PLUG-IN

T1

Personal Productivity Using IT

LEARNING OUTCOMES

1. Describe the four steps you can use to create a strong password.
2. Identify three tips you can use to manage your files.
3. Explain why you would use Microsoft's backup and recovery utility.
4. Describe the six common e-mail mistakes.
5. Explain spam and phishing and identify three ways that you can prevent each.
6. Explain the primary uses of spyware and adware.
7. Identify three things you can do to maintain your computer and keep it running smoothly.
8. Explain why you would install anti-virus protection software.
9. Describe the need for a personal firewall.

Introduction

A number of things can be done to keep a personal computer running smoothly and to protect it from such things as spyware and identity theft (see Figure T1.1). A few of these important items are covered in this plug-in, including:

- Creating strong passwords.
- Performing good file management.
- Implementing effective backup and recovery strategies.
- Using Zip files.
- Writing professional e-mails.
- Stopping spam.
- Preventing phishing.
- Detecting spyware.
- Restricting instant messaging.
- Increasing PC performance.

- Using anti-virus software.
- Installing a personal firewall.

Creating Strong Passwords

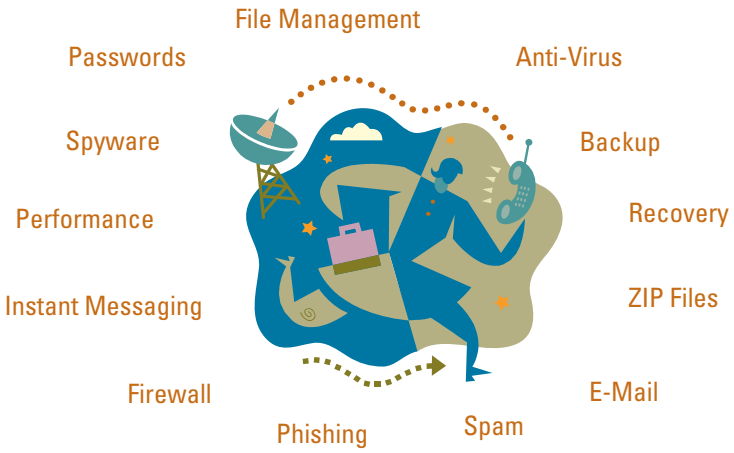


FIGURE T1.1
Maintaining and Protecting Your Computer

If you have ever lost your wallet or your purse, you know the sense of vulnerability that comes with it. Someone might be walking around with your identification, pretending to be you. If someone stole your passwords, he could do the same thing online. A hacker could be opening new credit card accounts, applying for mortgages, or chatting online disguised as you—and you would not know it until it was too late.

You probably already know not to create passwords using any combination of consecutive numbers or letters such as "12345678," "lmnopqrs," or adjacent letters on your keyboard such as "qwerty." In addition, never use your log-in name, your pet's name, or your birthday, or a word that can be found in the dictionary as a password. Hackers use sophisticated tools that can rapidly guess passwords based on words in the dictionary in different languages, even common words spelled backward.

If you use a common word as your password, you might think you are protected if you replace letters of that word with numbers or symbols that look like the letters such as M1cr0$0ft or P@ssw0rd. Unfortunately, hackers know these tricks too. The following are four steps you can use to create strong passwords:

1. Create strong passwords that you can remember.
2. Keep your passwords a secret.
3. Manage your passwords.
4. Monitor your accounts.

CREATE STRONG PASSWORDS THAT YOU CAN REMEMBER

You could come up with a completely random combination of numbers and symbols for a password, but that is not very practical. How would you remember it? Chances are you would write it down and keep it in the top drawer of your desk, and then it is no longer such a great password after all. A strong password is one that is at least eight characters, includes a combination of letters, numbers, and symbols and is easy for you to remember, but difficult for others to guess.

The easiest way to create a strong password that you will not have to write down is to come up with a passphrase. A *passphrase* is a sentence that you can remember, like "My favorite group is Cold Play and my favorite song is Arches." You can make a strong password by using the first letter of each word of the sentence, for example, mfgicpamfsia. However, you can make this password even stronger by using a combination of upper and lowercase letters, numbers, and special characters that look like letters. For example, using the same memorable sentence and a few tricks, your password is now MfGicp&mfsi@.

If you still think that is too hard to remember, you could try a more common phrase, such as "You can't teach an old dog new tricks." If you are using a common phrase make sure to inject at least one number or symbol into the password, such as U(t@0DnT1.

KEEP YOUR PASSWORDS A SECRET

Keeping your passwords safe means keeping them a secret. Do not give them to friends, and do not write them down and keep them at your desk or in an unprotected file on your computer. Your house could get broken into, or, more likely, you may give a friend access to your computer or your desk and that friend may not have the best motives when it comes to your privacy.

Even if you know not to write down your passwords or give them away to friends, you should also be wary when giving them to the Web site where you created the password in the first place. Microsoft, eBay, Amazon, PayPal, or any other reputable company will never ask you to send your password through e-mail. If you receive a request for your password, Social Security number, or other sensitive information via e-mail, notify the company immediately by phone or through the company Web site.

MANAGE YOUR PASSWORDS

The safest password technique is to create a new, strong password for every Web site or log-in that requests one. This is almost as impractical as remembering a long string of random characters. An easier solution is to create a handful of strong passwords and use those at sites you want to keep most secure, such as your bank, brokerage, or bill paying company. Then create another small set of easier to remember passwords that you can use everywhere else.

Remember, a strong password is one you change every few months. Just as you schedule updates, backup software, and clean out old programs, you should also regularly change passwords.

MONITOR YOUR ACCOUNTS

Creating stronger passwords can help protect you against identity theft. However, it does not guarantee that you are protected. If someone does steal your passwords, the faster you catch on and notify authorities, the less damage a hacker can do. Make sure to monitor all your monthly financial statements, and call the appropriate company or bank immediately to report issues. Also, review your credit report each year.

Performing Good File Management

Computer users today work with large numbers of different kinds of files such as documents, spreadsheets, presentations, graphics, and others. Keeping these files organized can be a task in itself. A couple of minutes a few times a day searching for files can add up. The key to minimizing this time is good file management.

