5

Would the Real Sender Please Stand Up?

How Spammers Spoof Email Identities

IN THIS CHAPTER

- **I'm Not Who I Say I Am**
- **John Doe Emailing**
- **Block Me If You Can**

We often treat email messages just like any other form of communication. Whether we receive instructions from bosses directly, in a phone call, or through an email doesn't matter a whole lot. We tend to treat them all the same. However, what happens when you receive an email from someone who isn't who he or she claims to be?

With a face-to-face visit, there's no doubt that you're dealing with the right person. With a phone call, you have the person's voice, demeanor, and small talk as clues that this is the correct person. However, with email, many of those clues are missing or aren't quite as evident.

To compound the problem, email programs tend to hide much of the information that would help determine an email's authenticity. Because most email you read isn't from a person pretending to be someone else, for usability reasons, often even email addresses are hidden from view.

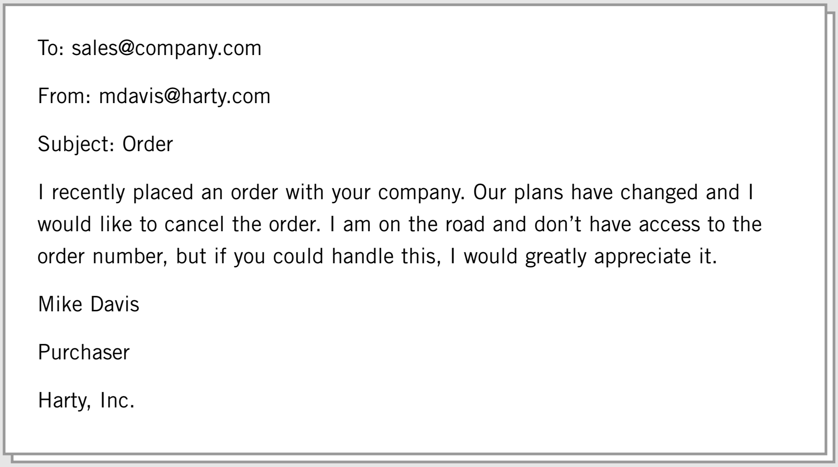
This chapter describes some simple techniques attackers can use to impersonate other users or mask their identities and how you can detect these spoofs. In addition, you'll learn about some of the problems that crop up with common techniques to combat email impersonation. For some people, the cure can be worse than the disease, so this chapter covers ways you can deal with this problem in a fashion appropriate for your email usage pattern.

I'm Not Who I Say I Am

Although much of this book discusses how you need to be more suspicious of your email, most people still place a great deal of trust in what they are told and who tells them. I've never met many of the people I work with; instead, I deal with them via email and the phone. How do I know if they are who I think they are? In this section, you see how easily an attacker can send you an email that appears to come from someone else.

Case Study 5-1

Sue opened her email to find the following message:



To: sales@company.com

From: mdavis@harty.com

Subject: Order

I recently placed an order with your company. Our plans have changed and I would like to cancel the order. I am on the road and don't have access to the order number, but if you could handle this, I would greatly appreciate it.

Mike Davis

Purchaser

Harty, Inc.

Sue had dealt with Mike Davis on several occasions and had sent him numerous emails, so she recognized the email address instantly. She looked up the order on her computer and canceled the order. She clicked Reply, emailed Mike that the order had been canceled, and then went on with her day.

Two weeks later, Sue was called into her boss's office. Mike Davis was there and looked very upset. Sue's boss told her that a critical order for Mike's company had been canceled, and the system showed her ID had been used. Sue was asked who authorized the cancellation.

Sue told them about the email. Mike denied ever sending the email message. They went to Sue's desk where she pulled up the email message. Upon further examination, it became obvious that not only had the email been sent from someone other than Mike, but also Sue's response had not gone to Mike to warn him. By the look on her boss's face, Sue realized the damage had already been done.

