



realtimepublishers.com™

*The Definitive Guide™ To*

# Controlling Malware, Spyware, Phishing, and Spam

**McAfee®**  
Proven Security™

*Dan Sullivan*

---

Chapter 5: Phishing and Identity Theft.....	86
Anatomy of Phishing Scams.....	86
Social Engineering and Phishing.....	87
Direct Questioning.....	87
Incremental Accumulation of Information.....	88
Physical Access.....	88
Reverse Social Engineering.....	88
Internet-Based Social Engineering.....	89
Phishing Trap.....	93
Limits of Social Engineering-Based Phishing.....	94
Malware-Based Phishing Techniques.....	95
Botnets and Phishing Attacks.....	95
Malicious Software for Phishing.....	97
Exploiting Browser Vulnerabilities.....	99
DNS Attacks.....	100
Economics of Phishing and Identity Theft.....	102
Impact on Consumers.....	104
Phishing and Identity Theft Countermeasures.....	105
Business Countermeasures.....	105
Consumer Countermeasures.....	106
Summary.....	106

## Copyright Statement

© 2005 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at [info@realtimepublishers.com](mailto:info@realtimepublishers.com).

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

## Chapter 5: Phishing and Identity Theft

Some of the most challenging security problems are based on people's behavior more than on device or application vulnerabilities. The term *phishing* has come into use to describe techniques for tricking individuals into disclosing confidential information, such as account numbers, Social Security numbers, or financial data. The practice of conning information and money is certainly not new, but like so many other operations, the Internet has changed how it is done. Email and bogus Web sites are now tools in the con men's toolboxes. With personal information in hand, criminals masquerade as the victim and withdraw money from bank accounts, sell investments, and transfer funds. Another troubling and increasing related problem is identity theft.

Identity theft occurs when a perpetrator uses a victim's identity for financial gain. Pretending to be someone else to secure loans, acquire telecommunications services, or apply for credit cards are common objectives. Identity thieves can get personal information in a number of ways, from sorting through trash looking for account statements, paycheck stubs, or other financial documents ("dumpster diving") to tricking the victim to reveal details through phishing scams.

This chapter will examine the nature of phishing scams with an emphasis on

- Anatomy of phishing scams
- Economics of phishing
- Countermeasures to phishing

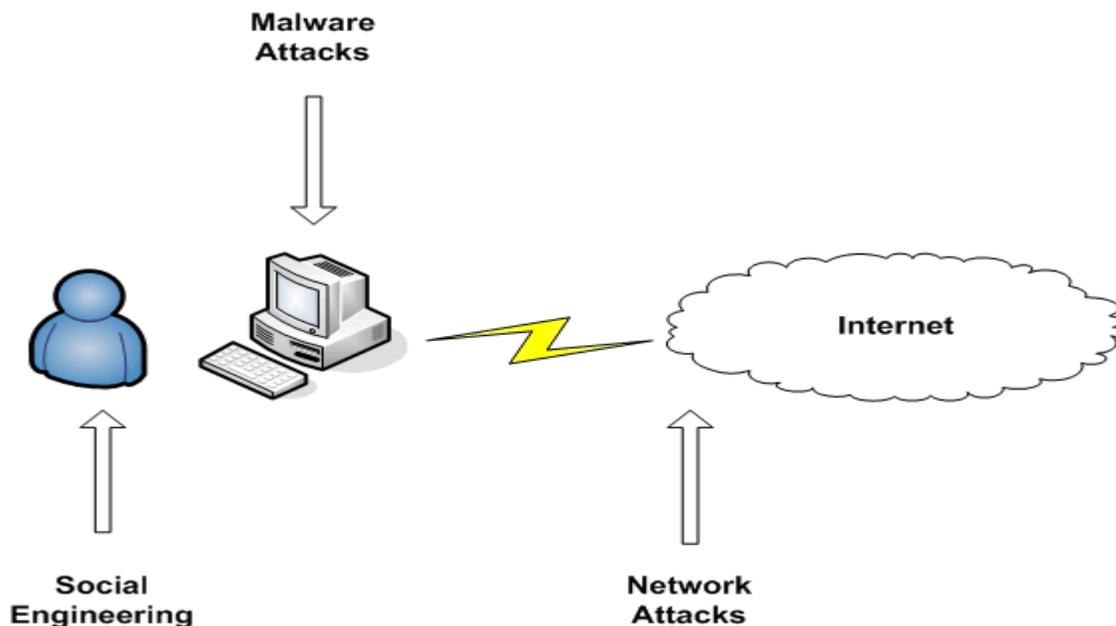
In the course of the discussion, we will also explore how phishing is evolving in the all too common game of cat-and-mouse played by security professionals and cyber criminals. The chapter will also include a discussion of identity theft and its relation to phishing.

### Anatomy of Phishing Scams

Phishing has evolved from a traditional social engineering operation to include malicious software for stealing credentials and network attacks to redirect traffic from legitimate sites. In general terms, the goal of phishing is to steal credentials. Three techniques are used:

- Tricking individuals to disclose information
- Deploying malware to capture user credentials and account information
- Attacking the Domain Name Services (DNS)

Each method presents a different set of challenges and requires particular countermeasures. As Figure 5.1 shows, these attacks target different parts of the computing infrastructure, including users, computers, and the network.



**Figure 5.1:** Phishing schemes use social engineering, malware, and network attacks to collect user information.

### **Social Engineering and Phishing**

Social engineering is the practice of tricking individuals into disclosing confidential information or collaborating in a malicious act. There are many ways to perform social engineering:

- Direct questioning
- Incremental collection of information
- Using physical access
- Reverse social engineering
- Internet-based social engineering

### **Direct Questioning**

The simplest and most direct phishing method is to simply ask people for information. Of course, virtually no one would give out the PIN number of their bank card to a stranger that walks up to them on the street and asks for it. There is not perceived trust in that situation; there is probably a fair amount of justified distrust. Consider another example.

An employee is working at her desk and receives a call from Bob Johnson in the Help desk support center. Bob introduces himself and goes on to say that there have been network problems and proceeds to ask a series of questions about network performance, access to shared drives, and any problems she might have with email. He then says he needs to verify that her account is correctly executing the latest login script so he'll need her username and password. At this point, Bob has probably built up some degree of trust with the employee and if the request seems reasonable, the employee might give out the information.

When employees and users are too savvy to fall for direct questioning other techniques are utilized.

## Incremental Accumulation of Information

Directly asking for a username and password is too blatant in many circumstances; a better approach is to acquire information incrementally. For example, a perpetrator could call the human resources department to get the names of key personnel, such as the name of the CIO or head of PC support. From there, the perpetrator could call the office of the key person claiming to be from a software vendor checking on licenses. In the process, the caller can acquire the names of key pieces of software used in the organization. This process can continue and although the perpetrator may never get a username and password, they may get enough information to leverage other techniques, such as gaining physical access.

## Physical Access

Gaining physical access to a site can open a number of opportunities for someone conducting social engineering; it enables the attacker to:

- Watch users as they type usernames and passwords
- Claim to be from another office with the need to “borrow” a PC to check email
- Pretend to be from a vendor and on-site to correct a configuration problem with an application
- Scan wireless networks for unencrypted or weakly encrypted information

Physical or logical access to a network can enable another form of social engineering, known as reverse social engineering.

