



Annual ADFSL Conference on Digital Forensics, Security and Law


2016
Proceedings

May 26th, 9:00 AM

Assessing the Gap: Measure the Impact of Phishing on an Organization

Brad Wardman
PayPal Inc., brad.wardman@yahoo.com

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Aviation Safety and Security Commons](#), [Computer Law Commons](#), [Defense and Security Studies Commons](#), [Forensic Science and Technology Commons](#), [Information Security Commons](#), [National Security Law Commons](#), [OS and Networks Commons](#), [Other Computer Sciences Commons](#), and the [Social Control, Law, Crime, and Deviance Commons](#)

Scholarly Commons Citation

Wardman, Brad, "Assessing the Gap: Measure the Impact of Phishing on an Organization" (2016). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 2.
<https://commons.erau.edu/adfsl/2016/thursday/2>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



ASSESSING THE GAP: MEASURE THE IMPACT OF PHISHING ON AN ORGANIZATION

Brad Wardman
PayPal Inc.
2211 N. 1st Street
San Jose, CA 95131
brad.wardman@yahoo.com

ABSTRACT

Phishing has become one of the most recognized words associated with cybercrime. As more organizations are being targeted by phishing campaigns, there are more options within the industry to deter such attacks. However, there is little research into how much damage these campaigns are causing organizations. This paper will show how financial organizations can be impacted by phishing and present a method for accurately quantifying resultant monetary losses. The methodology presented in this paper can be adapted to other organizations in order to quantify phishing losses across industries.

Keywords: phishing, cybercrime, economics

1. INTRODUCTION

The cybercrime referred to as ‘phishing’ is a social engineering attack used by the criminal to lure the victim into divulging information. These attacks typically employ spammed emails and fraudulent websites to obtain the information. The information collected by these attacks can be used in identity theft, to remove funds from a customer account, and in theft of online resources [12].

The number of phishing attacks reported by various researchers and organizations is continuing to rise; however, the associated losses appear widely divergent. For instance, industry security company RSA reported that in 2013 there were nearly 450,000 phishing websites that accounted for \$5.9 billion in estimated losses [9]. Interestingly, RSA reported that in 2012 there were around 445,000 phishing websites that accounted for

\$1.5 billion in estimated losses [10]. Note that over this period of one year there was an increase of only 5,000 phishing websites and yet a substantial rise in estimated losses of \$4.4 billion. Gartner Research reported in 2008 that over 3.6 million Americans alone lost an average of \$886 per phishing attack in 2007 [6]. Using these numbers, it was approximated that there was an estimated loss of \$3.2 billion. Other researchers claim that the estimated losses in 2007 caused by around 113,000 phishing websites was approximately \$61 million [5]. Given the lack of proper resources currently invested by organizations into anti-phishing strategies and research, the estimated loss of billions of dollars is unlikely. However, the question remains: how much does phishing cost organizations? Organizations understand that phishing is a problem, yet many do not measure what that loss is to the economic bottom line.

In order to accurately measure phishing it is important to understand that the number of phishing websites targeting an organization may not directly relate to the amount of money lost by that organization. Furthermore, the organization with the highest volume of phishing websites does not necessarily have the highest volume of customers visiting phishing websites. While PayPal is often deemed the most targeted organization using phishing URL volume [1] [4], it is yet to be determined which companies' customers visit the most phishing websites and perhaps lose the most information.

In addition, the phishing URL volume is a poor measurement of distinct phishing attacks because some phishing groups use dynamic machine names and URLs to redirect all traffic to the same phishing website. Consequently, thousands of phishing websites that appear to be unique attacks should actually be considered one attack. This mitigates the effects of blacklisting as well as some takedown efforts. Exact URL matches are required to take action and the multitude of dynamic machine names and URLs impedes blacklisting and overwhelms takedown queues [1].

Phishing is an ecosystem problem and thus needs to be properly handled by the entire industry. Phished information may be reused against other organizations, so data collected by phishers from social networking phishing websites may also be used to attempt logins on email and financial accounts. The anti-phishing community has ensured that some safety nets can be deployed such as browser-based blacklisting, which will prevent potential victims from visiting phishing websites in the browser [14]. In addition, methods of email authentication such as DMARC often prevent phishing emails and URLs from reaching customers. DMARC was standardized in March of 2013, and has currently blocked more

than two billion suspicious emails, and covers greater than 80% of typical US email users [3]. Nonetheless, organizations still need to understand how phishing attacks targeting their own organization impact the business' bottom line.

