Phishing: Crime That Pays

Philip J. Nero, Brad Wardman, Heith Copes, Gary Warner
University of Alabama at Birmingham

Abstract—Email phishing requires functional countermeasures, as does any crime that results in millions of dollars in yearly losses. Many financial institutions currently combat phishing by contracting takedown companies that remove relevant phishing websites as soon as possible after they are detected. By comparing the median time necessary for professionals to take a phishing website down to the average time it takes for a phishing website to turn a profit for its creator, I have demonstrated the overall effectiveness of the takedown process. On average, takedown companies fail to eradicate phishing websites before their creators garner valuable information from multiple victims. Furthermore, forensic evidence that could lead to the arrest of the cybercriminals responsible for the phishing websites is often ignored because these takedown companies do not profit from cooperating with criminal investigations. Therefore, website takedown is ineffective as a primary phishing countermeasure. An anti-phishing protocol that involves website takedown, but also includes investigation and eventual prosecution would likely be more effective than a self-perpetuating system that concludes after a malicious website is terminated.

***Index Terms*—Phishing, Investigations, Justice Science**

I. INTRODUCTION

In the second book of *Republic*, Socrates discusses the concept of the Ring of Gyges. This ring, when worn, renders the bearer invisible. Socrates states that, if such a ring were to exist, its bearer would inevitably turn to a life of immorality and crime. Socrates believed that a man could not resist criminal behavior if there were no consequences to deter it. Such undeterred criminality occurs today with the practice of phishing, which is the use of deceptive emails to convince victims to divulge confidential information. Phishers create and distribute emails that closely resemble emails from legitimate financial institutions. These emails might ask victims to respond to the email with their username, password, credit card number, social security number, and other exploitable information. The simplicity of this process is evidenced by the prevalence of the crime and the large amount of money that is stolen.

The 2010 Javelin Strategy Identity Theft & Fraud Survey shows that there were an estimated 11.1 million victims of identity theft and/or fraud in 2009 (Javelin, 2010). These victims lost over 54 billion dollars. A large percentage of these victims were victims of cyber-based criminal activity. According to a recent Gartner Research study, 3.6 million American consumers lost money to phishing scams in 2007 (Gartner, 2007). Each phishing victim lost an average of $361. Therein, the approximate financial loss to phishing in the United States in 2008 was nearly $2 billion. These studies also show that financial institutions accrue $1 billion in losses from phishing every year. The above statistics demonstrate serious criminal activity, but the real problem is that the vast majority of phishers go unpunished.

Volumes of studies describe the creation and evolution of phishing that has occurred over the last 15 years. Within this research, however, there are few studies discussing methods of gathering evidence against to successfully prosecute phishers (Wardman, 2010; Cova et al., 2008). The current research seeks to shed light on this unexplored problems. Specifically, it uses data collected through telephone interviews with online security departments to explore the online security practices of major financial institutions. These interviews were designed to elicit how each financial institution's online security functions. The interviews demonstrate how financial institutions identify phishing websites, take down the malicious content, and how they follow up with law enforcement to track, arrest, and prosecute the phishers. The assumption is that these interviews will demonstrate that little follow-up is completed by the financial institutions and only a small percentage of the phishers are prosecuted. If this is the case, then further research needs to be conducted to show how best to identify, track, and arrest phishers so that phishing no longer goes unpunished.

To explore the online security practices of major financial institutions, telephone interviews were conducted involving specialists within the online security departments. The names of the financial institutions and specific quantitative data pertaining to these financial institutions are intentionally excluded from this report to preserve the anonymity of these financial institutions. Next, phishing data pertaining to the relevant financial institutions was gathered. A large collection of fraudulent email was searched for phishing emails that mimic legitimate emails from the studied financial institutions.

The number of phishing emails, controlling for the online prevalence of the bank, are used as an objective means to demonstrate the effectiveness of each institution's corporate security procedures. Actions, attitudes, and response measures of the banking professionals may shed light on target selection. By interviewing financial institution fraud staff, this research hopes to identify causes of disproportionate targeting.

II. Related Work

The primary defense against phishing emails is the email provider. Most email providers, such as Google (Gmail), scan incoming mail in an attempt to filter out spam and phish. This is accomplished by searching each email for bit strings that are previously determined to be characteristic of spam and phishing emails (Wardman et al., 2009). Common points of deception in emails include misleading header information and misleading hyperlinks (Zhang et al., 2006; Zhang et al., 2007).

