PHISHING: A SURVEY

Jamie Yoo
Yale University
Department of Computer Science
Adviser: Robert Dunne

May 1, 2006
Abstract: Over the last decade, the amount of commerce is conducted online has increased dramatically and as a result the sea of victims that phishing scammers can target have grown considerably. Originating in the hacker youth culture of the 1990s, attacks have become increasingly sophisticated and malicious. Unfortunately for the e-commerce industry, fear of becoming victim to cyber crimes like phishing has become the dominant reason users have stayed away from doing business online. Thus it has become important for consumers, businesses, as well as government agencies to understand the techniques used for phishing attacks and effective mechanisms to fight against them. This paper is a survey on phishing.
TABLE OF CONTENTS

1 INTRODUCTION ........................................................................................................... 4
1.1 What is Phishing?......................................................................................................
1.2 Social Engineering....................................................................................................
1.3 The Early Years........................................................................................................

2 PHISHING TECHNIQUES: Delivery........................................................................... 11
2.1 Harvesting................................................................................................................
2.2 Delivering Spam Messages ......................................................................................

3 PHISHING TECHNIQUES: Deception......................................................................... 22
3.1 Domain Name Game ...............................................................................................  
3.2 Malware ..................................................................................................................
3.3 Man-in-the-Middle Attacks .....................................................................................
3.4 Hijacked Sessions ....................................................................................................
3.5 Cross-Site Scripting ............................................................................................... 

4 COUNTERMEASURES ............................................................................................... 29
4.1 Anti-Spam Techniques ............................................................................................
4.2 Anti-Phishing Techniques ......................................................................................
4.3 Consumer Vigilance ............................................................................................... 

5 LEGISLATION ............................................................................................................. 38
5.1 CAN-SPAM Act ......................................................................................................
5.2 Identity Theft Penalty Enhancement Act .................................................................
5.3 Virginia Computer Crimes Act .............................................................................
5.4 California Anti-Phishing Act ...................................................................................
5.5 Anti-Phishing Act of 2005 .....................................................................................

6 ENFORCEMENT AGENCIES ................................................................................... 43
6.1 Federal Trade Commission ......................................................................................
6.2 Department of Justice .............................................................................................
6.3 Federal Bureau of Investigation .............................................................................
6.4 Secret Service .........................................................................................................
6.5 Others ....................................................................................................................

7 ENFORCEMENT ACTIONS ....................................................................................... 46

8 SHORTCOMINGS OF LEGISLATION AND GOVERNMENT ACTION............ 49

9 CONCLUSION ............................................................................................................. 51

BIBLIOGRAPHY ............................................................................................................. 52
1 INTRODUCTION

“Microsoft did an internal “phishing IQ” test recently that asked respondents to decide which of 10 e-mail messages and 10 websites were legitimate or spoofs, Spiezle said: Even the “chief architect” at Microsoft -- Bill Gates -- got some wrong. When only 42 percent of people have heard of phishing, and half of those can explain it – figures from an AOL- National Cyber Security Alliance survey – what chance do consumers have to identify a phishing attempt?”

- Jules Polonetsky, AOL VP of Integrity Assurance
  Washington Internet Daily, March 13, 2006

Phishing is just one technique used for identity theft, which is a type of crime that has been around for much longer than the Internet. Identity theft, also known as identity fraud, “occurs when someone uses your personal information without your permission to commit fraud or other crimes” (US Federal Trade Commission). In a January 2006 report, the Federal Trade Commission said it received over 685,000 consumer fraud and identity theft complaints. Many incidents are not even reported to the police, let alone the FTC. According to two studies conducted in July 2003 (Gartner Research and Harris Interactive), approximately 7 million people became victims of identity theft in the prior 12 months, which averages to 19,178 per day, 799 per hour, or 13.3 per minute (Identity Resource Center). Phishing is merely a subset of identity theft, in which scammers use electronic communication mechanisms for the purpose of conning recipients into divulging personal information.

1.2 What is Phishing?

The word “phishing” stems from the metaphor that describes Internet scammers as fishers using e-mail lures to fish for passwords and financial data from a sea of Internet users.
Compromised accounts were referred to as “phish” and by 1997 phish were traded among hackers as a form of currency, usually for the purpose of acquiring hacking software or pirated applications or games (Anti-Phishing Workgroup). The practice of replacing “f” for “ph” in terminology is common with hacker pseudonyms and organizations and is believed to be a tribute to an early form of hacking known as “phone phreaking,” a term coined by John Draper, also known as “Captain Crunch,” who was famous for hacking telephone systems in the early 1970s. Draper discovered that a toy whistle distributed as prizes in Cap’n Crunch Cereal boxes could be modified to emit a tone at the same frequency used by AT&T telephone lines (Draper). Using this newly discovered vulnerability, Draper created the infamous Blue Box, which allowed a user to control phone switches, allowing him to bill calls to someone else’s phone number. The term “phreaker” is believed to be a portmanteau of the words “phone” and “frequency”.

The first known usage of the term “phishing” was in the Internet hacker newsgroup “alt.2600” in January 1996, although it possible that it may have been used even earlier in the popular hacker newsletter “2600” (Anti-Phishing Workgroup).

“It used to be that you could make a fake account on AOL so long as you had a credit card generator. However, AOL became smart. Now they verify every card with a bank after it is typed in. Does anyone know of a way to get an account other than phishing?”

— mk590, "AOL for free?", alt.2600, January 28, 1996

One of the earliest media citations referring to phishing was later in March 1997 by the Florida Times-Union.

“The scam is called ‘phishing’ -- as in fishing for your password, but spelled differently -- said Tatiana Gau, vice president of integrity assurance for the online service.

“Generally, the people who do this use a computer program that sends the message to many AOL subscribers at once, so it's unlikely you're being individually targeted. The
hacker at the other end is hoping just one person out of all those recipients will respond.”

–Florida Times-Union, March 16, 1997

Due to its high success rate, scammers have over the years moved beyond the classic phishing scam to more elaborate methods for luring victims into divulging their personal information. Phishers have also successfully tempted users with classic money laundering schemes delivered by e-mail. One particularly infamous scam that phishers used was the “Nigerian 4-1-9” scam, also known as the Advanced Fee Fraud scam, where the victim is promised a large sum of money but will need to pay various fees in advance (U.S. Secret Service).

**Example: Nigerian 419 Scam**

Subject: Awaitting your responce.

My name is Danjuma Sule, one of the sons of major Gen Gumel Danjuma Sule, The late Nigeria's former minister of mines and power in the regime of the late former Nigeria's military Head of state, Gen Sanni Abacha.

He married my mother on the agreement that my mother, Amina Fausat Sule, will maintain her family's name together with her children. Before he died in the German hospital on the 15th of November 1988 where he went to operate on the cancer of the knee, he fixed the Sum of $30,000,000.00 in the Central Bank of Nigeria under Intartrade Ventures Ltd on behalf of my mother. The 3 yrs maturity period placed on the money is due but the problem we are having now is that we lost the whole of the documents as a result of fire, which gutted our house 3 months ago.

We have discussed with our family attorney on how to collect the money with out hitches, he advised us to liaise with a foreigner who will act as the foreign partner of Intartrade Ventures Ltd and will purport that The money in question is urgently needed overseas for an important project.

