CHAPTER

6

Helping Your Organization Avoid Phishing

As you discovered in Chapter 5, it may be impossible to stop phishing completely. But your organization can take some concrete steps to limit the number of attacks and the damage caused by those attacks. Your organization should focus on improving two areas:

- How the organization interacts and communicates with its customers, including how it handles email communications and presents itself on the web
- The organization's methods for keeping the bad guys out and preventing the phishers from getting to its money

This chapter follows these two tracks and makes some recommendations that might, in the end, save your organization's bacon. First, you take a look at how your organization can improve email policies and some email authentication schemes. Then I show you how your company can make your website less of a breeding ground for parasites.

Next, on the client side, I help you try out some of the latest methods for hardening the walls of your fortress. This chapter concludes with some ways that you can proactively protect your company's assets.

Interacting with Customers

Not surprisingly, the first line of defense in the phish fight is the customer. Creating easily understandable standards for customer communications can go a long way in preventing a phishing attack, and recovering quickly from one.

Email

Email is currently the largest attack vector for phishing malware and ID theft exploits. This may change, as websites increasingly begin to employ advanced scripting techniques and automated functions; but email is still the hands-down winner.

You can take a number of steps to protect your business from fraudulent email, including the following:

- Standardizing your communications with the customer
- Implementing email authentication

The following sections discuss these topics in more detail.

Standard Customer Communication Policy

Even if you're not a financial institution, as an ISP or Internet company you should have a customer email policy. *Policy* is one of those terms that can mean several things. For example, there are security policies on firewalls, which refer to the access control and routing list information. Standards, procedures, and guidelines are also referred to as policies in the larger sense of a global information security policy. For example, a policy can provide protection from liability due to an employee's actions, or it can control access to trade secrets.

Companies need many types of policies, standards, guidelines, and procedures. But what I'm talking about here is creating a standard for emails from the company to the customer, which doesn't use the types of phish hooks you see in a phishing email. A standard customer communications policy should convey a consistent message and not confuse your customer.

Here are some basic customer email policy standards:

- Don't send email in HTML format.
- Don't send attachments.
- Don't include or ask for personal information.
- Use the full name of the user.

- Don't include hyperlinks.
- Use localized messages.

Read on to find out more about these individual standards.

Don't Require HTML Email

To be fair, HTML email has great advantages and great features. It's much more visually satisfying to receive HTML-formatted email versus plaintext email. In addition to graphics, HTML email sometimes has embedded links, animation, sound, and music. The advanced features of HTML mail are increasingly used in mass-marketing campaigns to grab readers' attention. But there's one really big drawback: HTML email is a security threat.

In email correspondence to your customers, don't use HTML; use plaintext-formatted email instead. As you now know, HTML code unleashes a whole raft of available exploits. Your company's email policy should explicitly recommend that plaintext be used in all correspondence with customers. Granted, this may make the email unreadable if the customer has an HTML-only reader configuration. But by making it company policy to send only plaintext email, your organization is taking a solid first step in helping customers learn how to protect themselves.

If the appearance of your message is important, save it as an .rtf or a .pdf document and post it to your website.

Don't Send Attachments

Legitimate emailers don't include attachments, so this is an obvious red flag for the recipient. Try not to send attachments if you don't have to.

Discourage Personal Information

Customers need to know that a real business will never ask them to reply to an email with their date of birth, credit card data, password, or other personal data. If the email provides a link to a website to supply the information, the customer should know not to click it.

You can post a message on your website instructing customers not to submit emails that contain sensitive or confidential information and not to use email for specific transaction-related requests. An email auto-responder is also useful. It can respond to all email submitted, thank the sender for the message, acknowledge that it was received, and reiterate your policy about customers not sending confidential or sensitive information.

Use the Customer's Full Name

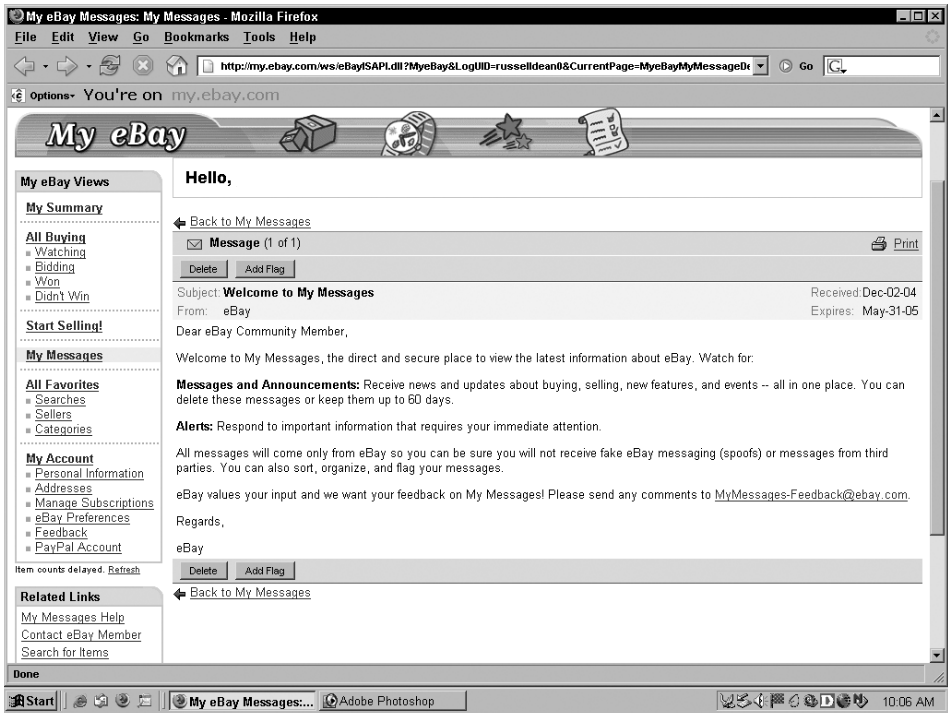
Several companies, such as Citibank and PayPal, have a policy of using the customer's full name in all communication. This is helpful because it's much harder to create spamming routines with the user's full name as opposed to the email or screen name. Only the financial institution should have the full name in its database. But because of the overhead added to marketing mailings that include the customer's full name, it's easier and cheaper to just reply to the email name. So some companies resist the full name policy.

Don't Use Hot Links

Obviously, if you use only plaintext email, it prevents the customer from easily clicking an embedded link. This is a good thing. PayPal, for example, just directs the customer to what links to click.

Use Localized Messages

eBay is trying out a new concept, My Messages. Essentially, this keeps private user communication on the eBay website, not via conventional email. Intended to make it easier to distinguish official eBay announcements from fraudulent emails, it offers a read-only inbox for logged-in users that contains the user's private trading and account information. Users can delete messages or they will be automatically deleted after 60 days. Figure 6-1 shows the new eBay My Messages area.



Hello,

Subject: **Welcome to My Messages**
Received: Dec-02-04
From: eBay
Expires: May-31-05

Dear eBay Community Member,

Welcome to My Messages, the direct and secure place to view the latest information about eBay. Watch for:

Messages and Announcements: Receive news and updates about buying, selling, new features, and events -- all in one place. You can delete these messages or keep them up to 60 days.

Alerts: Respond to important information that requires your immediate attention.

All messages will come only from eBay so you can be sure you will not receive fake eBay messaging (spoofs) or messages from third parties. You can also sort, organize, and flag your messages.

eBay values your input and we want your feedback on My Messages! Please send any comments to MyMessages-Feedback@ebay.com.

Regards,

eBay

Figure 6-1 eBay's My Messages.

This process of using private communication with the user might be a partial solution for other online firms concerned about phishing attacks. But one potential issue is that this solution could be quite labor intensive for a large user base. And it could be a bit tedious for users who are used to getting all messages delivered to them. If users participated in several services with a system similar to My Messages, they would have to log into each service, click the My Messages (or whatever) section, and get messages from there instead of being able to simply check their email for messages from all services. In addition, some users might still be duped into visiting bogus message portals, so warnings are still necessary.

Email Authentication Systems

Email authentication systems may provide an effective means of stopping email and IP spoofing. Email spoofing is probably one of the biggest current web security challenges. Without authentication, verification, and traceability, users can never know for certain if a message is legitimate or forged. Email administrators continually have to make educated guesses on behalf of their users on what to deliver, what to block, and what to quarantine.

The three main contenders for authentication are Sender Policy Framework (SPF), SenderID, and DomainKeys. APWG estimates that adopting a two-step email authentication standard (say, using both SPF and DomainKeys) could stop 85% of phishing attacks in their current form. Although all three systems rely on changes being made to DNS, they differ in the specific part of the email that each tests:

- **SPF:** Checks the "envelope sender" of an email message—the domain name of the initiating SMTP server.
- **SenderID:** Checks after the message data is transmitted and examines several sender-related fields in the header of an email message to identify the "purported responsible address."
- **DomainKeys:** Checks a header containing a digital signature of the message. It verifies the domain of each email sender as well as the integrity of the message.
- **Cisco Identified Internet Mail**: Adds two headers to the RFC 2822 message format to confirm the authenticity of the sender's address.

You should start preparing for email authentication. All email will eventually have to comply with some type of sender verification methods if you want it to get through. Successful deployment of email authentication will probably be achieved in stages, incorporating multiple approaches and technologies. The following sections discuss these three approaches in greater detail.

SOME SPAMMERS LOVE SPF

Although legitimate emailers are starting to quickly adopt SPF, apparently spammers are adopting it faster. A recent study by CipherTrust (www.ciphertrust.com) showed that 34% more spam is bypassing SPF checks than legitimate email. This means that a spam message is three times more likely to pass an SPF check than to fail it, as long as the address is registered. As long as spammers comply with the protocol, register their SPF records, and don't spoof the sender address, their messages will not be stopped. What this really means is that one email authentication solution alone will not stop the tide of spam; it's just one part of a fraud and spam prevention program.

The Sender Policy Framework

The Sender Policy Framework (SPF), formerly Sender Permitted From, is an extension to the older mail sending protocol, Simple Mail Transfer Protocol (SMTP), which provided almost no sender verification of email. SPF makes it easy to counter most forged "From" addresses in email, thus helping to counter email source address spoofing.

When a user sends you mail, an email server connects to your email server. When the message comes in, your email servers can, based on SPF published addresses of its email servers, tell if the server on the other end of the connection actually belongs to the sender.

AOL is a big supporter and deployer of SPF. It recently pulled out of development of Sender ID, another mail verification protocol. SPF is deployed around the world; the email servers of more than 86,000 domains use the authentication technology, as of this writing.

SPF is not an IETF standard yet, but it has a good chance of becoming a standard, and will be submitted soon. SPF is not expected to totally eliminate spam, but it's another weapon in the fight against spam and phishing.

Sender ID and the Death of MARID

Sender ID provides another authentication method. Microsoft began implementing SenderID to protect mailboxes at Hotmail and MSN. Sender ID is a proposed specification developed within the MARID IETF Working Group between May and October 2004. Sender ID works by looking at information both in the "envelope" of the email message and in the message itself.

Thought of as SPF + Caller ID, Sender ID compares that information with data published by domain owners in the Domain Name System (DNS), to confirm that the email actually came from the domain that it appears to be from.

For example, recipients could be sure an email from fred@yahoo.com was actually from someone at the yahoo.com domain. Sender ID consists of two parts: the SPF Classic plus PRA, allowing mail recipients to perform two kinds of checks.

Unfortunately, several major issues arose during the operation of the Sender ID working group, MTA Authentication for DNS (MARID), which led to its demise. Technical questions arose as to whether Sender ID would work as specified. Most of these questions were rooted in the basic differences between path authentication and message authentication and remain unresolved.

Microsoft also filed for patents on parts of Sender ID, making the developer community unhappy about the strict licensing and ownership control Microsoft exerted, such as requiring Sender ID implementers to sign a license agreement to protect undisclosed and unspecified patents. Although the actual patent application was eventually published toward the end of the life of MARID, it came too late.

Another factor in MARID's demise was that eager technology reporters frequently reported email authentication as the final cure for spam. This created great expectations for email authentication, which were dashed once the hard truth settled in that email authentication did not stop spam.

