Empirical Benefits of Training to Phishing Susceptibility

Ronald Dodge, Kathryn Coronges, Ericka Rovira

United States Military Academy, West Point, New York , USA
{ronald.dodge, kate.coronges, ericka.rovira}@usma.edu

Abstract. Social engineering continues to be the most worrisome vulnerability to organizational networks, data, and services. The most successful form of social engineering is the practice of phishing. In the last several years, a multitude of phishing variations have been defined including pharming, spear phishing, and whaling. While each has a specific reason for its success, they all rely on a user failing to exercise due diligence and responsibility. In this paper, we report on a recent phishing experiments where the effects of training were evaluated as well as gathering demographic data to explore the susceptibility of given groups.

1 Introduction

The use of technology has become pervasive in our work and home environments. While security technologies have continued to progress at a pace to parry the onslaught of technical attacks, users continue to expose our networks, data, and services to avoidable security risks. We have achieved little improvement in the awareness of users to detect and avoid one of the most prevalent forms of social engineering – phishing. [1,2,3] Phishing uses a variety of social engineering techniques to entice the user into doing something that they would not do if they understood the ramifications of the action. Regardless of how an organization employs encryption or two factor/token based authentication, a user can subvert all of these controls by simply opening an email.

A not for profit group, the Anti-Phishing Working Group [4], reported in the 2011 phishing report that phishing continues to be a pervasive threat. Of particular note was an increased sophistication by phishers using a technique called spear phishing. In spear phishing, elaborate, targeted emails that use either organizational or personal details are used to entice a user to click a link or open an attachment. The Anti-Phishing Working Group report further that spear phishing was the most concerning threat of 2011. The spear phishing campaigns were used to target organizations where security training might increase the awareness of users. Specific organizations included security companies, defense contractors, and financial institutions. These spear phishing attacks were a key component of the Advance Persistent Threat (APT). In 2007 Jagatic, et al. showed that a user is 4.5 times more likely to fall victim and follow the instructions in a phishing email if it is spoofed to come from someone they recognize. [5]

adfa, p. 1, 2011.

2 Efforts to Assess the Phishing Threat

Many studies and research projects have sought to explore detection and mitigation options for phishing emails. Some approaches employ advanced semantic processing and keyword scanning to block unwanted emails other techniques use visual clues in the email client to warn users of suspect emails. In most all studies, regardless of the technologies deployed, if the email is tempting enough, a user will fall victim. [6, 7]

The authors have conducted many studies in the effectiveness of training and education in stemming a person's susceptibility to phishing. In early studies, the focus of the studies focused on the simple effectiveness of phishing exercises. [8] In these early results, the authors constructed an infrastructure to execute a phishing exercise and achieved results indicating an average 40% susceptibility to phishing. These results were validate in a follow-on study [9] and further showed that exercises repeated over a short duration increased awareness and susceptibility reduced to under 5%. The most recent effort analyzed the social network impact on susceptibility [10]. In these results, there was an identifiable clustering of victims by organization; if an organizations leadership was vulnerable – it was likely that so to would the personnel in that organization. In Figure 1, the larger circles indicate supervisors and red circles indicate falling victim to the phishing exercise.

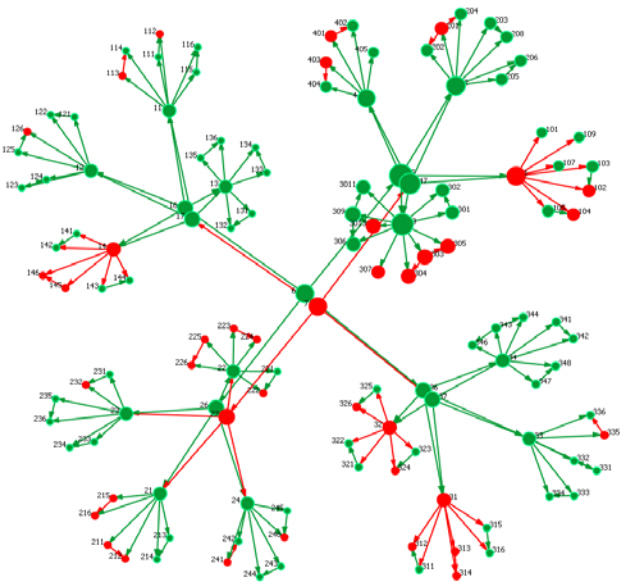

Fig. 1. Supervisorial Network: Phish Victims Sized by Centrality

3 Training Users: Effective or a Waste of Time?

Many large organizations require training to ensure employees are aware of the risks exposed to the organization by users falling victim to a phishing email. This training usually comes at a fiscal and manpower cost to the organization. Phishing exercises have emerged in the past few years to be an effective mechanism to provide a training capability that provides lower investment by the organization. However with the popularity of these exercises – is training still required? The research documented in this paper sought to explore that question and provide empirical evidence to answer.