It is on this basis I am seeking for assistance. Your percentage is negotiable. Please note; your age and profession doesn't really matter in this transaction. Waiting for your immediate response.

Regards,

Danjuma Sule

Source: http://antivirus.about.com/od/emailhoaxes/p/nigerian419.htm
Previously, these Nigerian 419 scams had been initiated via snail mail or fax, and some were extremely elaborate, involving forged or official documents in an effort to create the appearance of legitimacy (U.S. Secret Service).

Thus, over the years, phishing attacks grew from simply tricking users to reveal their AOL dialup account information into a more sinister criminal enterprise, targeting users of online banking, payment services such as PayPal, and online e-commerce sites such as eBay. Phishing attacks are growing quickly in number and sophistication, including the use of fake websites, Trojan horse key-loggers and screen captures, and man-in-the-middle data proxies, all delivered through a wide variety of electronic communication channel. Thus the concept of phishing has broadened to a general category of attacks that uses both social engineering and technical subterfuge to steal consumers’ personal identity data and financial account credentials.

1.2 Social Engineering

“The human factor is typically the most critical variable in information security systems. Even the best policies and technologies can be rendered completely ineffective if users do not take responsibility for safeguarding the information they control.”

– Amit Yoran, Director of National Cyber Security Division of the Department of Homeland Security

Phishing is fundamentally based on the concept of social engineering, which in terms of computer information security targets the human element of a system to gain access. The famous reformed hacker and security expert Kevin Mitnick when testifying in front of Congress admitted that his preferred technique of attacking any system was social engineering, stating, “I was so successful in that line of attack that I rarely had to resort to a technical attack” (Bridis).
In his testimony, Mitnick describes the details of his successful efforts to break into AT&T Corp.’s worldwide network, by posing as an executive calling a receptionist and convincing her to fax to him an important password, thus justifying his assertion that “the human factor is truly security’s weakest link” (Mitnick 3).

More broadly speaking, social engineering, or “gagging,” is defined as gaining intelligence through deception or also as using human relationships to attain a goal. From the perspective of phishers, social engineering in simply conning legitimate computer users into providing useful information that helps the hacker gain unauthorized access to their computer system, which is the common foundation of all phishing scams.

1.3 The Early Years

By the mid 1990s, America Online (AOL) had become one of the three largest online service providers, thanks to its easy-to-use graphical user interface (GUI). By that time also, there were programs, the most famous being one called AOHell, that automated the process of phishing for accounts and credit card information. Phishing at that time was not used as much in e-mail compared to Internet Relay Chat (IRC) or the message alert system that AOL used, sending users messages such as the following:

“Hi, this is an AOL Customer Service. We’re running a security check and need to verify your account. Please enter your username and password to continue.”

Thus phishers would imitate an AOL administrator and tell the victim that there was a billing problem and they needed them to renew their credit card and login information. By 1994, this process was automated by software programs, such as AOHell, which provided a number of
utilities that ran on top of the AOL client software. AOHell allowed a user to manipulate the AOL interface and included features such as a fake account generator and instant message and e-mail spamming tools as well as phishing tools (AOHell Documentation). Back then, because personal computers in the home combined with Internet usage were a fairly new experience, these basic methods proved to be quite effective, even though the targeted user base was nowhere near the numbers that phishing schemes reach today.

By 1996, there were already reports of Trojan horse phishing e-mails:

A group of hackers recently devised an ingenious way to steal passwords from America Online users. Posing as customer service representatives, they sent out e-mail with a file attached that masqueraded as a survey. The file was called AOLSRVY.EXE.

The e-mail promised that if users downloaded an attached file and took the survey, they’d get a few hours of free access. But the deal was bogus; the file was a program that would gather any passwords the users stored for quick log-ons. Then the file automatically e-mailed itself to the hacker’s account.

– Robert Bowden, The Tampa Tribune, March 8 1996

By March 1998, in a news article by the New York Daily News, AOL security chief Tatiana Gau said that “the majority of the security breaches at AOL occur through what’s known as password phishing where hackers pose as AOL employees and ask for your password,” forcing AOL to display a security message on instant message and e-mail windows in order to remind users that “no one working at AOL will ask for your password or billing information.”

Phishing has changed and expanded throughout the years, shifting their target from AOL customers to users of a wide variety of online services like online banking and PayPal. The number of reported phishing incidents has peaked in recent years, and news coverage dramatically escalated beginning in 2003. In July of 2003, the Washington Post reported on a
news conference at which “Internet service provider Earthlink Inc., the FTC, the FBI and the National Consumers League warned that phishing is a dangerous new trend” (Krim). Even to this very day phishing scams are continually evolving, with scammers claiming to be sending messages from the IRS, the FDIC, smaller banks rather than large nationwide banks, and even college students. The remaining parts of this paper will discuss the methods that phishers have developed over the years to execute these attacks and countermeasures that business, security experts and legislators have taken to fight against phishers.
Most phishing attacks are initiated by e-mail, using many of the same techniques and tools as mass e-mail marketers and conventional spammers. For instance, the lists of e-mail addresses used to deliver the phishing e-mails are frequently purchased from the same sources as conventional spam. In addition, phishers use other known exploitable elements of the e-mail system to forge various components of the e-mail in an effort to appear like legitimate messages from trusted parties.

“The worry now is that devious spammers will turn to other net-based money-making schemes, such as spyware and identity theft malware to make their dirty money…. There are fortunes to be made on the dark side of the Internet.”
– Graham Cluely, senior technology consultant, Sophos Plc
PR Newswires, October 12, 2005

For several decades now, spammers have developed a wide spectrum of techniques for sending large quantities of “electronic junk mail.” Already by 1975, Jon Postel felt it necessary to publish RFC 706 “On the junk mail problem.” In previous cases, however, spammers were largely marketing legitimate, albeit unwanted, products or services, the most frequent being Internet pornography. Because these well-developed techniques are now being implemented by phishers, the following sections will discuss common spamming methods.

2.1 Harvesting

In order to have their messages reach anyone, spammers and phishers first need to obtain a list of verified, or “live”, e-mail addresses. While traditional junk mailers had the luxury of using a phone directory of physical mailing addresses, there is no similar, convenient directory
for e-mail. Thus, spammers resort to other means of finding e-mail addresses. The techniques
developed for acquiring lists of e-mail addresses is commonly referred to as “harvesting”. The
most common ways of harvesting e-mail address are the following:

2.1.1 Purchasing E-mail List

The most obvious and easiest way of getting a hold of a list of e-mail addresses is to buy one. A considerable number of online services offer lists of millions of e-mail addresses that are
downloadable or available on CD. Many times these venders will falsely claim that the
addresses were all obtained legally, when in fact most were actually obtained illegally, probably
by one of the methods discussed later in this section.
2.1.2 Guess and Check

Although it is a slow and inaccurate process, spammers are known to have tried guessing and checking as a way of collecting addresses. A spammer can send a test e-mail to a list of invented e-mail addresses. If the e-mail address is not valid, then the e-mail will bounce back an error message. A spammer can also use mail headers to request that the delivery system and/or mail client send a confirmation of delivery or reading, further ensuring the spammer that the e-mail address is valid and active or “live”.