PayPal recently performed an analysis of the impact phishing has on its business and thinks it would be appropriate to share the methodology with other organizations in the hope that it will help those organizations better assess the status of their current phishing situation. The example numbers and percentages that follow are based on internal data and external research and will provide estimates that reflect the current situation. The paper's intent is to present a method that will allow companies to measure the effect of phishing on their business. We do not present empirical data because currently this is sensitive information for internal use exclusively and its omission does not impede the utility of the method. This paper therefore prepares financial organizations with starting criteria to measure the impact of phishing on their organization. The Different Impacts of Phishing section presents the various forms of impact that phishing can have on an organization.

The Direct Monetary Loss section provides an equation that can be used by financial organizations to measure the direct monetary loss caused by phishing. These same models can be slightly modified to measure the impact on other types of organizations such as social networking, gaming, and identity providers. The Example Calculations and Results section presents a scenario that demonstrates how the equation and variables can be used to obtain the direct monetary loss. Finally, there is the Limitations section that describes some of the limitations to this work and how additional measures can be taken to obtain more accurate results.

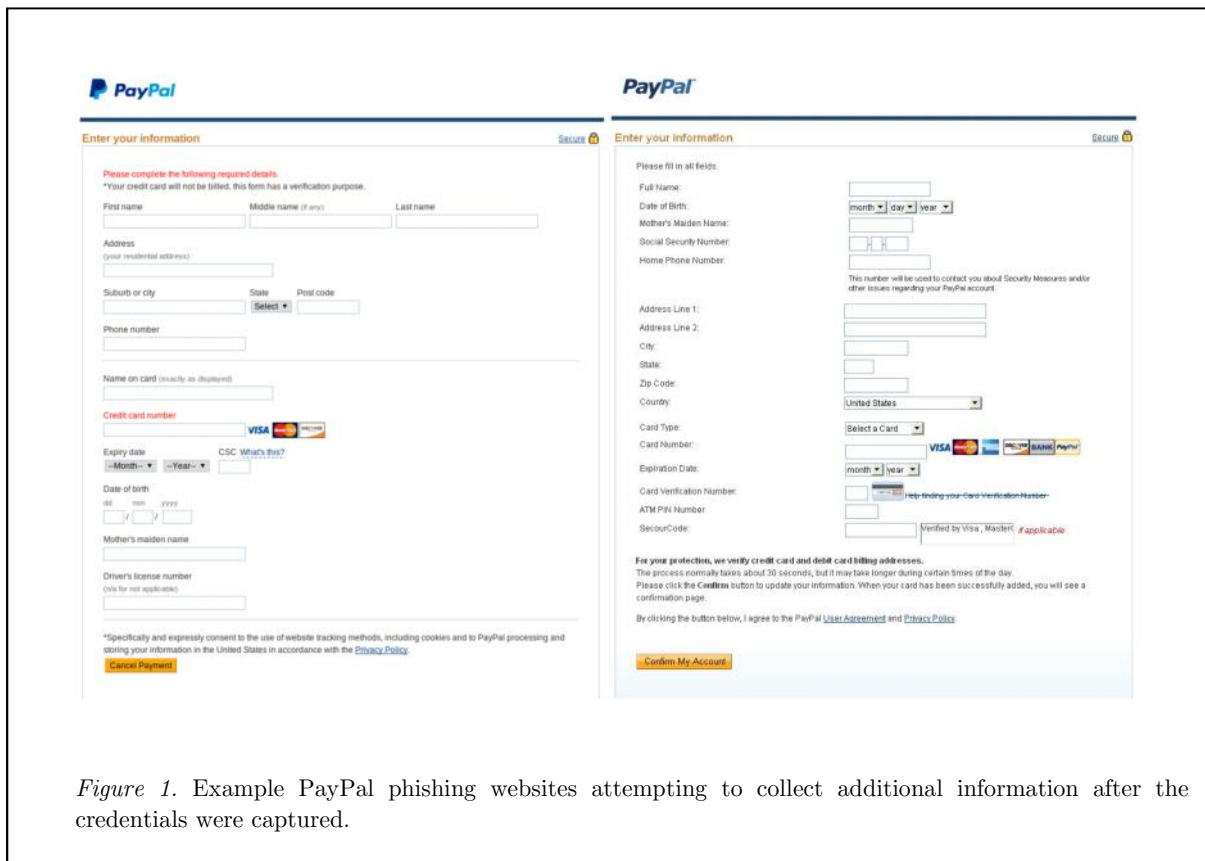


Figure 1. Example PayPal phishing websites attempting to collect information after the credentials were captured.

2. DIFFERENT IMPACTS OF PHISHING

2.1 Direct Monetary Loss

Direct monetary loss due to phishing determines the amount of monetary damage an organization incurs when its customers' information is lost. Typically, people think of phishing as synonymous with acquiring login credentials; however, normal phishing campaigns request numerous pieces of personally identifiable information as observed in the phishing website screenshots in Figure 1. Example data that is collected by phishers are login username and password, first and last names, credit and debit card numbers, CCV2, home addresses, and other pieces of information that can be used to steal a

person's identity [2]. Therefore, direct monetary loss determines how much money it costs the company to, for example, reimburse customers for the monetary loss they incur by losing their information or having their account compromised.

2.2 Operational Costs

Another loss that needs to be considered is the amount of money an organization spends on handling phishing attacks. Examples include but are not limited to:

2.2.1 Takedown efforts

The removal of the phishing content from domains, phone numbers used in vishing (voice phishing), and email addresses used as drop boxes or for spamming. Some organizations choose to perform takedowns using internal

resources, while others pay external takedown companies to handle the phishing campaigns.