3.1 Methodology

Eight hundred ninety-two (892) subjects selected at random at the <removed for review> participated in this study. Ages of the subjects ranged from 18-26. The phishing emails sent to all subjects included an embedded URL that when clicked takes users to a web site where they are asked to enter sensitive information (their network credentials). In all cases the email 'bait' leveraged knowledge of the users organization (spear phishing), where some sort of free or discounted service appealing to the target population was used. Emails were sent from a third party service provider outside the institution's boundary. The service selected was phishme.com [11]. Three emails were sent - one in November, another 10 days later in December, and another 6 weeks later in January. Prior to the study, all participants took the required institutional phishing awareness training (in September).

To support the hypothesis of the experiment, the population was broken down into three notification conditions. Notification condition was randomized by organizational group. Each group was made up of three organizational units. There were 287 participants in the group one, 298 in group two, and 307 in group three. The three notification conditions were:

Group 1 (No Notification): participants received the phishing email, however after the user entered data into the website and clicked submit, the page returned a server error and no additional information was provided to the user.

Group 2 (Notification): participants received the phishing email, after the user entered data into the website and clicked submit, the page returned a notice that they fell victim to a phishing attack and provided details as to what the user should have identified in the email.

Group 3 (Training): received the phishing email, after the user entered data into the website and clicked submit, the page returned a notice that they fell victim to a phishing attack and directed the user to take the institutions phishing awareness training.

The emails themselves were constructed to provide several clues designed to alert end users. By default, emails are displayed in plain text mode; users have the ability to choose to view in HTML after the email has been displayed in plain text. Figures 2 and 3 show both presentations of the email.

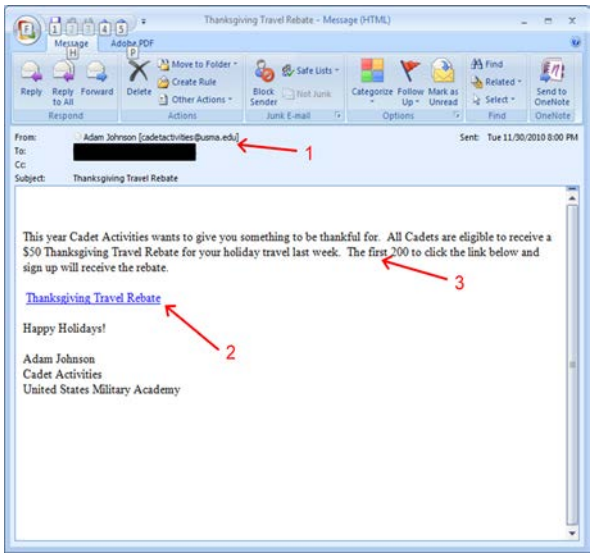

Fig. 2. HTML Email View

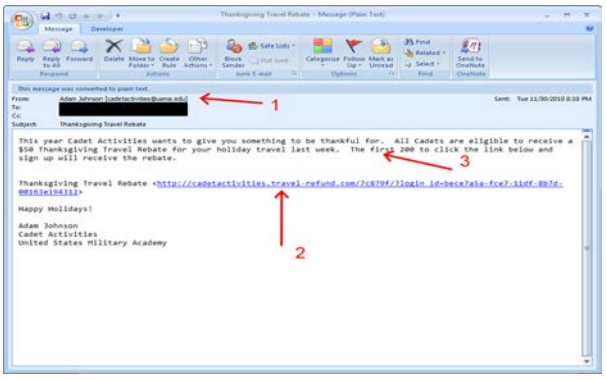

Fig. 3. Plain Text Email View

The following details are items that are part of the annual training our users receive and should have alerted them that the email was likely not legitimate.

1. Source email address (Adam Johnson [user@institution]): The email is from a person; however the source address is an institutional address. Further the user does not exist in our global list (accessible by all authorized users).
2. The URL in the email: In figure 2, the URL is shown in the middle using html formatting for email. This is not how email is delivered by default to our users. Instead the 'presentation text' is listed as well as the actual URL string, which is how it is first displayed to users (as shown in Figure 3).