## Reverse Social Engineering

Reverse social engineering plays on our natural inclination to appreciate help from others. In this con, the perpetrator disrupts operations on a network, server, or desktop (which implies that the person already had some logical or physical access to the systems). The perpetrator then arrives claiming to understand the problem and have the solution (which of course, he or she does). When the problem is fixed, the perpetrator is the hero of the day and users are inclined to reciprocate or engage in conversation that would then lead to a disclosure.

 Social engineering does not change with technology trends. See, for example Ira S. Winkler and Brian Dealy's 1995 paper "Information Security Technology? ... Don't Rely on It: A Case Study in Social Engineering" for a discussion of simple and rapid techniques used to acquire access information in a number of financial services companies. The paper is available at [http://www.usenix.org/publications/library/proceedings/security95/full\\_papers/winkler.ps](http://www.usenix.org/publications/library/proceedings/security95/full_papers/winkler.ps).

## Internet-Based Social Engineering

Phishing, Internet-based social engineering, utilizes emails and bogus Web sites to lure victims. Like other forms of social engineering, this technique depends on establishing trust and then convincing the victim to share information. Phishing scams based on social engineering use a two-part scam: the lure and the trap.

The lure in phishing is usually an email message that appears to be a request for some information or action from a legitimate business. eBay, PayPal, and banks are commonly portrayed as the senders. To get people's attention, phishers use subject lines that often raise users' concern. The following list highlights example messages lines (Source: the Anti-Phishing Working Group):

- Update Your Wells Fargo Access Online Information
- New email address added to your eBay account
- Credit Union Services: update your account records
- Credit Card Declined Notice
- Receipt of Your Payment to DELL

In general, phishers depend on three types of lures:

- Those based on fear
- Those that promise rewards
- Those that work with a victim's expectation of legitimate email

The fear-based phishing scams are probably the most prevalent judging from examples found in phishing databases, such as the Anti-Phishing Working Group's Archive.

 The Anti-Phishing Working Group's Archive is available at [http://www.antiphishing.org/phishing\\_archive.html](http://www.antiphishing.org/phishing_archive.html).

### ***Lure Number 1: Fear***

Phishers have taken an approach sometimes seen in technology sales—the appeal to fear, uncertainty, and doubt (FUD). In fear-oriented phishing scams, the subject line needs to generate enough concern to get the victim to read through message as the message tries to establish trust through a combination of visual cues and text.

For example, one scam purporting to be from eBay uses the eBay logo and links to eBay services such as search, discussion boards, and help. The message headline states that the user's credit/debit card must be updated immediately followed by an ironic warning that the recipient's eBay account has recently been accessed from a foreign IP address. It goes on to provide an IP address from which the access attempt occurred along with the ISP host. The message even advises the reader to "Please save this fraud alert ID for your reference." The cumulative effect of well-placed visual cues, such as logos, and well-written, official-looking text can be effective enough to get readers to take the next step, and click through to a bogus Web site, then provide their identifying information.

### Lure Number 2: Something for (Virtually) Nothing

The appeal of something for nothing, or very little, is bound to get someone's attention. Phishing scams have used the allure of prizes, gift cards, and other rewards to entice readers to click through to phishing sites. Just as some phishing scams can be very sophisticated and likely to catch even some wary readers, other scams are so poorly done it is difficult to imagine the scheme is very effective (see Figure 5.2).

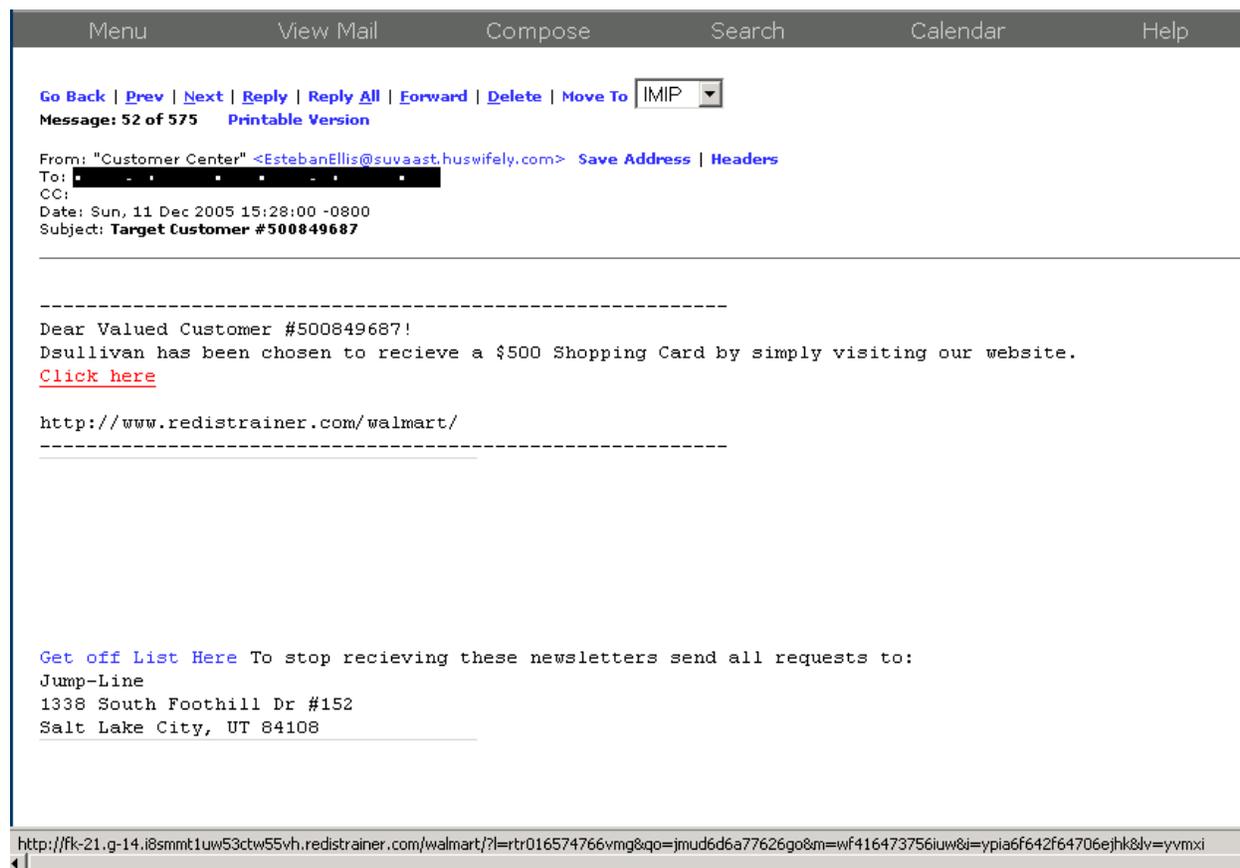
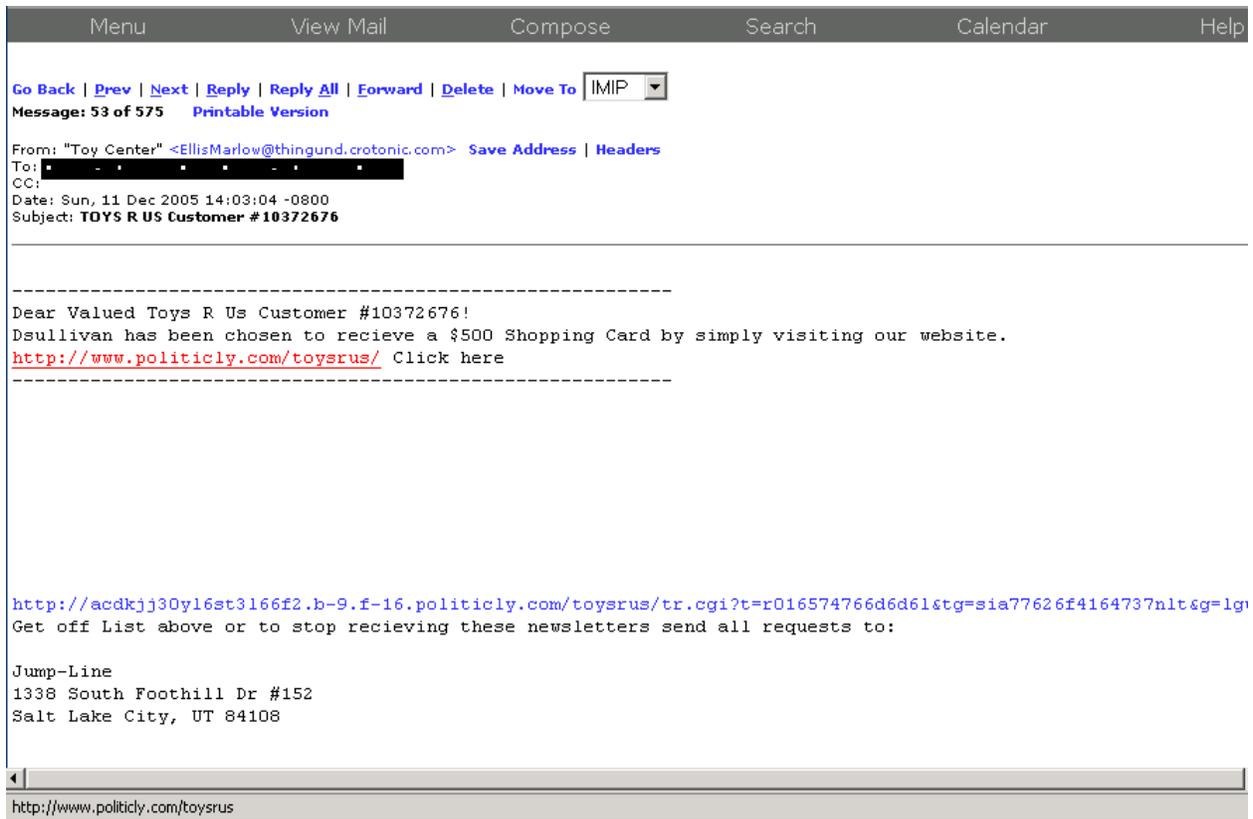