Case Study 5-2

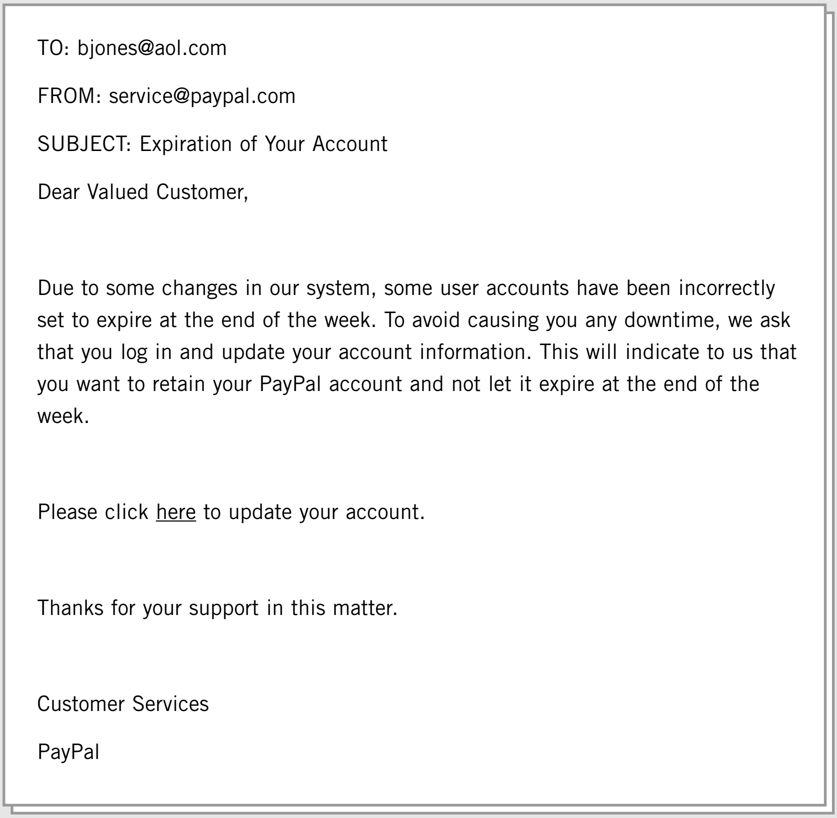
Randy decided to play a trick on his best friend, Peter. He sent an email to Sarah, one of their co-workers, expressing his affection for Sarah and making several crude jokes about how he hoped their relationship might develop. Then he changed the email to make it look like it came from Peter. He hit Send and went to bed.

The next morning, Randy left for work early so that he could warn Sarah about the email and explain what he was doing. He thought Sarah would go to Peter and demand an explanation. He could just imagine the look on Peter's face. However, a flat tire slowed Randy down, and when he got into the office, he completely forgot about the email.

Later that day, Peter came by to see him. He was upset and told Randy that Sarah had filed a sexual harassment claim against him because of an email he had sent. Peter told him he hadn't sent the email and didn't know how this could have happened. Randy realized his joke had badly backfired and didn't know what to do next.

Case Study 5-3

Bruce found the following email in his inbox:



TO: bjones@aol.com

FROM: service@paypal.com

SUBJECT: Expiration of Your Account

Dear Valued Customer,

Due to some changes in our system, some user accounts have been incorrectly set to expire at the end of the week. To avoid causing you any downtime, we ask that you log in and update your account information. This will indicate to us that you want to retain your PayPal account and not let it expire at the end of the week.

Please click here to update your account.

Thanks for your support in this matter.

Customer Services

PayPal

Bruce wanted to make sure his account didn’t expire because he used his PayPal account quite a bit. He clicked on the link, saw the PayPal logo, entered his information, and submitted it to the server.

A couple of days later, he received another email from PayPal. This message warned about a scam going on that involved sending PayPal users an email telling them to enter their account information at a Web site to avoid having their accounts canceled. The problem was that PayPal didn’t send the message, nor did it run the Web site where the information was entered.

Bruce realized he had been scammed, and some large unauthorized purchases on his next credit card bill confirmed his suspicions.