3. The email urgency: While not always a valid sign of phishing email, when an urgent email is received from a source outside the organization, it is highly suspect.
4. Finally, if they looking in the full mail headers (which is an option if they are concerned about the validity of the email); they would have seen that the originating email server is highly suspect. This is shown below using bolded and underline text.

```
Received: from localhost.localdomain (local-
host.localdomain [127.0.0.1]) by
 mail.phishme.managedmachine.com (Postfix) with ESMTP id
5DC6B10A43 for
 < user@institution >; Wed,  1 Dec 2010 01:05:14 +0000
(UTC)
Date: Wed, 1 Dec 2010 01:05:11 +0000
From:AdamJohnson < user@institution >
To: < user@institution >
Subject: Thanksgiving Travel Rebate
MIME-Version: 1.0
Content-Type: text/html; charset="utf-8"
X-Priority: 3
X-Pmsid:775892d4-fce0-11df-97b7-0163e4638cc
Message-ID:
<20101201010514.5DC6B10A43@mail.phishme.managedmachine.co
m>
```

Fig. 4. Full Mail Headers

3.2 Task Procedures and Experimental Design

The hypothesis posited is that the completion of mandatory training after falling victim to a phish would have significant impact on a student's future susceptibility. In addition, the group that simply received notification when they fell victim to the attatck was expected reduce their susceptibliy more so than the group that received no notification at all. Thus, group 3 (those that received training after falling victim to the phishing attack) was expected to improve their phishing vigilance the most, followed by group 2 (the notification group), with the no notification group improving the least.

Phishing "susceptibility" was operationalized as a binary variable indicating whether the participant clicked on a link in the phishing email (indicating a failure to detect the phish) or if they did not click on the embedded link in the phishing email (indicating either successful recognition of the email as a phishing attack, or that the participant never read the email at all).

A single factor between subjects design with three levels (training: none, notification only, training) was implemented to investigate susceptibility to phishing exercises. The first group of 287 participants received the phishing email, however after the user entered data into the website and clicked submit, the page returned a server error

and no additional information was provided to the user. The feedback only group consisted of 298 participants that received the phishing email, after the user entered data into the website and clicked submit, the page returned a notice that they fell victim to a phishing attack and provided details as to what the user should have identified in the email. The training group (307 participants) received the phishing email, after the user entered data into the website and clicked submit, the page returned a notice that they fell victim to a phishing attack and directed the user to take the institutions phishing awareness training.

3.3 Results

To Train or Not to Train.

The results indicate that over very short periods of time (10 days), there is no significant difference in susceptibility based on training. However, over longer periods of time (63 days), training does contribute significantly to the reduction in susceptibility. A 3x3 (training x phishing attempts) mixed factorial ANOVA was used to test the effects of training on phishing failures, and how those effects endured over time. Results indicated significant main effects of training ($F(2,874) = 15.78$, $p < .01$) and phishing attempts ($F(2,1748) = 223.70$). A significant interaction between type of training and phishing attempts was also found, $F(4,1748) = 5.91$, $p < .01$.

To investigate the interaction, three tests of simple effects examined whether the training had a significant effect on each of the phishing attempts. A one-way ANOVA showed a significant difference between the training groups at phishing attempt one, $F(2,874) = 6.08$, $p<.01$. Failure rates were 56%, 46%, and 42%, respectively. However, a one-way ANOVA showed no difference between the three groups at phishing attempt two, $F(2,874) = .634$, $p > .05$. Lastly, a one-way ANOVA showed a significant effect of training at phishing attempt three, $F(2,874) = 18.32$, $p < .01$. Failure rate was the least for the group that received training (24.5%), but increased for the group that only received feedback (32.08%) and was the highest for the group that received neither feedback nor training group (47.5%). Figure 5 shows that while there was some variability between the groups at phish one, at phish two there was no difference between the groups, and at phish three training reduces phishing susceptibility beyond feedback alone.

Failure rate for the second phish was drastically lower than for both the first and third phish attack. The reduction is most likely due to the timing of the phish: phish two was sent out only two weeks after the initial training. This was due to organizational events and unfortunately skewed the study findings. Phish three was sent out 2 months after phish 2.

