessing private data. Second, phishing remains an effective attack due to the relatively high response rate from the victims. Third, as online applications themselves diversify, so do the phishing tools. We will next look at some of these factors.

Why Do People Respond to Attacks?

Dhamija et al. surveyed 20 participants in order to determine a reason for why people fall prey to phishing attacks. They categorized three general reasons for phishing success: lack of knowledge, visual deception and bounded attention. When analyzing lack of knowledge, one can decompose it into lack of computer system knowledge, lack of knowledge of security and security indicators, lack of knowledge of web fraud, and erroneous security knowledge (Dhamija, Tygar, & Hearst, 2006). This ignorance of security leads to poor decisions when using the internet that can endanger a user’s own data. In one situation, Dhamija et al. describes a participant who used her actual username and password to test if the website in question was truly the authentic website. Her logic was that passwords are not as harmful as financial information for phishers to acquire (Dhamija et al., 2006). Visual cues are also enough to convince a weary user that a website is legitimate or fake.