Emails that attempt to elicit an email response must contain a significant amount of deceptive information to request the confidential information and convince the victim to send it. An email of this type will most likely contain bit strings that trigger the email provider's spam blocker. An email that functions only to send a reader to a fraudulent website might be more likely to avoid detection. Public education, which is perhaps the most important defense against cyber fraud, teaches the public to ignore links within emails, even if the source of the email appears to be legitimate (Sheng et al., 2010).

Once a phishing website is discovered, an analyst performs a WHOIS lookup on the URL. The information from a WHOIS search determines how best to proceed when attempting to take down the phishing website. When the phishing website's URL is entered into the WHOIS search field, the directory information reveals when the website was created and who registered it (Shah et al. 2009). If the phishing website was created within the last month, then it was likely created by the phisher through a negligent hosting company. If the website was created years ago and has corporate demographic information that seems to correspond to the URL, then the website may have been hacked. In the case of a hacked legitimate website, the investigator should contact the listed webmaster and inform them that their URL is now linked to a phishing website (Wardman et al. 2010). The webmaster will often rectify the situation personally. If it seems likely, however, that the website was created by a criminal to spoof a legitimate website, then different steps need to be taken.

Many factors determine how long a phishing website will stay active. First, the website must be detected. Some phishing websites are brought to the attention of the financial institution they spoof by alert customers who recognize the fraud. Major banks have links on their websites that allow customers to report fraudulent activity. Another method of detection used by both take-down companies and financial institutions involves honeypots. These honeypots collect phishing emails and extract link information that automatically detects the existence of a phishing website and begins the take-down process (Li & Schmitz, 2009).

A successful phishing attack involves eight basic steps: 1) Preparation: in this step, the phisher prepares for the attack. This involves registering domains and creating fraudulent websites. 2) Delivery of the Lure: as previously mentioned, the phisher has several potential methods to attract the victim to the phishing website. 3) Taking the Bait: the user follows a path, set forth by the phisher, which makes him or her susceptible to online theft. 4) Request for Confidential Information: the user is taken to a spoofed website that closely resembles a legitimate website representing a financial institution. This fraudulent website prompts the user to input their sensitive credentials. 5) Submission of Information: the victim relinquishes the target information. 6) Collection of Data: the phisher gathers the confidential data. 7) Impersonation: someone uses the compromised data to impersonate the victim. 8) Financial Gain: someone profits from the stolen information (Jakobsson & Myers, 2007). Current phishing countermeasures function by disrupting this process at one of the steps above.

Proactive countermeasures can interrupt the aforementioned process at Step 1 by preventing the creation of fraudulent websites. Email providers, such a Google and Yahoo, can halt the process at Step 2 by recognizing the signature of a fraudulent website and preventing it from being delivered to the user. The education of Internet users is the defense against Steps 3-5. An informed user can be instructed on how to spot a phishing email and thus, avoiding suspicious links (Step 3), or at least recognizing a spoofed website and not submitting confidential data (Steps 4-5) (Kumaraguru et al., 2007). The majority of professional anti-phishing techniques are designed to break the chain at Step 4 by taking down fraudulent websites (Moore & Clayton, 2007). Countermeasures that disrupt the process at Step 6 function at the server level. Once users submit their credentials, they are transmitted to a server, which then delivers the information to the phisher. Software can be implemented that will recognize credit card numbers, social security numbers, etc. and prevent them from being relayed to the phisher (Li & Schmitz, 2009). A multitude of security measures exist that attempt to thwart criminals from completing Steps 7 and 8 or profiting from a victim's stolen identity. However, they seem unable to stop the practice reliably as noted by the vast amount of money stolen yearly through phishing (Gartner, 2007).

Institution	Number of Phishing Related Employees	Median Take-Down Time	Rank Among These Banks in Level of Phishing Attacks	Frequency/Nature of Contact with Law Enforcement
Bank 1	3	24	4	Has worked with law enforcement in 2 or 3 cases, but only when approached by law enforcement
Bank 2	4	15	5	None
Bank 3	2	20	2	None
Bank 4	3	8	3	Works with FBI and Secret Service to aid in website site shutdown
Bank 5	4	24	1	None
			Average Number of Cases per Day per Analyst	
T-D 1	10	6	80	Delivers raw data to federal law enforcement via local field offices
T-D 2	20	5	100	Little to none
T-D 3	18	3	75	Works with federal and international law enforcement; seeks prosecution in ≥ 1% of cases
T-D 4	12	6	65	None
T-D 5	12	4	100	Rare interaction; delivers raw data to local FBI field office

Table A: Key Data for Comparison from Interviews

III. Methods

The goal of this study is to analyze currently used anti-phishing measures and determine their effectiveness. Both qualitative data and quantitative data were gathered. Through comparative analysis of the two types of data, a correlation between techniques and observed phishing activity emerged.