Example headers:

- **Return-Receipt-To**: `<e-mail-address>` will send a delivery confirmation
- **X-Confirm-Reading-To**: `<e-mail-address>` will send a reading confirmation

2.1.3 Links

A simple method of verifying “live” e-mail addresses is to just include a link within the e-mail, such as an “unsubscribe” link. In reality, these links are often unique identifiers that are associated with the recipient’s e-mail address, and thus when a user clicks on the link, the browser will then contact the malicious spam server with that unique identifier, allowing the server to recognize the e-mail address as valid.

2.1.4 Webcrawling

A spambot is a type of Web crawler that collects e-mail addresses from the Internet for the purpose of building mailing lists used for sending unsolicited e-mail. A Web crawler, also known as a Web spider or ant, is a computer program that methodically searches the Internet by
recursively browsing a site and then visiting all other sites it references. A spambot or e-mail spider is a specific type of Web crawler that finds e-mail addresses by scanning for while browsing each site. In the early days, these harvesting spiders searched for “from” or “reply-to” on headers on postings and sites, but nowadays spiders will search for any use of the ‘@’ character.

Some examples of sources of e-mail address are Web sites, newsgroups, special-interest group postings, and chat-room conversations.
By 2002, the FTC reported on an investigation where 250 e-mail addresses were seeded on 175 different locations on the Internet, including Web pages, newsgroups, chat room, message boards, and online directories for Web pages, instant message users, domain names, resumes, and dating services (FTC Consumer Alert 2002). In the given 6-month period of the investigation, the investigators found that 86 percent of the addresses posted to Web pages received spam, regardless of where the address was posted, so long as it included an ‘@’ symbol. They also reported that 86 percent of addresses posted on newsgroups received spam, and that chat rooms were “virtual magnets for harvesting”. Spammers may also sign up for mailing lists and they have also taken advantage of the fact that DNS and WHOIS systems require the publication of technical contact information for all Internet domains:

<table>
<thead>
<tr>
<th>WHOIS information for microsoft.us:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name:                        MICROSOFT.US</td>
</tr>
<tr>
<td>Domain ID:                          D749411-US</td>
</tr>
<tr>
<td>Sponsoring Registrar:              REGISTER.COM</td>
</tr>
<tr>
<td>Domain Status:                      ok</td>
</tr>
<tr>
<td>Registrant ID:                      C41493487-NXUS</td>
</tr>
<tr>
<td>Registrant Name:                    Domain Administrator</td>
</tr>
<tr>
<td>Registrant Organization:            Microsoft Corporation</td>
</tr>
<tr>
<td>Registrant Address1:                One Microsoft Way</td>
</tr>
<tr>
<td>Registrant City:                    Redmond</td>
</tr>
<tr>
<td>Registrant State/Province:         WA</td>
</tr>
<tr>
<td>Registrant Postal Code:             98052</td>
</tr>
<tr>
<td>Registrant Country:                 United States</td>
</tr>
<tr>
<td>Registrant Country Code:            US</td>
</tr>
<tr>
<td>Registrant Phone Number:            +1.4258828080</td>
</tr>
<tr>
<td>Registrant Facsimile Number:        +1.4259367329</td>
</tr>
<tr>
<td>Registrant E-mail:                  <a href="mailto:domains@microsoft.com">domains@microsoft.com</a></td>
</tr>
<tr>
<td>Billing Contact E-mail:             <a href="mailto:cctld-billing@register.com">cctld-billing@register.com</a></td>
</tr>
<tr>
<td>Technical Contact Facsimile Number: +1.4259367329</td>
</tr>
<tr>
<td>Technical Contact E-mail:           <a href="mailto:msnhst@microsoft.com">msnhst@microsoft.com</a></td>
</tr>
<tr>
<td>Domain Registration Date:           Fri Apr 19 22:03:37 GMT+00:00 2002</td>
</tr>
<tr>
<td>Domain Expiration Date:             Wed Apr 18 23:59:59 GMT+00:00 2007</td>
</tr>
<tr>
<td>Domain Last Updated Date:           Wed Jun 09 19:00:20 GMT+00:00 2004</td>
</tr>
</tbody>
</table>

In an attempt to avoid having their e-mail addresses harvested by spambots, many website operators practice “address munging” or “e-mail obfuscation,” which is essentially the
practice of disguising e-mail addresses. Techniques vary and the following are some common examples with the address “richard.levin@yale.edu”:

<table>
<thead>
<tr>
<th>Obfuscation Technique</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple rewriting</td>
<td>richard DOT levin AT yale DOT edu</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:richard.levin@yale.edu.removeme">richard.levin@yale.edu.removeme</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:richard.levin@yale.REMOVEME.edu">richard.levin@yale.REMOVEME.edu</a></td>
</tr>
<tr>
<td></td>
<td><a href="mailto:ude.elay@nivel.drahcir">ude.elay@nivel.drahcir</a></td>
</tr>
<tr>
<td>Encoding</td>
<td><a href="mailto:richard.levin@yale.edu">richard.levin@yale.edu</a> encoded as</td>
</tr>
<tr>
<td></td>
<td>&lt;a href=&quot;mailto:richi...&quot; Richard Levin&lt;/a&gt;</td>
</tr>
<tr>
<td>Image</td>
<td><a href="mailto:richard.levin@yale.edu">richard.levin@yale.edu</a></td>
</tr>
</tbody>
</table>

Unfortunately, determined spammers have developed intelligent spambots that are able to unobfuscate many of the example methods listed above.

2.1.5 Viruses

According to a 2005 whitepaper published by Sophos Plc, a world leader in integrated threat management solutions, “Approximately 40 percent of spam is now sent from hijacked consumer systems, and over 800 new viruses are discovered each month – many looking for new ways to take control of computers for the purpose of sending spam” (Sophos 2005). For example, in November of 2003, a virus called W32.Mimail.D not only harvested e-mail addresses but also caused infected computers to attack anti-spam websites, such as Spamhaus.org and Spews.org by bombarding them with requests. W32.Mimail.D was a worm that scanned through any e-mail accounts hosted on the infected computer and then spread via e-mail
using the addresses harvested from the hard drive of the infected computer. All e-mail addresses found on the computer were saved in a file named \texttt{eml.tmp} in the Windows folder. Viruses such as this scans through any e-mail accounts hosted on the infected computer and then e-mails itself to all the addresses that it finds.

2.1.6 Web Bug

Also known as a “Web beacon,” “pixel tag,” or “invisible GIF,” the Web bug is typically either a regular visible image or a tiny one-pixel, transparent GIF image that is embedded in an HTML-format e-mail. As the user opens the e-mail and attempts to download the image, the user’s browser or mail client makes a request server storing it. The URL of the Web bug carry a unique identifier that is chosen when the e-mail is sent and thus the server can thus “know” every recipient who opens the e-mail message.

2.1.7 Other Harvesting Methods

Over the years, spammers have shown a considerable amount of creativity in collecting e-mail addresses. A good example is Richard Douche’s infamous “Free CDs” chain letter, which promised a free CD for every person to whom the letter is forwarded to as long as it was cc’ed to Douche, who claimed to be associated with Amazon and Music blvd, among other companies. Yet he supplied no references to Web pages and used a free E-mail address. All Richard wanted was to get people to send him valid E-mail addresses in order to build a list of addresses to spam and/or sell.