As a result, any useful work of the MARID group slowed to a crawl with the IETF eventually shutting down the group. Recently AOL has withdrawn its support and is falling back on Sender Policy Framework (SPF). Evidently AOL has technical concerns that Sender ID may not be fully backwardly compatible with the original SPF specification.

Domain Keys to the Kingdom

In 2004, Yahoo! started signing all its outgoing email with DomainKeys headers, and EarthLink is testing DomainKeys prior to deployment. DomainKeys is a Yahoo!-proposed system for verifying the domain of an email sender. DomainKeys prevents forged emails from claiming to be from a domain it's not.

DomainKeys is an attempt to give email providers a mechanism for verifying both the domain of the email sender and the integrity of the messages sent. Once the domain can be verified, it can be compared to the domain used by the sender in the From: field of the message, to detect forgeries.

DomainKeys uses public key encryption technology at the domain level to verify the sender of email messages. If it's a forgery, it can be dropped without impact to the user. If it's valid, the domain is known, so a persistent reputation profile can be established for that sending domain that can be tied into antispam policy systems, shared between service providers, and even exposed to the user.

Sending Domain-key email: DomainKeys begins by performing a secure hash of the contents of a mail message using the SHA-1 algorithm, encrypting the result using a private key with the RSA algorithm and then encoding the encrypted data using Base 64.

The resulting string is then added to the email as the first SMTP header field with the key *Domain-keys:*, thereby adding a digital signature to the email. It doesn't encrypt the actual message; it just adds a digital signature to the header.

ASYMMETRIC (PUBLIC) KEY ENCRYPTION

Asymmetric (public) key encryption is a cryptographic system that employs two keys: a public key and a private key. The public key is made available to anyone wishing to send an encrypted message to an individual holding the corresponding private key of the public/private key pair. Any message encrypted with one of these keys can be decrypted with the other. The private key is always kept private. It should not be possible to derive the private key from the public key.

The sending process is as follows:

1. **Setup:** The owner of the email-sending domain first generates a public/private key pair to digitally sign all outbound email. The private key is distributed to outbound email servers and the public key is made available.
2. **Signing:** After an email is created, the server uses the stored private key to generate the digital signature, which is attached as an email header and sent.

Receiving Domain-key email: The receiving server uses the name of the domain from which the mail originated to perform a DNS lookup, getting that domain's public key. The receiver then decrypts the hash value in the header field and recalculates the hash value for the mail body that was received. If the two values match, this proves to a very high degree of confidence that the mail did in fact originate at the purported domain and has not been tampered with in transit.

One advantage of using DomainKeys is that it doesn't require the cumbersome signing of the public key by a certificate authority (CA). DomainKeys allows for multiple public keys to be published in DNS at the same time, thereby allowing companies to use different key pairs for the various mail servers they run. It's also easy to revoke, replace, or expire keys at a company's convenience, permitting the domain owner to revoke a public key and shift to a new key pair at any time.

Yahoo hopes that DomainKeys will help stop spam by

- Allowing receiving companies to drop or quarantine unsigned email that comes from domains known to always sign their emails with DomainKeys.
- Allowing email service providers to begin to build reputation databases that can be shared with the community and applied to spam policy.
- Allowing server-level traceability by eliminating forged From: addresses.

- Allowing abusive domain owners to be tracked more easily. Spammers will be forced to only spam companies that aren't using verification solutions.

The absence of a verifiable digital signature header in an email claiming to be from a domain that has a DomainKeys DNS record is likely to be seen as proof that the email is a forgery.

DomainKeys is expected to help fight phishing by positively identifying the email's originating domain and identifying forged emails more quickly. In addition, the DomainKeys domain owner may realize a big reduction in email abuse complaints. DomainKeys has been designed to be compatible with most of the proposed extensions to email.

The following issues may crop up with DomainKeys, however:

- **Spoofing:** If the key-pair authentication is somehow spoofed, the email easily bypasses the filters. A second level of filtering is still required.
- **Forwarding:** Mail is often forwarded by various servers outside the control of the sending party. If the message is modified by a server in transit, the digital signature will no longer be valid and the email will be rejected.
- **Overhead:** Older, slower mail servers may have a problem with the computational overhead added by generating the cryptographic checksums. This really isn't much of a problem, though, because it's probably only around 10%.

Cisco Identified Internet Mail

Designed to help identify fraudulent email, Cisco Identified Internet Mail (IIM) is the proposed Cisco Systems signature-based email authentication standard. Implementing IIM makes the sending domain more accountable for email originating from its domain and limits the ability of spammers and malware distributors to forge return addresses or disguise the identity of infected systems.

To establish the authenticity of an email message, IIM verifies that the message sender is authorized to send messages using a given email address and that the original message was not altered in any consequential manner. IIM adds two headers to the message format: IIM-Signature and IIM-Verification. It also applies user-defined policies depending on the outcome of the message verification process.

Web

Adopt website policies to make it harder for phishers. Don't require advanced scripting for your site. Create simple coding standards that may make the look and feel of the site basic, but allow your customers to protect themselves. Users actually prefer sites that use base-level code, and just as important, search engines prefer such sites. Create content that consists of standard HTML that can be read by any browser.

Here are some examples of website policies that can help to thwart phishing attacks:

- Allow customers to turn scripting off in their browsers.
- Don't save passwords by setting autocomplete="off".
- Don't use IE-specific coding.
- Allow users of different operating systems access to all features of the site

Sites that adopt this strategy can devote more effort to content rather than form, which further enhances the site's appeal. It should not come as a surprise that such sites often rate well.

JavaScript

There is a growing movement to limit the use of JavaScript (also sometimes referred to as ECMAscript and JScript) coding on websites. One reason for this is to ensure that your site is accessible to browsers that do not implement JavaScript or have JavaScript turned off for security reasons. True, JavaScript can do some things that you can't do with normal HTML, but I think the problems may outweigh the benefits. The following sections discuss several problems with allowing JavaScript coding on your website.

JavaScript Has Security Holes

JavaScript has a long history of exploitable security holes. It has exploited email by embedding a few lines of JavaScript code in an email message. The code can forward a reply to an email message to a foreign website for later review.

JavaScript can be used to violate a browser and operating system without violating the browser security policies. It does this by executing a simple piece of code—an infinite loop—that eats up memory or other resources quickly and crashes the browser or the operating system itself.

An *infinite loop* is a programming routine whose exit condition is never fulfilled. A script can create an infinite looping state, which has the effect of freezing the browser and requiring a reboot. Infinite loops are often unstoppable.

JavaScript can stump the browser in other ways, too. It is able to open up an endless series of dialog boxes or create an infinite amount of page fetches. This prevents any user action because the browser is too busy to perform other tasks.

JavaScript Behaves Differently from Browser to Browser

Even in browsers that support JavaScript, it behaves differently depending on the browser. Only the simplest JavaScript will work on most browsers. Text-only browsers, such as Lynx, for disabled users don't support JavaScript. Web phones and many new Internet appliances also don't support JavaScript.

Extra Programming Effort Required

If you code client-side data validation in JavaScript (and you'd better, because any cracker can reverse-engineer your plaintext JavaScript code), you still need to duplicate the coding for your web server. Then you have to synchronize that duplicate code on all web servers.

JavaScript Cookies

Although this is not specifically a JavaScript issue, since much JavaScript code drops cookies, it's important to remember that cookies can be persistent. Users with older OSs are at a security risk if the cookies store login names and/or passwords for periods longer than the session. Nonpersistent session cookies are a better idea, and newer browsers can distinguish between persistent and session cookies.

One last point: Using a lot of JavaScript can cut down on traffic to your site. If you're a site that wants hits, requiring JavaScript makes the site off-limits to anyone who disables it, thus cutting down on eyeballs.

Cross-Site Scripting Flaws

Cross-site scripting (XSS) flaws are used to send malicious code from an apparently trusted source. This exploit begins when an attacker alters a web application to send malicious script. The target's browser will execute the script because it thinks the script came from a trusted source and has no way to know that it did not.

XSS attacks usually come in the form of embedded JavaScript; however, any embedded active content is a potential source of danger, including ActiveX, VBScript, and Flash.

The XSS flaw exploit can cause serious problems, including accessing the user's session cookie, thereby allowing an attacker to hijack the session and take over the account. It can also install malware, redirect the browser, and disclose sensitive information.

User-Agent Strings

When Internet users visit a website, a text string, called a *user-agent string*, is generally sent to identify the user agent to the server. This test string typically includes information such as the host operating system, application name, the version, and the language used.

One way to control security of how the web page is viewed is through the use of the agent strings. Identification of these strings is useful for determining if the user surfing the site is using an upgraded or up-to-date version of the browser. Using an upgraded version of the browser helps cut down greatly on the possibility that the site could be phished from a violated browser. If the agent string identifies a browser that is too far out of date, the site should prevent the connection and send the user to the update site

The practice of identifying these agent strings is also called *browser sniffing*. Browser sniffing can identify the browser used to access the website and any plugins installed, and is useful if you need to gather data about market share and Internet trends.

Here are some examples of browser user-agent strings:

- **Internet Explorer 5.5 on Windows 2000:** Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
- **Internet Explorer 6.0 in MSN on Windows 98:** Mozilla /4.0 (compatible; MSIE 6.0; MSN 2.5; Windows 98)
- **Konqueror 3.1 (French):** Mozilla/5.0 (compatible; Konqueror/3.1; Linux 2.4.22-10mdk; X11; i686; fr, fr_FR)
- **Mozilla 1.6 on Linux:** Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.6) Gecko/20040113
- **Mozilla Firefox 1.0 on Windows XP:** Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20041107 Firefox/1.0
- **Netscape 4.8 on Windows XP:** Mozilla/4.8 [en] (Windows NT 5.0; U)
- **Netscape 7 on Sun Solaris 8:** Mozilla/5.0 (X11; U; SunOS sun4u; en-US; rv:1.0.1) Gecko/20020920 Netscape/7.0
- **Opera 6.03 on Windows 2000, cloaked as MSIE:** Mozilla/4.0 (compatible; MSIE 5.0; Windows 2000) Opera 6.03 [en]
- **Opera 7.23 on Windows 98:** Opera/7.23 (Windows 98; U) [en]
- **Opera 8.00 on Windows XP:** Opera/8.00 (Windows NT 5.1; U; en)
- **Safari v125 on Mac OS X:** Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/124 (KHTML, like Gecko) Safari/125

You can find a more complete list of User Agent Strings at www.pgts.com.au/pgtsj/pgtsj0208c.html.

Browser sniffing has some of the following problems:

- Increased maintenance because of the need to constantly update the string code and create branching routines for all browsers. This could be considerable.

- Some backlash, not unrelated to an early decision by Microsoft (later abandoned) to limit access to MSN to IE surfers only.
- Some users may feel they're being discriminated against if they don't have the latest and greatest browser or if the site shuts out minor browsers inadvertently.
- Many minor browsers allow users to change the user-agent information to make these sites think they are a more popular browser. In fact, even browsers like Internet Explorer allow you to change the user-agent header if you are willing to modify the registry.
- Unreliability is a problem because many browsers allow users to set their own agent strings. The agent string can be set to "I'm not tellin'" or some four-letter word.

Client-Side Solutions

In addition to the polices and standards I mentioned in the preceding section, there are methods you can implement to ensure that your customers aren't inundating you with spam and malware. This section looks at various ways your company can authenticate the user and his transaction.

Authentication

Identification and authentication are the keystones of successful access control systems. *Identification* is the act of a user professing an identity to a system, usually in the form of a logon ID to the system. Identification establishes user accountability for the actions on the system.

Authentication is verification that the user's claimed identity is valid, and it is usually implemented through a user password at logon time. Authentication is based on the following three factor types:

- **Type 1:** Something you know, such as a personal identification number (PIN) or password
- **Type 2:** Something you have, such as an ATM card or smart card
- **Type 3:** Something you are (physically), such as a fingerprint or retina scan

Two-Factor Authentication

Two-factor authentication refers to the act of requiring two of the three factors to be used in the authentication process. For example, withdrawing funds from an ATM machine requires a two-factor authentication in the form of the ATM card (something you have) and a PIN number (something you know).