For example with 40,000 phishing websites per year:

- Takedown by an external party costs \$35 per website
- Takedown operational costs = \$1.4M per year

2.2.2 Customer service phone calls

Customers with questions frequently contact customer service agents about whether a suspicious email is legitimate or a phish. Such calls often last much longer than typical customer service calls as they require the agent to go through a number of steps to identify phishing indicators as well as to properly comfort the customer.

For example with 40,000 phishing websites per year:

- Customer service agents receive \$10 per hour
- Each call lasts on average 20 minutes
- Average of 2 calls per phishing attack
- Customer service phone call operational costs = ~\$267K per year

2.2.3 Handling incoming customer emails and feeds

Infrastructure and software is required to properly handle phishing reported by customers, researchers, and feeds from industry in an appropriate manner.

2.2.4 Building anti-phishing technologies

Building anti-phishing technologies requires building or buying software capable of

collecting data on phishing attacks, whether it is to identify attacks faster, identify the culprits behind the attack, or develop other ways that organizations collect more information on phishing attacks (e.g. passive DNS, intelligence feeds, and DKIM bounces). In addition, building anti-phishing technologies requires coming up with new industry standards to prevent phishing such as DMARC.

2.2.5 Investigations

A significant amount of resources is invested in third-party or in-house investigative services.

2.3 Brand Damage

This variable is typically overlooked when trying to quantify the monetary impact of phishing on an organization. Brand damage is very difficult to determine and predict; however, there are three important variables that can help in this calculation.

The first is measuring the number of customers that leave and/or close their accounts with the company because they were phished. An organization would need to compare their normal attrition rate to the attrition rate of customers that they can identify as being phished. The past revenue on each of those accounts can then be used to derive the future revenue that was lost on each account, thus providing some estimate of brand damage caused by phishing.

The second variable is to look at accounts that were not closed in response to a phishing attack, but that experienced a significant drop in transaction frequency or dollar value. By measuring the drop, an organization can assess a level of loss that may be triggered from the customer losing trust in the brand or in their ability to safely use the service.

The final variable is the cost to the organization to gain new customers. An organization is likely taking a substantial loss

if it has to replace the customers who left due to phishing with an equal number of new customers. Unlike the previous two variables many organizations have marketing departments that do calculate the cost of acquiring new customers, but this number has not generally been used by organizations to associate with equations on losses due to phishing or accounts being compromised.