How the Attack Works

As much as we use and trust email, it seems incomprehensible that we could get mail that claims to be from one person but is really from another. In reality, however, email isn’t all that different from sending a letter through the U.S. mail. You can put any return address on an envelope and sign the letter as anyone. The person receiving the letter can only be sure that the letter was sent through a particular post office because of the postmark on the envelope. If you get a letter from Aunt Martha who lives in Miami, but the postmark is Seattle, you might think it’s odd unless Aunt Martha is visiting relatives on the West Coast.

In the same way, email messages can be marked as being from anyone and have their return address marked as anyone. The only thing recipients can count on with any assurance is the servers that passed the email message on to them. If the servers that passed the message from the sender to you don’t seem to match the servers this user would be sending from, there might be a problem.

Because of useability issues, email programs typically hide email headers from view. However, most email programs include an option for displaying headers, usually through a menu choice such as View, Headers. These headers look something like this:

```
Return-Path: <fekhb@hongkong.com>
Received: from [66.38.203.132] by e-hostzz.comIP with HTTP;
    Sun,: 31:55 +0400
From: “Erin” <fekhb@hongkong.com>
To: testuser@test.com
Subject: Re: YRQJZ, then styopa pulled
Mime-Version: 1.0
X-Mailer: mPOP Web-Mail 2.19
X-Originating-IP: [e-hostzz.comIP]
Date: Sun, 04 Jan 2004 11:37:55 -0700
Reply-To: “Erin Hammond” <fekhb@hongkong.com>
Content-Type: multipart/alternative;
    boundary=”--ALT--HFWW15948118488179”
Message-Id: <SQGUNWV-0001103085276@dan>
```

The lines of interest for this discussion are the From and Reply-To headers. As you can see, these headers are simply text strings with the header name followed by a colon and the header value. Because no part of the email sending process validates whether this From field is correct, any value can be entered for the From header. When the From field is displayed in an email program, most people trust that the email came from that user and treat the email accordingly.

You can see this process at work by going to a major news site, such as CNN. Find a news story that interests you, and use the Web site to email the story to yourself. In the To field, enter your email address so that you'll receive the message. In the field that asks for your email address, enter `god@heaven.org`. You should receive an email shortly from `god@heaven.org` with the news item. To avoid being struck by lightning or a plague, you might want to choose the news story you send carefully to make sure it's one that God would send you. Now you can impress your friends and family with your new penpal. However, when a malicious user makes use of the same technology, the results can be devastating.

In Sue's case, she actually replied to the email. If the attacker had used Mike's email address in the From and the Reply-To fields, Mike would have received Sue's email about the order and could have stopped the cancellation request. However, the attacker used a different email address for the Reply-To field, which Sue didn't notice when she sent her message (see Figure 5.1).

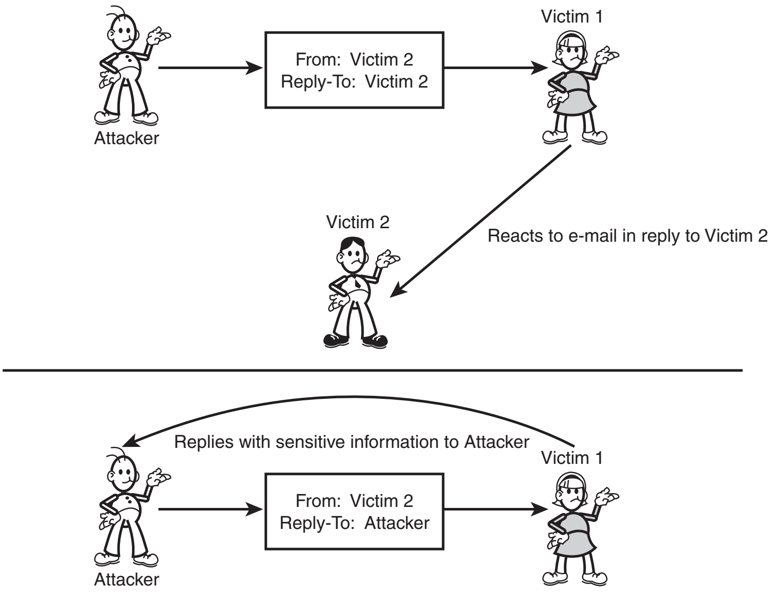


Figure 5.1 *Spoofing email headers can target different victims.*

If you realized that the email message from `support@microsoft.com` containing a patch you need to load right away might not be from Microsoft, you might not be so quick to load the patch. Unless you look at the other headers more closely, these emails are indistinguishable from the real thing.