Tokens in the form of credit card–sized memory cards or smart cards, or those resembling small calculators, supply static and dynamic passwords. These types of tokens are examples of something you have. An ATM card is a memory card that stores your specific information. Smart cards provide even more capability by incorporating additional processing power on the card.

A smart card or access token is often part of a complete Enterprise Identity Management system, used to track the location of employees and manage secure access. A smart card can be coupled with an authentication token that generates a one-time or challenge-response password or PIN. Although two-factor (or dual-factor) authentication is most often used for logical access to network services, it can be combined with an intelligent card reader to provide extremely strong facility access control.

Several different types of authentication systems are in use; the following sections look at a few of them.

PassMark System

To guarantee that users are logging into a real financial website, not a bogus one, PassMark has created a system that shows a personalized image to the user during login. The image can be provided by the user during registration or chosen from the company's image library.

PassMark calls this 2 x 2 authentication: *two-way*, in that the user is authenticated to the site by a password and the site is authenticated to the user with the PassMark image, and *two-factor* because it uses two-factor authentication in the password and the image.

No special hardware or software needs to be installed on the user's computer, making the system very scaleable. In large organizations, users can be randomly assigned an image from a large pool, enabling them to be enrolled in large numbers.

Users can select a different image when changing their passwords. The PassMark system can also be used to authenticate company emails to the customer, in addition to the web login authentication.

One drawback may be the costs of the system. Software fees for the first 1 million customers are between 50 cents and 60 cents per customer per year. For small banks, however, the cost can be as high as $1 per client. Figure 6-2 shows how the customer initially registers her PassMark.

Figure 6-3 shows what the PassMark looks like to a customer logging into a financial site.

Cell Phone SMS Messaging

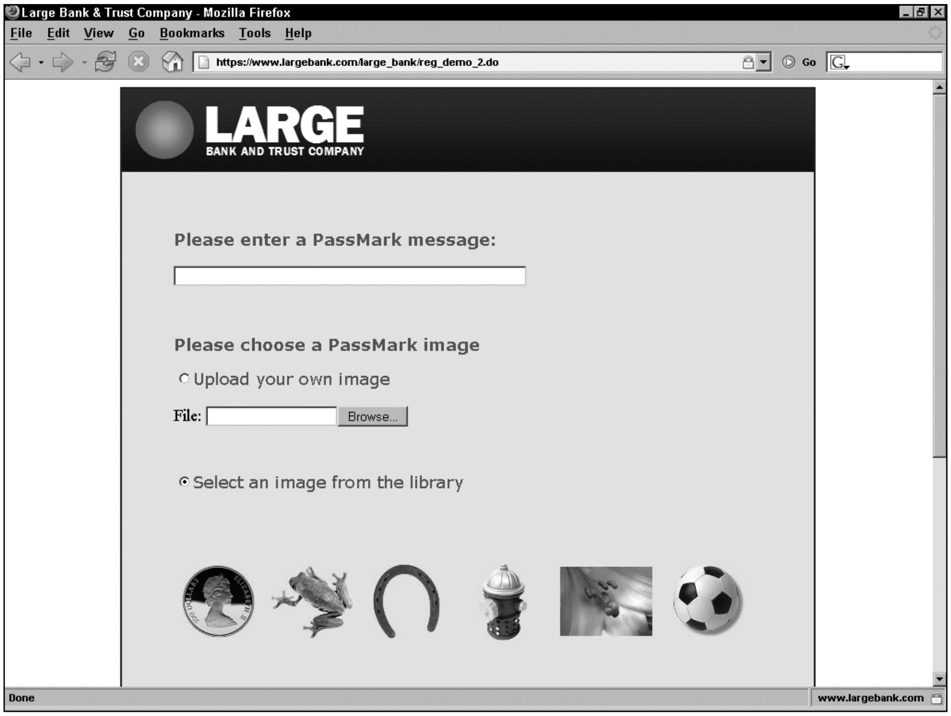
Two banks in New Zealand are experimenting with two-factor authentication with cell phones. The banks are implementing a system to help cut down on online fraud. Customers who want to remit more than $2500 into a third-party account via Internet banking receive an eight-digit text message to their cell phone. The customer must enter the text message into an online site within three minutes to complete the transaction.

It's more secure than a simple username and password because a cracker would also need the customer's cell phone to obtain the eight-digit code. As security technologist and author Bruce Schneier has pointed out (www.schneier.com/blog), the vulnerabilities lie in the area of intercepting the SMS text message or cloning the cell phone. It seems that it would be as easy to get the victim's cell phone number as to get their bank username and password.

It's probably not a viable option here, yet, however, as cell phone saturation isn't high enough yet to make this technique a standard.

Challenge/Response Secret Questions

One of the most common techniques used to reset passwords and verify that the user is authentic is the challenge/response use of secret questions. You know them: What is your mother's maiden name? Where were you born? What color are your eyes?


Large Bank & Trust Company - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://www.largebank.com/large_bank/reg_demo_2.do
Go
LARGE
BANK AND TRUST COMPANY
Done
www.largebank.com

Please enter a PassMark message:

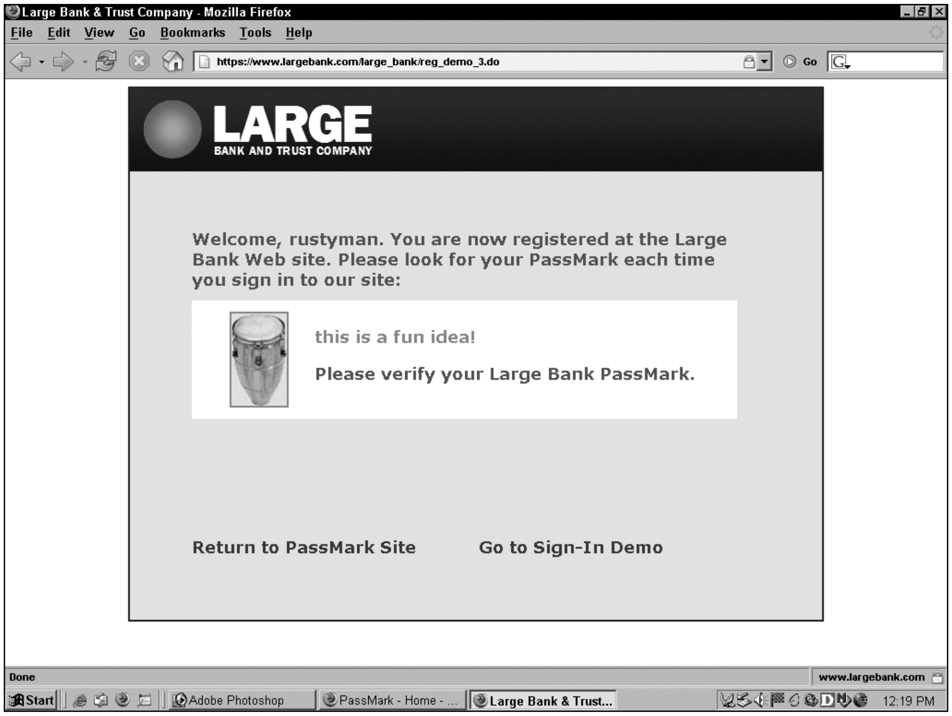
Please choose a PassMark image

○ Upload your own image

File: Browse...

● Select an image from the library

Figure 6-2 Registering an image with PassMark.



Welcome, rustyman. You are now registered at the Large Bank Web site. Please look for your PassMark each time you sign in to our site:

this is a fun idea!

Please verify your Large Bank PassMark.

Figure 6-3 Entering a PassMark-enabled site.

Because these questions aren't really that secure, especially if the cracker knows the victim, a better system provides the user with a way to define his own questions. In some cases, as many as five questions can be created.

Of course, you don't have to create the correct answer. That is, you can manufacture a different answer to your mother's maiden name question. You can make it something like *Edna Dinklehoffer of Clams Casino,* but be sure to remember it!

Challenge/response is also commonly used for spam blocking by sending a question back to the emailer to answer before the message is allowed through. You can find some of the pros and cons of the challenge/response technique for spam filtering at www.templetons.com/brad/spam/challengeresponse.html.

European Solutions

European companies spend a lot more on fraud prevention and seem to be able to reap the benefits much more than American companies. Perhaps they have the advantage of watching the Americans spend little and get hit with high rates of fraud to keep them on their toes. Several European security standards and implementation are worth looking into here.

Chip and Pin

Introduced in October 2003 in the UK, a point-of-sale (POS) hardware security solution to cut fraud called *chip and pin* uses a smart chip on credit or debit cards rather than using the standard magnetic strip. More than three-quarters of UK cardholders already hold one of the new chip and pin cards, with all UK cards expected to be switched to chip and pin by the end of 2005.

Instead of using a signature to verify payments, the buyer is asked to enter a four-digit personal identification number (PIN). Up to 130 million new chip and PIN cards will be sent out by the end of the year. At that point, retailers who haven't introduced the new scheme become liable for fraudulent transactions.

But there are fraud possibilities with the new cards. Security researchers have noted that crackers may be able to capture card and PIN data to create forged cards. They can make up forged cards and use them at cash machines. And once a cracker knows a PIN, he doesn't need to copy the chip. Because the same PIN is used for the chip and the magnetic strip, the cracker just needs to copy the magnetic strip and use the card in some ATMs that read only the strip.

In the past, card crooks have employed a variety of means such as pinhole cameras and card skimmers to get PINs from cards. In fact, what's happening to the new chip and pin cards is that the same old method of stealing the cards is it's biggest vulnerability right now.

UK bad guys are intercepting replacement cards in the mail in huge numbers, with London police alone disclosing that several people a day are reporting such thefts. One issue is that victims are often unaware that their bank has sent them a new card because their previous card remains valid.

In some instances, crooks managed to steal not just new chip and pin cards but the PIN number that goes with them, allowing crooks to empty accounts at ATMs.

Transactional Access Numbers

Transactional access numbers (TAN) are used to safely manage online transactions. Banks send TAN lists by mail in the form of a number list. These numbers can be used only once, as they are generated using a one-way hash algorithm, such as MD5. TANs are also used for phone transactions.

ONE-WAY HASH AND MD5

Also known as a *message digest,* a one-way hash function is a mathematical function designed to make it almost impossible to decrypt an encrypted message by reversing the cryptographic process, thus, the name *one-way*.

MD5 is an algorithm that was developed by Ronald Rivest in 1991. MD5 takes a message of an arbitrary length and generates a 128-bit message digest.

A common TAN list has 50 five-digit passwords, originally received by the user in an inactive state, along with an inactive smart card. Using the first password on the list activates that specific list, and the last password serves to trigger a new password list. The rest of the 48 passwords are used to confirm online transactions.

Five input errors will block access to the active list, which must be unblocked by a bank operator after security verification of the user. A list may be deleted if tampering is suspected either with the list or its delivery, or if the list is lost. The deleted lists obviously are unusable, as are used lists. The customer usually has a group of five lists at any one time, and only one list is active at any given time.

The administration of the TAN lists results in some serious overhead for both the bank issuer and customer. The bank has to generate the TAN lists and ensure their secure delivery. The customer must have the TAN list at hand during the transaction. TAN lists engender a pretty cumbersome process, so they are being replaced by HBCI in some areas.

HBCI

HBCI stands for Home Banking Computer Interface, a German banking authentication standard for online banking. There are several implemented versions of the standard, with the most recent version using a secret key generated by the bank for the customer. The key is stored either on a smart card or on a disk. It's not considered a complete security solution, but it is used with SSL and other components for transaction integrity and user authentication.

The HBCI-enabled bank produces two pairs of keys, one for integrity and one for nonrepudiation. Both MAC and RSA-based encryption procedures are supported. The client signs a letter confirming receipt of the key and promises to keep it secure.

The HBCI banking standard also comes in a PIN/TAN (Personal Identification Number/TransAction Number) incarnation, which is a PIN coupled with a TAN list. This is called HBCI+. But since one of the purposes of HBCI is to eliminate the input of TANs, the earlier version is more common.

Financial Transaction Services

One more German standard, developed in 2003, should be mentioned: FinTS (Financial Transaction Services). FinTS is a multibank signature card to help prevent fraud. FinTS is designed to be used online in a variety of electronic banking services by integrating the one-time password mechanism PIN/TAN into smart cards and magnetic media. FinTS is currently supported by more than 2000 German banks.