Figure 5.2: An example of both a “something-for-nothing” lure and a poorly crafted phishing message.

The subject line “Target Customer #500849687” is not particularly promising, but when the reader does open the message, he or she finds a simple one-line enticement to receive a \$500 shopping card just for visiting a Web site. Given that this message is purportedly from Target, it is hard to imagine why the company would use their competitor's name in the URL listed in the message, <http://www.redistrainer.com/walmart>.

The target URL listed in the bottom of the browser window shows what looks like a generated URL. This URL could be unique to the this message so that the phisher can link a click-through back to this email address even if the reader does not fill in any information at the bogus Web site.

Another telltale sign of mass generated phishing messages is that the basic form is repeated but the phisher impersonates a different business. Figure 5.3 shows another phishing message received less than 90 minutes earlier by the same recipient. The content is the same except the retailer's name has changed and the URL no longer mentions a competitor.



**Figure 5.3: Mass-produced phishing messages with little variations are easy to spot.**

These phishing examples represent one end of the phishing spectrum: mass generation, multiple versions, poorly edited, few if any graphics to provide visual indications of a legitimate site. As with spam, the cost of creating these phishing messages is so low, a positive return on investment can be realized if only an extremely small number of readers fall for the lure. At the other end of the spectrum are carefully crafted messages that take into account the readers' expectations for legitimate email.

### **Lure Number 3: Expectations of Legitimate Email**

A more difficult-to-prevent form of phishing is known as context-aware phishing. (This discussion is based on the work on Markus Jakobsson of Indiana University.) This form of phishing is targeted to a specific audience, such as eBay customers that bid on particular types of products, unlike the mass emailed fear- and enticement-style scams. The messages are designed to appear to be an expected message, such as an announcement that the recipient is a winner of an eBay auction. This format increases the likelihood that a reader will respond to the message.

Context-aware phishing is a three step process:

- Identity linking
- Victim selection
- Context-aware password phishing

In the first step, identity linking, the phisher links identity information of a user, such as an eBay user name, with public identity information, such as an email address. There are three forms of identity linking:

- Inside-out linking, which starts with identity information used inside an application and links it to outside information
- Outside-in linking, which starts with external information (for example, email) and links to internal information
- Epidemic linking, in which accounts compromised by one of the other two accounts are exploited to find other username/email pairs

In some cases, linking is trivial because application names are the same as the user's email address. In other cases, the way an application works is exploited to get inside or outside identities. For example, a bidder on eBay can request the email address of a seller after making a bid for an item. When questions are asked of eBay users, if they do not respond using the anonymous response method provided, phishers are given users' email addresses.

If a phisher has an email address but needs a user account, the phisher could send a bogus message purportedly from eBay requesting that users provide their eBay user IDs. The message might specifically say a password is not needed and in fact should never be shared with anyone.

Once the phisher has a set of email addresses and application identifiers, he or she can move on to victim selection. During the victim selection step, the phisher will select application users who are plausible targets. For example, the phisher could monitor eBay items to determine the highest bidder at any time and select all users listed at any time. This step requires knowledge of the target application, such as an eBay auction, and the ability to cull specific information from such data-rich systems. One of the advantages of services, such as eBay, is that they build the trust of their users by sharing so much information about the histories and evaluations of buyers and sellers. It is, however, also one of the aspects of such sites that phishers can exploit.

The final stage is the password phishing step. Once the victims have been identified, they are sent an email in response to their bids, such as a congratulation message saying they have won an auction. The email will contain a link to a phisher-controlled site that looks like the real eBay site and the user will be prompted for his or her user ID and password. Since the user is expecting, or at least not surprised, to find a message from eBay, this type of attack has a higher probability of succeeding than cruder phishing attacks.

 For more information about context-aware phishing and methods of prevention see Markus Jakobsson's "Modeling and Preventing Phishing Attacks" at [http://www.informatics.indiana.edu/markus/papers/phishing\\_jakobsson.pdf](http://www.informatics.indiana.edu/markus/papers/phishing_jakobsson.pdf).

The phishing lure is designed to get victims to click through to a phisher-controlled site. Phishers will use fear and enticement as well as more sophisticated attack methods. Some phishing schemes are so poorly executed they are easy to spot; others, like context-aware phishing, are challenging even for the cautious recipients. For whatever reason, the recipient clicks through; once they reach the bogus Web site controlled by the phisher, they are operating within the phishing trap.