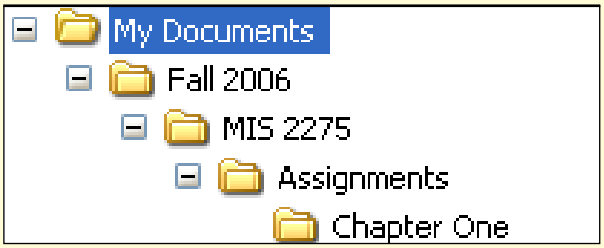
The best way to manage files effectively is a lot like managing paper files. They can be organized into folders and then stored in specific locations and recalled quickly when you need them. Just like paper files and folders, if you do not have a good way to organize them, they will get lost and you could spend hours searching for files. Whether you save your files on your computer's hard drive or a shared network location, the tips displayed in Figure T1.2 can help save time and reduce the headaches of searching for files.

Implementing Effective Backup and Recovery Strategies

Tracie Whiteley lost everything in a flash. When she left for work, her home computer was fine. When she came home, all the clocks in the house were blinking 12:00, and her computer was dark. There had been a lightning storm that day. Whiteley, a

Tips for Managing Your Files

1. **Use My Documents**—To open My Documents in Windows, click **Start**, and then click **My Documents**. My Documents provides an easy way for you to store your personal documents and perform the following:
   - **Find files**—It is easy to access the My Documents folder (and its subfolders) in many different places in Windows including the Start menu, the task pane in Windows Explorer, common File Open and File Save dialog boxes, and other places. (Note: Windows Explorer displays the structure of files and folders on your computer. To open Windows Explorer, click **Start**, point to **All Programs**, point to **Accessories**, and then click **Windows Explorer**.)
   - **Back up files**—Keeping all your files in one place is an essential first step in developing a practical backup strategy.
   - **Keep files separate from programs**—Separating personal files from program files reduces the risk of accidentally deleting personal files when you install or upgrade programs.
2. **Limit file name length**—Even though Windows allows long file names, it is not always a good idea. Long file names produce cluttered displays. Short file names promote clarity. Let your folders do some of the naming. For example, rather than create a file called **Fall06 MIS2275 Assignment Chapter One.doc**, you can build a file structure similar to the sample below.



3. **Archive completed work**—To keep the My Documents folder from becoming unmanageable, store only files you are currently working on. This reduces the number of files you need to search through and the amount of data you need to back up. Every month or so, move the files you are no longer working on to a different folder or location, preferably not in My Documents. You can archive them on a folder on your desktop (you could even label it Archives) or move them to a backup tape or recordable CD. This limits the size of your My Documents folder, which you should back up frequently.
4. **Use shortcuts instead of multiple copies**—If you need to get to the same file from multiple locations, do not create copies of the file. Create shortcuts to it instead. To create a shortcut, **right-click** on the file and click **Create Shortcut.** You can drop-and-drag the shortcut to other locations. Put a shortcut to My Documents on the desktop.
5. **Use abbreviations**—Keep file names short by using common abbreviations, such as "MTG" for meeting or "ACTG" for accounting. This makes the file names more descriptive, and you can more easily find files through Search if it is necessary. To make it easier to search for documents, name your files and folders with easily found names, such as model numbers, project names, or the project lead in the title.
6. **Use thumbnails**—Search through folders in the Thumbnail view. They are easier to see and you can put a picture or clip art on the folder so that it is more recognizable. For example, a folder that contains information about a product can have a picture of the product, or something else that reminds you of the folder contents. To view your folder list in Thumbnail view, on the My Documents folder, in the toolbar click **View** and then select **Thumbnail**. To put a picture on the folder, **right-click** the folder and click **Properties**. In the Properties dialog box, click the **Customize** tab. In the Folder pictures area, click **Choose Picture**.
7. **Do not save unnecessary files**—Be selective about the files you keep. You probably do not need to keep them all. With e-mail, for example, you rarely need to keep everything you receive.
8. **Use My Recent Documents**—To find a file you just worked on, use My Recent Documents in the Start menu.

FIGURE T1.2
File Management Tips

finance specialist at a large automation technology company, said, "The computer was on when I left for work, and it was not on when I came home. When I tried to start it there was a burning smell and smoke. Everything inside it was fried." Whiteley lost both professional and personal data in that storm. The computer held the only copies of her family's e-mail messages, school projects, finances, and letters. "All our information disappeared," she says. "The computer had to be replaced."

You can unintentionally lose information on a computer in many ways—a child playing the keyboard like a piano, a power surge, lightning, a flood, and even equipment failures. If you regularly make backup copies of your files and keep them in a separate place, you can get some, if not all, of your information back if something happens to the originals on your computer.

DETERMINING WHAT TO BACK UP

Deciding what to back up is highly personal. Anything you cannot replace easily should be at the top of your list. The key to a successful backup is getting a copy of your data off your hard drive. Do not try to copy programs like Microsoft Word or Excel; they can be reinstalled from the original CDs you purchased. Likewise, the operating system software—Windows itself and any software provided by your computer manufacturer—can usually be recovered from the installation or "System Restore" CDs that came with the computer. Before you get started, make a checklist of files to back up. This will help you determine what to back up, and give you a reference list in the event you need to retrieve a backed-up file. Here are some file suggestions to get you started:

- Bank records and other financial information.
- Digital photographs.
- Software purchased and downloaded from the Internet.
- Music purchased and downloaded from the Internet.
- Personal documents.
- E-mail address book.

There are several different types of external storage for your backup files including Zip disks, external hard drives, recordable CDs, DVDs, tape cartridges, and flash drives. You can even upload your data to an Internet-based file storage service such as www.mydocsonline.com.

To find the solution that is best for you, compare the convenience, price, and ease of use offered by each approach. For example, a 100 MB Zip drive costs much less than a tape drive, but a single tape cartridge can hold as much as 300 Zip disks.

HOW TO BACK UP YOUR COMPUTER FILES

A simple backup in Windows XP requires no special software or skills. To copy a file or folder, just right-click on the file or folder and select **Copy** from the pop-up menu that appears. Choose the disk or drive where you want to store the duplicate copy, right-click again and then select **Paste** from the pop-up menu. It is that easy. Be sure to label the backup disks clearly, noting the date and time of the backup. Do not erase the previous backup until you have made a newer one.

You can also copy files in Windows operating systems using a drag-and-drop method—hold down the right mouse button while dragging a file or folder, then select **Copy Here** from the pop-up menu that appears.

Your e-mail messages and address book list can be exported and then backed up along with other personal data. This process varies depending on which e-mail software is used on your computer.

Perform Regular Backups

How often should you back up your data? If you use your computer occasionally, a weekly backup might be enough. If you use your computer every day, a daily backup is a good idea. Whatever backup option you choose, be sure to check that it works. Duplicate a single folder or group of files, and then try to recover those backup files to a different drive or folder. Do not wait until it is too late to find that the restore process does not work.