Bruce fell victim to an attack known as *phishing*, which usually starts as an email message to get users to go to a Web site to enter their personal information for use in an identity scam. The Web site might have all the graphics and verbiage that the real site does, but usually it's just a copy of the real thing. By starting with determining whether the email is legitimate or not, you can reduce your chances of falling for one of these scams.

An Ounce of Prevention

When dealing with email impersonation, begin with common sense. Although any email can be spoofed, most emails are from whom they say they are, at least those that aren't obviously spam related. Although the problems Sue and Peter had do happen, most email you receive isn't being spoofed by a mysterious hacker out to get you.

You can take two steps to deal with this problem. First, consider how you use email. What would you have done in Sue's position? Would you have canceled the order based on Mike's email, or would you have required other information to confirm the email's identity? Not taking the time to confirm the sender's identity for important emails makes you more vulnerable to impersonation attacks.

Not every email needs phone call verification, but if you receive an email that's out of character for the person or directs you to take action that seems odd for this particular person, taking a moment to validate the message's authenticity can be a benefit to all concerned.

Besides changing the way you respond to email, you can also try to confirm the authenticity of email messages yourself. To do this, review the email headers you looked at previously. This time, note the lines that start with Received. Multiple lines start with the Received header, and the order of the lines is important.

The top Received line is the last server to route the mail message—the mail server where you retrieve the email message. In a non-forged email message, the bottom Received line represents the sender's mail server, which receives the email message and starts the send process. Every mail server the message passes through, from the sender to you, is represented by a new Received header line.

The format for the Received line varies from mail server to mail server. The important information in each line is the machine name and IP address assigned to the server. To determine whether a message has been forged, you need to determine the authenticity of the machines the email was routed through.

Although attackers can add their own Received lines to an email message, after it leaves their server, they lose control over the subsequent Received lines added to the header. If the machine name on a Received line doesn't match the IP address, it's likely a forgery, and all lines that follow should not be trusted. You can look up an IP address in a WHOIS database, such as http://www.arin.net/whois/.

Here's an example of an email header from a legitimate Yahoo! email account to me:

```
Return-Path: <testEmailAddress@yahoo.com>
Delivered-To: canningspam@appdefense.com
Received: (qmail 8250 invoked from network); 11 Feb 2004
01:49:40 -0000
Received: from unknown (HELO web12102.mail.yahoo.com)
(216.136.172.22)
  by 0 with SMTP; 11 Feb 2004 01:49:40 -0000
Received: from [192.168.0.123] by web12102.mail.yahoo.com
via HTTP;
  Tue, 10 Feb 2004 17:49:39 PST
Date: Tue, 10 Feb 2004 17:49:39 -0800 (PST)
Subject: Test Message
From: testEmailAddress@yahoo.com
To: canningspam@appdefense.com
```

If you start with the bottom Received line, you see that the email message was sent via the Yahoo! mail server from the IP address of the sender (192.168.0.123). In the second Received line, you see that it passed through the Yahoo! mail server (216.136.172.22). A quick check on WHOIS shows the following:

```
Search results for: 216.136.172.22

Cable & Wireless SC5-3 ( NET-216-136-128-0-1 )
                                  216.136.128.0  -
216.136.255.255
Yahoo EC20-2-YAHOO1 ( NET-216-136-172-0-1 )
                                  216.136.172.0  -
216.136.175.255

# ARIN WHOIS database, last updated 2004-02-09 19:15
# Enter ? for additional hints on searching ARIN's WHOIS
database.
```