## Phishing Trap

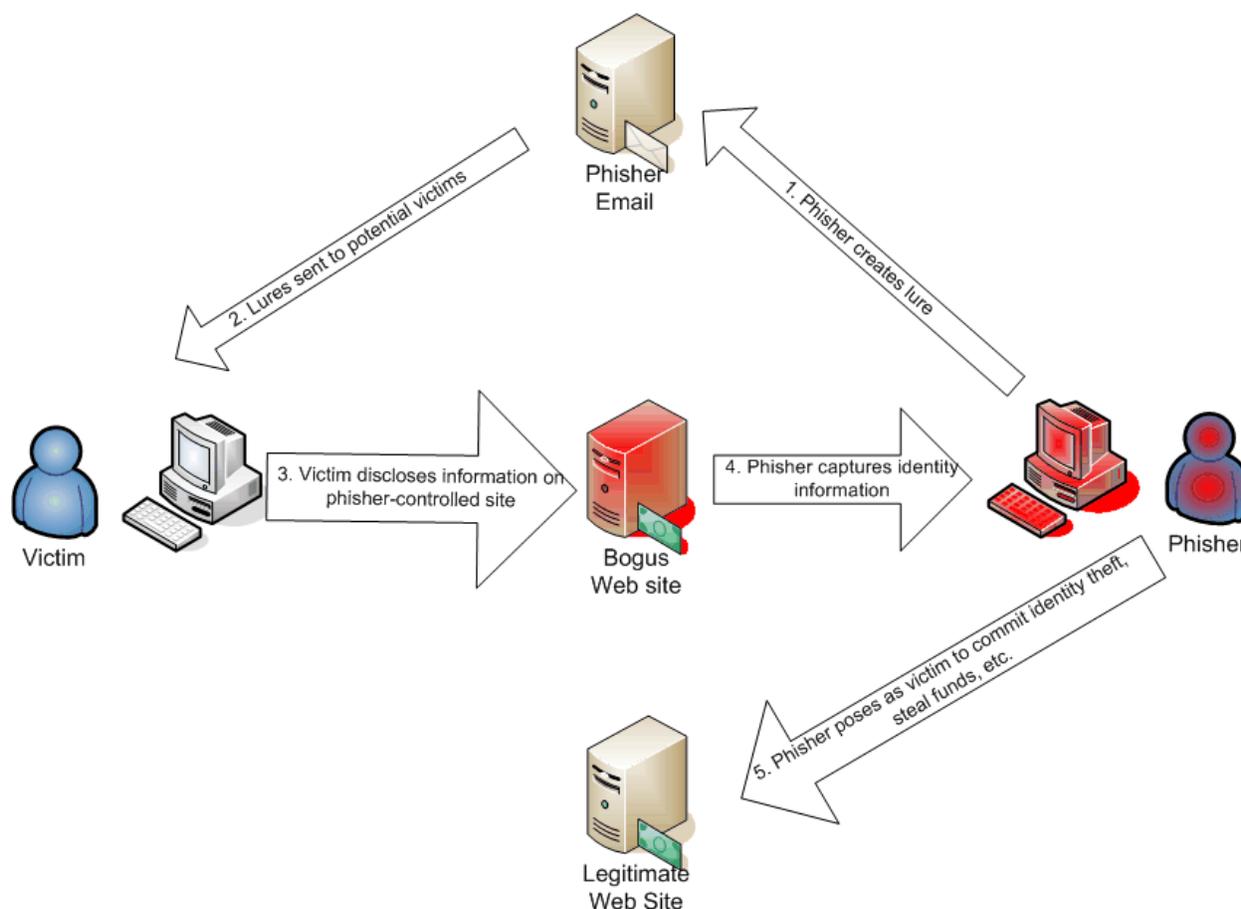
The phishing trap is the Web site that appears legitimate but is controlled by the phisher. This trap is where the phisher collects victim's information. Once in hand, the phisher can then go on to use the victim's credentials to gain access to the victim's accounts, funds, and other resources. The full phishing process is depicted in Figure 5.4.

Once at the site, there may be additional cues to indicate the site is not legitimate. These can include:

- Suspicious-looking URLs
- Use of HTTP instead of HTTPS protocols
- Text with grammatical errors
- Asking too many personal questions for a simple update lure

Phishers use a variety of techniques to mask their sites, such as using IP addresses rather than domain names or using punctuation in a URL to create one similar to a legitimate Web site but still distinct. Hexadecimal encoding can also be used to replace literal characters with their numeric encoding. In still other more-difficult-to-detect cases that have been demonstrated but not necessarily used yet, character sets can be mixed so that most letters in a URL are in ASCII while Cyrillic characters are used for letters similar in both character sets (such as a, c, p, and t).

Another indication of an illegitimate site is the use of the non-secure HTTP protocol. Few if any legitimate businesses ask customers to provide confidential information, such as account numbers, without using Secure HTTP protocol (SSL encryption). Secure Web sites have URLs that begin with `https://` rather than `http://`.



**Figure 5.4:** Phishing is a multi-step attack that, when successful, results in the attacker gaining access to the victim's identity, funds, and other resources.

Other indications of bogus sites are ungrammatical text and poor editing. When large numbers of bogus sites are put up at once, the quality of the content may reflect that speed. The email examples mentioned earlier that referenced Wal-Mart in an email purportedly from Target demonstrates that this lack of quality can happen even in the lure.

### Limits of Social Engineering-Based Phishing

Social engineering-based phishing is becoming more sophisticated with techniques such as context-aware phishing, but awareness of the problem will limit the effectiveness of less-sophisticated approaches. Some common suggestions to prevent phishing attacks are becoming better known:

- Do not open emails from unknown senders
- Do not click on links in emails
- Type in URLs instead of clicking through from an email
- Examine URLs more closely for variations in business names or suspicious-looking addresses

As users become more careful, phishers are turning to technology-based methods to acquire personal information—especially the use of malware.

## Malware-Based Phishing Techniques

In addition to traditional social engineering approaches, some phishers are turning to malware to collect personal information. If we were to argue about definitions, this type of malware might be considered spyware and not a phishing attack. However, some researchers, such as Jason Milletary of the CERT Coordination Center, argue that some spyware should be dealt with as phishing attacks. Milletary makes three points:

- Phishers/spyware developers often use some type of social engineering to trick users into downloading the malicious software onto users' systems.
- Common techniques and tools are used to distribute phishing emails and malware.
- Countermeasures deployed to stem threats still leave other avenues of attack, so it is important to understand and address the broad range of techniques that criminals have at their disposal.

 For more information about this topic, see Jason Milletary's "Technical Trends in Phishing Attacks" at [http://www.cert.org/archive/pdf/Phishing\\_trends.pdf](http://www.cert.org/archive/pdf/Phishing_trends.pdf).

This gray area between phishing attacks and spyware includes three sub-areas that require distinct countermeasures:

- Use of botnets
- Malicious software installed on victims' machines
- Exploitation of browser vulnerabilities

These techniques are used in other information security threats, such as viruses, worms, and spam. Fortunately for the rest of us, that means the countermeasures deployed to combat one type of threat may address others at the same time.