MICROSOFT'S BACKUP AND RECOVER UTILITY

Microsoft's Backup Utility and Recovery Console are installed by default on Windows XP Professional. However, you can manually install both the Backup Utility and Recovery Console for Windows XP.

Backup Utility

The Backup Utility in Windows XP helps you protect your data if your hard disk fails or files are accidentally erased due to hardware or storage media failure. By using Backup, you can create a duplicate copy of all the data on your hard disk and then archive it on another storage device, such as a hard disk or a tape. If the original data on your hard disk is accidentally erased or overwritten, or becomes inaccessible because of a computer malfunction, you can easily restore it from the disk or archived copy by using the Restore or Automated System Recovery Wizards. To start Backup or to access Restore and Automated System Recovery:

1. Click **Start** and then click **All Programs**.
2. Select **Accessories**, then **System Tools**, and then **Backup**.

Recovery Console

You can use the Recovery Console to perform many tasks without starting Windows XP, including starting and stopping services, reading and writing information on a local disk drive, and formatting drives. However, you must install the Recovery Console while your computer is still functioning. The Recovery Console feature should be used only by advanced users. Before using the Recovery Console, it is recommended that you back up your information on a tape drive, because your local hard disks might be reformatted—thus erased—as part of the recovery. You can also run the Recovery Console from the Windows XP CD. To install the Recovery Console as a Startup option:

1. Log on to Windows XP as an administrator or as a user with administrator rights. If your computer is connected to a network, network policy settings may prevent you from completing this procedure. If this is the case, contact your network administrator for assistance.
2. Insert the Windows XP CD into your CD-ROM drive. If you are prompted to upgrade to Windows XP, click **No**.
3. From the command prompt—or from the Run command in the Start menu—type the path to the appropriate Winnt32.exe file (on your Windows XP CD), followed by a space and /cmdcons to reference this switch. For example: *e:*\i386\winnt32.exe/cmdcons.
4. Follow the instructions that appear.

To run the Recovery Console on a computer if Windows XP does not start:

1. Restart your computer, and then choose **Windows Recovery Console** from the list of operating system options.

2. Follow the instructions that appear. Recovery Console displays a command prompt.
3. Make the required changes to your system.

Using Zip Files

Compressing files, folders, and programs decreases their size and reduces the amount of space they use on your hard drives or removable storage devices. Folders that are compressed using the Compressed (zipped) Folders feature use less drive space and can be transferred to other computers more quickly. You can work with a compressed folder and the files or programs it contains just as you would an uncompressed folder. Once you have created a compressed folder (identified by the zipper on the folder icon), you can compress files, programs, or other folders by dragging them to it. You can open files directly from compressed folders, or you can extract files before opening them. You can run some programs directly from zipped compressed folders, without decompressing them. However, to run programs that are dependent on other files, you must first extract them. Figure T1.3 displays a few of the features in the Windows Compressed (zipped) Folders.

TO CREATE A ZIPPED COMPRESSED FOLDER

1. Click **Start**, and then click **My Computer.**
2. Double-click a drive or folder.
3. On the **File** menu, point to **New**, and then click **Compressed (zipped) Folder**.
4. Type a name for the new folder, and then press **ENTER**.
5. You can also create a zipped compressed folder by right-clicking the desktop, pointing to **New**, and then clicking **Compressed (zipped) Folder**.
6. You can identify compressed folders by the zipper on the folder icon.

TO ADD FILES TO A ZIPPED COMPRESSED FOLDER

1. Open **My Computer**, and then locate the compressed folder.
2. Drag files into the compressed folder to compress them.

FIGURE T1.3
Zip File Features

Features of Windows Zipped Files
You can run some programs directly from compressed folders without decompressing them. You can also open files directly from compressed folders.
Zipped compressed files and folders can be moved to any drive or folder on your computer, the Internet, or your network, and they are compatible with other file compression programs.
Folders compressed using this feature are identified by a zipper icon.
You can protect files in a zipped compressed folder with a password. This protects your data if you save it in a shared network folder, attach it to an e-mail message, or move it between work and home on floppy disks.
Using Compressed (zipped) Folders will not decrease your computer's performance.
To compress individual files using Compressed (zipped) Folders, create a compressed folder and then move or copy the files to that folder.

TO EXTRACT FILES FROM A ZIPPED COMPRESSED FOLDER

1. Open **My Computer**, and then locate the compressed folder. Do one of the following:
   a. To extract a single file or folder, double-click the compressed folder to open it. Then, drag the file or folder from the compressed folder to a new location.
   b. To extract all files or folders, right-click the compressed folder, and then click **Extract All**. In the Compressed (zipped) Folders Extraction Wizard, specify where you want to store the extracted files.
2. When you extract a file, a compressed version remains in the compressed folder. To delete the compressed version, right-click the file, and then click **Delete**.
3. When you extract a file from a compressed folder that is password-protected, the extracted file is no longer protected.

TO OPEN A ZIPPED COMPRESSED FOLDER

1. You open a compressed folder the same way you open other folders in Windows: Double-click the compressed folder.
2. You can identify compressed folders by the zipper on the folder icon.
3. To view percentages of compression and other file information for a compressed folder, on the **View** menu, click **Details**.
4. When you open or view compressed folders, you cannot use the **Up** or **Back** buttons on the toolbar, or move up or down levels from the folder.

Writing Professional E-Mails

E-mail is almost like talking. We use it so much that we do not always think about it. But there are rules and courtesies, just as there are with verbal conversation. And there are other considerations involved in communicating by written word only. Giving an e-mail additional thought could make your e-mail experience more satisfying and your recipients much happier. Figure T1.4 displays six common e-mail mistakes to avoid.

In addition, be careful about sharing your e-mail or instant message address. Figure T1.5 displays several methods you can use to protect your e-mail address.

NETIQUETTE 101

Surfing the Internet can be fun, useful, and social. But it is important for all new Internet citizens, also called *netizens*, to remember that there are other surfers out there. Like real surfing or any other public activity, there are implied rules of behavior or etiquette to follow. Failing to grasp the netizen ropes could result in more than just missed opportunities—saying the wrong thing at the wrong time could provoke harassment or other problems. The following sections provide a few guidelines that can help you to handle almost any situation in cyberspace.

Using Emoticons

It is often difficult to convey emotion, intent, or tone through text alone, early Internet users invented *emoticons*, which are virtual facial expressions made from basic keyboard characters, like the colon and right parentheses (emoticons lay on their sides at 90 degrees).