Finally, my email server receives the email, which appears to be a legitimate email from a Yahoo! user. Here's another email from the same user, or at least that's what it looks like at first glance:

```
Return-Path: <testEmailAddress@yahoo.com>
Delivered-To: canningspam@appdefense.com
Received: (qmail 8803 invoked from network); 11 Feb 2004
01:51:40 -0000
Received: from unknown (HELO relay.clickability.com)
(208.184.224.72)
```

```
  by 0 with SMTP; 11 Feb 2004 01:51:40 -0000
Received: (qmail 12218 invoked from network); 11 Feb 2004
01:51:40 -0000
Received: from localhost (HELO relay.clickability.com)
(127.0.0.1)
  by localhost with SMTP; 11 Feb 2004 01:51:40 -0000
Received: from unknown (HELO web12102.mail.yahoo.com)
(140.112.101.6)
  by 0 with SMTP; 11 Feb 2004 01:49:40 -0000
Received: from [192.168.0.123] by web12102.mail.yahoo.com
via HTTP;
  Tue, 10 Feb 2004 17:49:39 PST
Date: Tue, 10 Feb 2004 17:51:40 -0800 (PST)
Subject: Test Message
From: testEmailAddress@yahoo.com
To: canningspam@appdefense.com
```

Notice that most of the headers are identical in the two messages. The Return-Path, Delivered-To, Subject, From, and To headers all match. The only difference is in the Received headers.

Starting with the bottom Received line, you see that the email message was sent via the Yahoo! mail server from the IP address of the sender (192.168.0.123). In the second Received line, you see that it passed through the Yahoo! mail server (140.112.101.6). A quick check on WHOIS shows the following:

```
Search results for: 140.112.101.6

OrgName:    Asia Pacific Network Information Centre
OrgID:      APNIC
Address:    PO Box 2131
City:       Milton
StateProv:  QLD
PostalCode: 4064
Country:    AU

ReferralServer: whois://whois.apnic.net

NetRange:   140.109.0.0  - 140.138.255.255
CIDR:       140.109.0.0/16, 140.110.0.0/15, 140.112.0.0/12,
140.128.0.0/13,
140.136.0.0/15, 140.138.0.0/16
NetName:    APNIC-ERX-140-109-0-0
NetHandle:  NET-140-109-0-0-1
Parent:     NET-140-0-0-0-0
NetType:    Early Registrations, Transferred to APNIC
Comment:    This IP address range is not registered in the
ARIN database.
Comment:    This range was transferred to the APNIC Whois
Database as
```

```
Comment:    part of the ERX (Early Registration Transfer)
project.
Comment:    For details, refer to the APNIC Whois Database
via
Comment:    WHOIS.APNIC.NET or http://www.apnic.net/apnic-
bin/whois2.pl
Comment:    ** IMPORTANT NOTE: APNIC is the Regional
Internet Registry
Comment:    for the Asia Pacific region.  APNIC does not
operate networks
Comment:    using this IP address range and is not able to
investigate
Comment:    spam or abuse reports relating to these
addresses.  For more
Comment:    help, refer to
http://www.apnic.net/info/faq/abuse
RegDate:    2003-07-14
Updated:    2003-08-06

OrgTechHandle: AWC12-ARIN
OrgTechName:   APNIC Whois Contact
OrgTechPhone:  +61 7 3858 3100
OrgTechEmail:  search-apnic-not-arin@apnic.net

# ARIN WHOIS database, last updated 2004-02-10 19:15
# Enter ? for additional hints on searching ARIN's WHOIS
database.
```

This email doesn't look like a legitimate email message from Yahoo!. The IP address doesn't match the server name that was given. Next, the message is routed through `relay.clickability.com` (208.184.224.72). A quick check on WHOIS shows the following:

```
Search results for: 208.184.224.72

Abovenet Communications, Inc ABOVENET-6 ( NET-208-184-0-0-1
)
                                  208.184.0.0  -
208.185.255.255
CLICKABILITY MFN-B422-208-184-224-64-27 ( NET-208-184-224-
64-1 )
                                  208.184.224.64  -
208.184.224.95

# ARIN WHOIS database, last updated 2004-02-10 19:15
# Enter ? for additional hints on searching ARIN's WHOIS
database.
```

Obviously, this isn't a Yahoo! server either, but it's probably a legitimate server that the email message was routed through. This message was probably spoofed and should be treated as spam or any other email attack message.