## Botnets and Phishing Attacks

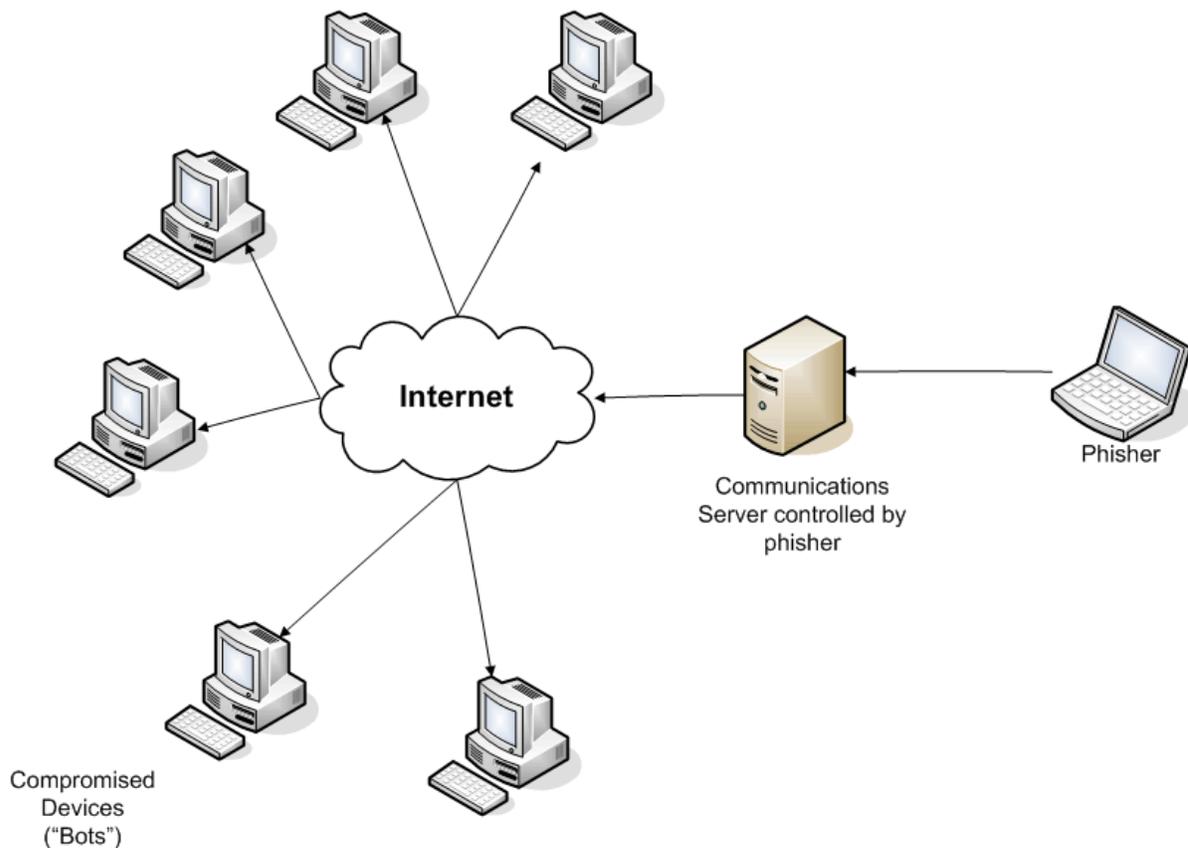
Botnets are sets of compromised computers that can be controlled from a single source (see Figure 5.5). Usually, a malicious piece of software is downloaded to a victim's computer, performs basic installation steps, then communicates with or waits for communication from a command system. The infected machine (the "bot") and command system can communicate over instant messaging, Internet chat protocols, peer-to-peer protocols, or other protocols.

Botnets are used as distributed computing platforms for performing tasks for the controller of the botnet. Some common uses are:

- Distributing spam
- Launching social-engineering-based phishing attacks
- Launching Distributed Denial of Service attacks (DDOS)
- Deploying additional malware, such as Trojan horses, to collect passwords and account information

In one of the more sophisticated botnet attacks to date, a group of three bot programs worked in conjunction to infect a large number of systems. The attack began with a malware program named Glieder-AK, which infects systems and opens backdoors for other programs to exploit. The second step in the attack came from the Fantibag Trojan, which disabled security features and prevented compromised machines from contacting antivirus vendors for updates. The attacks concluded when Mitglieder was downloaded, which opened further backdoors and left the system under the control of the botnet.

 The multi-Trojan attack is discussed in more detail in *The Register* "Hackers Plot to Create Massive Botnet" at [http://www.theregister.co.uk/2005/06/03/malware\\_bltz/](http://www.theregister.co.uk/2005/06/03/malware_bltz/).



**Figure 5.5:** Botnets are computers infected with malware that provides for remote control of the compromised host.

Botnets are tools of cyber criminals; the botnet itself is not typically the end goal, rather they are platforms for deploying and controlling other malware.

## Malicious Software for Phishing

The goal of the phisher is to collect information about a user that can be exploited for financial gain. Several kinds of malware are in use for this purpose; in general, these programs are referred to as Trojan horses or Trojans for short.

A Trojan is a program that appears to be for one purpose but is actually carrying out a malicious task instead of or in addition to its purported purpose. The malicious tasks include:

- Monitoring keystrokes
- Copying video frames
- Changing security settings
- Harvesting information from caches and other data sources

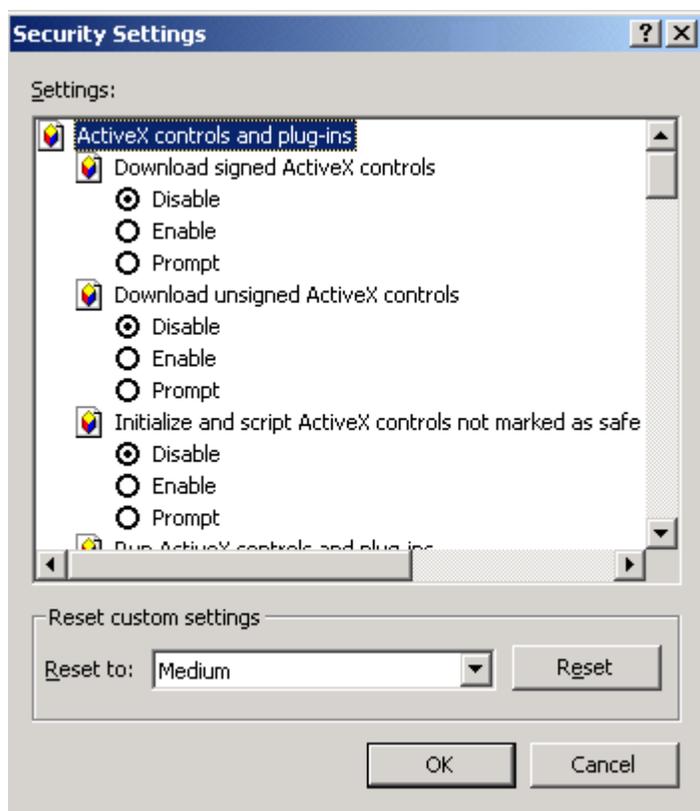
Keystroke monitoring uses a program or hardware device to capture each keystroke as it is typed. This technique has many legitimate uses, from evaluating human-computer interactions and testing software to law enforcement. It is also a well-known method for capturing user IDs, account numbers, and passwords.

One way to avoid using the keyboard to enter passwords is to use a virtual keyboard displayed on the screen. Users then mouse over characters on the virtual keyboard and click to enter the character. This method effectively avoids the potential for keyboard monitors to capture the confidential information. As you would expect, when security professionals and systems developers deploy a countermeasure, another avenue of attack is opened by hackers. In this case, it is the use of video-frame grabbers.

The purpose of a video frame grabber is to make a copy of the image that appears on a computer monitor at any time (such as when a mouse is clicked). Malware can use features of the operating system (OS) to intercept messages from the mouse or keyboard to detect a particular type of event and then take some action, such as copy the contents of the video buffer.