A. Qualitative Methodology

Anti-fraud investigators from five major financial institutions were interviewed. The financial institutions contacted were chosen because of their national rank among banks pertaining to consolidated assets. All five of the institutions are listed within the top twenty financial institutions based on consolidated assets and volume of online transactions. All of these banks have headquarters in the Southeastern United States, so it was not difficult to find a reference that knew the bank employees and could make introductions. For the purposes of anonymity, these representatives will be referred to as follows: Bank Employee 1, Bank Employee 2, Bank Employee 3, Bank Employee 4, and Bank Employee 5. The financial institutions were ordered from one to five based on the consolidated assets reported between 2008 and 2009.

The five anti-fraud investigators were interviewed, by telephone, using semi-structured interviews. (The interview questions are listed in Appendix A.) These interviews lasted an average of thirty minutes. The questions pertained to the day-to-day operations and the skill sets of the individuals interviewed. Initial interviews showed that it was common for these financial institutions to outsource to third party take-down companies. Representatives from five of these third party companies were contacted and interviewed to determine what methods they used to combat phishing. Similarly to the financial institutions, the names of the take-down companies remain anonymous. The five take-down companies were chosen because they are major companies that have been in existence for several years and they have well-established practices. None of the companies is currently employed by any of the five banks used in this study. For purposes of anonymity, these employees will be referred to individually as Take-Down Employee 1, Take-Down Employee 2, Take-Down Employee 3, Take-Down Employee 4, and Take-Down Employee 5. The numbering within this group is arbitrary. The interview questions for the take-down company personnel are listed in Appendix B.

B. Quantitative Methodology

The quantitative section of this study was designed to show which financial institutions were most affected by phishing. The guideline for this measurement comes from an analysis of a database containing millions of phishing emails. Queries reveal the financial institutions that have the most phishing emails accumulated from month to month over a two-year period (Wardman, 2010). In Table A, financial institutions were ranked from 1 to 5, 1 representing the highest level and 5 the lowest, demonstrating how their phishing levels related to one another. This level was determined by examining UAB's phishing database.

The UAB Spam Data Mine is a collection of spam emails from numerous sources. Multiple companies have programmed their spam filters to block undesired spam messages from their customers and employees and forward the messages to UAB's data mine. Through this process, the data mine accumulates millions of spam

emails daily. The content of these spam emails varies, including fraudulent product sales (e.g., Acai berry diet formulas, prescription pills, and small personal electronics), advance fee fraud (US Dept. of State, 1997), and phishing emails. These emails are sorted upon receipt and potential phishing emails are compiled separately. Using a simple program, link URL's from within these phishing emails are stripped and catalogued. These URL's are then tested by a human analyst to determine if they resolve to an active phishing website.

Once a phishing website is discovered, the analyst determines which legitimate financial institution the website is imitating. The phishing websites are finally sorted into groups based upon which institution they are mimicking. The resulting data was used in this study to determine which of the selected, major financial institutions had accumulated the most unique phishing websites. A query of the categorized phishing database showed the number of phishing emails recorded in 2008 and 2009. These results were then searched and categorized to reveal the number of phishing emails pertaining specifically to the banks involved in this study. These emails were then analyzed to determine the phishing website to which these emails resolved. This was a much smaller number because thousands of emails could potentially resolve to the same website. The financial institutions were then ranked from 1 to 5 by the number of phishing websites that were created with their name. The financial institutions were also ranked according to consolidated assets as of December 31, 2010 (Federal Reserve Statistical Release, 2010). Financial institutions were initially chosen for this study because they ranked highly on this list.

IV. Results

A. Quantitative Results

The quantifiable data from the interviews is presented in Table A. The first column in Table A shows the number of employees within each phishing team. This data for the banks reflects the current number of phishing-related employees, though some bank employees mentioned that they had more people involved when they were taking down their own phishing websites. Interviews with the five bank employees and five take-down company employees revealed median take-down times ranging from three to twenty-four hours. The take-down companies reported median take-down times that was considerably lower than those claimed by the financial institutions. This could be due to over-reporting by the take-down companies or possibly the financial institutions were reporting the average take-down time rather than the median.