SecurID

SecurID is the granddaddy of hardware two-factor authentication. Having been acquired by RSA some time ago, it is being updated into a group of products—from time-synchronous tokens to smart cards—to aid in user authentication and secure access control. The product comes in either hardware (key fob, card and PINpad) formats, or software tokens for various platforms and Internet appliances.

The fundamental concept behind the RSA SecurID Authenticators lies in that each end user is assigned a token, which generates a new, unpredictable code every 60 seconds. The user then combines this number with a secret PIN to log in to protected resources. SecurID uses a symmetric key combined with an algorithm to generate each new time-based code. Only the authentication manager knows which number is valid at that moment in time for that user/authenticator combination.

i-STIK

Touted as an Internet safety tool for America's children, the i-STIK is a USB two-factor authentication token that can be carried on a key chain and used at school, at home, or in any computer with a USB port. The token is an attempt to eliminate the problem of child predators posing as other teens and children.

A collaboration between i-SAFE America and VeriSign, it's hoped that the Digital Credential Program, as it's called, will reduce the vulnerability of grade school students by giving each a unique digital identity as they surf.

The i-STIK permits young people to enter an age-appropriate chat room with confidence that everyone logged in will be who they say they are, by verifying a child's age and sex. School administrators will provide lists of students, with their dates of birth and sexes, and VeriSign will encode that information onto the i-Stick tokens.

Although the idea of token-based two-factor authentication has been around in the business world for some time (SecureID, for example), the idea that a hardware-based dongle device alone can protect young people from predators is a dangerous one.

The token verifies only the age and sex of the person to whom it was issued, not of the person using it. Anyone might be using it, and no doubt sex criminals will be scrambling to get their hands on one of their own, through loss, theft, or bribery.

Once the tokens become popular and widely available, one can expect a brisk trade in them on bulletin boards, and law enforcement will of course have to be supplied with plenty of them so that they can hang out in chatrooms to catch pedophiles.

Also, no teens will want to use these things. They are likely to hack them to make themselves appear older or simply throw them away. And the tokens will probably be abused by online marketing to children, trying to target them more precisely with advertising.

THE GUMMI BEAR CAPER

Although highly secure, a Japanese cryptographer named Tsutomu Matsumoto found he could fool fingerprint recognition devices four times out of five by using gelatine (such as Gummi Bears) and a plastic mold to create a fake finger. He also created some more advanced processes, using cyanoacrylate adhesive, PhotoShop, and a photosensitive printed-circuit board. Matsumoto tried these attacks against 11 commercial fingerprint biometric systems and was able to fool them about 80% of the time.

Biometrics

An alternative to using passwords for authentication in logical or technical access control is biometrics. Biometrics is based on the Type 3 authentication mechanism—something you are. *Biometrics* is defined as an automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics. In biometrics, identification is a one-to-many search of an individual's characteristics from a database of stored images. Authentication in biometrics is a one-to-one search to verify a claim to an identity made by a person.

Biometrics is used for identification in physical controls and for authentication in logical controls.

There are three main performance measures in biometrics:

- **False Rejection Rate (FRR) or Type I Error:** The percentage of valid subjects that are falsely rejected
- **False Acceptance Rate (FAR) or Type II Error:** The percentage of invalid subjects that are falsely accepted
- **Crossover Error Rate (CER):** The percent in which the FRR equals the FAR

Almost all types of detection permit a system's sensitivity to be increased or decreased during an inspection process. If the system's sensitivity is increased, as in an airport metal detector, the system becomes increasingly selective and has a higher FRR. Conversely, if the sensitivity is decreased, the FAR will increase. Thus, to have a valid measure of the system performance, the CER is used.

Toolbar Mania

Add-in toolbars for the browser is one of the most recent surfing developments. These toolbars plug into your browser and provide additional functions and features such as:

- Identification of spoofed sites
- Pop-up blocking
- eBay auction monitoring
- Security rating of the website you're viewing
- Enhanced web searching

Big companies such as Google, EarthLink, eBay, and Yahoo! have debuted toolbars, and so have smaller companies, such as CoreStreet. All feel they have specific features that can make them stand out in the crowd. Some are configured for only Internet Explorer, whereas others can be used with alternative browsers, such as Firefox.

SpoofStick

SpoofStick by Core Street (www.corestreet.com) is a simple browser extension that helps users detect spoofed websites. The 1.0 version of SpoofStick for Internet Explorer and Firefox can be downloaded at www.corestreet.com/spoofstick. SpoofStick makes it easier to spot a spoofed website by prominently displaying the real domain information.

For example, if you're on a legitimate URL, such as Yahoo!, SpoofStick will say: "You're on yahoo.com." If, for some reason, you access a spoofed website, say, www.yahoo.com@192.168.1.110/, SpoofStick will say: "You're on 192.168.1.110."

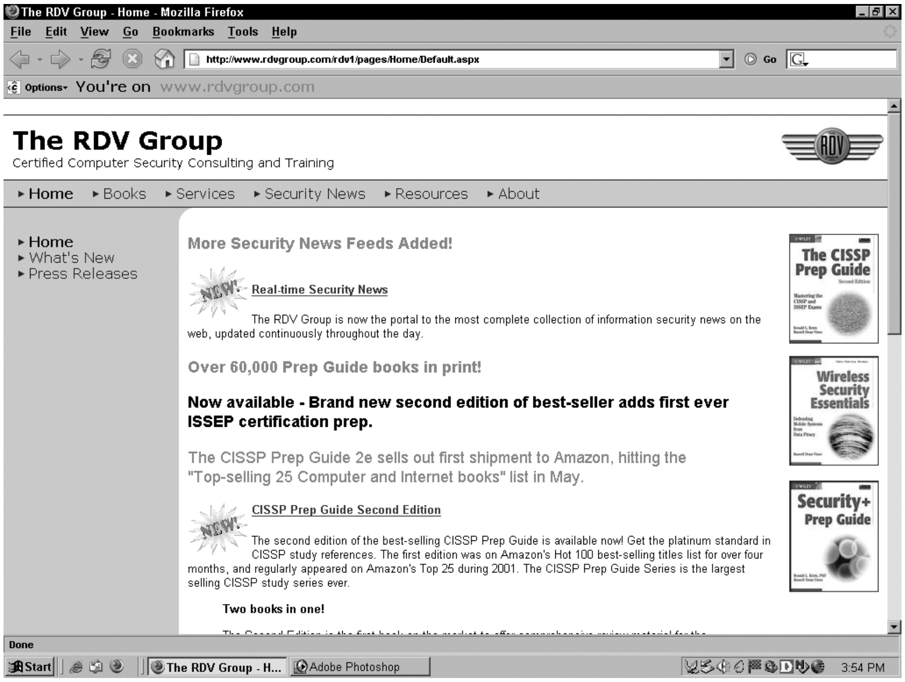
Figure 6-4 shows the SpoofStick toolbar as you surf a site.

Figure 6-5 shows the preferences you can set.

EarthLink Toolbar

Stung by criticism that, in its early days, it had very lax security and was a haven for malware distributors, EarthLink has intently focused on security as a marketing tool. Its free toolbar employs the ScamBlocker security feature. ScamBlocker displays a visual safety rating for each web page the surfer visits, offering real-time fraud analysis of the site. It alerts the user if the site has characteristics commonly associated with fraudulent websites. It will also alert you, if you click on a web page that appears on its list of known phishers. Figure 6-6 shows the toolbar installed just under the Address box.

Other useful features of the toolbar are a pop-up blocker tool, an integrated Google search box, and live news headlines. Figure 6-7 shows the site rating feature.


The RDV Group - Home - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.rdvgroup.com/rdv1/pages/Home/Default.aspx
Go
Options▾ You're on www.rdvgroup.com
Home Books Services Security News Resources About
Home
What's New
Press Releases
NEW!
The CISSP Prep Guide
Wireless Security Essentials
Security+ Prep Guide
Done
Start
The RDV Group - H...
Adobe Photoshop
3:54 PM

The RDV Group
Certified Computer Security Consulting and Training

More Security News Feeds Added!

Real-time Security News

The RDV Group is now the portal to the most complete collection of information security news on the web, updated continuously throughout the day.

Over 60,000 Prep Guide books in print!

Now available - Brand new second edition of best-seller adds first ever ISSEP certification prep.

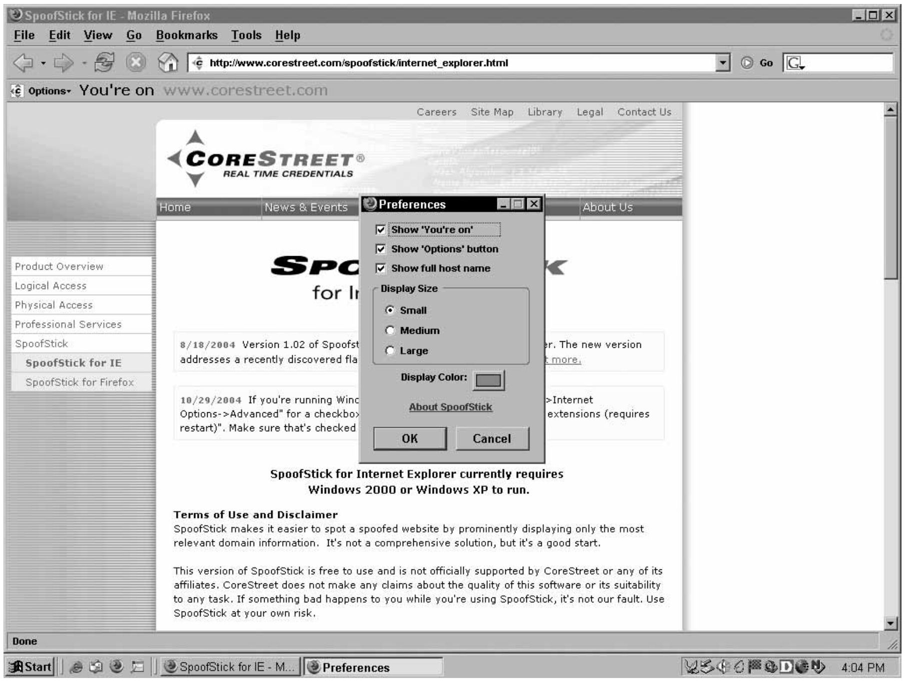
The CISSP Prep Guide 2e sells out first shipment to Amazon, hitting the "Top-selling 25 Computer and Internet books" list in May.

CISSP Prep Guide Second Edition

The second edition of the best-selling CISSP Prep Guide is available now! Get the platinum standard in CISSP study references. The first edition was on Amazon's Hot 100 best-selling titles list for over four months, and regularly appeared on Amazon's Top 25 during 2001. The CISSP Prep Guide Series is the largest selling CISSP study series ever.

Two books in one!

Figure 6-4 SpoofStick in action.



Preferences

☑ Show 'You're on'
☑ Show 'Options' button
☑ Show full host name

Display Size
● Small
○ Medium
○ Large

Display Color: ▨

8/18/2004 Version 1.02 of Spoofst… …r. The new version addresses a recently discovered fla… …t more.