 The Windows Win32 API implements a number of hooks for programmers to intercept messages between objects, such as windows, the mouse, and the keyboard. For more information, see “Win32 Hooks” at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwui/html/msdn\\_hooks32.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwui/html/msdn_hooks32.asp).

Trojans used in phishing and spyware attacks may also change security settings on the infected system. For example, if a malware program infects a computer and executes in the context of an account with administrative privileges, it can change registry and browser settings that define access controls. (See Figure 5.6 for examples of Microsoft Internet Explorer—IE—security settings and their options.)



**Figure 5.6:** Once a computer is infected, malware can further reduce the security of the compromised machine by changing security settings, such as IE settings.

Once malware is on a system, it can capture information that has been left after its legitimate use has finished. For example, browser caches improve performance and ease of use by maintaining recently used information. Trojans can use this information to capture identifying information such as email accounts, user names, and recently visited Web sites.

This information alone may not be enough to compromise the user's financial accounts, but it can provide seed information for a successful context-aware phishing attack. For example, if a user recently made a hotel reservation, a phisher could send a bogus email stating that an error occurred in processing the reservation and the user needs to re-enter his or her credit card information.

Malicious software provides a number of methods for phishers to conduct their attacks. Like social engineering-based phishing, malware phishing can be used to incrementally collect information that is combined with details captured from multiple methods. A single piece of malware does not have to implement a full-blown phishing attack to be effective. This fact is made apparent when considering the impact of browser vulnerabilities.

## Exploiting Browser Vulnerabilities

Several vulnerabilities in popular Web browsers, particularly Microsoft IE and Mozilla Firefox, provide avenues for phishing attacks or at least help to obfuscate the instances of attacks. Past vulnerabilities have included (these have all been fixed with patches or in new versions):

- A bug in Mozilla Firefox truncates the status bar display when the mouse is moved over it and the href referenced in the URL contains a %00. (For details, see [https://bugzilla.mozilla.org/show\\_bug.cgi?id=228176](https://bugzilla.mozilla.org/show_bug.cgi?id=228176).)
- A bug in Mozilla Firefox allows a malicious page to appear encrypted with SSL and present the certificate of another site. (For details, see [https://bugzilla.mozilla.org/show\\_bug.cgi?id=240053](https://bugzilla.mozilla.org/show_bug.cgi?id=240053).)
- A bug in IE causes requests to some objects to be mishandled, which allows attackers to execute arbitrary code with the privileges of the user running IE. (For details, see <http://www.kb.cert.org/vuls/id/887861>.)
- A bug in IE DHTML allows attackers to exploit an ActiveX control that can download malicious code, read cookies, and change the content of Web pages. (For details, see <http://www.kb.cert.org/vuls/id/356600>.)

Although fixes are available for these vulnerabilities, any unpatched versions would still be vulnerable. It is important to note that vulnerabilities range from relatively low-impact problems, such as the bug in Mozilla Firefox that truncates a status bar display, to severe vulnerabilities that can allow arbitrary code to execute with the privileges of the user logged in to the system. (This is enough to give pause to systems administrators who surf the Web from privileged accounts).

One should also note that these are just examples of browser vulnerabilities that are known to exist. Others exist and have been patched, and we are likely to find others in the future. As the number of features in browsers increase, so do the opportunities for attackers to exploit those features.

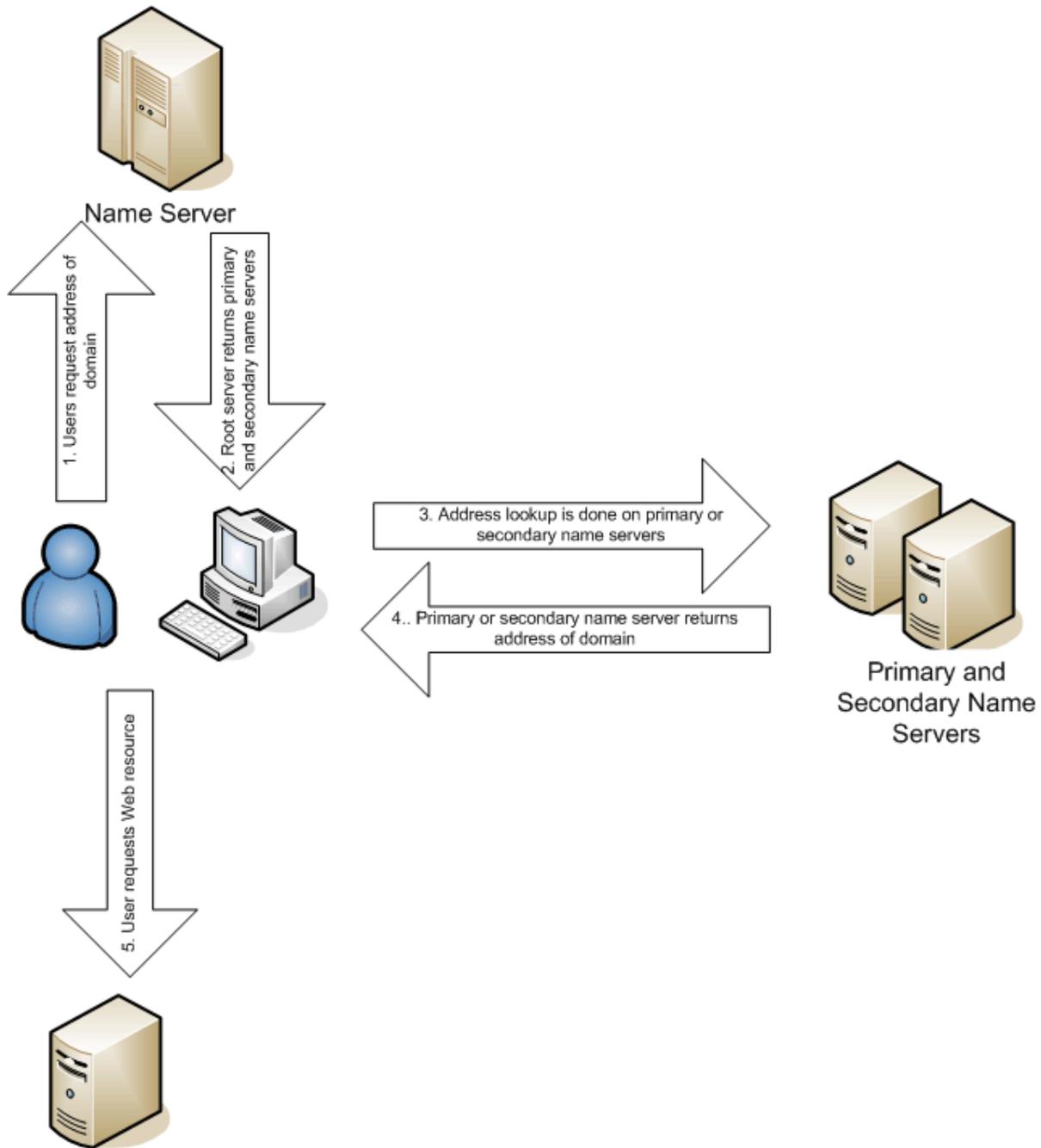
Malware-based phishing techniques range from sophisticated networks of bots that can launch mass phishing and spam email campaigns to Trojans targeted to gathering information from a single device to Web browser components that exploit vulnerabilities in browsers to conduct phishing attacks. Both social engineering attacks and malware phishing attacks present more than enough challenges to systems administrators and security managers; unfortunately, there is still one more category of phishing attacks they must address.