Instead of evaluating every Received line, comparing the email you think might be a forgery to a known good email could quickly tell the real story. The servers the email passes through can change, but comparing the Received lines in previous email messages from this sender can quickly confirm whether this message is likely to be from the sender listed in the From line.

Following each Received line can tell you more about who sent the message. The Received line just before the forgery is the first server the message passed through after it left the attacker's hands, so this line can often pinpoint the ISP being used. For most attacks, recognizing the email as an attack is more important than tracking down the perpetrator.

A Pound of Cure

If you think you have been attacked with a spoofed email, the damage has already been done. There's nothing you can do to undo the damage other than evaluate how you reacted to the email. Depending on the action you took, you might need to contact the real sender and take the necessary steps to fix what the attacker was trying to get you to do.

What's important is learning to recognize this type of attack and change your behavior the next time it happens. By being more cautious and validating the message's authenticity, you'll be less likely to be burned a second time around.

Checklist

- ✔ If an email seems to be out of character for a particular person, make sure you verify its authenticity before overreacting.
- ✔ If an email's authenticity is in doubt, check the headers to see whether anything appears odd.
- ✔ Evaluate how you trust what you read in email, and see whether you need to add a verification step to some of your messages.

John Doe Emailing

Pretending to be someone else is easy, but email headers give you away. However, even headers might not tell the true tale of where the email originated. Many email servers are poorly configured and allow external users to route or relay email messages through them. This relaying makes it seem as though an email message originated from one source when it really came from an attacker. This can make it difficult to validate the email's authenticity and track down the culprit.

Case Study 5-4

Curt received an email from a person who claimed to have information about some security weaknesses in the company Web site. The person offered to help Curt close the vulnerabilities for a large sum of money. If Curt chose not to pay for the assistance, the attacker would disclose the information to the public.

Curt immediately contacted the authorities as well as the company's network security team. As the network security team began looking for weaknesses in the Web site, the authorities reviewed the email Craig had received.

They explained to Curt that it would be difficult to track down who had sent the email message because the attacker had sent it through an offshore anonymous relay server to protect his identity. Curt would have to wait for the attacker to contact him again and see whether he slipped up.

How the Attack Works

As you saw in the previous attack, spoofing the From field is extremely easy and most people don't detect it. However, this attack can be detected by looking at the servers the message passed through. When a message leaves the attacker's control, the rest of the information in the email headers is accurate and can be used to trace the email's route.

To keep someone from tracing a message back to the ISP that was used, *anonymous relays* have been established. Sometimes these relays are established intentionally so that email users can send messages anonymously. This anonymity can be used in a positive way, such as when a person from a country with an oppressive government uses anonymous email to communicate with the outside world. Many times, however, these relays are simply email servers that haven't been configured properly. In either case, these servers accept email messages and send them on to the desired recipients. The difference between anonymous relays and the ones used to trace an email's origin is in how they deal with email headers.

An email relay adds its server information to the email header. An anonymous relay extracts the email's recipient and subject header, but relays the email message on with a new header. This step removes all the previous servers used to pass the email message along and gives the sender a degree of anonymity. If the anonymous relay doesn't log any information, determining the message's actual sender can be impossible.

To complicate things from a legal standpoint, anonymous relays are often established in countries that don't require the same legal cooperation with international authorities that the United States does. An attacker can also send an email message through a series of anonymous relays, essentially ensuring that the email can't be traced to its source.

An Ounce of Prevention

This attack is difficult to prevent. Typically, your best defense is how you respond to these emails. As with all email attacks, you can't prevent someone from sending emails to you. If someone sends you an anonymous email, you need to determine how you're going to react to the situation.

You can add the server where the anonymous email originated to a blacklist to avoid receiving emails from this server in the future. A *blacklist* is a list of servers that you will not accept mail from and can be useful when a lot of spam originates from particular servers through which legitimate email wouldn't be sent. Although this step is effective in blocking email from a particular server, anonymous email relays constantly come and go, so this preventive measure doesn't block all future anonymous emails, only those that come from a particular server.

