



Measuring the Effectiveness of In-the-Wild Phishing Attacks

Trusteer
December 2, 2009

Executive Summary

Trusteer measured the effectiveness of in-the-wild phishing attacks, and normalized the data for a single bank over one year, across one million customers. This method provides financial institutions with a yard stick to calculate losses associated with phishing attacks. Our key findings are:

- Each phishing attack compromises a very small number of customers (0.000564%), but due the large number of phishing attacks, the aggregated number is significant.
- 45% of bank customers who are redirected to a phishing site divulge their personal credentials.
- 0.47% of a bank's customers fall victim to Phishing attacks each year, which translates to between \$2.4M-\$9.4M in annual fraud losses (per one million online banking clients).

Introduction

There are a multitude of research findings and statistics on phishing attacks, which are based on monitoring spam lists, feedback from customers, and additional sources. As such, they can provide useful information on the number of phishing attacks per industry and per brand over time. For example, the Anti-Phishing Working Group publishes its Phishing Attacks Trend Report twice per year, which provides excellent data collected from various sources on the number of attacks over a six month period. However, no one today provides information on how successful these attacks are, how many users actually respond to phishing attacks, and how many submit their login information to criminal websites. The reason is simple – this information is extremely hard to collect.

The Trusteer platform provides a unique view into the success and failure of phishing attacks via its Rapport plug-in, which is installed on approximately three million computers across North America and Europe. Rapport constantly monitors phishing attacks against the computers it protects. The platform can also identify when users are trying to submit login information to phishing websites. These very unique characteristics allow Trusteer to collect valuable intelligence on the phishing industry, and on the damage suffered by banks and other victims as a result of this problem.

This paper summarizes findings and insights into Phishing outcomes that have never been available before now.

Phishing Refresher

Phishing attacks are attempts by criminals to lure internet users into divulging their personal information, such as online banking credentials, social security numbers, etc. This is accomplished by enticing users to visit a web site that resembles their bank's site or other trusted destination, and then requesting that they fill out forms that capture usernames, passwords, and other personal information.

Typically, a phishing attack begins with a spam email (which is the first contact point between the user and the attacker), allegedly from a legitimate banking institution. This email presents the user with a link, asks the user to click it, and then navigates the user to a website that appears to be operated by the bank. At this look alike site, the user is asked for login credentials (which may mimic the bank's login page), and possibly for other personal information (such as payment card details, phone number, mother's maiden name, and more).

This data is recorded by the site (which is operated by criminals). The user may be redirected to the genuine site at the end of the phishing flow.

Methodology

Our research is based on statistics gathered from Rapport web browser plugins running on users' PCs. Rapport detects phishing sites in two phases. First, it detects whether a user is accessing a phishing website. Then, it detects if the user attempts to type credentials into the site. These users are called "victims".

We collected data over a period of three months, during which phishing events from 10 large banks across the US and Europe were analyzed.

The data was normalized for the purposes of this paper per one million users. Hence, when we discuss the number of victims per bank, we are referring to the number of victims per one million users who are customers of that specific financial institution.

Phishing Statistics

How Many Phishing Attacks Reach the Customer's Browser?

Phishing usually starts with a fraudulent email that includes a link. Some of these messages are blocked by anti-spam systems and email-based phishing filters, and never even reach their intended targets. In addition, phishing take-down services used by many banks are very quick to react whenever a new phishing website is detected. As a result, many of these websites are taken down before users even have the chance to click through the email link and

reach the criminal site. Some browsers also include phishing filters which are updated when a new phishing website is reported, they so they can block the user from accessing malicious sites.

We only recorded phishing websites reached by users, that is, those that were live at the time that the user accessed them, and that were not blocked by any of the security mechanisms described above.

We found that over a three month period:

- Each financial institution was targeted, on average, by 16 phishing websites per week
- This translates to 832 phishing attacks per year per brand

According to the H1 Anti-Phishing Group report, the average number of phishing URLs per brand in June 2009 was 190. When compared to our findings, which only recorded successful Phishing events, we can conclude that just 1 out of each 2.7 phishing URLs actually reach their intended targets.

How Many Users Access Each Phishing Website?

Assuming that a phishing attack manages to reach its targets before the website can be taken down, how many users visit each phishing website?

To arrive at this number we need to consider several factors:

- The number of users that were served with the fraudulent link
- The effectiveness of phishing filters at the time of the attack
- The effectiveness of the messaging in the fraudulent email
- The period of time that the phishing website was live

On average, we found that 12.5 out of one million customers from a given bank visited each phishing website. Note that this is not the number of customers that received a phishing email or were targeted, but rather the number of customers that reached each phishing website, regardless of how many customers were actually targeted by each attack.

This ratio translates to just 0.00125%, a relatively small number. However, taking into account the large number of phishing attacks that occur over the course of 12 months, 1.04% ($12.5 * 832 = 10,400$) of a bank's customers visit a phishing website each year.

How Many Users Enter Their Login Information to Phishing Websites?

The most interesting finding from our research is the number of users who lose their login information to criminals. We found that approximately 50 percent of the time, users enter and submit their login information to phishing websites they visit. This means that for every one million users, 4,700 login details are lost to criminals each year. This represents 0.47% of a bank's customers.

Note that while some Phishing emails are very well-crafted and use very convincing messaging, once the user clicks on the link and accesses the website, there are a few visual clues that indicate they are not at the bank's legitimate site. One clue is the phishing website URL, which is different than the bank's real URL. While criminals try to confuse users by selecting URLs that look similar to the bank's address, a close examination of the URL can reveal that it is not a genuine website. Another indicator is that these websites do not usually use SSL, and if they do, their certificate does not match the bank's address.

Calculating Financial Losses

Estimating and calculating the monetary losses associated with each compromised online banking account can be achieved using several assumptions. For example, if we assume that on average, the loss per compromised account is \$2,000, this translates to \$9.4 million per year per each one million customers, or \$9.4 per customer per year. If we assume an average loss of \$500 per compromised account (a number we believe is very low), the total losses per one million customers per year is \$2,350,000 or \$2.35 per customer.

Note that these numbers reflect losses from phishing attacks only. There are other very successful attack vectors, mainly malware, that also cause huge financial losses for banks.