FIGURE T1.4
Common E-Mail Mistakes

Six Common E-Mail Mistakes to Avoid

1. **Failing to follow e-mail etiquette**—An old adage states, "You catch more flies with honey than with vinegar." Here are a few points to consider:
   - Try not to write or respond to an e-mail when you are angry; wait 24 hours. Calm down. Be reasonable. Have someone else edit your e-mail.
   - Try not to use sarcasm. You may think you are clever, but the recipient will not always agree and might even fail to realize that you are being sarcastic.
   - DO NOT USE ALL UPPERCASE LETTERS. This is the e-mail equivalent of YELLING. Your recipient will not be appreciative. Go easy on the exclamation marks, too. Overuse dulls their effectiveness.
   - Use clear subject lines. That will help people decide whether to read the e-mail now or later.
   - Keep it short. If your e-mail is more than two paragraphs, maybe you should use the telephone.
   - Limit what you forward. Unless the recipient has previously agreed, do not forward poems, jokes, virus warnings, and other things. You are just wasting valuable time and bandwidth.
2. **Attempting anonymity**—If you are sending nasty or inappropriate messages, you might think no one will be able to figure out that the e-mail came from you. After all, you set up a phony Web address. Think again. E-mail contains invisible information about the sender. That information is in the header. All major e-mail programs can display header information. Remember the header if you are tempted to send an anonymous e-mail. You may be less anonymous than you think.
3. **Sending e-mail to the wrong person**—Today's e-mail programs want to make it easy to send e-mail. This means that when you start typing the address of a recipient to whom you have previously sent mail, the "To:" field may already be populated. Be careful. Always double-check that the recipient is the intended one.
4. **Using one e-mail address for everything**—Try to have different e-mail addresses for work and for personal use. Some people have four or more different e-mail addresses: private, public, one for online mailing lists, and another for online shopping. These addresses attract mail for those specific areas. Most e-mail providers will give users a half-dozen e-mail accounts. You can also use addresses on the Web for personal accounts. Both Hotmail and Yahoo! are good choices.
5. **Clicking "Send" too fast**—Reread every e-mail before you send it. E-mails with misspellings and missing words typically end up in the same place: the garbage. Try not to depend on the spell-checker. It will catch misspellings. But if you use "four" instead of "for," or "your" for "you're," it will not tell you. It also is not likely to catch any missing words in a sentence that you inadvertently failed to include. So take a minute and reread your text.
6. **Forgetting the attachment**—This seems obvious, but it happens frequently. When you get ready to send your e-mail, think: "What am I forgetting?"

Here are some examples of commonly used emoticons:

- :-) Happy or joking.
- ;-) Winking.
- :-(Unhappy.
- :-| Ambivalent.
- :-o Surprised or concerned.
- :-x Not saying anything.
- :-p Sticking out your tongue (usually in fun).

Learning Online Acronyms

Another method of streamlining communication is the use of acronyms. Because typing takes longer than speaking, savvy netizens like to reduce common phrases to a few simple letters. Here are some examples of commonly used acronyms:

Protecting Your E-Mail Address
Share your primary e-mail address only with people you know. Avoid listing your e-mail address in large Internet directories and job-posting Web sites. Do not even post it on your own Web site (unless you disguise it as described below).
Set up an e-mail address dedicated solely to Web transactions. Consider using a free e-mail service to help keep your primary e-mail address private. When you get too much spam there, simply drop it for a new one.
Create an e-mail name that is tough to crack. Try a combination of letters, numbers, and other characters—Don2Funk9@example.com or J0e_Y0ng@example.com (substituting zero for the letter "O"). Research shows that people with such names get less junk e-mail.
Disguise your e-mail address. When you post your address to a newsgroup, chat room, bulletin board, or other public Web page, add some camouflage such as SairajUdin AT example DOT com. This way, a person can interpret your address, but the automated programs that spammers use often cannot.
Watch out for prechecked boxes. When you buy things online, companies sometimes preselect check boxes to indicate that it is fine to sell or give your e-mail address to responsible parties. Clear the check box if you do not want to be contacted.
Read the privacy policy. When you sign up for Web-based services such as banking, shopping, or a newsletter, carefully read the privacy policy before revealing your e-mail address so you do not unwittingly agree to share confidential information. The privacy policy should outline the terms and circumstances regarding if or how the site will share your information. If a Web site does not post a privacy statement, consider taking your business elsewhere.

FIGURE T1.5
Protecting Your E-Mail Address

- ASAP (As soon as possible).
- BBL (Be back later).
- BRB (Be right back).
- LOL (Laughing out loud).
- ROFL (Rolling on the floor laughing).
- BTW (By the way).
- OIC (Oh, I see).
- CUL (See you later).
- OTOH (On the other hand).
- GMTA (Great minds think alike).
- IMHO (In my humble opinion).
- RUOK? (Are you OK?).
- TIA (Thanks in advance).
- J/K (Just kidding).
- TTFN (Ta-ta for now).

Stopping Spam

If you send or receive e-mail, you have probably received junk e-mail, also known as *spam*. Unfortunately, spam is not always limited to e-mail. It has spilled over to instant messages (IM) as well and has become enough of a problem for instant messaging spam to warrant its own word, *spim*.

Recent research estimates that 80 percent or more of all e-mail sent these days is spam. An astonishing figure, yet you may see only a tiny portion of that deluge. Many Internet service providers (ISPs) or e-mail programs provide junk e-mail filters that serve as the first line of defense against spam. For example, MSN Hotmail uses patented Microsoft SmartScreen Technology and other tools to keep more than 3.2 billion messages from reaching its customers' e-mail accounts every day.[1]

Sending spam is a lucrative business. It costs spammers next to nothing to send out millions, even billions, of e-mail messages. In addition, consider this: If even a tiny percentage of a hundred million people buy something in response to a junk message, that is a lot of sales! According to a report by the Pew Internet & American Life Project, an independent research organization, five percent of U.S. e-mail users—or 6 million people—said they had ordered a product or service as a result of unsolicited e-mail.[2]

HOW DO SPAMMERS GET E-MAIL ADDRESSES?

Spammers steal, swap, or buy lists of valid e-mail addresses (and the addresses of people who have responded to spam command a premium). Spammers also build their own lists using special software that rapidly generates millions of random e-mail addresses from well-known providers, such as MSN Hotmail and others, and then sends messages to these addresses. Invalid e-mail accounts return e-mail to the sender, so the software very rapidly records which e-mail addresses are active and which are not.