The key issue is not to respond to the attacker. Don't open a dialogue or provide any information that might enable him to launch further attacks against you.

A Pound of Cure

If you have received an anonymous email message from someone that mentions illegal activity, informing the authorities can be a good step. Attackers play on our fears, however, and that fear often gives them a decided advantage.

Sometimes, as in Curt's situation, blackmail is in play. Although blackmail is obviously illegal, some companies feel compelled to deal with this extortion to avoid the bad press of a security flaw. Another recent ploy is an anonymous email threatening to send the recipient child pornography if he or she doesn't pay a particular sum of money. The idea behind this attack is that people would rather pay the money than have to explain to the authorities how they came into possession of illegal material.

Although the fear factor certainly kicks in here, cybercrime is a growing problem, and the authorities' knowledge, experience, and resources to combat these issues are growing with it. Getting this information in the hands of the proper people early can keep you out of trouble and help keep others from being caught in a nasty trap. If you are a home user, start with your ISP; company users should contact their security department or system administrators. When illegal activity is clearly going on, going to the police or the FBI might be necessary. Many police departments now have specialists in cybercrime, and the FBI is developing extensive experience in this area. Here in St. Louis, the FBI and the police work together in a cybercrime taskforce, which I have had the pleasure of speaking to on a variety of security issues. All these people have a vested interest in security and in containing threats on the Internet. They can help direct you to the best resources to help you with your specific problem.

Checklist

- ✔ Blacklist the server.
- ✔ Never respond to anonymous emails.
- ✔ If illegal activity is being discussed, refer to your company's security division or the authorities.

Block Me If You Can

Depending on the type of spam you get, you might find that much of it originates from a relatively small number of servers. Assuming you don't receive legitimate email from those servers, you can quickly and easily eliminate those spam messages by refusing email messages from those servers. This technique is known as blacklisting. To avoid maintaining the list yourself, you can subscribe to services that do the work for you. Although blacklisting services can be effective for certain types of spam, they can also hurt you. If you use an email server that has been used to send spam, you could find that your email messages are being blocked by these types of services.

Case Study 5-5

Tanya sent an email to a vendor asking for a meeting the following week. Later that afternoon, she noticed a message in her inbox that told her the email hadn't been delivered. She tried sending it again with the same result.

She called the vendor, who agreed to the meeting and told her he would look into why her email was rejected. The next day, he called to tell her that someone else using the same ISP as her company had been sending lots of spam to the vendor. The vendor had blacklisted that IP range, which effectively blocked the spam but also had the unintentional effect of blocking Tanya's email.

Case Study 5-6

Alex uses a service that maintains a list of well-known spammers to help filter out the bulk of spam he receives. This morning he noticed a big reduction in the amount of email in his inbox. Normally, he had about 50 legitimate emails every morning, but today there were only 7.

He noticed on a technical news site that spammers were attacking the service he uses. They had developed a program that denied access to the list. This denial-of-service attack had been going on for hours and was probably the cause of Alex's missing email.

How the Attack Works

One way to deal with unwanted spam is to establish a whitelist of addresses you will accept email from or a blacklist of email addresses you won't accept email from. These approaches can work well, unless valid email messages are lost in the cross-fire.

Typically, what happens is a side effect of trying to block a spammer or an email attacker. In an attempt to blacklist the IP addresses where spam is originating, valid users are blocked as well.

For example, imagine an ISP that owns the following block of IP addresses. For this example, I'm using IP addresses that can't be routed to the Internet to avoid using someone's real address:

- `192.168.10.1`
- `192.168.10.2`
- `192.168.10.3`
- `192.168.10.4`
- `192.168.10.5`
- `192.168.10.6`

An email attacker is sending spam from IP addresses `192.168.10.1`, `.2`, `.4`, and `.6`. If your IP address is `192.168.10.3`, you could get caught by someone's blacklist that blocks everything starting with `192.168.10`. If your IP address is dynamic rather than static, as with dial-up or some broadband connections, you could get assigned one of the blocked IP addresses the next time you log in. That could cause emails sent to certain domains to work at some times and be blocked at other times.