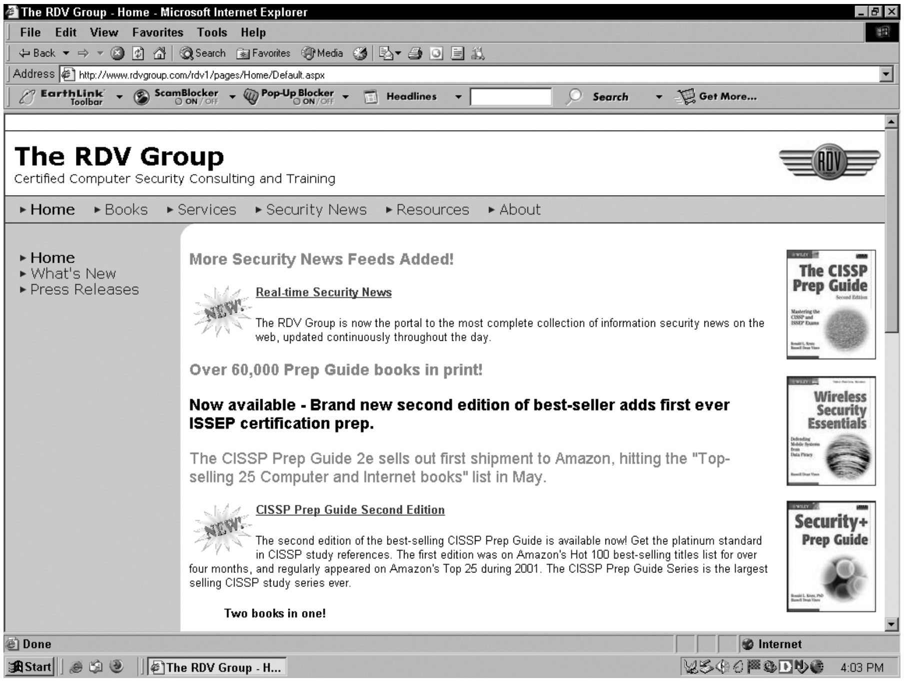
10/29/2004 If you're running Winc… …>Internet Options->Advanced" for a checkbo… …extensions (requires restart)". Make sure that's checked

SpoofStick for Internet Explorer currently requires Windows 2000 or Windows XP to run.

Terms of Use and Disclaimer
SpoofStick makes it easier to spot a spoofed website by prominently displaying only the most relevant domain information. It's not a comprehensive solution, but it's a good start.

This version of SpoofStick is free to use and is not officially supported by CoreStreet or any of its affiliates. CoreStreet does not make any claims about the quality of this software or its suitability to any task. If something bad happens to you while you're using SpoofStick, it's not our fault. Use SpoofStick at your own risk.

Figure 6-5 SpoofStick preferences.


The RDV Group - Home - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.rdvgroup.com/rdv1/pages/Home/Default.aspx
EarthLink Toolbar
ScamBlocker ON / OFF
Pop-Up Blocker ON / OFF
Headlines
Search
Get More...
Home Books Services Security News Resources About
Home What's New Press Releases
NEW!
Done
Internet
Start
The RDV Group - H...
4:03 PM

The RDV Group
Certified Computer Security Consulting and Training

More Security News Feeds Added!

Real-time Security News

The RDV Group is now the portal to the most complete collection of information security news on the web, updated continuously throughout the day.

Over 60,000 Prep Guide books in print!

Now available - Brand new second edition of best-seller adds first ever ISSEP certification prep.

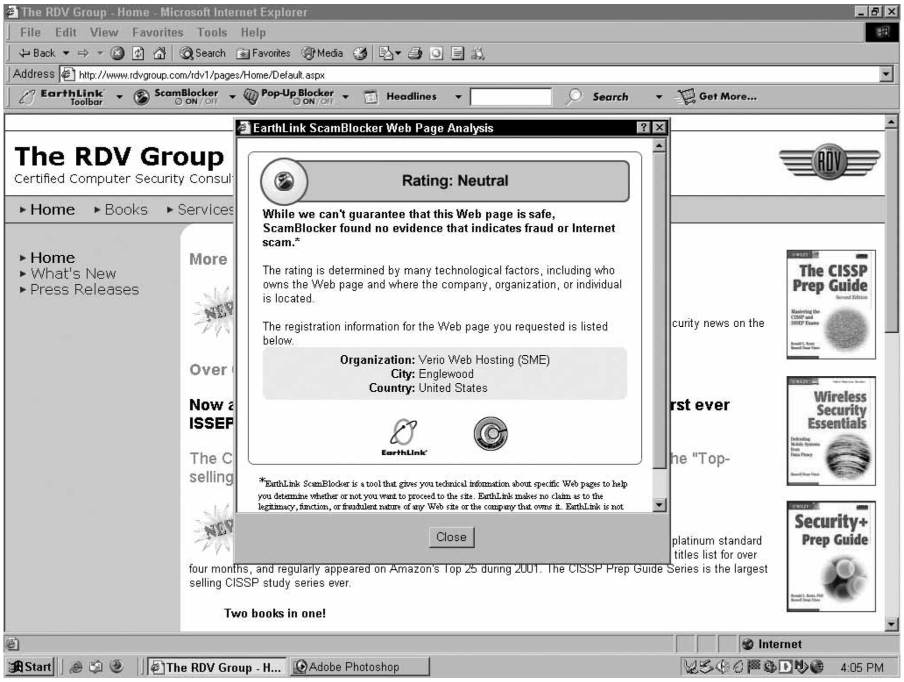
The CISSP Prep Guide 2e sells out first shipment to Amazon, hitting the "Top-selling 25 Computer and Internet books" list in May.

CISSP Prep Guide Second Edition

The second edition of the best-selling CISSP Prep Guide is available now! Get the platinum standard in CISSP study references. The first edition was on Amazon's Hot 100 best-selling titles list for over four months, and regularly appeared on Amazon's Top 25 during 2001. The CISSP Prep Guide Series is the largest selling CISSP study series ever.

Two books in one!

Figure 6-6 The EarthLink ScamBlocker toolbar.



EarthLink ScamBlocker Web Page Analysis

Rating: Neutral

While we can't guarantee that this Web page is safe, ScamBlocker found no evidence that indicates fraud or Internet scam.*

The rating is determined by many technological factors, including who owns the Web page and where the company, organization, or individual is located.

The registration information for the Web page you requested is listed below.

Organization: Verio Web Hosting (SME)
City: Englewood
Country: United States

*EarthLink ScamBlocker is a tool that gives you technical information about specific Web pages to help you determine whether or not you want to proceed to the site. EarthLink makes no claim as to the legitimacy, function, or fraudulent nature of any Web site or the company that owns it. EarthLink is not

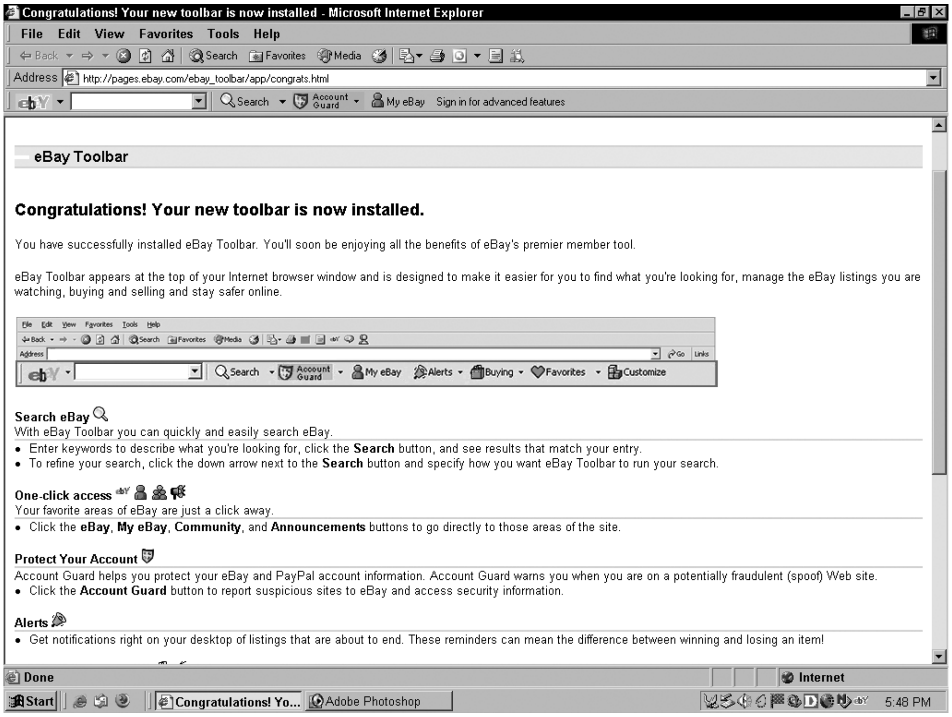
Figure 6-7 EarthLink toolbar site rating feature.

eBay Toolbar

The eBay toolbar is interesting and demonstrates through its advanced functionality where the toolbar concept is headed. This free toolbar gives quick access to eBay functions from the browser, supplying a ton of useful features for eBay addicts. It's available in several languages, but currently only for IE. Figure 6-8 shows the toolbar just installed.

The eBay toolbar includes these features:

- Single-click title search
- Auction end alerts
- eBay and PayPal account information
- Spoofed site warning
- Item buying status
- Item selling status
- eBay Favorites


Congratulations! Your new toolbar is now installed - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://pages.ebay.com/ebay_toolbar/app/congrats.html
Search Account Guard My eBay Sign in for advanced features
File Edit View Favorites Tools Help
Back Search Favorites Media
Address Go Links
Search Account Guard My eBay Alerts Buying Favorites Customize
Done
Internet
Start
Congratulations! Yo...
Adobe Photoshop
5:48 PM

eBay Toolbar

Congratulations! Your new toolbar is now installed.

You have successfully installed eBay Toolbar. You'll soon be enjoying all the benefits of eBay's premier member tool.

eBay Toolbar appears at the top of your Internet browser window and is designed to make it easier for you to find what you're looking for, manage the eBay listings you are watching, buying and selling and stay safer online.

Search eBay

With eBay Toolbar you can quickly and easily search eBay.

- Enter keywords to describe what you're looking for, click the **Search** button, and see results that match your entry.
- To refine your search, click the down arrow next to the **Search** button and specify how you want eBay Toolbar to run your search.

One-click access

Your favorite areas of eBay are just a click away.

- Click the **eBay**, **My eBay**, **Community**, and **Announcements** buttons to go directly to those areas of the site.

Protect Your Account

Account Guard helps you protect your eBay and PayPal account information. Account Guard warns you when you are on a potentially fraudulent (spoof) Web site.

- Click the **Account Guard** button to report suspicious sites to eBay and access security information.

Alerts

- Get notifications right on your desktop of listings that are about to end. These reminders can mean the difference between winning and losing an item!

Figure 6-8 The eBay toolbar installed.

Figure 6-9 shows the Alerts and Sign-in tab from the Toolbar Options dialog box.

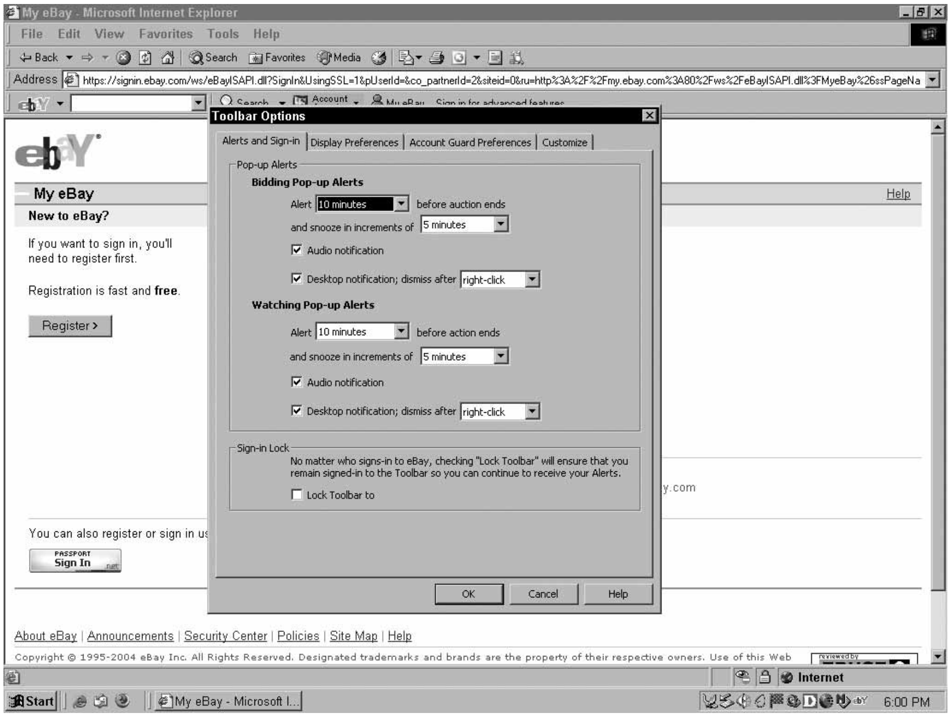
Figure 6-10 shows the Account Guard Preferences tab.