## DNS Attacks

The last form of phishing attack addressed in this chapter targets the infrastructure of the Internet. DNS is a protocol used to map easy-to-remember names of sites, such as McAfee.com, to the IP address of those sites, such as 216.49.81.129. Resolving an IP address from a domain name takes several steps (see Figure 5.7):

- A client requests the location of the server that has the address mapping of a site, such as MySite.com.
- A name receives the request and responds with the address of the domain's primary and secondary domain name server.
- If available, the primary domain server returns the IP address of the domain to the client making the request; otherwise, the secondary domain sends the information.
- Once the browser has the IP address, it requests the Web resource (for example, an HTML page) from the target site.
- The target site responds to the request by sending the resource to the client.

The relationship depends on implied trust. If the name server does not point to the correct primary and secondary domain servers, the client won't get the proper IP address. If the primary or secondary domains servers have inaccurate information, then again, the client will not find the site they are looking for. In the case of phishing attacks, the result is worse: the client is redirected to a bogus site.



**Figure 5.7:** DNS is compromised when inaccurate information is loaded into name servers.

Corrupting DNS is known as *DNS poisoning* and is a long-known and understood problem. It is also known as *pharming* in the context of phishing attacks. For the phisher, there are definite advantages to DNS poisoning over other methods. Most importantly, large numbers of potential victims can be trapped by corrupting a single server rather than luring victims through emails or infecting client devices with malware.

Another potential problem with DNS is the use of wildcards in DNS entries. Originally intended to manage mistyped URLs, wildcards have been exploited to lure victims to bogus Web sites.

 The case of a DNS wildcard phishing scam against Barclay's bank in the UK is described in *InformationWeek* "Phishers Turn to DNS Wildcards, Cache Poisoning" at <http://informationweek.com/story/showArticle.jhtml?articleID=60407745>.

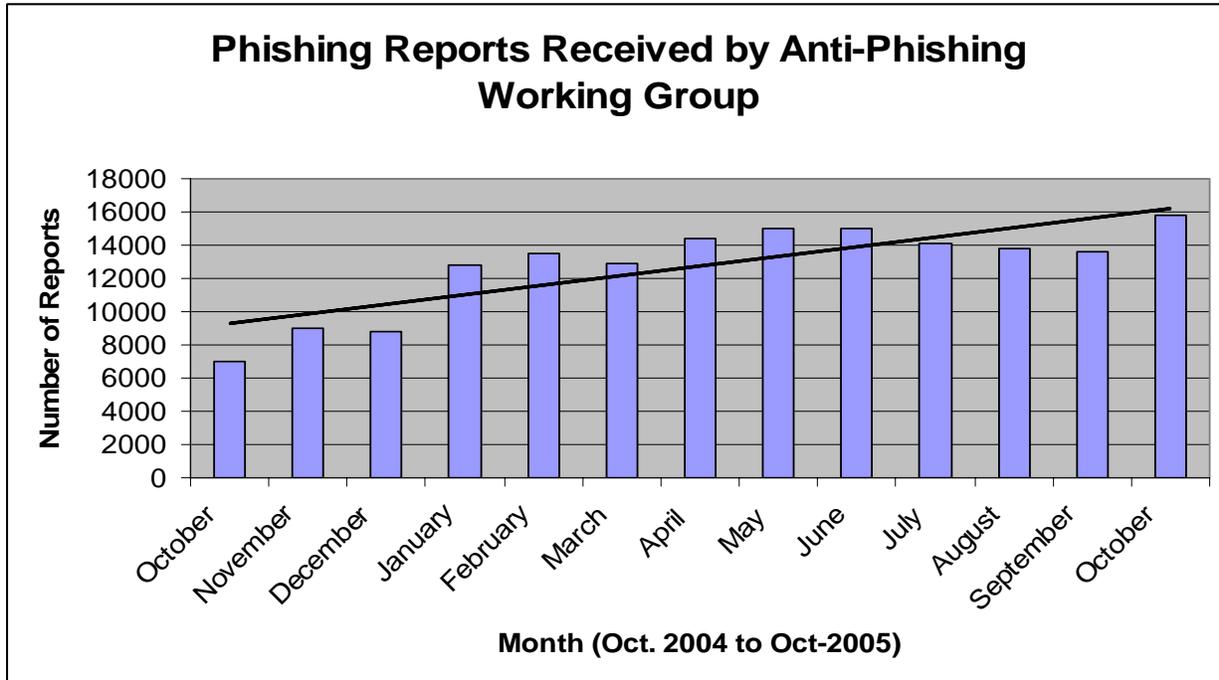
Both DNS poisoning and wildcard vulnerabilities stem from the underlying trust assumed in the DNS protocol. A new protocol, DNS Security Extension (DNSSEC), uses digital certificates to authenticate parties involved in the exchange of DNS information. However, servers that do not use this protocol are still vulnerable to some DNS poisoning attacks. Some DNS servers, such as Berkeley Internet Name Domain (BIND), have added countermeasures that operate with the DNS protocol, such as ignoring messages unrelated to a query.

 For more information about DNSSEC, see <http://www.dnssec.net/>. For details about BIND security, see <http://www.isc.org/index.pl?sw/bind/>.

There are limits to social engineering and malware-based attacks and network attacks, such as DNS poisoning, are additional tools for the phisher. These attacks also demonstrate the overlap in techniques used by virus writers, spammers, phishers, and cyber criminals. Regardless of the technique, the objectives of phishers are the same: collect personal and confidential information that can be used for identity theft and financial gain.

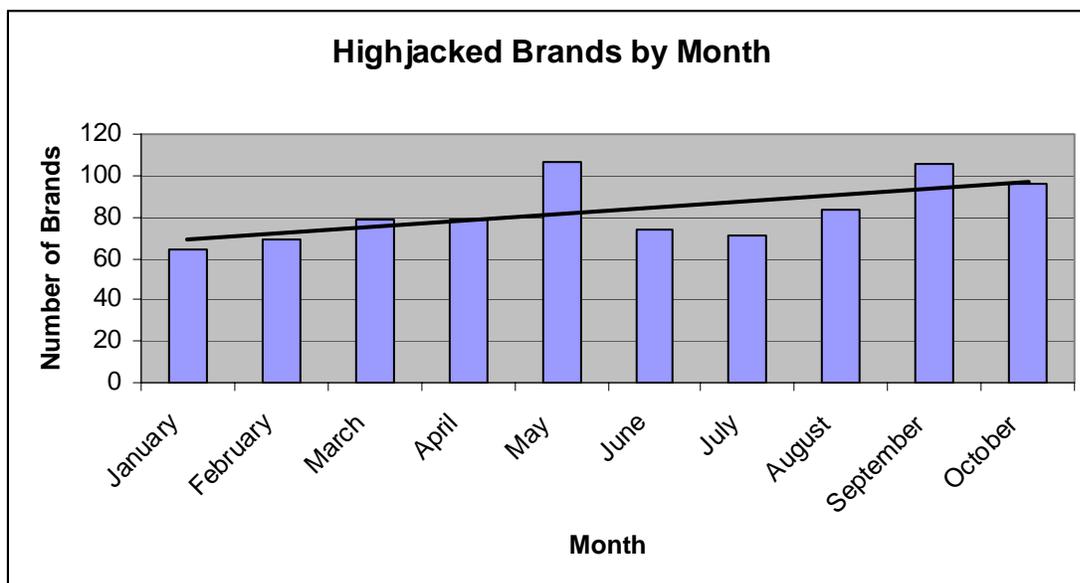
## Economics of Phishing and Identity Theft

The economics of phishing and identity theft can be considered from the perspective of both the perpetrator and the victim. The economic benefit of phishing to the perpetrators is apparent from recent trends in the number of phishing attacks. Figure 5.8 provides recent statistics about phishing attacks. Like spamming, phishing attacks are low-cost endeavors, so even extremely low response rates can make the effort worth the expense.