Some spammers also gather or *harvest* addresses from Web sites where people sign up for free offers, enter contests, and so on. Harvesters may also use programs (known as Web bots) that trawl for e-mail addresses anywhere they are posted for all to see—on Internet white pages, job postings, newsgroups, message boards, chat rooms, and even personal Web pages.

HOW TO HANDLE SPAM

Despite your best efforts, you no doubt have received e-mail and instant messages you did not request. Figure T1.6 displays a few things you can do to help stop spam.

Preventing Phishing

A new form of spam e-mail is on the horizon. This spam is more than just unwanted and annoying. It could lead to the theft of credit card numbers, passwords, account information, or other personal data. Thieves use a method known as *phishing* to send e-mail or instant message spam that meticulously imitates messages from reputable, well-known companies, including Microsoft and others. The forged message capitalizes on your trust of the respected brand by enticing you to click a link on a Web page or in a pop-up window. Clicking it could download a virus or lead you to reveal confidential information such as a bank account and Social Security numbers.

WHAT IS PHISHING?

Phishing is a type of deception designed to steal your identity. In phishing scams, scam artists try to get you to disclose valuable personal data, such as credit card numbers, passwords, account data, or other information, by convincing you to provide it under false pretenses. Phishing schemes can be carried out in person or over the phone, and are delivered online through spam e-mail or pop-up windows.

HOW DOES PHISHING WORK?

A phishing scam sent by e-mail may start with con artists who send millions of e-mail messages that appear to come from popular Web sites or sites that you trust, like your bank or credit card company. The e-mail messages, pop-up windows, and Web sites they link to appear official enough that they deceive many people into believing that

Tips to Stop Spam
Delete junk e-mail messages without opening them. Sometimes even opening spam can alert spammers.
Do not reply to spam unless you are certain that the message comes from a legitimate source. This includes not responding to such messages that offer an option to "Remove me from your list."
Do not give personal information in an e-mail or instant message. It could be a trick. Most legitimate companies will not ask for personal information by e-mail. If a company you trust, such as your credit card company or bank, appears to ask for personal information, check into it further. Call the company using a number you retrieve yourself from the back of your credit card, bill, phone book, or the like—not a number from the e-mail message. If it is a legitimate request, the company's customer service department should be able to help you.
Think twice before opening attachments or clicking links, even if you know the sender. If you cannot confirm with the sender that an attachment or link is safe, delete the message. (If you must open an attachment that you are less than sure about, save it to your hard disk first so that your anti-virus software can check it before you open it.)
Do not buy anything or give to any charity promoted through spam. Spammers often swap or sell the e-mail addresses of those who have bought from them, so buying something through spam may result in even more spam. Plus, spammers can make their living (and a lucrative one, too) on people's purchases of their offerings. Resist the temptation to buy products through spam, and help to put spammers out of business.
Do not forward chain e-mail messages. Not only do you lose control over who sees your e-mail address, but you also may be furthering a hoax or aiding in the delivery of a virus. Plus, there are reports that spammers start chain letters expressly to gather e-mail addresses. If you do not know whether a message is a hoax or not, a site like Hoaxbusters can help you separate fact from fiction.

FIGURE T1.6
What to Do With Spam

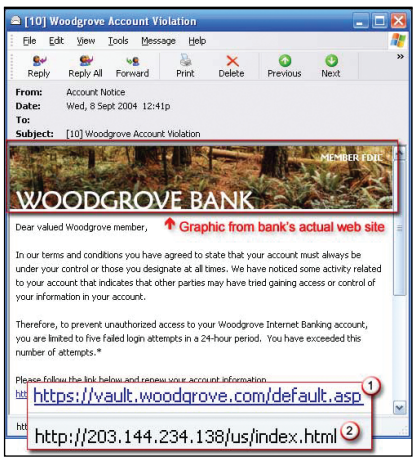
they are legitimate. Unsuspecting people too often respond to these requests for their credit card numbers, passwords, account information, or other personal data.

WHAT DOES A PHISHING SCAM LOOK LIKE?

As scam artists become more sophisticated, so do their phishing e-mail messages and pop-up windows. They often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites. Figure T1.7 shows what a phishing scam e-mail message might look like.

If you receive an e-mail message from Microsoft asking you to update your credit card information because of a recent change in Microsoft policy, please do not respond. This is a scam that is designed to steal your money or to install unwanted software on your computer that may have the ability to spy on you while you surf the Internet. Even though it may appear that Microsoft sent these e-mail messages, it did not. Microsoft does not send unsolicited e-mail requesting personal or financial information.

FIGURE T1.7
Sample Phishing Scam E-Mail Message



HELP PREVENT IDENTITY THEFT FROM PHISHING SCAMS

Most phishing scams are sent through e-mail. By following the guidelines in Figure T1.8, you can help protect yourself from these tricky scams.

Detecting Spyware

Spyware is a general term used for software that performs certain behaviors such as advertising, collecting personal information, or changing

FIGURE T1.8
Preventing Phishing

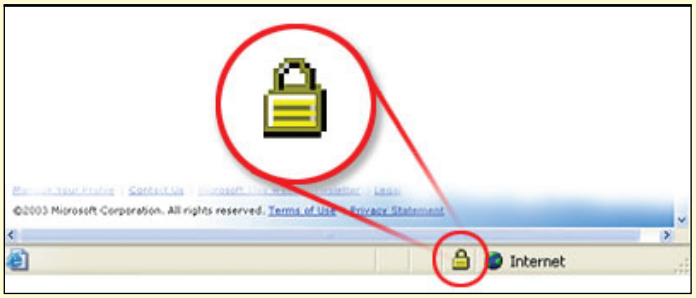
Tips for Preventing Phishing

Report suspicious e-mail. If you suspect you may have received phishing e-mail designed to steal your identity, report the e-mail to the faked or "spoofed" organization. Contact the organization directly—not through the e-mail you received—and ask for confirmation. If it would make you more comfortable, call the organization's toll-free number (if one exists) and speak to a customer service representative. You should also report the e-mail to the proper authorities including the FBI, the Federal Trade Commission (FTC), and the Anti-phishing Working Group.

Be wary of clicking on links in e-mail messages. Links in phishing e-mail messages often take you directly to phony sites where you could unwittingly transmit personal or financial information to con artists. Avoid clicking on a link in an e-mail message unless you are sure of the destination. Even if the address bar displays the correct Web address, do not risk being fooled. Con artists can display a fake URL in the address bar on your browser.