Google

Version 1.0 of the Google toolbar has a lot of features designed to make using Google more efficient, primarily by placing a Google search box directly into your browser. The toolbar also includes a forms auto-fill feature. You can enable or disable popups with one click, and it gives a quick visual ranking of the popularity of the site you're visiting. Figure 6-11 shows the toolbar just installed.

The toolbar is very customizable. You can design your search to include just the site you're visiting or just the page you're viewing. You can also use the toolbar to find similar pages, or sites that link back to that page.

At the time of this writing, Google was just about to release Version 2.0.


My eBay - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&UsingSSL=1&pUserId=&co_partnerId=2&siteid=0&ru=http%3A%2F%2Fmy.ebay.com%3A80%2Fws%2FeBayISAPI.dll%3FMyeBay%26ssPageNa
Search
Account
My eBay
Sign in for advanced features
My eBay
Help
New to eBay?
If you want to sign in, you'll need to register first.
Registration is fast and free.
Register >
You can also register or sign in us
PASSPORT Sign In
About eBay | Announcements | Security Center | Policies | Site Map | Help
Copyright © 1995-2004 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web
Internet
Start
My eBay - Microsoft I...
6:00 PM

Toolbar Options

Alerts and Sign-in | Display Preferences | Account Guard Preferences | Customize

Pop-up Alerts

Bidding Pop-up Alerts

Alert 10 minutes before auction ends

and snooze in increments of 5 minutes

☑ Audio notification

☑ Desktop notification; dismiss after right-click

Watching Pop-up Alerts

Alert 10 minutes before action ends

and snooze in increments of 5 minutes

☑ Audio notification

☑ Desktop notification; dismiss after right-click

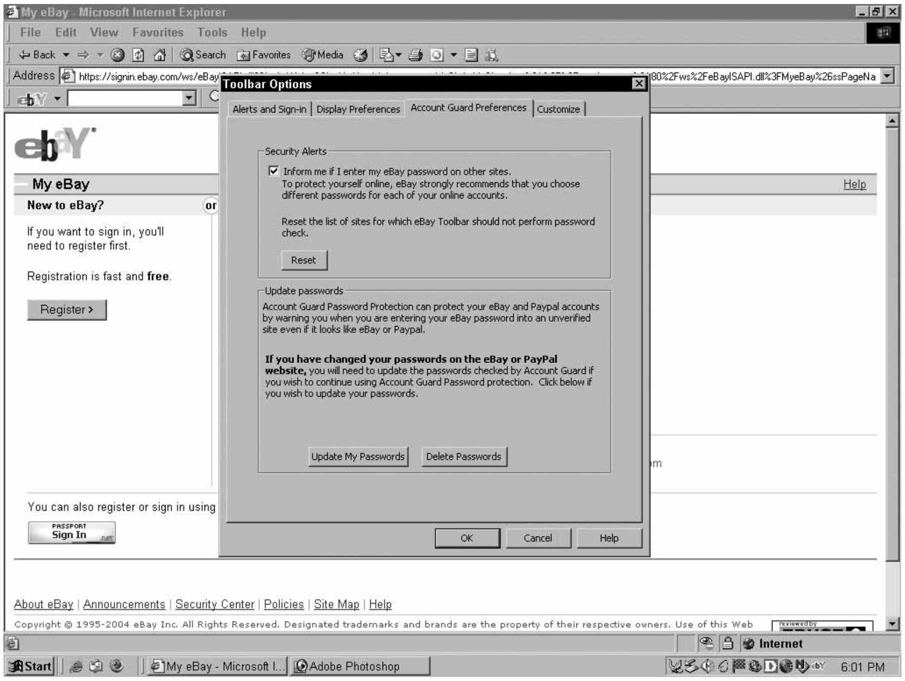
Sign-in Lock

No matter who signs-in to eBay, checking "Lock Toolbar" will ensure that you remain signed-in to the Toolbar so you can continue to receive your Alerts.

☐ Lock Toolbar to

OK | Cancel | Help

Figure 6-9 eBay Alerts and Sign-in tab.


My eBay - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://signin.ebay.com/ws/eBay
80%2Fws%2FeBayISAPI.dll%3FMyeBay%26ssPageNa
My eBay
Help
New to eBay?
or
Register >
PASSPORT Sign In
Internet
Start
My eBay - Microsoft I...
Adobe Photoshop
6:01 PM

Toolbar Options

Alerts and Sign-in | Display Preferences | Account Guard Preferences | Customize

Security Alerts

☑ Inform me if I enter my eBay password on other sites.
To protect yourself online, eBay strongly recommends that you choose different passwords for each of your online accounts.

Reset the list of sites for which eBay Toolbar should not perform password check.

Reset

Update passwords

Account Guard Password Protection can protect your eBay and Paypal accounts by warning you when you are entering your eBay password into an unverified site even if it looks like eBay or Paypal.

If you have changed your passwords on the eBay or PayPal website, you will need to update the passwords checked by Account Guard if you wish to continue using Account Guard Password protection. Click below if you wish to update your passwords.

Update My Passwords | Delete Passwords

OK | Cancel | Help

If you want to sign in, you'll need to register first.

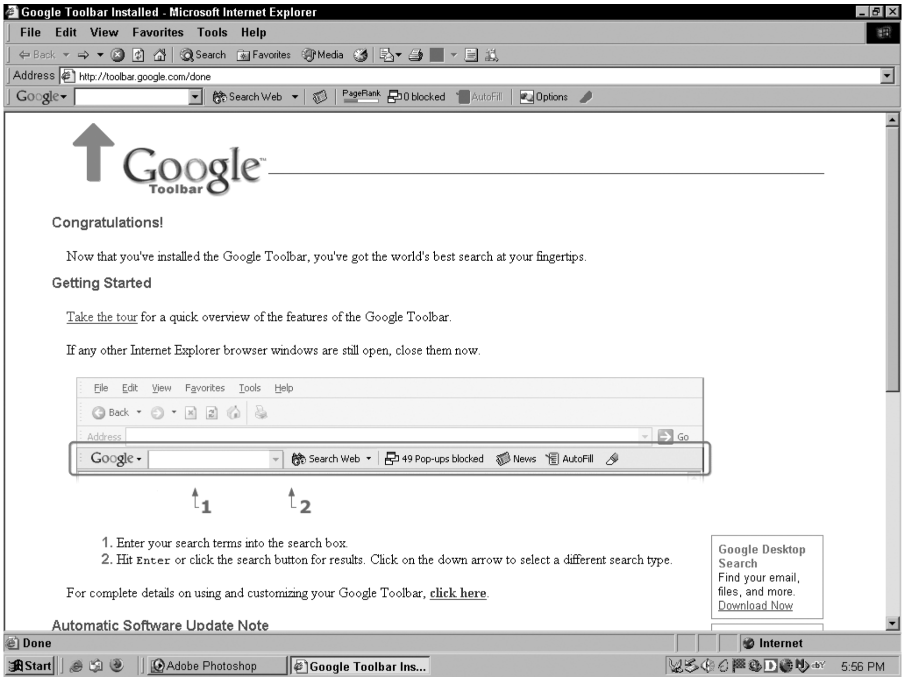
Registration is fast and **free**.

You can also register or sign in using

About eBay | Announcements | Security Center | Policies | Site Map | Help

Copyright © 1995-2004 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web

Figure 6-10 eBay Account Guard Preferences tab.


Google Toolbar Installed - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://toolbar.google.com/done
Google Search Web PageRank 0 blocked AutoFill Options
Google Toolbar
File Edit View Favorites Tools Help
Back
Address
Go
Google Search Web 49 Pop-ups blocked News AutoFill
1
2
Done
Internet
Start
Adobe Photoshop
Google Toolbar Ins...
5:56 PM

Congratulations!

Now that you've installed the Google Toolbar, you've got the world's best search at your fingertips.

Getting Started

Take the tour for a quick overview of the features of the Google Toolbar.

If any other Internet Explorer browser windows are still open, close them now.

1. Enter your search terms into the search box.
2. Hit `Enter` or click the search button for results. Click on the down arrow to select a different search type.

For complete details on using and customizing your Google Toolbar, **click here**.

Google Desktop Search
Find your email, files, and more.
Download Now

Automatic Software Update Note

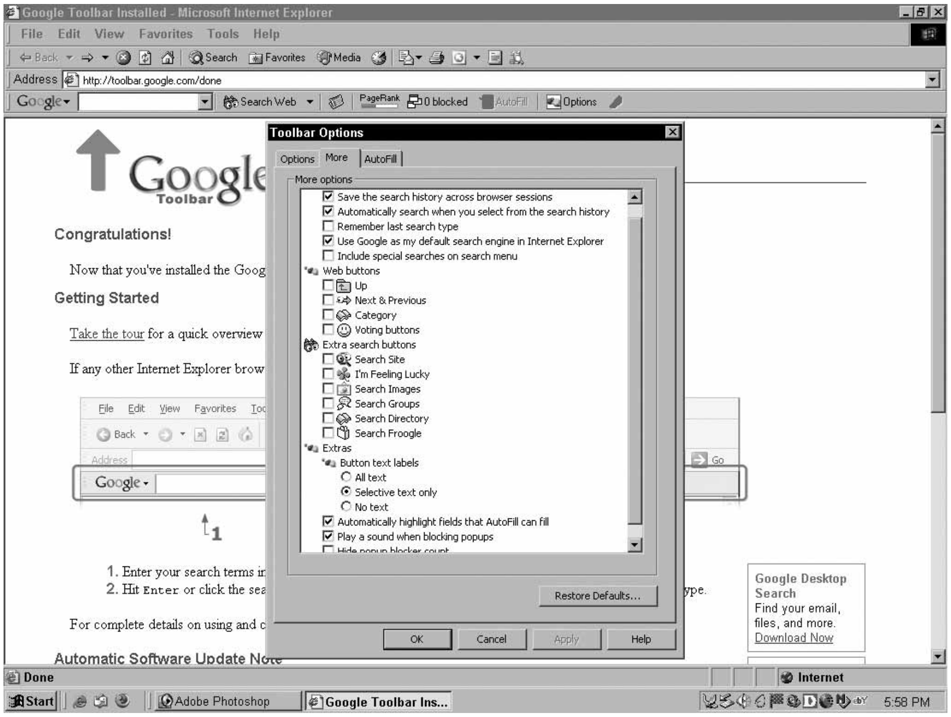
Figure 6-11 Google toolbar installed.

Figure 6-12 shows some of the searching options available from the Toolbar Options dialog box.

Netcraft

The Netcraft toolbar (http://toolbar.netcraft.com) protects users against phishing sites. Whether a phishing site is reported via the toolbar or through some other channel, Netcraft blocks access for everyone using the Netcraft toolbar. Currently only available for Internet Explorer on Windows 2000/XP or later, the Netcraft toolbar has a lot of features:

- Blocks pop-up windows
- Stops suspicious URLs
- Displays sites' real hosting location
- Provides other relevant information about the site, such as how long it's been running


Google Toolbar Installed - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://toolbar.google.com/done
Google Search Web PageRank 0 blocked AutoFill Options
Google Toolbar
Congratulations!
Getting Started
Automatic Software Update Note
Google Desktop Search
Find your email, files, and more.
Download Now
Done
Internet
Start Adobe Photoshop Google Toolbar Ins...
5:58 PM

Toolbar Options

Options | More | AutoFill

More options

☑ Save the search history across browser sessions
☑ Automatically search when you select from the search history
☐ Remember last search type
☑ Use Google as my default search engine in Internet Explorer
☐ Include special searches on search menu

Web buttons
☐ Up
☐ Next & Previous
☐ Category
☐ Voting buttons

Extra search buttons
☐ Search Site
☐ I'm Feeling Lucky
☐ Search Images
☐ Search Groups
☐ Search Directory
☐ Search Froogle

Extras
Button text labels
○ All text
● Selective text only
○ No text
☑ Automatically highlight fields that AutoFill can fill
☑ Play a sound when blocking popups
☐ Hide popup blocker count

Restore Defaults...

OK Cancel Apply Help

Figure 6-12 Google toolbar search options.