The third column is split to show one data value for financial institutions and another for the take-down companies. As previously mentioned, the financial institutions were ranked from 1 to 5, 1 representing the highest level and 5 the lowest, demonstrating how their phishing levels related to one another. For example, when compared to the other four banks in the study, Bank 5 had the most documented phishing attacks within the two-year study period. This merits attention because Bank 5 is named such because it ranks fifth in consolidated assets within the group. The bottom half of this column relates to the workload experienced by analysts at the take-down companies. The last column within this table denotes the level of interaction with law enforcement. This data is subjective, but it is notable that several banks and take-down companies incorporate little or no law enforcement involvement.

B. Qualitative Results

This project sought to determine which phishing countermeasures used by financial institutions are most successful. Success was to be objectively determined by comparing the consolidated assets of the bank to the number of phishing websites discovered in the UAB Spam Data Mine. Theoretically, consolidated assets should be directly correlated to number of observed phishing websites. However, the previous analysis demonstrated that this presumption was incorrect. The data retrieved from the initial interviews gave an overview of the anti-phishing techniques used by each of the financial institutions. An unexpected pattern emerged; few financial institutions that were contacted perform their own phishing investigations. All but one of the financial institutions had contracts with take-down companies. The purpose of these take-down companies is to discover phishing sites and take them down as quickly as possible. It was postulated, therefore, that the number of observed phishing websites must be primarily affected by the phishing countermeasures incorporated by the financial institutions. After interviewing the five representatives from the financial institutions, it became clear that a larger issue existed. Namely, not one of the financial institutions interviewed sought prosecution against the criminals responsible for the phishing websites.

The bank and take-down company employees gave multiple reasons for not working with law enforcement. Bank Employee 4 stated:

> "We just don't get anything out of working with law enforcement. They're usually pretty slow and this is a game of speed. We've gotta get these sites down as quickly as possible. Law enforcement usually wants to keep the [phishing] sites active as long as possible so they can get a lot of evidence against the phisher. We still work with them when we absolutely need them, but it's kind of a last resort."

This was a common complaint from the financial institutions. The take-down companies had a different reason for not working with law enforcement.

The take-down companies saw law enforcement as either an unnecessary entity, or worse, as a threat to their business. Take-Down Company Employee 4 stated:

> "Why should [we] deal with law enforcement? I know it sounds bad, but phishing is our business. Say we give evidence to the feds and they make a huge bust and the volume of phish is cut in half. We'd be out of business! As long as there are sites to shut down, our clients will pay us to remove them."

This mentality may have been exaggerated for effect, for this employee later agreed that it is unlikely that law enforcement involvement will reduce phishing to the point that these companies are no longer needed. Take-Down Company Employee 3 stated that he recognizes the importance of working with law enforcement and he believes that more cooperation between civilian analysts and law enforcement is necessary to reduce phishing worldwide.

Education-related interview questions yielded mixed answers. The bank employees described experience in finance and business management from Bank Employee 3,while Bank Employee 2 only had on the job training as he has worked for this institution for two decades. A few questions at the end of the interviews pertained to ongoing education. Both the bank employees and the take-down company employees were adamant about the need for continuing education because this field is developing so rapidly. Take-Down Company Employee 5 said:

> "We send our analysts to seminars around the country multiple times a year. Anytime something pops up on our grid that looks promising, we make sure that at least one of our number [people] is present and accounted for. This way, hopefully, we can stay on top of our game and stay one step ahead of the competition."

Overall, the take-down companies deemed that ongoing education was a greater priority compared to the banks, who stated its importance, but were unsure of specific seminars attended by their employees.

In pursuit of the initial hypothesis, representatives from the fraud departments of five major banks were interviewed. Four out of the five interviewees disclosed that their respective financial institutions no longer pursued their own phishing cases. These four banks outsourced to third party vendors. These companies were on contract to find and take-down phishing websites disguised as the websites of the banks by whom they are employed.

Bank Employees 1-4 stated that they processed their own phishing emails until the workload got so great that it was more cost effective to outsource. Bank Employee 2 stated:

> "Until a several years ago, we had a very manual system. It worked, but it took a lot longer than some of the automated systems that are used nowadays. Due to the merger, we experienced a phishing spike in [year removed to avoid identification] that had my team dealing with upwards of 1,500 phish a day. This workload eventually led us to outsource to a site removal company and downsize our phishing department."