Type addresses directly into your browser or use your personal bookmarks. If you need to update your account information or change your password, visit the Web site by using your personal bookmark or by typing the URL directly into your browser.

Check the security certificate when you are entering personal or financial information into a Web site. Before you enter personal or financial information into a Web site, make sure the site is secure. In Internet Explorer, you can do this by checking the yellow lock icon on the status bar as shown below.



If the lock icon is closed, this signifies that the Web site uses encryption to help protect any sensitive, personal information that you enter, such as your credit card number, Social Security number, or payment details. This symbol does not need to appear on every page of a site, only on those pages that request personal information. Unfortunately, even the lock symbol can be faked. To help increase your safety, double-click the lock icon to display the security certificate for the site. The name following **Issued to** should match the name of the site. If the name differs, you may be on a fake site, also called a "spoofed" site. If you are not sure whether a certificate is legitimate, do not enter any personal information. Play it safe and leave.

Do not enter personal or financial information into pop-up windows. One common phishing technique is to launch a fake pop-up window when someone clicks on a link in a phishing e-mail message. To make the pop-up window look more convincing, it may be displayed over a window you trust. Even if the pop-up window looks official or claims to be secure, you should avoid entering sensitive information, because there is no way to check the security certificate. Close pop-up windows by clicking on the red X in the top right corner (a "cancel" button may not work as you would expect).

the configuration of your computer, generally without appropriately obtaining your consent. You might have spyware or other unwanted software on your computer if:

- You see pop-up advertisements even when you are not on the Web.
- The page your Web browser first opens to or your browser search settings have changed without your knowledge.
- You notice a new toolbar in your browser that you didn't want, and find it difficult to get rid of.

- Your computer takes longer than usual to complete certain tasks.
- You experience a sudden rise in computer crashes.

Spyware is often associated with software that displays advertisements (called *adware*) or software that tracks personal or sensitive information. That does not mean all software that provides ads or tracks your online activities is bad. For example, you might sign up for a free music service, but "pay" for the service by agreeing to receive targeted ads. If you understand the terms and agree to them, you may have decided that it is a fair trade-off. You might also agree to let the company track your online activities to determine which ads to show you.

Other kinds of unwanted software will make changes to your computer that can be annoying and can cause your computer to slow down or crash. These programs have the ability to change your Web browser's home page or search page, or add additional components to your browser you do not need or want. These programs also make it very difficult for you to change your settings back to the way you originally had them. These types of unwanted programs are also often called spyware.

The key in all cases is whether or not you (or someone who uses your computer) understand what the software will do and have agreed to install the software on your computer.

Spyware or other unwanted software can get on your system in a number of ways. A common trick is to covertly install the software during the installation of other software you want such as a music or video file-sharing program. Whenever you are installing something on your computer, make sure you carefully read all disclosures, including the license agreement and privacy statement. Sometimes the inclusion of unwanted software in a given software installation is documented, but it may appear at the end of a license agreement or privacy statement.

PREVENTING SPYWARE

Figure T1.9 displays a list of actions that can be taken to help prevent spyware infections.

Tips for Preventing Spyware
1. Ensure that desktop settings are configured to prompt you whenever a Web site tries to install a new program or Active X control. If possible, configure your browser to reject Active X controls to lessen the likelihood that spyware could be installed on your computer through normal Internet browsing.
2. Keep your desktop systems up-to-date with security patches. Several spyware programs take advantage of known vulnerabilities that, if patched, would limit the spyware's effectiveness.
3. Install and maintain current versions of anti-virus and anti-spyware programs.
4. Expand the risk-assessment process to consider threats from spyware. This ensures that all risks to private information are considered and appropriate steps are taken to mitigate those risks.
5. Install and configure firewalls to monitor all traffic (discussed later in this plug-in).
6. Implement tools to filter out spam and viruses from incoming e-mail. E-mail scanning can limit the likelihood that you could unknowingly infect your computer by viewing or reading e-mail that contains spyware. Filtering outbound e-mail for viruses also gives you an alert that an internal computer is infected.
7. Implement tools to restrict or prevent pop-up windows. This limits the likelihood that spyware will be downloaded through pop-up windows, either automatically or through user error.

FIGURE T1.9
Preventing Spyware

HOW TO GET RID OF SPYWARE

Many kinds of unwanted software, including spyware, are designed to be difficult to remove. If you try to uninstall this software like any other program, you might find that the program reappears as soon as you restart your computer. If you are having trouble uninstalling unwanted software, you may need to download a tool to do the job for you. Several companies offer free and low-cost software that will check your computer for spyware and other unwanted software and help you remove it.

Some ISPs include antispyware software in their service packages. Check with your ISP to see if it can recommend or provide a tool. Keep in mind that removing unwanted software with these tools may mean you will no longer be able to use a free program that came with the spyware.

To remove spyware:

1. Download a spyware removal tool (such as Microsoft Windows AntiSpyware).
2. Run the tool to scan your computer for spyware and other unwanted software.
3. Review the files discovered by the tool for spyware and other unwanted software.
4. Select suspicious files for removal by following the tool's instructions.

Restricting Instant Messages

Like e-mail viruses, instant message viruses are malicious or annoying programs that are designed to travel through IM. In most cases, these viruses are spread when a person opens an infected file that was sent in an instant message that appeared to come from a friend. Figure T1.10 provides an example of what an IM virus sent through an infected file might look like.

When unsuspecting people open these files, their computers can become infected with a virus. Because of the virus, their computers may slow down or stop responding, or they may not notice any change. However, the virus might have installed a covert program on the computer that could damage software, hardware, or important files, and that may include spyware, which can track information entered on a computer.

A computer infected by a virus may continue to spread the infection by sending copies of the virus to everyone on your IM contact list. A contact list is the collection of IM names (similar to an e-mail address book) that you can store in your IM program. As with most threats on the Internet, you can help keep yourself safe by taking basic precautions. If you know how to avoid e-mail viruses, you will already be familiar with many of the steps highlighted in Figure T1.11 and Figure T1.12.