<table>
<thead>
<tr>
<th>Example: “Free CDs” chain letter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Subject:</strong> CD's</td>
</tr>
<tr>
<td>Hi. My name is Richard Douche. I am the president of the Cyber Promotions for Columbia House. We are</td>
</tr>
</tbody>
</table>
in a fierce competition with companies such as Amazon.com and Music Blvd, among many others. Because of this, I have been authorized to offer 10+ free cd's of your choice to any person who participates in our promotion.

We at Columbia House understand that your time is very important to you, and that you don't want to have to fill out a form and mail it to us. With this in mind, we have developed a simplistic way for anyone who receives this e-mail to participate. All you have to do is send this message on to your friends! Yes, it is that simple. Now you are wondering how many CDs you get, and how to get them. It all depends on how many people you send this message to. You are required to send this e-mail to the address below to receive your first 10 CDs.

Cyberpromotions@n2music.com

In addition, you get another CD for every person you forward this to. For example, if you send this to Cyber Promotions, along with 10 of your friends, you would receive a total of 20 CDs. Remember to send this to Cyber Promotions or you WON'T RECEIVE YOUR CDS!! We will e-mail you back promptly asking for your CD selections. Again, thank you for your participation!!

2.2 Delivering Spam Messages

2.2.1 Webmail

A simple and cheap way for spammers to deliver their messages has been to create “throw-away” accounts on free webmail services, such as Hotmail, usually requiring several accounts due to the quantity of mail being sent. In recent years, however, webmail service providers have made an effort to cut down on this abuse, by implementing a system called the “Completely Automated Public Turing Test to Tell Computers and Humans Apart,” or captcha. Users attempting to create a new account are presented with a graphic of a word, which uses an uncommon and often obfuscated font, on a difficult to read patterned background.
Humans are able to read these graphics, while it is harder for computers to obtain accurate readings. Spammers have, however, found a means of circumventing this measure. For instance, some have reportedly set up sites offering free pornography and in order to get access to the site, a user is presented with a captcha test from a webmail site.

2.2.2 Open Relays

In the 1990s, the most common way spammers did this was to use open mail relays, which was a mail server configured to pass along messages sent to it from any location, to any
recipient. This process was the default in the original SMTP system and it meant that a user could send mail to practically any mail server, which would pass it along towards the intended recipient’s mail server. Thus, spammers could forward batches of spam through open relays without having to directly connect to the individual mail servers of recipients. However, in response to this practice, mail system administrators began to demand that other mail operators configure mail servers to cease being open relays.

2.2.3 Open Proxies

As open relays became rare, spammers began to use open proxies. A proxy is a network service used for making indirect connections to other network services. More specifically, the client connects to a proxy and instructs it to connect to a server, which sees the incoming connection as coming from the proxy but does not see the original client. Practically, proxies have many purposes, including Web-page caching, protection of privacy, filtering of Web content, and selectively bypassing firewalls. An open proxy creates connections for any client to any server, without authentication. Thus, a spammer could direct an open proxy to connect to a mail server, and send spam through it. The mail server logs a connection from the proxy and not the spammer's own computer. This allows for greater anonymity for the spammer than the open relay, since most relays log the client address in the headers of messages they pass. As a result, open proxies have frequently been used to conceal the sources of attacks against other services besides mail, such as Web sites or IRC servers.
2.2.4 Viruses

In recent years, spammers began using computer viruses designed to establish proxies and other spam-sending tools. As a result, spammers could harness hundreds of thousands of end-user computers. In fact, most major Windows e-mail viruses released in 2003, including the Sobig and Mimail viruses were designed for the specific purpose of making infected computers available as spamming tools. Besides sending spam, spammer viruses serve spammers in other ways.

The term “zombie computer” is used for innocent machines that have been infected with a bot program that allows them to be used for attacks. The ‘bot’ will typically report to a controller channel in order to download and execute instructions from it. A zombie computer can then be used by the attackers for several purposes including sending spam, sending viruses, creating mail relays, or harvesting passwords or e-mail addresses. According to CipherTrust, about 70 percent of all spam and 99 percent of all phishing e-mails are sent through zombies.
3 PHISHING TECHNIQUES: DECEPTION

Phishers have developed a wide variety of techniques that they can use in order to give their e-mails the air of legitimacy and to convince the user that the sender is indeed an AOL or bank system administrator. The following section will discuss these methods.

3.1 Domain Name Game

Phishers have been known to take advantage of users’ lack of knowledge regarding Web browsers and domain names. Phishers will set up their sites at domain names that often look very similar to those of legitimate sites. For instance, notice in the following example phishing e-mail that the login link points to <wwwchase.com>:

![Sample phishing e-mail](image-url)
Other times, phishers will use numeric IP addresses instead of a host name in their links.

Unfortunately, it is difficult for users to distinguish these fake domains from legitimate one. For instance, consider the following Bank of America monthly statement notification:

![Bank of America Monthly Statement Notification](image)

Thus, phishers will create links that are intentionally complex and many unknowing users will be unable to recognize an illegitimate link. Additionally, it also does not help that there is no set standard for legitimate websites to use for their domain names. For instance, the Verizon Wireless online store uses the domain name `<vzwshop.com>`:
A more creative way of obfuscating a malicious site’s URL has been to take advantage of the browser’s encoding systems. Because browsers are required to support local languages, it must be able to support alternate encoding schemes. Phishers have thus implemented schemes, such as “escaped-encoding,” also called “percent-encoding,” which involves representing characters within a URL that may need special syntax handling to be correctly interpreted, to manipulate the displayed URL.

3.2 Malware

Malware refers to software designed to infiltrate or damage a computer system without the user’s consent. In recent years, phishers have gone beyond simply using e-mails and
websites to falsely obtain personal information. The following section will discuss various types of malware commonly implemented by phishers.

3.3 Man-in-the-Middle Attacks

In a man-in-the-middle attack, the phishing attacker places itself between a customer and a legitimate site, and thus making itself a proxy for all communications between the customer and that site. Once a customer is directed to the site, believing that it was the real site, the attacker would simultaneously connect to the real site. For a phishing attacker to be able to do this, the user must be directed to the attacker’s proxy server instead of the real legitimate server. This can occur when a user clicks on a fake link in a phishing e-mail, going to the phishing attacker’s server directly.

Sometimes, attackers have been able to manipulate the process by which a user’s browser interprets the address a user has entered in his browser’s URL bar. Operating systems like Windows oftentimes will use shortcut “hosts” file used to look up host names quickly before performing a DNS (Domain Name System) lookup. Malicious programs, however, have been known to modify this file, thus routing legitimate website addresses to malicious sites. Additionally, a phishing attacker may also try to modify the user’s DNS cache with incorrect information in order to reroute the user to malicious sites.