Bank Employee #1 elaborated further on the cost/benefit analysis that is involved in the decision to outsource to a third-party vendor. Bank Employee 1 stated, "[t]ake-down companies are pretty expensive. We did it all ourselves until the higher-ups decided that the money it took to keep our department afloat was more than it would cost to hire someone else to do it." Take-down companies are likely to be more efficient than specialists within a financial institution because these companies have the advantage of experience from removing phishing websites for numerous clients.

The take-down companies have a clearly defined modus operandi for phishing website detection and shutdown. These methods vary from company to company, and some appear to be more effective than others. It should be noted that take-down companies are highly competitive. It is possible that some of the data gathered in the interviews was possibly exaggerated to make a particular take-down company sound more effective than they actually are. Take-Down Company Employee 3 stated:

> "We're able to detect phishing sites anywhere from 4 to 7 hours faster than our competitors because we use technology to strip out URLs and crawl sites and score them for phishing content. And so what is left for us to review as human beings is a finely tuned stream of 99% accurate URL's relating directly to our customers. That's much more efficient than having a human being sift through a couple million emails an hour, 24-hours a day trying to find the URL's that mean something."

Methods of detection included forwarding of complaint emails from contracted financial institutions, to collection of data from honeypots, to the analysis of server logs from hosting companies that frequently host phishing websites.

Using various detection methods, take-down companies discover phishing websites targeting customers of the institutions with whom they have contracts. These fraudulent websites are recorded and the URL's are emailed to the institutions' fraud departments. Once a website is deactivated, the take-down company sends a report to the institution. The fraudulent URL is

tracked by the take-down company for the life of the contract to ensure that it is not reactivated by the phisher. Based on the volume of phishing websites and the median take-down time, the institution will decide whether or not to renew the contract. Due to the cost of employing a take-down company, some banks handle their own phishing cases.

Only one of the studied banks currently handles phishing countermeasures internally. Bank Employee 5 managed a team of three employees. These employees were scheduled so that at least one person is working 24 hours a day during the week and during regular business hours on the weekend. These four workers were responsible for all of the phishing websites affiliated with Bank 5. This amounts to 42,000 phishing websites that have been removed in the last three years. Bank Employee 5 states that his team is able to handle this workload by automating the take-down process as much as possible. On this bank's legitimate website, concerned customers can follow an email link to report phishing websites. According to Bank Employee 5, his team collects 95% of its phishing websites from this email account. This retroactive approach is inherently problematic because the crime has been committed prior to the attempt to remove the website. Bank 5 uses a method similar to that of the take-down companies to remove the phishing websites. Bank Employee 5 stated, "We use an internally created algorithm to sift the [Bank 5] phish from the chaff of our 2 million emails." This method was echoed by some of the take-down companies, but Bank 5's median shutdown time of 24 hours was well below the average shutdown time reported by the other take-down companies.

The general steps followed by analysts wishing to take down a phishing website can be summarized as follows: the analyst uses email and telephone communication to contact host servers, ISP's and, if necessary, registrars and law enforcement agencies. The analyst follows the control hierarchy of the website until he or she reaches someone capable/willing to shut the website down. First, the analyst attempts to contact the domain owner, or webmaster, using either email or a phone call. In the case of a hacked legitimate website, this approach is particularly effective as the domain owner does not want to be associated with malicious content. The next step would be to contact the hosting company. If the hosting company is unreachable or unwilling to invade the privacy of its customer, then the registrar is contacted and the domain is revoked. The goal of this process is to shut the phishing website down as quickly as possible so that a minimal number of potential victims have an opportunity to divulge their sensitive information. According to the aforementioned steps taken by a successful phishing enterprise, these countermeasures serve to interrupt the process at Step 4. Ideally, the take-down companies remove the phishing website before potential victims have the chance to access it.

V. Discussion

Phishing is a multi-billion dollar industry (Javelin, 2008). Consider the case of the small Romanian town called RâmnicuVâlcea, which is nestled in the Transylvanian Alps. This town is colloquially known to cyber law enforcement as "Hackerville." Over the last decade, RâmnicuVâlcea has become the hub of online crime in Eastern Europe (Bhattacharjee, 2011). According to Bhattacharjee (2011), "expensive cars choke the streets of RâmnicuVâlcea's bustling city center—top-of-the-line BMWs, Audis, and Mercedes driven by twenty- and thirty-something men sporting gold chains and fidgeting at red lights." "Hackerville" represents a concentrated example of how current phishing countermeasures are dysfunctional and the situation is not improving. Javelin research demonstrates that financial losses due to fraud have steadily increased from 2007-2009 (Javelin, 2010). This is likely due to three major factors: 1) phishers have multiplied and made technical improvements to their phishing websites; 2) take-down companies only remain profitable if phishing is controlled, not if it is eradicated; and 3) phishers are almost never prosecuted.