**Figure 5.8:** The number of distinct phishing reports received by the Anti-Phishing Working Group shows a trend upwards (Source: Phishing Activities Trend Report, October 2005, [http://antiphishing.org/apwg\\_phishing\\_activity\\_report\\_oct\\_05.pdf](http://antiphishing.org/apwg_phishing_activity_report_oct_05.pdf)).

Another measure of phishing activity is the number of brands that are highjacked per month (see Figure 5.9). Although useful, this measure may be under reported. Analysts have noted a trend to target smaller businesses and to distribute smaller numbers of emails. This phishing method is known as spear phishing. The likely objective is to “fly under the radar” and remain undetected. There is no way of measuring the success of those attempts.



**Figure 5.9:** Tracking the number of highjacked brands is another measure of phishing activity.

In addition to those creating and launching the attacks, there are attackers who earn money renting their botnets for attacks. Attackers earn income by launching DDoS attacks. According to *New Scientist*, attackers with control of botnets are charging between \$500 and \$1500 per attack or \$1 to \$40 per bot for a smaller network (Source: Celeste Bieber “How Zombie Networks Fuel Cybercrime” at <http://www.newscientist.com/article.ns?id=dn6616>).

The cost to individuals and businesses is difficult to calculate, and the estimates vary widely. One reported estimate from *The Industry Standard* puts the cost of phishing as high as \$1.2 billion dollars; others estimate it to be as low as \$137 million.

 For more information about the estimate of phishing costs, see Linda Rosencrance “TECF Aims to Fight Online Fraud” at <http://www.thestandard.com/article.php?story=20040617173836939> and Greg Goth’s “Phishing Attacks Rising but Dollar Losses Down” at <http://csdl2.computer.org/comp/mags/sp/2005/01/j1008.pdf>.

### **Impact on Consumers**

Those that are victims of phishing attacks risk identity theft and theft of funds. In addition, recovering from identity theft can take years. According to one study by the Identity Theft Resource Center (ITRC), victims spent on average 600 hours over a period of years recovering. The same study found that victims continue to deal with the effects of identity theft even after the initial recovery period. The impacts include:

- Increased insurance or credit card fees
- Inability to find a job
- Need to pay higher interest rates
- Difficulties with collection agencies

Although difficult to estimate, the study concluded that businesses lose between \$40,000 and \$92,000 per stolen identity.

 These and other statistics on identity theft are available at <http://www.idtheftcenter.org/facts.shtml>.

Phishing and identity theft are just two forms of fraud that businesses have to address. Citing research from Gartner, the Bank Administration Institute (BAI) reports both an increase in identity theft and a shift in the tactics of phishers:

- Rather than focusing on widely recognized, large financial institutions such as Bank of America, phishers are targeting smaller community banks.
- Thieves are using business accounts, rather than consumer accounts, because screening for the former accounts is not as effective as consumer account screening.
- Organized crime is finding identity theft a lucrative and less risky operation than some traditional areas of organized crime.

 The source of for these points is Clint Swift and Karen Epper Hoffman “Fraud Looms Large” at BAI Online at <http://www.bai.org/bankingstrategies/2004-jul-aug/fraud/>.

The impacts extend beyond the cost of losses due to fraud and the expense of countermeasures deployed by businesses and individuals. Fear of phishing will likely curtail the use of online services to the detriment of both the consumer and businesses. Consumers lose flexibility while businesses will incur higher costs as those services shift to higher cost operations such as call centers.

## **Phishing and Identity Theft Countermeasures**

Countermeasures are available to both businesses and individuals to help minimize the problems of phishing and identity theft.

### ***Business Countermeasures***

Businesses can implement a number of countermeasures to the threats of phishing, both to prevent the use of their business identity in a phishing scam and to prevent their information infrastructure from being used by phishers.

In the first case, business logos and Web copy are used to trick individuals into believing a bogus site is actually associated with a legitimate institution. Phishers use a number of tricks, including linking to images and linking to parts of the legitimate site, such as a help or FAQ page. Systems administrators should monitor network traffic for suspicious activity. For example, a business could identify a phishing attack in progress if it detects a spike in traffic to download a particular JPEG.

In other cases, desktops and servers within an organization's network could be compromised and become part of a botnet. Regular use of desktop antivirus and inbound content filtering at the gateway can minimize the likelihood of this occurrence. If a machine were compromised, content filtering on outbound traffic and firewalls could detect and block suspicious activity, such as communications with an IRC chat room. Fortunately, the countermeasures in place for antivirus, anti-spam, and content filtering are capable of countering many of the tasks involved in phishing attacks.

## Consumer Countermeasures

The first step individuals should take is to become better educated about identity theft, phishing, and related threats to online business. The United States Federal Trade Commission (FTC) provides the following advice to consumers:

- Do not reply to pop-up ads that ask for personal information or click through on links in pop-up ads.
- Use antivirus software and personal firewalls to prevent malware infections and to control communications between a PC and a phisher's system.
- Do not use email to transmit financial information.
- Review credit card and bank statements for suspicious charges.
- Exercise caution when opening email attachments, regardless of the sender.
- Report phishing scams to the FTC at [spam@uce.gov](mailto:spam@uce.gov) and to the business or organization presented in the phishing email.
- Victims of identity theft should file a complaint with the FTC at <http://www.consumer.gov/idtheft>.



Individuals should also understand their online agreements with financial service providers—not all accounts are insured against fraud. For example, funds lost due to bank fraud against a personal checking account are generally restored by the bank. The regulations that protect consumer accounts do not necessarily apply to business accounts. Similarly, investment accounts and their financial instruments may not be insured and the investor may bear the risk of cyber crime. See some relevant examples at [http://www.usatoday.com/money/industries/technology/2005-11-02-cybercrime-online-accounts\\_x.htm](http://www.usatoday.com/money/industries/technology/2005-11-02-cybercrime-online-accounts_x.htm).

## Summary

Phishing and identity theft are one of several threats to online commerce. Confidence schemes are not new, and banks have had to deal with fraud for as long as they have existed. The mechanics of these criminal activities is changing and requires new methods to address them.

Phishers are resorting to a combination of traditional social engineering techniques coupled with mass emails to reach a wide audience. As users become more aware of the phishing problem and educated about social engineering techniques, phishers have become more resourceful. They now use malware and botnets, similar to those used by attackers and spammers, to lure victims and collect account and password information without user interaction. More sophisticated social engineering techniques, such as context-aware phishing, and more stealthy operations, such as spear phishing, make these activities more difficult to detect.

Countermeasures are available to reduce the threat of phishing. Many of the information security measures already deployed in organizations—such as antivirus software, firewalls, and content filtering—are readily leveraged to combat phishing attacks and the potential use of an organization's systems in phishing scams. The driver behind phishing of course is economic gain. The low cost of launching phishing attacks, the relative low risk, at least when compared with other crimes, and the high returns imply this problem will not be fading away.

## Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.