3. DIRECT MONETARY LOSS

3.1 Direct Monetary Loss Equation

Of all of the variables presented above, measuring the direct monetary loss is typically what the business wants to better understand. This section provides the variables that can be used to determine the direct monetary loss value per year. The equation that can be used is:

$$\text{Direct Monetary Loss} = \text{numSites} \times \text{avgVisit} \times \%Creds \times \text{monetized} \times \text{avgLoss}$$

Where:

- *numSites* is the number of phishing websites per year
- *avgVisit* is the average number of customers visiting each website
- *%Creds* is the percentage of valid credentials acquired by each phishing website
- *monetized* is the number of credentials that undergo attempted monetization
- *avgLoss* is the average amount of loss due to a compromised account

The following section will describe ways to obtain the values for each variable. If properly collected, the data can be used to get within an order of magnitude of direct monetary loss,

and sometimes even more accurate, as demonstrated in an example below.

3.2 How to Collect the Data

The first variable, *numSites*, is probably the easiest variable to collect. The industry understands that there are gaps in phishing data; however, the aggregation of internal and industry sources can often lead each organization to a near complete data. More research would then need to be performed to determine exact coverage. The additional research would consist of aggregating data across a variety of different sources such as blacklists, security companies, and industry groups and comparing the aggregate data set to that collected by the organization. An organization can use that research to estimate what their coverage is and use it within the equation to account for websites that the organization may have missed.

The second variable, *avgVisit*, requires organizations to perform more research. One method for collecting data on the visits (i.e. by IP address) to phishing websites is to use organizational web server logs. Many phishing websites use the resources (e.g. graphics, JavaScript files, and CSS files) of the organization they are phishing to render their website [11]. In fact, one of PayPal's internal feeds identified that over 65% of the phishing websites use at least one PayPal resource. An example strategy an organization could employ is analyzing the web server logs to look for resources being used on confirmed phishing websites. The web server logs would provide all IP addresses that visited the phishing URLs. This data could be used to calculate the average number of distinct IPs that visit each phishing website. But this calculated average does not necessarily only consist of the number of customers that visited. Included in this number are visits by takedown specialists, security researchers, and other organizations

such as Google and Microsoft that crawl these websites over and over again to confirm that they are malicious (i.e. phishing) and to ensure they are still active. There are a number of ways to differentiate customers from the anti-phishing communities. One way is to use WHOIS information to parse out the IP addresses that are confirmed to be associated with certain anti-phishing organizations. Another way is to use only IP addresses that visit one of the phishing pages per year. We understand that this may lose a few victims that are on a shared IP or that some anti-phishing communities use cloud services to visit the pages, but largely, this filter should work properly. The example in the next section will back this idea.

The third variable, *%Creds*, is the percentage of credentials that were harvested by the phishing website. Potential victims do not lose their credentials to a phishing website just because they visit the web page. Therefore, this variable calculates the percentage of victims who lose their legitimate credentials. *%Creds* is the hardest variable to obtain and fully measure without the support of email providers and law enforcement; however, there are a number of ways to collect such information on a smaller scale. The first method is by collecting “drop files” in which the phishing websites write the stolen data to a temporary file in order to store the information for later retrieval. Analysis of the collected data can be used to determine the *%Creds* variable. Another method is based on the fact that some phishing websites log the user into the legitimate organization after the login credentials are submitted to the phishing website. This lures users into believing they are entering their credentials into the proper website and enables a check of the validity of the credentials. Organizations can then analyze the credentials submitted by the phishing website to the organization’s login page to

determine the percentage of valid credentials to invalid credentials. This variable is important as it allows the organization to know what percentage of visiting customers entered legitimate data.

The *monetized* variable is also organizationally dependent. This variable is used to calculate the number of stolen valid credentials that the criminals will attempt to monetize. Organizations can collect the *monetized* variable by comparing the number of accounts of which user credentials are known to be compromised (through methods such as detecting account password validation and unauthorized account access) to the number of accounts that had advanced functionalities performed on the account such as transferring money, changing account information, and selling goods. Essentially, there is a major difference between attackers checking if a password is valid versus actually trying to monetize the account by making a transaction. While currently there are no published numbers by organizations on monetized variables, observations on internal and external data suggest that many organizations consider attempted monetization on accounts that are harvested to be around 10-20%.