Phishing has come a long way since being brought to national attention over a decade ago. Early phishing attacks often displayed misspellings, poor grammar and shoddy graphics. These attempts were created by non-English speakers and they only worked because victims were naïve and ignorant about phishing. Though some obviously fraudulent websites are still being created, many of the phishing websites targeted by take-down companies are almost identical to the legitimate websites that they are imitating. Also, more tech savvy phishers use links within phishing emails to inject malware onto victims' computers. These programs are designed to retrieve and transmit confidential information from the victim to the phisher without the victims' knowledge. Fast flux phishing is another new technique that was discussed by Take-Down Company Employee 3. The Spamhaus website states, "[f]ast flux domain hosting involves the use of botnet zombie drones on broadband IPs infected to act as reverse proxies for the spammer's website or nameservers. The spamvertised domain, or its nameserver, is pointed at a rapidly changing series of zombie IPs (hence the name) with very short 'TTL (Time To Live)' values -- usually less than five minutes (300s)" (Spamhaus, 2011). Anti-phishing technology is often created in response to known threats, therefore phishers are always one step ahead of those who attempt thwart them. Take-down companies are effective in the sense that they remove the fraudulent websites from the

Internet, but punitive action is necessary to deter phishing.

Research shows that much of the valuable data gathered from phishing websites is harvested within a short period of time, far sooner than previously thought (Klein, 2010). Specifically, Klein (2010) states:

> "50 percent of phishing victims' credentials are harvested by cyber criminals within the first 60 minutes of phishing emails being received. Given that a typical phishing campaign takes at least one hour to be identified by IT security vendors, which doesn't include the time required to take down the phishing Web site, we have dubbed the first 60 minutes of a phishing site's existence is the critical 'golden hour"(Klein, 2010)

Klein (2010) goes on to elaborate that 80 percent of the useable data is gathered within the first 5 hours and by 10 hours, 90 percent of the data that a phishing website is likely to collect is already harvested. The companies and institutions that participated in this study had median take-down times between three and twenty-four hours. In light of the facts presented by Klein (2010), this represents a major blow to the effectiveness of the take-down process. Clearly, proactive phishing detection and retroactive prosecution are required to make phishing less profitable to online criminals. From the perspective of the take-down companies, however, it is difficult to justify changing their approach when they are financially successful as they are.

The take-down companies are capitalist organizations that profit by securing contracts with organizations that recognize phishing as a legitimate threat. Take-Down Company Employee 5 stated:

> "The whole idea behind doing take down is mitigating the threat. The most pain you can cause a phisher is to make him start over from scratch. The sooner you achieve that, the less value they get out of their effort. And if they get less value out of their effort, then they will probably go after somebody else."

It is this last statement that illuminates the problem with reliance upon take-down companies to eradicate phishing. These companies hope to drive phishers toward other institutions so that these institutions will have incentive to hire the take-down company. After a successful period in which phishing websites are rapidly recognized and removed, an institution with a contract might not see anymore phishing websites. If they decide not to renew their contract with the take-down company, then the tracked URL's will likely be reactivated and unchecked phishing websites will resume.

An appropriate analogy would a freelance police force that is paid to protect a neighborhood from a violent gang. The police might prevent most violence against the neighborhood, but since they do not arrest the gang members the violence diverts to the adjacent neighborhoods. This is not an ethical enforcement method. Instead, it is an example of businesses that profit from criminal behavior.

Building a criminal case against a phisher or a phishing crime ring is time consuming. It is also significantly more costly than merely shutting phishing websites down. These take-down companies garner no profit for building cases against individual phishers or even from giving their phishing data to law enforcement. The one take-down company interviewed that did submit information to law enforcement did not organize it and just relinquished the raw data. Unless the law enforcement agency has agents specially trained to interpret this data and pursue the case, the data are likely to be ignored.

Large phishing busts are exceedingly rare. One example is Operation Phish Phry. Fifty American citizens and fifty Egyptian citizens were charged in this case. According to the FBI's website, "The defendants in Operation Phish Phry targeted U.S. banks and victimized hundreds and possibly thousands of account holders by stealing their financial information and using it to transfer about $1.5 million to bogus accounts they controlled." (fbi.gov, 2009) This was the largest case handled by the National Cyber Investigative Joint Task Force, which was created within the FBI in 2008. This task force is a tremendous step in the right direction. Further research is necessary to determine how various law enforcement agencies view phishing. The formation of the National Cyber Investigative Joint Task Force demonstrates that the federal government recognizes the seriousness of the threat created by phishing, but more action must be taken at the local and state level to reduce the prevalence of phishing in the United States.