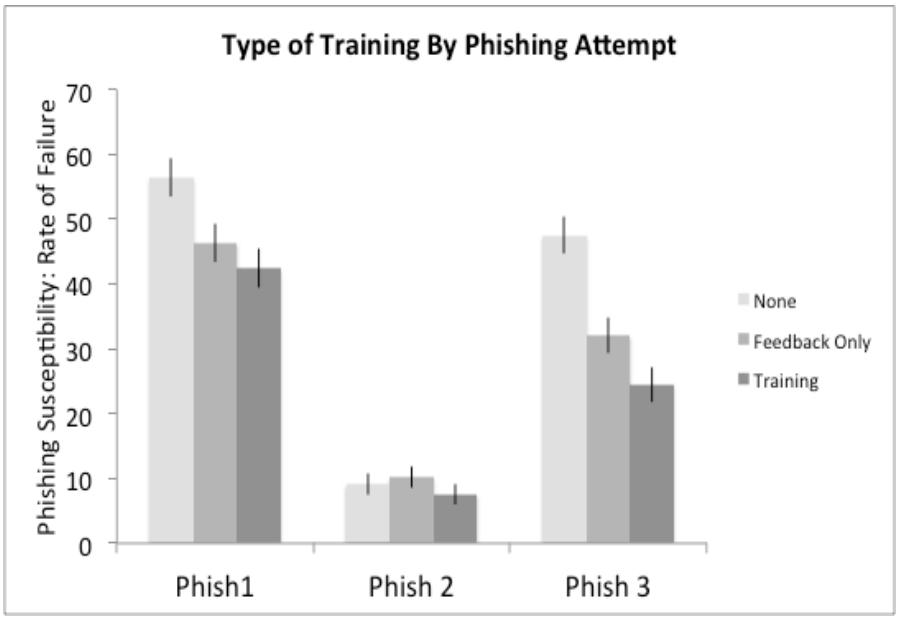

Fig. 5. Phishing Rate of Failure – Training Comparison

4 Conclusions and Recommendations

The outcomes of the experiments documented in this paper indicate several results that can be used to contribute to effective mitigation of phishing susceptibility. The major result shows that while the phishing exercise alone does lead to an increased level of awareness when the participant is notified that they fell victim, phishing training still provides a better return. As with all security program components, the business case for the increased level of awareness must be determined by the organization. Specifically, the organization has to balance the importance of reducing susceptibility of security threats with the increased time and organizational efforts involved with providing security training resources, as well as the additional efforts to make that training mandatory

There are several types of training that are available that follow different pedagogical approaches. In future work, the authors will further validate the results in this report, while exploring the effectiveness of different training programs in reducing phishing susceptibility. In addition, future research will seek to identify broad demographic characteristics within the user population that may lead to a higher general susceptibility. This knowledge could help organization develop targeted training or increased awareness exercises where they would produce the highest payoff.

5 References

1. Downs, J., Holbrook, M., & Lorrie, C. (2006). Decision Strategies and Susceptibility to Phishing. Symposium on Usable Privacy and Security.

2. Hicks, D. (2005). Phishing and Pharming: Helping Consumers Avoid Internet Fraud. Communities and Banking , 29-31.

3. Stajano, F. and Wilson, P. Understanding scam victims:Seven principles for systems security. Commun. ACM 54, 3 (Mar. 2011), 70–75.

4. The Anit Phishing Working Group 2011 Annual Report, http://www.antiphishing.org/reports/apwg_trends_report_h1_2011.pdf, accessed 13 Jan 2012.

5. Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. Social phishing. Commun. ACM 50, 10 (Oct. 2007), 94–100.
6. Markoff, J. Larger prey are targets of phishing. New York Times (Apr. 16, 2008); http://www.nytimes.com/2008/04/16/technology/16whale.html

7. Hong, J. Why have there been so many security breaches recently? Blog@CACM (Apr. 27, 2011); http://cacm.acm.org/blogs/blog-cacm/107800-why-have-there-been-so-many-security-breachesrecently/fulltext

8. Dodge, R., and Ferguson A., "Using Phishing for User Email Security Awareness," Proceedings of the 21st IFIP International Information Security Conference, Karlstadt, Sweden, May, 2006.

9. Dodge R., Rovira E, Radwick Z, and Shevchik J., “Phishing Awareness Exercises,” Proceedings of the 15th Colloquium for Information Systems Security Education, pg 120-125, 13-15 June 2011
10. Coronges, K., Dodge R., Mukina, C., Rovira E, Radwick Z, and Shevchik J., “The Influences of Social Networks on Phishing Vulnerability,” 2012 45th Hawaii International Conference on System Sciences, pg 2366-2773, 4-7 January 2012

11. www.pishme.com, accessed 15 Decemeber 2011