Whitelists tend to be built by email users or built automatically from their address books; blacklists, on the other hand, are time consuming to maintain. Spammers are constantly shifting and moving, so keeping a blacklist up to date is difficult at best. Many people rely on centralized blacklists, such as Spamhaus and SpamAssassin, which keep centralized lists of spammer addresses and can be used to block many of the spam messages sent every day. Although you don't have to maintain the list, you don't control what's put on the list. Therefore, situations such as Tanya's are possible, and valid email could be blocked.

> ***You can find more information on centralized blacklists at***
>
> `http://www.spamhaus.org`
> `http://spamassassin.org`

In a concerning trend, spammers, virus writers, and hackers are starting to work together to launch attacks. In the past year, denial-of-service attacks have been launched against some top spam blacklists in an attempt to interfere with their ability to block spam.

An Ounce of Prevention

For your own use, blacklists such as Spamhaus or SpamAssassin can substantially reduce the amount of spam that makes it to your email program. Keep in mind, however, that there's some risk of losing legitimate mail when blocking or filtering techniques are used. It's that line between blocking unwanted email and ensuring that legitimate email isn't lost that makes the entire spam issue so difficult to deal with.

To keep from being caught in a blacklist block, as Tanya was, choose ISPs that take a hard line on spam and other attacks. ISPs that restrict use of their accounts and carefully monitor usage are less likely to be used by spammers and other email attackers. Therefore, they are less likely to be blocked as part of a blacklist crackdown.

This doesn't guarantee that you won't be caught in this blacklist problem, but it can help reduce the risk. One company I worked at was caught up in a similar blacklist situation. Not being able to email certain clients made it difficult to conduct business. After the problem was solved, we were able to get back to normal, but because of someone else's actions, we were blocked for several weeks from being able to communicate through normal channels.

A Pound of Cure

If you're caught up in a blacklist block, contact the site you're being blocked from to try to resolve the situation. Obviously, you need to do this through other channels, such as a different IP address, phone, or snail mail. If you aren't involved in spam or other email attacks, most companies and organizations will work with you to refine their blacklist so that legitimate email is allowed.

However, this problem can take some time to solve. Setting up a block can take only seconds, but going through the approval process to to relax a block can be much more time-consuming. However, be patient and work through the situation with these sites. They're also trying to get rid of unwanted email, and as you'll see throughout this book, getting rid of unwanted email can often have unintended side effects. If it could be done easily with the push of a button, the problem would have been solved long ago.

In extreme cases, such as your ISP being blocked because actual spam or other email attacks have originated from there, getting the blacklist block fixed might not be possible. In this case, if access to that site is important enough, you might have to consider choosing a new ISP. If you do, try to choose an ISP that is less likely to have these problems in the future.

Checklist

- ✔ Use blacklists to block spam, but only as part of an overall approach.
- ✔ Choose ISPs with a hard line on spam and other email attacks.
- ✔ If you're being blocked, contact the site from a different IP address or via phone or snail mail.
- ✔ If your IP address is blocked and you can't get the block released, you might need to change IP addresses or ISPs.

Summary

Realizing that the email message you're reading might not be from who it claims to be is frightening to many people. With email, the normal clues you have with direct contact or phone conversations are missing. People tend to rely much more on trust with email than with other forms of contact.

To compound the problem, email programs tend to hide much of the information that would help determine an email's authenticity. For useability reasons, even email addresses are often hidden from view.

Many simple techniques can be used to pretend to be a different person. You can detect spoofing, but unless other clues prompt you to do the extra checking, most people normally skip this step.

You also learned about anonymous email relays, which can mask who sent an email message. Whitelists and blacklists can be used to deal with the problem of anonymous email, but these approaches also present some problems. Although they can substantially reduce the amount of unwanted email, care needs to be taken to ensure that important emails aren't lost or blocked.