VI. Conclusion

This research demonstrates that phishing is a lucrative criminal enterprise with little or no deterrence against the perpetrators. The take-down countermeasure is unsuccessful because the phishing websites often collect and transmit the majority of the stolen credentials faster than they can be deactivated. Evidence that could be used to pursue, arrest, and prosecute the phishers is being gathered, but is rarely being put to use. Open, direct communication between take-down companies and law enforcement is essential so that the viable information can be relayed and utilized in order to bring phishers to justice. A small group within a federal organization, such as the FBI or the Secret Service, could liaise with take-down companies and financial institutions. This group could gather the raw data, process it, and coordinate with agents across the globe to bring about more busts like Operation Phish Phry. Only such a cooperative effort has

the potential to reduce the level of phishing in the United States and worldwide.

VII. Appendix A – Interview Questions for Financial Institution Personnel

1) What is your job title?
2) Did you replace someone in this position when you were hired, or was the position created for your skill set?
3) Describe your educational background?
4) Describe your previous work experience?
5) How does your financial institution combat phishing?
6) Is this how your institution has always dealt with phishing?
7) How much of your workload is phishing related?
8) On average, how many cases do you work on simultaneously?
   a) Do you feel that your department is staffed to handle that workload?
9) How are phishing cases typically initiated?
10) What types of evidence do you collect?
    a) Of those types, which are generally most valuable toward your investigations?
11) What are the criteria for initiating a case? (i.e., dollar loss, number of customers affected, etc.)
12) Walk me through a typical phishing case from initiation to the completion of your involvement.
13) Describe your relationship with law enforcement on phishing cases.
14) Do you have primary contacts at large corporations, especially email providers? (i.e., Google, Microsoft, Mozilla, Yahoo, etc.)
15) When evidence leads you to believe that a suspect is operating overseas, how do you proceed?
    a) Do you have working contacts overseas?
    b) How do you overcome the language barrier?
16) What percentage of your fraud loses do you believe are phishing related?
17) Are you ever reluctant to bring a case to the attention of law enforcement because you believe that it will result in bad publicity for your financial institution?
18) If financial institutions could report cybercrime anonymously, do you believe that more cybercrime would be reported?
19) Do you believe that your financial institution is as prepared as it should be for phishing defense?
    a) Is it as prepared as it COULD be?
20) Does your financial institution send electronic communications to its customers that encourage clicking of links?
    a) Anti-phishing efforts teach consumers not to click on links in email messages. As a fraud investigator, do you have thoughts on this dilemma?
21) How do you feel that your institution compares to others regarding phishing security?

VIII. Appendix B – Interview Questions for Take-Down Company Personnel

1) What is your job title?
2) Did you replace someone in this position when you were hired, or was the position created for your skill set?
3) Describe your educational background?
4) Describe your previous work experience?
5) How much of your workload is phishing related?
6) On average, how many cases do you work on simultaneously?
   a) Do you feel that your department is staffed to handle that workload?
7) How are phishing cases typically initiated?
8) What types of evidence do you collect?
   a) Of those types, which are generally most valuable toward your investigations?
9) Walk me through a typical phishing case from initiation to the completion of your involvement.
10) What is your median take-down time?
11) Describe your relationship with law enforcement regarding phishing cases.
12) Do you have primary contacts at large corporations, especially email providers? (i.e., Google, Microsoft, Mozilla, Yahoo, etc.)
13) When evidence leads you to believe that a suspect is operating overseas, how do you proceed?
    a) Do you have working contacts overseas?
    b) How do you overcome the language barrier?
14) How do you feel that your institution compares to others regarding take-down statistics?
15) To the best of your knowledge, does further education or training exist that you believe would better prepare you for your investigations?
    a) In such a rapidly advancing field, how do you stay updated with the newest technologies and techniques?
    b) Are you aware of The Seven Phases of Phishing Investigation, which was enumerated upon at the Microsoft Digital Crimes Consortium in 2010?
16) Which agency do you prefer to work with?
    a) Why?
17) Do you ever feel that law enforcement requires further computer forensic education in order to perform phishing investigations more effectively?
18) When gathering information for a case, who do you contact to gather evidence? (i.e., law enforcement, other financial institutions, victims, etc.)
19) Once you have presented your evidence to law enforcement, do you continue to monitor the case or do you move on to another?