The last variable, *avgLoss*, allows organizations of various types to insert their own measurement of loss to determine the direct monetary impact that occurs when a customer’s account is compromised. For financial institutions, this number may be derived from the amount of money the organization has reimbursed a customer or a merchant because the phished account was used to make some purchase or transfer money.

4. EXAMPLE CALCULATIONS AND RESULTS

One interesting result from the use of this method at PayPal was that variations in the variables only slightly affected the direct loss that the organization incurred. The example scenario below demonstrates how this works.

4.1 Example Variables on One Year of Data

- We will continue with the previous example of 40,000 (*numSites*) phishing websites per year.
- Of the 40,000 URLs, 60% of the URLs had IP address data found within the web server logs. That means that there are 24,000 URLs with IP address data. One limitation to this equation is the fact that this proportion may not be representative of the entire data set. See the Limitations section below for further discussion.
- 90,000 IP addresses only visited one of the 24,000 URLs. We hypothesize that there should be an insignificant number of phished customers that visit 2+ phishing websites and lose data within a year.
- The 90,000 distinct IPs suggests that the average number of visitors to each phishing website per year is 3.75 (*avgVisit*).
- In this scenario, which is close in numbers to internal research, only 96,000 distinct IPs visited one to four different phishing URLs. The 96,000 would move the *avgVisit* to

only 4, which will be demonstrated to be insignificant.

- Finally, the organization’s loss per set of credentials is set to \$40 (*avgLoss*).

4.2 Estimated Yearly Loss

From the data above it is apparent that there are some values that have been estimated; however, it can be demonstrated in the results below that these variations have little effect. Table 1 shows the direct monetary loss resulting from the variation in the proportion of submitted valid credentials (Y-axis) and monetization (X-axis).

Table 1
Direct losses incurred with IP addresses visiting one phishing website using variations in the percentage of valid credentials (y-axis) and percentage monetized (x-axis)

	10%	25%	50%	75%	90%
20%	\$120K	\$300K	\$600K	\$900K	\$1.1M
33%	\$198K	\$495K	\$990K	\$1.5M	\$1.8M
50%	\$300K	\$750K	\$1.5M	\$2.3M	\$2.7M

The calculation may be further illustrated assuming 50% of attacks submitted credentials and 10% attempted monetization. Along with the hypothetical inputs above (40,000 websites x 3.75 average visitors x 50% submitted valid credentials x 10% attempted monetization x \$40 as value for compromised credential), the final loss equals \$300K.

Even when varying the attempted monetization, the values do not drastically increase until levels of 50% and 75% are attained, which are extreme for large organizations, but may be realistic for smaller

organizations who have accounts sold or traded less often.

Taking into account the IP addresses that visited phishing websites one to four times does not strongly affect the overall loss numbers. Comparing values from Tables 1 and 2 shows that there is only the 0.25 increases in these values.

Table 2
Direct losses incurred using IP addresses that visited one to four phishing websites

	10%	25%	50%	75%	90%
20%	\$128K	\$320K	\$640K	\$960K	\$1.2M
33%	\$211K	\$528K	\$1.1M	\$1.6M	\$1.9M
50%	\$320K	\$800K	\$1.6M	\$2.4M	\$2.9M

5. LIMITATIONS

We understand that there are limitations to the method presented. The first noticeable limitation is differentiating the customer IP addresses from anti-phishing and researcher IP addresses. We stand by our statement that the chance of the same IP address being used by multiple customers to visit the same phished organization from the same phishing site within a year is insignificant. In PayPal’s research, we found that there was very little difference between the number of IP addresses visiting one phishing website and the number of IP addresses visiting up to four phishing websites. Also, we have observed that WHOIS data analysis can be used to filter out a substantial number of the anti-phishing IP addresses.

Another limitation is that the percentage of URLs of the number of victim IP addresses visiting phishing websites (60% in the above example) may not be representative of the

entire data set. If the data was collected randomly then it should be accurate. However, if the data was not collected randomly it will be slightly less accurate as different attacks may entice different numbers of users to visit and submit information. PayPal found that one security tool was able to collect IP data on over 60% of its phishing URLs, while another source of information had greater than 35% coverage. Organizations should aggregate data across all tools if possible. If a complete investigation is needed, an organization can perform an analysis on the remaining URL data set with a statistically significant sample. An example might consist of the organization requesting the sample size in web server logs from the web server owners that were hosting the phishing content. These logs can be parsed to determine the number of visitors and thus add to the strength in the variable *avgLoss*.