In other cases, phishers have been able to override a user’s browser setup and set proxy configuration options to force all web traffic through their server.
3.4 Hijacked Sessions

In other cases, phishers will install malicious browser components that wait for a user to log into a legitimate secure site, beginning a secure session, which the malicious software will then “hijack” in order to perform malicious actions. More specifically, HTTP and HTTPS are both stateless protocols, which means that websites must develop other methods of tracking a users activity and of managing access to areas that require authentication. Typically, this is done using Session Identifiers, or Session ID’s, something through the use of cookies or hidden fields or fields in page URLs. Improperly implemented state managements systems can allow client connections to define a Session ID, which the Web application will use to track the user, although still requiring the user to authenticate themselves by logging in for access to restricted
pages. Thus, phishers will send messages that contain a link to the real Web application server but using a predefined Session ID field. As soon as the legitimate user logs into the legitimate site using this Session ID, the phisher can then use that Session ID for access to the user’s account.

3.5 Cross-Site Scripting

Phishers have recently been taking advantage of a cross-site scripting (XSS) vulnerability that is caused by the failure of a legitimate Web application to validate potentially malicious user supplied input. The malicious input is usually entered in the form of a hyperlink. The phishing attacker will encode the malicious portion of the link to the site in HEX, or other encoding methods, so the request is less suspicious. After the legitimate application accepts the malicious input, it creates an output page containing the malicious data, but the malicious data is usually displayed such that it appears as valid content from the website. This can result with cookie theft, account hijacking, and various other malicious activities. A classic example of this is in site search engines. If a searches query includes a string that includes HTML special characters, often the search string will be redisplayed on the result page. If all occurrences of the search terms are not HTML quoted, a XSS vulnerability will result.

In one particularly well-known phishing attacks exploiting cross-site scripting involved the U.S. Internal Revenue Service (Keizer). In the fall of 2005, phishers sent e-mails posing as a notification of a tax rebate. The fake e-mail claimed to have been sent from the address tax-refunds@irs.gov and stated that the recipient was eligible to receive a tax refund. The link provided in the e-mail was particularly convincing because it used a cross-site scripting flaw in the federal government's benefits Web site, <govbenefits.gov>.
3.6  Keylogging and Screen Scraping

Keyloggers are programs that are designed to capture the user’s keystrokes, and was originally intended to help administrators determine sources of error in computer systems. By implementing various keylogging technologies, phishers are then able to capture user’s login name and passwords. For instance, a phisher might install a browser help object that detects changes to the URL and log information when a URL is at particular sites, such as a bank website or PayPal. A more sophisticated technique has been to use screenloggers, or screen scrapers, in conjunction with keyloggers to track user activities. An example of this type of being used is the Banker-AJ Trojan, which waited for users to visit an online banking site, at which point the program captured passwords and took screenshots of the session (news.com).
4 COUNTERMEASURES

Since many phishing attacks involve malware installed on users computers without permission, simple measure such as secure patching of Windows and using antivirus software can do a lot for protecting against phishing. The first line of defense, however, would be to prevent phishing e-mails from entering a user’s inbox to begin with. Thus, the following section discusses various methods for fighting spam and bulk e-mail in general.

4.1 Anti-Spam Techniques

4.1.1 E-mail Filtering

By far, the most pervasive technique for blocking spam and phishing e-mails is to analyze the contents of the message to determine if it is spam. There are two variations of this. The first is statistical filtering, which builds a statistical model of messages manually identified as spam. As the number of spam messages grows, the accuracy of the model improves. As electronic mail arrives, the filter scans each message, and if the statistics of the message are “close enough” to those of the model, the message is labeled as spam. The model can be static in which case it is not updated, or it can be dynamic in which case the statistics of the newly identified spam message are incorporated into the model. Types of filters include Bayesian filters, neural nets, and genetic algorithms. This technology is common with applications with as SpamAssassin. Spammer have been known to try to evade filters by obtaining copies of the filters and statistical models of spam messages, which are often distributed with the filters. The spammers then attempt to craft messages that the spam filter will not flag as spam.
The second type of filtering method looks for specific keywords and other non-statistical indicators of spam in the message. One common indicator is a hyperlink in which the displayed URL does not match the hyperlinked URL. Another common indicator is if the URL is on a blacklist of known spammers.

### 4.1.2 Authentication Services

An authentication server validates the identity of a sender. This may happen at any of three levels: user, host and domain. A user authentication server validates the identity of the sender of a message. When a user sends a message, he or she digitally signs the message. When a receiving program receives the message, it determines the appropriate user authentication server to use based upon the sender’s address. It then queries that server, and using information from that server determines whether the user digitally signed the message. Examples of this technology are PGP and PEM. User authentication servers tie the origin of the letter to a user. The problem here is that users may be transient. A host authentication server validates that a message came from the sending computer. When a message is sent from a computer, the computer’s mail server digitally signs the letter. When a receiving program receives a message, it determines the appropriate computer authentication server to use based upon the sender’s address. It then queries that server, and using information from that server determines whether the computer digitally signed the message. A domain authentication server validates that a message came from the sending domain. When a message is sent from a computer in a domain, the message is digitally signed. When a receiving program receives the e-mail message, it determines the appropriate domain authentication server to use based upon the sender’s address.
It then queries that server, and using information from that server determines whether the message was digitally signed by the domain. Domain Keys is an example of this technology.

4.1.3 Authorization Services

An authorization server identifies those computer authorized to send electronic mail from a given domain. For example, if an MTA receives an e-mail from pantheon-po5.its.yale.edu, the MTA asks the authorization server for domain its.yale.edu if the computer called pantheon-po5.its.yale.edu is authorized to send mail from that domain. If so, the e-mail is accepted. If not, the e-mail is either rejected, or it is labeled as suspect. The Sender Policy Framework (SPF) is an example of a protocol for authorization servers. The problem is that if the message is sent from an authorized computer, it could still be spam. This is especially true if the computer allows messages to be relayed through it, or if a spammer sets up the domain. In the latter case, the authorization server will simply confirm that the system used by the spammer is authorized to send e-mail, defeating the purpose of the authorization server.

4.1.4 Reputation-Based Services

Reputation-based services come in several forms, with the most common being whitelists and blacklists. A blacklist, sometimes called a “realtime black list” or RBL is a list of addresses or domains that have been deemed as having a poor reputation for bad behaviors, such sending spam. If an e-mail message was sent from an address or domain listed on a RBL, then it is flagged as spam. An example of a blacklist is the Spamhaus Block List and the effectiveness of these lists depends entirely on the quality and comprehensiveness of the lists. A whitelist, on the
other hand, maintains a list of trusted addresses or domains, and e-mail is accepted only if sent from a member of the list, while all other messages are discarded or marked as potential spam. For example, Spamhaus has plans to maintain a “.mail” top level domain by checking sites in the domain to eliminate registrants who might send spam, the goal being that e-mail from any computer in that domain may be accepted without fear that the mail is spam.

There are some concerns with using reputation-based servers. For instance, reputation is dependent on the a virtual identity of the user and not the actual user himself, which means that a spammer need only establish a good reputation for one identity to send his spam. By the time that identity has been labeled with a bad reputation, the spammer could simply establish a new second identity and begin building a new reputation.

4.1.5 Challenge-Response

Challenge-response involves having a user asserts an identity, presenting him with a question, and waiting for the user to response with the correct answer before validating his identity. Thus, a challenge-response technique can be used to require that the sender of e-mail confirm that the e-mail is not spam. More specifically, when an mail client receives an e-mail message, it would place the message into a temporary queue, contact the sender and request that the sender reply to a challenge of some sort, such as a a simple puzzle. When the response is received and validated, the e-mail is delivered. The sender may also be placed on a whitelist, to avoid future challenges. If no response is received, the letter is marked suspect or discarded.