IX. REFERENCES

Bhattacharjee, Yudhijit. (2011). "How a Remote Town in Romania Has Become Cybercrime Central". *Wired*, February, 2011. Retrieved on March 29, 2011 from http://www.wired.com/magazine/2011/01/ff_hackerville_romania/.

Cova, M., Kruegel, C., Vigna, G. (2008). **"**There is No Free Phish: An Analysis of 'Free' and Live Phishing Kits".USENIX Workshop on Offensive Technologies. July 28, 2008. San Jose, CA.

Emigh, Aaron. (2005). "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures". October 3, 2005. Retrieved on March 26, 2011 from http://www.antiphishing.org/Phishing-dhs-report.pdf.

Federal Bureau of Investigation. (2009) "Operation Phish Phry: Major Cyber Fraud Takedown". October 7, 2009. Retrieved on April 1, 2011 from http://www.fbi.gov/news/stories/2009/october/phishphry_100709.

Gartner Research. (2007). "Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks". Stamford, Conn., December 17, 2007. Retrieved on March 14, 2011 from http://www.gartner.com/it/page.jsp?id=565125.

Jakobsson, M. and Myers, S., Eds. (2006). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, Wiley-Interscience, Hoboken, NJ.

Javelin Strategy & Research. (2010). "Javelin Study Finds Identity Fraud Reached New High in 2009, but Consumers are Fighting Back". February 10, 2010. Retrieved on March 14, 2011 from https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail.

Klein, Amit. (2010). "The Golden Hour of Phishing Attacks". *Trusteer*. Retreived on April 15, 2011 from http://www.trusteer.com/blog/golden-hour-phishing-attacks.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L., and Hong J. (2007). 'Teaching Johnny Not to Fall for Phish'. ACM Transactions on Internet Technology V(N). 1-31.

Li, S. and Schmitz, R. (2009). "A Novel Anti-Phishing Framework Based on Honeypots". APWG eCrime Researchers Summit. October 20-21, 2009. Tacoma, WA.

Federa

Moore, T., and Clayton, R. (2007). "Examining the Impact of Website Take-down on Phishing". APWG eCrime Researchers Summit. October 4-5, 2007. Pittsburgh, PA.

Shah, R., Trevathan, J., Read, W., Ghodosi, H. (2009). "A Proactive Approach to Preventing Phishing Attacks Using a Pshark". Information Technology: Next Generation. April 27-29, 2009. Las Vegas, NV.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., and Downs, J. (2010) "'Who falls for phish?' A demographic analysis of phishing susceptibility and effectiveness of interventions". Conference on Human Factors in Computing Systems. April 10-15, 2010. Atlanta, GA.

Spamhaus Project, The. (2008). "What is 'fast flux' hosting?". From SAC 025: SSAC Advisory on Fast Flux Hosting and DNS. Retrieved on April 1, 2011 from http://www.spamhaus.org/faq/answers.lasso?section=ISP%20Spam%20Issues#164.

Stamm, S., Ramzan, Z., and Jakobsson, M. (2006). "Drive-by Pharming". Information and Communication Security 2007. Zhengzhou, China.

United States Department of State. (1997). "Nigerian Advance Fee Fraud". Department of State Publication 10465, Bureau of International Narcotics and Law Enforcement Affairs. Retrieved on April 18, 2011 at http://www.state.gov/www/regions/africa/naffpub.pdf.

Wardman, B., Shukla, G., and Warner, G. (2009). "Identifying Vulnerable Websites by Analysis of Common Strings in Phishing URLs". APWG eCrime Researchers Summit. October 20-21, 2009. Tacoma, WA.

Wardman, B. (2010). 'UAB Phishing Data Mine'. University of Alabama at Birmingham Computer and Information Sciences DepartmentTechnical Report Number : UABCIS-TR-2010-111710-1. November 17, 2010.

Zhang, Y., Egelman, S., Cranor, L. and Hong, J. (2006), 'Phinding Phish: Evaluating Anti-Phishing Tools', CyLab Technical Report, CMU-CyLab-06-01, November 13, 2006.

Zhang, Y., Hong, J.I., and Cranor, L.F. (2007). 'Cantina: A Content-based Approach to Detecting Phishing Web Sites'. International Conference on World Wide Web. May 8-12, 2007. Banff, Alberta, Canada.