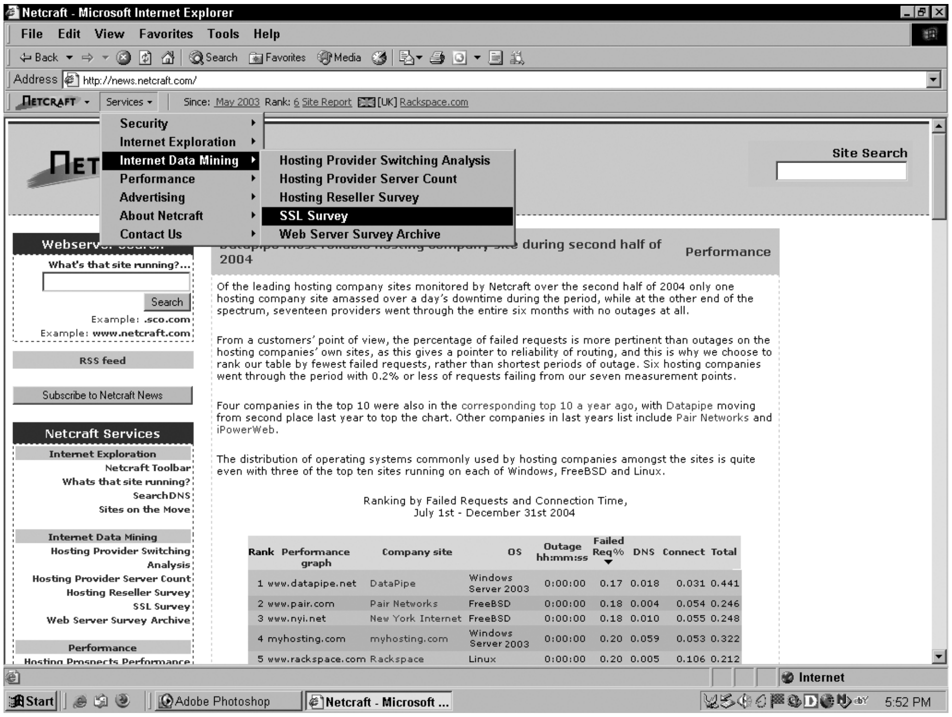
The toolbar provides information about other services Netcraft provides to Internet companies. Figure 6-13 shows some of the options Netcraft provides on its Services menu.

Here is where you can get the toolbars mentioned in the preceding sections:

- **SpoofStick Toolbar:** www.corestreet.com/spoofstick
- **EarthLink Toolbar**: www.earthlink.net/home/software/toolbar
- **eBay Toolbar**: pages.ebay.com/ebay_toolbar
- **Google Toolbar**: toolbar.google.com
- **Netcraft Toolbar:** toolbar.netcraft.com

Much, Too Much, Toolbar

Finally, if you can't decide, go for all of them, as shown in Figure 6-14. Of course, you won't have much room left for the actual browser!



Datapipe most reliable hosting company site during second half of 2004

Performance

Of the leading hosting company sites monitored by Netcraft over the second half of 2004 only one hosting company site amassed over a day's downtime during the period, while at the other end of the spectrum, seventeen providers went through the entire six months with no outages at all.

From a customers' point of view, the percentage of failed requests is more pertinent than outages on the hosting companies' own sites, as this gives a pointer to reliability of routing, and this is why we choose to rank our table by fewest failed requests, rather than shortest periods of outage. Six hosting companies went through the period with 0.2% or less of requests failing from our seven measurement points.

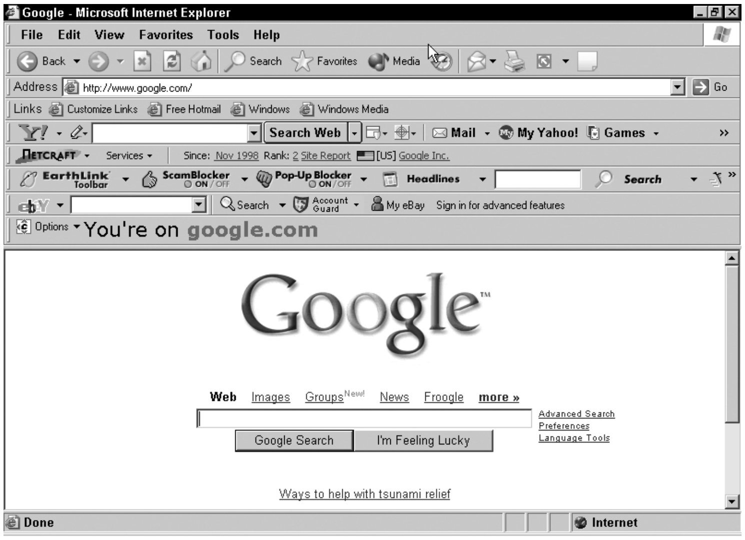
Four companies in the top 10 were also in the corresponding top 10 a year ago, with Datapipe moving from second place last year to top the chart. Other companies in last years list include Pair Networks and iPowerWeb.

The distribution of operating systems commonly used by hosting companies amongst the sites is quite even with three of the top ten sites running on each of Windows, FreeBSD and Linux.

Ranking by Failed Requests and Connection Time,
July 1st - December 31st 2004

Rank	Performance graph	Company site	OS	Outage hh:mm:ss	Failed Req%	DNS	Connect	Total
1	www.datapipe.net	DataPipe	Windows Server 2003	0:00:00	0.17	0.018	0.031	0.441
2	www.pair.com	Pair Networks	FreeBSD	0:00:00	0.18	0.004	0.054	0.246
3	www.nyi.net	New York Internet	FreeBSD	0:00:00	0.18	0.010	0.055	0.248
4	myhosting.com	myhosting.com	Windows Server 2003	0:00:00	0.20	0.059	0.053	0.322
5	www.rackspace.com	Rackspace	Linux	0:00:00	0.20	0.005	0.106	0.212

Figure 6-13 Netcraft Toolbar Services


Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Links Customize Links Free Hotmail Windows Windows Media
Search Web Mail My Yahoo! Games
NETCRAFT Services Since: Nov 1998 Rank: 2 Site Report [US] Google Inc.
EarthLink Toolbar ScamBlocker ON / OFF Pop-Up Blocker ON / OFF Headlines Search
Search Account Guard My eBay Sign in for advanced features
Options You're on google.com
Google
Web Images Groups New! News Froogle more »
Advanced Search
Preferences
Language Tools
Google Search I'm Feeling Lucky
Ways to help with tsunami relief
Done Internet

Address http://www.google.com/

Figure 6-14 Toolbar mania!

Server-Side Solutions

Two areas where you can make important improvement to your vulnerability is in the way you use your images and how you protect your domain name.

Images

One exploit that has been in the news recently is *image referring*—the technique of using your web images to direct the user to an illegitimate site. It's based on the standard web technique of linking directly to non-HTML objects that are not on your own server and is primarily used for image objects such as JPGs and GIFs. Often called *bandwidth stealing*, this practice is frowned upon by most developers because the victim's server is robbed of bandwidth (and in turn hits) as the violator enjoys showing content without having to pay for its deliverance.

EMAIL BOUNCES

One piece of evidence that a spammer may be using your From: address is the receipt of hundreds of returned undeliverable messages a day. What's happening is that a virus or a spammer is inserting your domain into the From: address, and the recipients have their servers configured to blindly return or "bounce" spam to the sender, apparently you.

Phishers do this to make their phony site look more genuine. Photo hosting sites commonly employ this technique. Prevent anyone from hot linking to your images; force them to download them. If you've been phished, check to see if the images on the bogus site are linked from your site. If so, change them to warn customers.

The file .htaccess is an ASCII script file that can be created to send commands to an Apache web server. Using .htaccess (www.javascriptkit.com/howto/htaccess10.shtml) you can disallow hot linking on your server, so those attempting to link to an image on your site are either shown the door via a broken image or another image of your choice.

Near-Miss Domains and Webjacking

You should actively monitor the web for URLs that are slightly misspelled from your domain name. Spammers often fraudulently use these domains for mass mailings, and the credibility hit can be huge for your company. Although suing the owners of these near-miss domains is an option, the time and expense is usually not worth it, so the same bad domain gets reused on different servers for months.

Real webjacking is changing of your domain name records to the webjacker's information, by filing a forged domain change request with the registrar. This is not as common as it once was, because legal systems are catching up to the practice, and several companies have successfully sued to get their name back. But it was a headache for the companies I know that had to do it.

You can find a detailed description of webjacking issues at www.inet-sec.org/docs/spoofing/webhijack.html.

Sharing Information

The importance of gathering and sharing information with your peers cannot be overstated. Knowing what's going on out there is vital to keeping clean. Let's look at some of the ways you can keep up with the curve, like knowing what standards are being developed and interacting with anti-phishing groups.

IETF Draft Proposals

Several current proposals aimed at designing mechanisms to reduce the spoofing of email headers and delivery of spam exist in IETF draft form. Here are the primary ones:

- MTA Authentication Records in DNS (MARID)
- Sender Policy Framework (SPF)

- Caller ID for Email
- Domain-Based Email Authentication Using Public-Keys (DomainKeys)

It's valuable to keep up on the status and industry adoption level of these proposals, mainly because a day will likely come when you will need to implement one or more of them. You can find details on these and a couple of other proposals at

- **MTA Authentication Records in DNS—**IETF source: www.ietf.org/internet-drafts/incoming/fixed/draft-ietf-marid-core-01.txt.
- **Sender Policy Framework (SPF)—**A Convention to Describe Hosts Authorized to Send SMTP Traffic. IETF source: www.ietf.org/internet-drafts/draft-mengwong-spf-01.txt.
- **Caller ID for Email—**IETF source: www.ietf.org/internet-drafts/draft-atkinson-callerid-00.txt.
- **The RMX DNS RR and Method for Lightweight SMTP Sender Authorization—**IETF source: www.ietf.org/internet-drafts/draft-danisch-dns-rr-smtp-04.txt.
- **SMTP Service Extension for Indicating the Responsible Submitter of an Email Message—**IETF source: www.ietf.org/internet-drafts/draft-ietf-marid-submitter-00.txt.
- **Domain-based Email Authentication Using Public-Keys Advertised in the DNS—**www.ietf.org/internet-drafts/draft-delany-domainkeys-base-00.txt.
- **Lightweight MTA Authentication Protocol (LMAP) Discussion and Applicability Statement—**Reference: 'draft-irtf-asrg-lmap-discussion-01'. 24 pages.

Info Groups

Although I've mentioned a lot of links in the book, and this book includes an appendix of sites in the back, here are some of the places you need to check out regularly.

Anti-Phishing Working Group

Mentioned earlier in the book, the Anti-Phishing Working Group (APWG), at Antiphishing.org, is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing and email spoofing of all types. APWG is huge and growing larger. You should make stopping by part of your regular routine.

Digital PhishNet

Digital PhishNet, (www.digitalphishnet.org), is a joint enforcement initiative between industry and law enforcement designed to trap phishermen. Its goals are to "identify, arrest and hold accountable, those that are involved in all levels of phishing attacks to include spammers, phishers, credit card peddlers, reshippers and anyone involved in the further abuse of consumers' personal information." Members currently include ISPs, online auctions, and financial institutions, they and work with law enforcement to include the most agencies.

Internet Crime Prevention & Control Institute

The Internet Crime Prevention & Control Institute (ICPCI at www.icpci.com) is a private member organization created to take preemptive actions against Internet crimes and educate groups regarding Internet crime issues. It also works to research future threats and trends in Internet crime and provide information and contact resources for victims of Internet crimes.

The ICPCI operates an Internet Crime First Response Center, which has the capability to centrally analyze, coordinate, and communicate with an array of third-party organizations to stop criminal attacks, hopefully proactively. An interesting part of its mission is to provide a 5-minute coordinated full-response time from the detection of the attack.

It also offers extensive education and awareness training on Internet crimes and tries to match victims of Internet crimes with public and private victim resources.

Law Enforcement and Federal Agencies

In addition to the FBI cybersites, you may find real benefit in keeping up with various other law enforcement and government agencies, such as the ones described in the following sections.