Unfortunately, this challenge-response system is extremely inefficient and inconvenient. The sender may not respond in a timely manner, which would cause the message to be delayed
or discarded. Not only that but the challenge-response system would be problematic for legitimate mass mailings.

4.1.6 Port Blocking and Rate Limiting

“Port blocking” or more specifically “blocking port 25 traffic” involves having the ISP refuse to allow some computers, such as those listed on a blacklist, to send mail. ISPs often designate some set of systems as trusted mail servers, and allow outgoing mail only if mail originates at one of those servers. This method is particularly effective against the use of zombies implanted on a home user’s system, since those systems are not designated as mail servers and thus would be blocked. A similar technique implemented by ISPs is “rate limiting” or “port throttling,” which involves the ISP limiting the rate at which the computer can send mail. For example, the ISP may allow the computer to send no more than 100 letters a day.

4.1.7 Image Blocking

Blocking images that are embedded in e-mails helps to prevent consumers downloading images located on a malicious Web server. Spammers and phishers have been known to use this process to confirm “live” e-mail addresses. Blocking images and requiring the recipient to approve images before downloading helps to prevent unauthorized image downloads.

4.1.8 Keywording

To enable a legitimate recipient to get around the spam block, some mail clients can be configured to accept e-mail containing a key word or password. This is a form of whitelisting, but involves a keyword in the message rather than an originating address. One challenge for this
process is the difficulty in informing legitimate recipients about the keyword. One possibility is to post the keyword on the recipient’s Web page, which most spammers will not check.

4.2 Anti-Phishing Techniques

4.2.1 Beyond Passwords

Some banks have reexamined their reliance on simple typed passwords and have chosen to use two-factor authentication instead. Passwords vulnerabilities have existed in almost all computer systems. With respect to electronic commerce, the problem is that users have a tendency to use the same password for all accounts. Thus, a phishing attack that compromises one of the user’s account, the phisher may then have access to multiple accounts. Some sites have begun to require the user to provide the answer to a secret question.

Bank of America has recently implemented their SiteKey Service, which requires the user to login from a secure machine and presents the user’s individual personal image that serves to confirm that the site an authentic Bank of America website. The service is provided by PassMark Security and stores a “secure cookie” on the user’s PC in order to link it to Bank of America’s server. The process of creating the secure cookie, however, has been criticized as vulnerable because it requires the user to enter traditional personal information such as the user’s mother’s maiden name, social security number, and so forth. It would not be too difficult for phishers to claim that the user’s site key has expired and to require the user to re-enter the personal data.
4.2.2 Browser Improvements

In recent years, security experts have begun developing software specific for protecting against phishing attacks. The common theme of all these efforts have been to make Web-browsing environment much more secure. For instance, there are now anti-phishing browser plug-ins available. With one type of these plug-in will check each URL to verify that the requested server host is not currently on a known list of phishers. Netcraft’s toolbar implements these types of techniques against phishing. DeepNet 3.1 is a browser that will implement this feature into the browser itself.
4.2.3 Third Party Certifications

One possible method of distinguishing to malicious websites being used in phishing scams is to use third parties to certify a site as legitimate and authentic. For several years, business have been using third party certification by established organizations, such as Better Business Bureau, TrustE or Verisign, in effort to establish the appearance of trustworthiness. Unfortunately, many of these systems have been subverted. For instance, these seals are often simply digital images that can be relatively easily copied and displayed by malicious website. Furthermore, many times the seals only confirm that the merchant complies with a privacy policy and has no mechanism for confirming the security of the merchants site.

4.3 Consumer Vigilance

The most effective way of protecting the public against phishing attacks is to increase consumer awareness and vigilance, particularly since phishing attackers have proven themselves to be very creative and efficient in developing new ways of executing their attacks. While
technological and legislative improvements are effective and important as well, simple steps taken by consumers can protect them from most attacks. These include behavior such as avoiding clicking on links embedded in e-mails and instead going to organization website directly. Thus many government agencies as well as individual banks and other online businesses have established a fraud section of their website that list and encourage good consumer behavior.

Example: Bank of America Fraud Prevention Site

Source: www.bankofamerica.com
5 LEGISLATION

Phishing because they use false and fraudulent statements to deceive people into disclosing valuable personal data violates several existing federal laws. Identity theft, wire fraud, credit card fraud, bank fraud, and computer fraud are all already prohibited by various federal and state laws. Nevertheless, tracking and prosecuting offenders has been particularly difficult, especially since it was unclear as to which government agency was responsible. Thus, in recent years the federal and state legislatures have begun to pass legislation the specifically targets online identity theft. First were broad efforts to fight spam and online identity theft and has culminated in the Anti-Phishing Act, which has yet to be voted on by the senate. Generally these acts are intended to define specific crimes and prescribe minimum sentences and fines. The following section will look at a sample of various types of laws that have been passed and used to fight phishing scams.

5.1 CAN-SPAM Act

The Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003, or the CAN-SPAM Act, was signed by President Bush on December 16, 2003, and became law on January 1, 2004. It was aimed at preventing senders of commercial e-mail from misleading recipients about the origin and content of e-mail and requiring senders to provide recipients the option of declining to receive additional commercial e-mail. The act includes a prohibition against false or misleading transmission information, a prohibition against deceptive subject headings, mandatory inclusion of a return address, a prohibition against transmission of spam after recipient objection, mandatory inclusion in spam of information identifying the message as
an advertisement or solicitation, mandatory provision of the opportunity to decline to receive further unsolicited messages from the sender, mandatory inclusion of the sender's physical address, a prohibition against initiating transmission of spam to a protected computer, a prohibition against using automated means to register for multiple e-mail accounts for the transmission of spam, and a prohibition against relaying an unsolicited message that is unlawful under this section. The Act provides various penalties for violations, such as “two years’ imprisonment for knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person during and in relation to specified felony violations” (S.877 CRS Bill Summary). The Act also requires the FTC to issue regulations defining the “criteria to facilitate the determination of the primary purpose of an electronic mail message.”

In some sense, the Act serves as a “best practices” standard for sending bulk commercial e-mail, providing guidelines to companies who wish to send commercial e-mail. However, this was the main criticism of the Act at the time it was signed. Anti-spam activists expressed deep disappointment in the fact that the Act appears to give Federal approval to the practice of sending spam. “CAN-SPAM legalized spamming itself,” said Steve Linford, the founder of the Spamhaus Project, a leading anti-spam organization, in a February 2005 New York Times articles (Zeller). Furthermore, the federal CAN-SPAM Act overrode state laws, which in many cases had stronger provisions against spam. For example, a California anti-spam law allowed recipients to sue spammers and also required that recipients opt-in to any commercial e-mail. The CAN-SPAM Act, on the other hand, sets an “opt-out” standard, and it denies individuals the right to sue spammers.