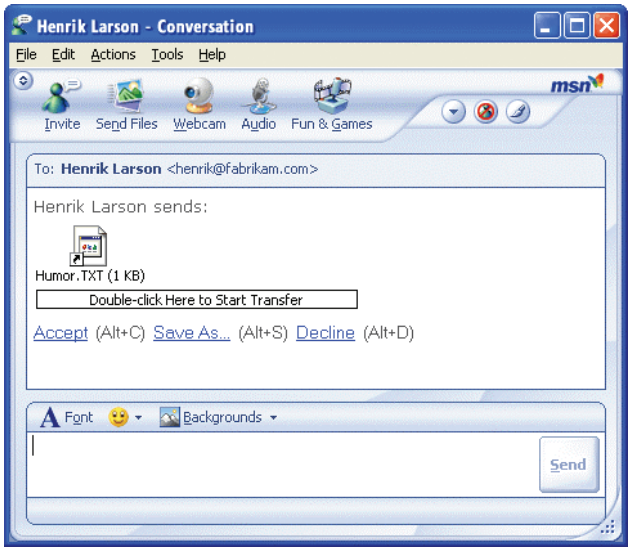


FIGURE T1.10
Sample IM Virus

Increasing PC Performance

To maintain your computer and keep it running smoothly, follow these guidelines:

- Free disk space.
- Speed up access to data.
- Detect and repair disk errors.

FREE DISK SPACE

By freeing disk space, you can improve the performance of your computer. The Disk Cleanup tool, a utility that comes installed with Microsoft Windows, helps free space on your hard disk. The utility identifies files

Steps to Help Avoid Instant Message Viruses
Be careful downloading files in IM. Never open, accept, or download a file in IM from someone you do not know. If the file comes from someone you do know, do not open it unless you know what the file is and you were expecting it. Contact the sender by e-mail, phone, or some other method to confirm that what was sent was not a virus.
Update your Windows software. Visit the Windows Update Web site to scan your computer and install any high-priority updates that are offered. If you have Automatic Updates enabled, the updates are delivered to you when they are released, but you have to make sure you install them.
Make sure you are using an updated version of your IM software. Using the most up-to-date version of your IM software can better protect your computer against viruses and spyware. If you are using MSN Messenger, install the updated version by visiting the MSN Messenger Web site and clicking the **Download Now!** button.
Use anti-virus software and keep it updated. Anti-virus software can help to detect and remove IM viruses from your computer, but only if you keep the anti-virus software current. If you have purchased a subscription from an anti-virus software company, your anti-virus software may update itself when you are connected to the Internet.
Use anti-spyware software and keep it updated. Some IM viruses may install spyware or other unwanted software on your computer. Anti-spyware software can help to protect your computer from spyware and remove any spyware you may already have.

FIGURE T1.11
How to Avoid Instant Message Viruses

that you can safely delete, and then enables you to choose whether you want to delete some or all of the identified files. You can use the Disk Cleanup Utility to:

- Remove temporary Internet files.
- Remove downloaded program files (such as Microsoft ActiveX controls and Java applets).

Tips for Safer Instant Messaging
Never give out sensitive personal information, such as your credit card number, Social Security number, or passwords, in an IM conversation.
Only communicate with people on your Contact List or Buddy List.
Never agree to meet a stranger in person whom you have met on IM.
Never accept files or downloads from people you do not know. Never accept files that you were not expecting from people you do know.
Each IM program assigns you a name, not unlike an e-mail address. This name is usually called a screen name. Choose a name that does not give away your personal information. For example, use SassySue instead of DetroitSue.
Just like an e-mail address, do not post your screen name online. People might find it and use it to send you unsolicited IM messages.
Do not send personal or private instant messages at work. Your boss may have a right to view those messages.
Most instant message programs allow you to automatically log on when you start your computer so that you do not have to enter your password every time you want to use the program. If you use a public computer, make sure not to configure your IM program for automatic log-on.
Be careful how you reveal when you are online or not. IM programs allow people on your contact list to see if you are available. However, using this feature may offer people more information about you than you feel comfortable giving. Windows Messenger and MSN Messenger both allow you to control how you appear to people on your contact list.

FIGURE T1.12
Safer Instant Messaging

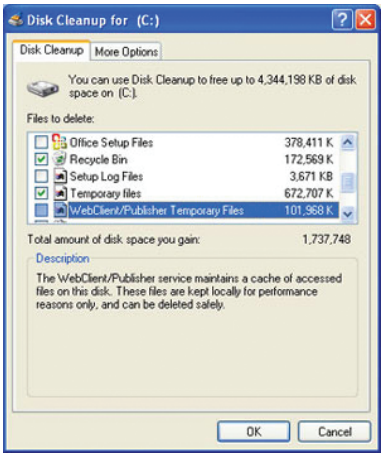


FIGURE T1.13
Disk Cleanup Dialog Box

- Empty the Recycle Bin.
- Remove Windows temporary files.
- Remove optional Windows components that you do not use.
- Remove installed programs that you no longer use.

(**Note:** Typically, temporary Internet files take the most amount of space because the browser caches each page you visit for faster (later) access.)

To Use Disk Cleanup

1. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Disk Cleanup.**
2. If several drives are available, you might be prompted to specify which drive you want to clean.
3. Disk Cleanup calculates the amount of space you will be able to free.
4. In the **Disk Cleanup for** dialog box, scroll through the content of the **Files to delete** list.
5. Choose the files that you want to delete, as displayed in Figure T1.13.
6. Clear the check boxes for files that you do not want to delete, and then click **OK**.
7. When prompted to confirm that you want to delete the specified files, click **Yes**.
8. After a few minutes, the process completes and the Disk Cleanup dialog box closes.

SPEED UP ACCESS TO DATA

Disk fragmentation slows the overall performance of your system. When files are fragmented, the computer must search the hard disk when the file is opened to piece it back together. The response time can be significantly longer. Disk Defragmenter is a Windows utility that consolidates fragmented files and folders on your computer's hard disk so that each occupies a single space on the disk. With your files stored neatly end-to-end, without fragmentation, reading, and writing to the disk speeds up.

When to Run Disk Defragmenter

In addition to running Disk Defragmenter at regular intervals, optimally monthly, certain events warrant running the utility outside of the normal interval. You should run Disk Defragmenter when:

- You add a large number of files.
- Your free disk space nears 15 percent.
- You install new programs or a new version of Windows.

To Use Disk Defragmenter

1. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Disk Defragmenter**.
2. Click **Analyze** to start the Disk Defragmenter (see Figure T1.14).
3. In the **Disk Defragmenter** dialog box, click the drives that you want to defragment, and then click the **Analyze** button.

After the disk is analyzed, a dialog box appears, letting you know whether you should defrag the analyzed drives. **Tip:** You should analyze a volume before defragmenting it to get an estimate of how long the defragmentation process will take.

4. To defragment the selected drive or drives, click the **Defragment** button.
5. After the defragmentation is complete, Disk Defragmenter displays the results.