Internet Fraud Complaint Center

The Internet Fraud Complaint Center (IFCC at www1.ifccfbi.gov/index.asp) is a partnership between the FBI and the National White Collar Crime Center (NW3C) formed to address Internet fraud. IFCC provides a reporting mechanism that alerts authorities of a suspected criminal or civil violation. IFCC also offers a central repository for complaints related to Internet fraud, works to quantify fraud patterns, and provides timely statistical data of current fraud trends.

Computer Crime and Intellectual Property

Although this site may not be that useful to most companies, it's interesting to check. The Computer Crime and Intellectual Property Section (CCIPS at www.cybercrime.gov/index.html) is a Department of Justice (DOJ) site that consists of about 40 lawyers who focus exclusively on computer and intellectual property crime.

These attorneys train and advise federal prosecutors and law enforcement agents and coordinate, litigate, and propose legislation to combat computer crime.

Other areas of expertise possessed by CCIPS attorneys include encryption, electronic privacy laws, search and seizure of computers, e-commerce, hacker investigations, and intellectual property crimes.

The Internet Crime Complaint Center

The Internet Crime Complaint Center (IC3 at www.ic3.gov) was created to be a central repository to receive, develop, and refer criminal complaints about cyber crime. It's intended to give the victims of cybercrime a reporting mechanism that alerts authorities of suspected criminal or civil violations. IC3 provides a central referral mechanism for complaints involving Internet-related crimes for law enforcement and regulatory agencies at the federal, state, and local level.

Apres-Phish

This final section looks at how you can detect phishers and fraudsters and minimize the benefit they get from their labors. This section also examines a few legal statutes that affect how you deal with this fraud.

Identity-Scoring Systems

Two companies, Fair Isaac and ID Analytics, are the major players in the arena of identity-scoring systems. These systems are designed to help clients, such as bank and credit agencies, detect fraud behavior before it becomes a major problem.

Fair Isaac

Fair Isaac's fraud management solution, Falcon Fraud Manager, uses neural network models and other predictive technologies to protect bank credit, debit, and corporate card portfolios from payment card fraud.

It employs profiling technology to detect fraud by identifying abnormal spending patterns. It helps its clients develop fraud management rules representing industry best practices and their unique business strategy, workflow processes, and requirements.

Probably the largest system of its kind, Falcon currently protects 85% of credit card transactions in the U.S. and 65% of credit card transactions worldwide, consisting of more than 450 million payment card accounts.

ID Analytics

The San Diego company ID Analytics uses data from its national ID network to score identities based on patterns of fraud indicators. ID Analytics establishes a baseline of what normal behavior patterns look like. They then determine what anomalies to the pattern signal fraud. If an identity doesn't behave normally, it therefore must be an anomaly. If it's an anomaly, it may be fraud.

Hundreds of thousands of additional fraud indicators are added to the network daily by ID Analytics' customers, including market leaders among bank and retail card issuers, wireless carriers, online retailers, banks, and public agencies.

Problems with Identity-Scoring Systems

Privacy is a big issue with these systems. Building these big data networks presents massive privacy challenges, especially since so much data is aggregated in one area. Many regulations restrict data aggregation, and personally identifiable data must not be delivered outside the network, just the ID scores. The data in the network must be used only for the prevention of fraud and not sold or used for any other purpose.

Because privacy laws in Europe are much more strict than in the United States, both companies must guarantee that they are operating with the privacy regulations of those jurisdictions.

Another issue is that the price of these systems is high; the average corporation can't afford it.

But here's the main problem with behavior pattern recognition systems: not all anomalous patterns are frauds. Members of the network, using a scoring method much like a credit report, place too much emphasis on this number, not understanding that it's merely a tool to engender further examination. The major problem with systems like this and Falcon, is that the results are often interpreted as hard and fast, and somehow quantifiable. Some consumers have had their credit damaged with misinterpretation of the ratings, and rectifying it is a very intensive proposition.

Other Fraud-Alerting Products

Here are a couple of other fraud-alerting products worth mentioning:

- **Cyota's FraudAction:** Contains several modules, including its Real-time Detection and Alerts Module, offered as an outsourced option.
- **Digital Envoy's IP Inspector E-scam:** Allows consumers to verify the origin of suspect emails and check the validity of embedded URLs in emails.

Intrusion Detection Systems

An intrusion detection system (IDS) is a system that monitors network traffic or monitors host audit logs in order to determine whether any violations of an organization's security policy have taken place. An IDS can detect intrusions that have circumvented or passed through a firewall or that are occurring within the local area network behind the firewall.

If you have an active intrusion detection system, it may be possible to get the signatures of known phishers, thereby blocking their IP addresses. Most IDS vendors provide such information. You should get those IP addresses—especially if you have been phished. One product that can do this is RealSecure, from Internet Security Systems.

Honeypot Systems

A honeypot is a system on the network intentionally configured to lure intruders. Honeypots simulate one or more network services, hoping that an attacker will attempt an intrusion. Honeypots are most successful when run on known servers, such as HTTP, mail, or DNS servers because these systems advertise their services and are often the first point of attack. They are often used to augment the deployment of an IDS system.

A honeypot is configured to interact with potential hackers in such a way as to capture the details of their attacks. These details can be used to identify what the intruders are after, what their skill level is, and what tools they use.

Honeypots should be physically isolated from the real network and are commonly placed in a DMZ. All traffic to and from the honeypot should also be routed through a dedicated firewall.

Generally, you configure a honeypot by installing the operating system using defaults and no patches, and by installing an application designed to record the activities of the intruder.

Evidence of an intrusion into a honeypot can be collected through the following:

- The honeypot's firewall logs
- The honeypot's system logs
- Intrusion detection systems or other monitoring tools

A properly configured honeypot monitors traffic passively, doesn't advertise its presence, and provides a preserved prosecution trail for law enforcement agencies.

Honeypot Issues

It's important to be aware of legal issues arising out of implementing a honeypot. Some organizations discourage the use of honeypots, citing the legal concerns of luring intruders, and feel that no level of intrusion should be encouraged.

Before the intrusion occurs, it's advisable to consult with local law enforcement authorities to determine the type and amount of data they will need in order to prosecute and how to properly preserve the chain of evidence.

Also, as the honeypot must be vigilantly monitored and maintained, some organizations feel it is too resource-intensive for practical use.

Dealing with Customers

Several points are very important to remember when the company interacts with customers to stop phishing. Your customer service representatives must be trained to properly identify phishing clues and interact courteously and professionally.

The site should have an area devoted to fraud and ID theft education: how to stop it, how to prevent it, what to do if it happens, who to contact, and so on. As an example, eBay and EarthLink do this quite well.

If your customer has been phished or is a victim of ID theft, be helpful! Customers need to feel that the financial institution wants to correct the problem, not just brush it off. The customer is liable to take his business elsewhere if he feels he has been left out in the cold.

Due Diligence

Senior management has the final responsibility through due care and due diligence to preserve the capital of the organization and further its business model through the implementation of a security program. While senior management does not have the functional role of managing security procedures, it has the ultimate responsibility to see that business continuity is preserved.

The concepts of due care and due diligence require that an organization engage in good business practices relative to the organization's industry. Training employees in security awareness could be an example of due care, unlike simply creating a policy with no implementation plan or follow-up. Mandating statements from the employees that they have read and understood appropriate computer behavior is also an example of due care.

Due diligence might be mandated by various legal requirements in the organization's industry or through compliance with governmental regulatory standards.

For example, the 1991 U.S. Federal Sentencing Guidelines

- Treat the unauthorized possession of information without the intent to profit from the information as a crime.
- Address both individuals and organizations.
- Make the degree of punishment a function of the extent to which the organization has demonstrated due diligence (due care or reasonable care) in establishing a prevention and detection program.
- Invoke the prudent man rule that requires senior officials to perform their duties with the care that ordinary, prudent people would exercise under similar circumstances.
- Place responsibility on senior organizational management for the prevention and detection programs with fines of up to $290 million for nonperformance.

Due care and due diligence are becoming serious issues in computer operations today. In fact, the legal system has begun to hold major partners liable for the lack of due care in the event of a major security breach. Violations of security and privacy are hot-button issues that are confronting the Internet community, and standards covering the best practices of due care are necessary for an organization's protection.

Because of the concept of due diligence, stockholders may hold senior managers as well as the board of directors personally responsible if a disruptive event causes losses that adherence to base industry standards of due care could have prevented. For this reason and others, it is in the senior managers' best interest to be fully involved in the security process.

Privacy and the Law

Some recent acts of Congress have been enacted to help ensure customers' privacy and give them legal recourse from ID theft. Any company using customer data today must be sure they are in compliance with a number of regulations. Your legal, auditing, and regulatory departments are well acquainted with these laws, but the following sections offer a brief look at them in case you're not.

Gramm-Leach-Bliley

The Gramm-Leach-Bliley (GLB) Act of November 1999 is an act that removes Depression-era restrictions on banks that limited certain business activities, mergers, and affiliations. It repeals the restrictions on banks affiliating with securities firms contained in sections 20 and 32 of the Glass-Steagall Act. GLB became effective on November 13, 2001.

The GLBA also requires health plans and insurers to protect member and subscriber data in electronic and other formats. These health plans and insurers will fall under new state laws and regulations that are being passed to implement GLB because GLB explicitly assigns enforcement of the health plan and insurer regulations to state insurance authorities (15 U.S.C. §6805). Some of the privacy and security requirements of Gramm-Leach-Bliley are similar to those of HIPAA.

The GLBA is also known as the Financial Services Modernization Act of 1999 and provides limited privacy protections against the sale of your private financial information.

There are three principal parts to the GLBA privacy requirements: the Financial Privacy Rule, the Safeguards Rule, and pretexting provisions.

The Financial Privacy Rule oversees collection and disclosure of customers' personal financial information and applies to all companies who receive such information—even nonfinancial companies.

The Safeguards Rule also applies not only to financial institutions but also to other companies, such as credit agencies, that collect information from and about their own customers. It requires all organizations to design, implement, and maintain safeguards to protect this information.

The pretexting provisions prohibit the use of false pretenses, including impersonation and false statements, to obtain personal financial information such as bank balances. The GLBA also prohibits the knowing solicitation of others to engage in pretexting.

Sarbanes-Oxley

After major corporate scandals like Enron, WorldCom, and Global Crossing, the Sarbanes-Oxley Act of 2002 was drafted to establish controls on accounting and other financial management. Named for the two congressmen who sponsored it, on the surface it doesn't have much to do with IT security. The law was passed to restore the public's confidence in corporate governance by making chief executives of publicly traded companies personally validate financial statements and other information.

Some groups are claiming that some provisions within the Sarbanes-Oxley Act are debilitating to businesses from a cost standpoint. These groups argue that while it's appropriate for firms of 250,000 workers, its intentions are mislaid when it comes to businesses employing just 250 people. The cost, which includes the retention of auditors, is beneficial to the accounting industry but excessive for small public companies.

The Data Protection Act and 95/46/EC

Because many financial institutions have overseas activities, and phishing is an international problem, it's probably good to also look at the recent Data Protection Act enacted by the European Union. The original Data Protection Act of 1988 was a law governing data protection in Ireland. It was updated into the Data Protection (Amendment) Act 2003 and signed into law on April 10, 2003, by the European Parliament. The new act addresses "protection of individuals with regard to the processing of personal data and on the free movement of such data."

Highlights of the law include

- Extension of rules for the first time to certain manual filing systems
- Definitions of various key terms such as "data," "personal data," and "processing"
- Details of when data relating to individuals may be processed
- Clarification of security measures to be considered when processing personal data
- Clarity on what constitutes fair processing of personal data
- Extension of the role of the data protection commissioner
- Details of when personal data may be transferred outside the European Economic Area
- Amendments to provisions relating to direct marketing initiatives
- Amendments to the registration regime for those intending to process data

HIPAA

The Kennedy-Kassebaum Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a set of regulations that mandates the use of standards in health care recordkeeping and electronic transactions. The act requires that health care plans, providers, insurers, and clearinghouses do the following:

- Provide for restricted access by the patient to personal health care information
- Implement administrative simplification standards
- Enable the portability of health insurance
- Establish strong penalties for health care fraud

Now that you've examined some steps your organization can take to avoid phishing expeditions, the next chapter looks at ways a company can respond to phishing when it occurs.