The effectiveness of the Act has been proven to be minimal. According the New York Times, “Since the Can Spam Act went into effect in January 2004, unsolicited junk e-mail on the
Internet has come to total perhaps 80 percent or more of all e-mail sent...up from 50 percent to 60 percent of all e-mail before the law went into effect” (Zeller). Furthermore, all phishing e-mails violate the provisions of the Act, which prohibits the transmission of false or misleading information.

5.2 Identity Theft Penalty Enhancement Act

On July 15, 2004, President Bush signed the Identity Theft Penalty Enhancement Act (ITPEA), which he said, “sends a clear message that a person who violates another's financial privacy will be punished” (White House Press Release). The act is aimed at fighting identity fraud by increasing penalties for identity-theft related crimes and establishing a new crime of “aggravated identity theft,” which is defined as using a stolen identity to commit other crimes, including phishing. It prescribes mandatory minimum sentences to be imposed in addition to the punishments provided for the related felonies, requiring that anyone who, while engaged in any of the crimes specified by the law, knowingly “transfers, possesses, or uses, without lawful authority” another person’s identification will be sentenced to an extra prison term of two years with no possibility of probation. Furthermore, the law prohibits the mere possession of the “identification of another person with the intent to commit, or to aid or abet.”

Besides the usual debates regarding the wisdom of mandatory minimums, there are hopes that the ITPEA will help with the enforcement across state borders. Chris Hoofnagle, deputy director of the Electronic Privacy Information Center in Washington, D.C. commented that “there are problems with state authorities who tend not to want to deal with the problem. If you're a Washington, D.C., resident and someone in California steals your identity, both
Washington and California police will play ping-pong with your case to avoid dealing with it” (Zeller).

5.3 Virginia Computer Crimes Act

Virginia was said to have passed the nation’s first law that specifically targeted phishing when it passed its Computer Crimes Act in January of 2005. The Act defined phishing as “fraudulently obtaining, recording or accessing from a computer any number of sensitive data points, including a person’s Social Security, driver’s license, and bank account numbers” (Greenemeier) and categorized phishing as a felony. That Act also imposes strict penalties on persons who sell or distribute information obtained through a phishing scheme. Virginia’s Computer Crimes Act’s provisions and penalties against phishing is considered tougher than conventional identity theft laws that require the state to prove that a person was going to do something unlawful with the information. According to Stewart Petoe, director of legal affairs for the Virginia State Crime Commission, “The can be very, very difficult in the world of cybercrime, so mens rea, or the offender’s mental state, isn’t required” (Greenemeier).

5.4 California Anti-Phishing Law of 2005

In October of 2005, Governor Arnold Schwarzenegger signed the California Anti-Phishing Law, which is said to be the nation’s first law that makes it “unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business” (SB 355). It provides civil remedies may also be pursued such that “a person who is engaged in the
business of providing Internet access service to the public, owns a Web page, or owns a trademark, and is adversely affected by a violation...may seek to recover the greater of actual damages or five hundred thousand dollars.” Individuals who have been damaged by phishing may bring a direct action to recover the greater of three times the amount of actual damages or $5,000 per violation.

5.5 Anti-Phishing Act of 2005

In July of 2004, Senator Patrick Leahy (D-VT) introduced the Anti-Phishing Act of 2004, which was stalled in committee without ever coming to a vote before the end of the congressional session. Then in February of 2005, Senator Leahy introduced the Anti-Phishing Act of 2005, which is virtually the same bill that, if passed, is similar to the California law in that it would criminalize the act of sending a phishing e-mail regardless of whether any recipients of the e-mail suffered any actual damages and the act of creating a phishing website regardless of whether any visitors to the website suffered any actual damages. As Senator Leahy says, “The [Act] protect the integrity of the Internet in two ways. First, it criminalizes the bait. It makes it illegal to knowingly send out spoofed e-mail that links to sham websites, with the intention of committing a crime. Second, it criminalizes the sham website that are the true scene of the crime” If the bill were to become law, then each and every element of the scam would become a felony subject to five years in prison and/or a fine up to $250,000. The Act averts free speech issues by exempting parodies and political speech from its reach by stipulating that the perpetrator must have the specific criminal purpose of committing a crime of fraud or identity theft. Unfortunately, the bill does not provide any guidance or allocation of additional resources for its enforcement.
6 ENFORCEMENT AGENCIES

In the last couple of years, several government agencies have begun to devote their resources to informing the public on ways to avoid becoming phishing victims and to finding and prosecuting phishers.

6.1 Federal Trade Commission

The Federal Trade Commission (FTC) is responsible for protecting consumers by preventing fraudulent, deceptive, and unfair business practices in the marketplace and providing information to help consumers spot, stop, and avoid them. In 1998, Congress enacted the Identity Theft and Assumption Deterrence Act, directing the FTC to establish the federal government’s central repository for identity theft complaints and to provide victim assistance and consumer education, and since then the FTC has maintained and disseminated information from the Identity Theft Data Clearinghouse. With Internet, telemarketing, identity theft, and other fraud-related complaints, the FTC maintains Consumer Sentinel, an online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad. The FTC also maintains OnGuardOnline.gov, a website that “provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information” (onguardonline.gov).

The FTC also established a special Criminal Liaison Unit to expand criminal prosecution of consumer fraud. The Criminal Liaison Unit “identifies enforcement agencies that may bring specific types of consumer fraud cases, educates criminal law enforcers in areas of FTC
expertise, and coordinates training with criminal authorities to help the FTC prepare cases for referral and parallel prosecutions” (FTC “FTC, Justice Department Halt Identity Theft Scam”). Thus the unit helps FTC efforts to ensure appropriate criminal prosecution of consumer fraud and led to a joint law enforcement initiative by the FTC and the DOJ in March of 2004, who brought two separate actions to shut down a phishing operation that fraudulently used AOL and PayPal logos to con hundreds of consumers into providing credit card and bank account numbers.

6.2 Department of Justice

The Department of Justice (DOJ) prosecutes cases of identity theft and fraud under a variety of federal statutes, including the Identity Theft and Assumption Deterrence Act of 1998. This legislation created a new offense of identity theft, which prohibits “knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit” (S.512). Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation, the United States Secret Service, and the United States Postal Inspection Service to prosecute identity theft and fraud cases.

6.3 Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) is responsible for investigating “cyber threats,” which include “traditional criminal activity facilitated by computers and the Internet, such as theft of intellectual property, online sexual exploitation of children, and Internet fraud” (FBI). The FBI also partnered with the National White Collar Crime Center (NW3C) established the Internet Crime Complaint Center (IC3) “to serve as a means to receive Internet related
criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate” (www.ic3.gov). The IC3 was formerly known as the Internet Fraud Complaint Center (IFCC) and was renamed in October 2003.

6.4 Secret Service

The Secret Service investigates crimes associated with financial institutions. More specifically, the Financial Crimes Division (FCD) plans, reviews, and coordinates criminal investigations involving Financial Systems Crimes, including computer fraud. The USA PATRIOT ACT OF 2001 ordered the Director of the U.S. Secret Service to take appropriate actions to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the nation for the purpose of preventing, detecting and investigating various forms of electronic crimes.