A final, major limitation that needs clarification for the whole industry is ascertaining the validity of the percentage of credentials submitted per visitor. Scenarios for calculating this variable were presented above, so we will not restate those strategies; however, we would like to revisit how collaborative work with email providers and even law enforcement can greatly assist with this metric. The anti-phishing community is well aware that most of the stolen information is communicated to the phisher using “drop email addresses” [13] or “drop mail boxes” [8]. These email addresses are collected from phishing kits by a number of researchers and security companies [7]. Industry could perform a large-scale study checking the validity of the credentials sent to these email addresses from phishing websites.

6. CONCLUSIONS

The ultimate goal of this work is to help organizations better understand how to gauge the impact that phishing has on its business.

There are a variety of ways that an organization is affected by phishing, including direct monetary loss, operational costs, and brand damage. Each of these metrics is equally important when considering the amount of money that should be invested into counteracting phishing attacks. In addition to defining the various ways that phishing can impact an organization, this paper presents and details an equation and associate variables that can be used to measure the direct monetary loss a financial organization incurs due to phishing. There are limitations to the equation and its variables; however, most organizations do not know if phishing is costing them thousands, tens of thousands, hundreds of thousands, or even millions of dollars. PayPal hopes that the research presented in this paper will be used by organizations to better assess the status of their current phishing situation.

REFERENCES

- Aaron, G., & Rasmussen, R. (2014), Global Phishing Survey: Trends and Domain Name Use in 2H2013. Retrieved May 31st, 2014. APWG, http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2013.pdf.
- Cyren, Internet Trends Threat Report. Retrieved May 31st, 2014. <http://www.cyberoam.com/downloads/ThreatReports/CyberoamCYRENInternetThreats2014April.pdf>.
- DMARC. DMARC – Overview. Retrieved June 1st, 2014. <http://www.dmarc.org/overview.html>.
- Greenberg, A. (2014), PayPal phishing websites spike in 2014, easy vector for attackers. Retrieved May 31st, 2014. <http://www.scmagazine.com/paypal-phishing-websites-spike-in-2014-easy-vector-for-attackers/article/349084/>.
- Herley, C. and Florencio, D. (2008), “**A profitless endeavor: phishing as tragedy of the commons**”. *NSPW 08' Proceedings of the 2008 workshop on New security paradigms*. Pages 59-70. ACM.
- McCall, T. (2007). Gartner Survey Shows Phishing Attacks Escalated in 2007; More than \$3 Billion Lost to These Attacks. Gartner.
- McCalley, H., Wardman, B. and Warner, G. (2011), “Analysis of Back-Doored Phishing Kits”, *Advances in Digital Forensics VII: IFIP Advances in Communication Technology Volume 361*. 2011.
- Moore, T. and Clayton, R. (2012), “Discovering phishing dropboxes using email metadata” *APWG eCrime Researchers Summit*, October 2012.
- RSA, 2013 A Year in Review. Retrieved June 1st, 2014. <http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf>.
- RSA, The Year in Phishing. Retrieved June 1st, 2014. <http://www.emc.com/collateral/fraud-report/online-rsa-fraud-report-012013.pdf>.
- Wardman, B., Britt, J., and Warner, G. (2014) “New Tackle to Catch a Phisher”, *International Journal of Electronic Security and Digital Forensics*.
- Wardman, B., Kelly, L., and Weideman, M. (2013) “Voice of the Customer: What is the Real Experience?”, *APWG eCrime Researchers Summit*, October 2013.
- Wardman, B., Warner, G., McCalley, H., Turner, S., and Skjellum, A. (2010) “Reeling in Big Phish with a Deep MD5 Net”, *Journal of Digital Forensics, Security and Law*. 5(3).
- Whittaker, C., Ryner, B., and Nazif, M. (2010) “Large-Scale Automatic Classification of Phishing Pages” *NDSS '10*.