6.5 Others

Various government agencies have devoted resources into investigating identity theft as well as helping to educate the public on how to guard against attempts at theft. Some examples are the Federal Deposit Insurance Corporation at <http://www.fdic.gov/consumers/consumer/index.html>, the U.S. Postal Inspector Service at <http://www.usps.com/postalinspectors/id_intro.htm>, and various state agencies.
In July of 2003, the Federal Trade Commission brought its first law enforcement action targeting phishing. The case was brought against a minor who “who allegedly used hijacked corporate logos and deceptive spam to con consumers out of credit card numbers and other financial data” (FTC Press Release). More specifically, he “sent spam messages to United States consumers indicating that there had been a problem with the billing of the consumers’ AOL accounts...[stating] that if the consumers did not respond by providing their billing information, they risked possible termination and/or deletion of their accounts” (*Federal Trade Commission, Plaintiff, v. _________, a minor*). He used information users entered to charge online purchases and open accounts with PayPal. The final settlement, which was considered mild by many legal analysts due to the fact that the defendant was a minor, bars the defendant “from sending spam in the future” as well as requiring him “to give up $3,500 in ill-gotten gains” (FTC Press Release).

In October 2003, Microsoft filed a lawsuit against an unnamed individual in Seattle after a phishing scam targeted Microsoft’s MSN customers. Eventually, the company tracked the scam back to 21-year-old Jayson Harris of Davenport, Iowa. Microsoft later won a $3 million judgment against Harris for trademark violations. The FBI seized three of Harris's computers and is in the latter stages of its own criminal investigation into the matter. Almost two years later, in March 2005, Microsoft filed 117 civil phishing enforcement lawsuits in the U.S. District Court for the Western District of Washington against unnamed individuals, hoping to discover the identities of those responsible for a flood of fraudulent e-mail messages targeted specifically at customers of Microsoft’s MSN Internet and Hotmail e-mail services.
In the fall of 2004, in an undercover investigation dubbed “Operation Firewall,” the U.S. Secret Service netted 28 individuals in seven countries for credit card fraud, identity theft, computer fraud, and conspiracy (Krebs). It was the first ever wiretap on a computer network that agents used to locate the thieves. The investigation was a joint operation of the Secret Service, the U.S. Department of Justice, foreign law enforcement agencies and investigators from the financial services industry. The investigation started in July 2003 when the Secret Service began investigation of an unspecified financial crime. By going undercover on a website called Shadowcrew.com, investigators were able to monitor the site’s 4,000 members for criminal conduct. The group traded stolen credit card numbers and bank account information as well as counterfeit passports, drivers' licenses, Social Security cards, credit cards, debit cards, birth certificates, college student ID cards, and health insurance cards, according to the indictment.

In February of 2006, America Online was first to take advantage of Virginia’s anti-phishing law when the company sued three international groups that allegedly stole information from unsuspecting AOL users by sending e-mail that claimed to be legitimate messages from the company (Associated Press). The suits alleged that 30 unidentified phishers violated the 2005 Virginia anti-phishing act as well as federal computer fraud law and the Lanham Act, which protects trademarks. The phishers were believed to be part of a multinational network spanning the United States, Germany and Romania. A month later, Microsoft also announced a global enforcement effort on March 20, 2006, (Microsoft Press Release), announcing that by the end of June 2006 it will have initiated legal actions on more than 100 cases in Europe, Middle East and Africa against individuals suspected of committing online fraud. According to Microsoft, “the legal actions are linked to a larger Microsoft program, the Global Phishing Enforcement Initiative (GPEI), launched by the company to coordinate and expand its many anti-phishing
efforts worldwide to fight phishers through consumer protection, partnerships and prosecution” (Press Release).

It is important to note that most of the above lawsuits that have been chosen to illustrate current efforts have been filed against unidentified individuals because of the inherent difficulty in tracking phishers, particularly if the attacks originated abroad. Situation such as these makes it obvious that the government cannot tackle the phishing problem. In other words, the laws mentioned in previous sections are only as effective as the technology used to track suspects down.
Like all legislative efforts aimed at punishing Internet-related offenses, the acts listed above face formidable hurdles. For instance, there is inherent difficulty in tracking and locating the perpetrator of an on-line crime. Furthermore, the Internet is virtually borderless and thus obtaining personal jurisdiction is difficult. Even beyond these challenges, the most legislative measures thus far have had limited effect in preventing phishing because they generally provide remedial measures, although according to the *New York Times*, “a dozen states…have set up procedures for residents afraid of identity theft to lock and unlock their credit reports” (Darlin C1). While many hail such measures as a step in the right direction, lobbyists for agencies, like Equifax, are pushing Congress to override.

Finally, few laws stipulate or provide funding for a particular government agency to be responsible for investigating phishing crimes. Although there has been an increased number of phishers being caught and prosecuted, this number is relatively few compared to the number of attacks that occur. For instance, if a person become a victim of a phishing attack, they are encouraged to report it to the Internet Crime Complaint Center, a joint project of the FBI and the National White Collar Crime Center at <http://www.ic3.gov> or the Federal Trade Commission’s identity theft center <http://www.consumer.gov/idtheft/>, but they also have the option of calling the SEC’s Office of Internet Enforcement Complaint Center at <http://www.sec.gov/complaint.shtml>, or the Secret Service <http://www.secretservice.gov/alert419.shtml> if the e-mail is Nigerian Advance Fee Fraud spam, not to mention a list of various state agencies.
It is unclear if there really is any clear and simple way for law enforcement agencies to fight against phishing. However, while it is easy to criticize legislative and enforcement efforts as minimally effective, these efforts are arguably still significant mainly because they increase the public trust in electronic commerce, which appears to be a greater concern to many businesses than the phishing problem itself. It is easy for consumers to gain a heightened sense of urgency regarding security concerns of Internet commerce particularly since many of their inboxes are inundated with phishing e-mails. Thus, in more ways than one, it is important for both businesses as well as federal and state legislatures and law enforcement agencies to make the effort to control the phishing problem.
In the beginning, phishing was simply a challenge for young hackers. Then, as an increasing percentage of businesses began offering services online, phishing has become a lucrative criminal enterprise with relatively low probability of prosecution. Although eliminating the phishing problem completely is almost certainly impossible, it is important that business and government agencies make efforts to minimize the effectiveness of attacks, particularly since trust is an important element to electronic commerce. While technical and legal solutions are indeed important to develop for both practical security as well as consumer trust, in the end, consumers must also realize that the most effective means of fighting phishing attacks is vigilance.
BIBLIOGRAPHY


Department of Justice: Criminal Division. “Special Report on ‘Phishing’.”


Identity Theft and Fraud Site. United States Department of Justice Criminal Division/Fraud Section. 9 Jan 2006; cited 22 Mar 2006


Microsoft Press Release. “Microsoft Targets Cybercriminals With Launch of Global Phishing

Mitnick, Kevin D., and William L. Simon. The Art of Deception: Controlling the Human

   and ‘PHARMING’ that Steal Billions of Dollars Annually from Consumers.” 28 Feb
   2005.

   Internet Daily. 13 Mar 2006.


   <http://cc.uoregon.edu/cnews/spring2004/epend.html>.

Stansel, Ed. “Don’t get caught by online ‘phishers’ angling for account information.” Florida

United States Secret Service. “Public Awareness Advisory Regarding ‘4-1-9 or ‘Advance Fee