6. To display detailed information about the defragmented disk or partition, click **View Report.**
7. To close the **View Report** dialog box, click **Close**.
8. To close the Disk Defragmenter utility, click the **Close** button on the title bar of the window.

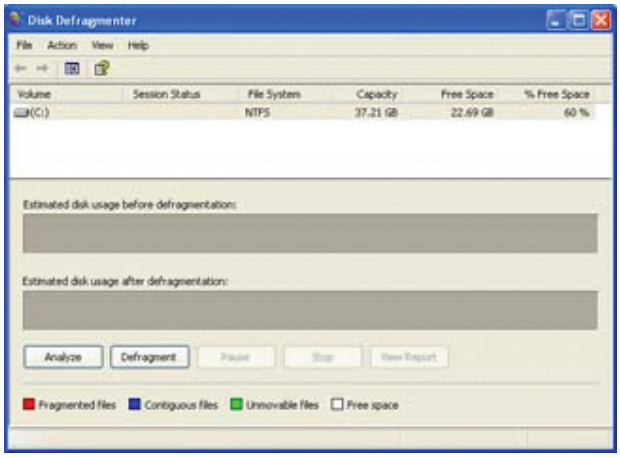


FIGURE T1.14
Disk Defragmenter Dialog Box

DETECT AND REPAIR DISK ERRORS

In addition to running Disk Cleanup and Disk Defragmenter to optimize the performance of your computer, you can check the integrity of the files stored on your hard disk by running the Error Checking utility. As you use your hard drive, it can develop bad sectors. Bad sectors slow down hard disk performance and sometimes make data writing (such as file saving) difficult, or even impossible. The Error Checking utility scans the hard drive for bad sectors, and scans for file system errors to see whether certain files or folders are misplaced. If you use your computer daily, you should try to run this utility weekly to help prevent data loss.

To Run the Error Checking Utility

1. **Important:** Be sure to close all files before running the Error Checking utility.
2. Click **Start**, and then click **My Computer**.
3. In the My Computer window, right-click the hard disk you want to search for bad sectors, and then click **Properties**.
4. In the **Properties** dialog box, click the **Tools** tab.
5. Click the **Check Now** button.
6. In the **Check Disk** dialog box, select the **Scan for and attempt recovery of bad sectors** check box, and then click **Start** (see Figure T1.15).
7. If bad sectors are found, you will be prompted to fix them.

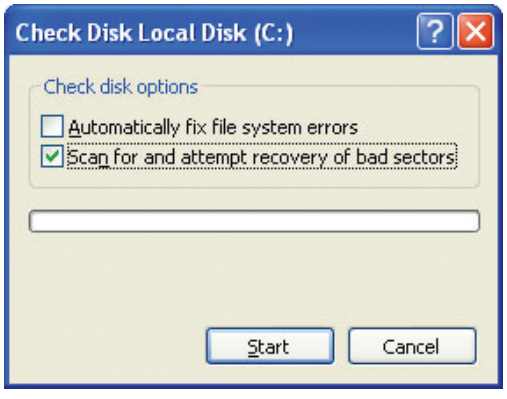
   (**Note:** Only select the **Automatically fix file system errors** check box if you think that your disk contains bad sectors.)

Using Anti-Virus Software

The Internet is an excellent resource, and no doubt has changed the way most people communicate. Unfortunately the Internet, e-mail in particular, has created an easy medium for the spread of computer viruses, which can cause chaos to whole networks of computers.

A *virus* is basically a malicious computer program. The effects of viruses differ, some either modify, delete, or steal data, and others may give control of your PC over to their creators via the Internet. One thing they all have in common is that if you get infected and you don't have anti-virus software, you might not know you have it until it is too late.

FIGURE T1.15
Check Disk Dialog Box



A *worm* refers to a virus that can replicate and spread by itself over a network (the Internet for instance). These are getting very common and are among the biggest troublemakers on the Internet.

A virus or worm can sit on a computer for months (potentially even years) without doing anything and then be triggered by a certain date and time to do what it has been designed to do. As these viruses and worms become more advanced, the need for anti-virus software has never been so great.

Like its biological equivalent, a computer virus is a program that spreads unwanted and unexpected actions through the

insides of a computer. Not all viruses are malicious, but many are written to damage particular types of files, applications, or operating systems.

The results of virus infections vary according to the maliciousness of the author. Many viruses are designed only to spread from file to file and therefore from computer to computer without any serious damage. The only real effect to an end user is loss of credibility when an e-mail to a customer or a friend is rejected by an anti-virus program. But many viruses carry sinister payloads. Some actively destroy files, some overwrite the boot sectors on disks to render computers unbootable, and an increasing number install backdoor programs that allow virus writers to take control of computers remotely. Computers with backdoor software installed are called *zombies* and are often used for computer crime such as distributed denial of service (DDoS) attacks. There are three main types of viruses in circulation: (1) boot sector viruses, (2) macro viruses, and (3) file infecting viruses. Figure T1.16 explains each of these in detail.

ANTI-VIRUS SOFTWARE

Anti-virus (AV) is a term applied to either a single program or a collection of programs that protect a computer system from viruses. Anti-virus software is designed to keep your PC free of computer viruses and worms. It does so by scanning your PC's file system looking for known viruses; if a virus is found, the software will inform you and then take steps to remove the virus threat.

FIGURE T1.16
Types of Viruses

Type of Virus	Definition
Boot sector viruses	The boot sector is the very first sector on a floppy or hard disk. It contains executable code that helps to operate the PC. Because the PC's hard disk boot sector is referred to every time the PC powers or "boots" up, and is rewritten whenever you configure or format the setup of the system, it is a vulnerable place for viruses to attack. Boot sector viruses are usually spread through the boot sector of floppy disks left in disk drives when systems are rebooted. From there, they infect the boot sector of hard disks, loading themselves into memory each time the system is booted and waiting for an opportunity to write themselves to more disks to spread. This kind of virus can prevent you from being able to boot your hard disk.
Macro viruses	Macro viruses are by far the most common viruses in circulation, accounting for about 75 percent of viruses found "in the wild." These can be obtained through disks, a network, the Internet, or an e-mail attachment. Macro viruses do not directly infect programs, but instead, infiltrate the files from applications that use internal macro programming languages, such as Microsoft Excel or Word documents. They are then able to execute commands when the infected file is open, which spreads the virus to other vulnerable documents. In turn, users who share files can also spread the virus to other systems.
File infecting viruses	File infecting viruses infect executable files, such as EXE and COM files. Once the original infected program is run, the virus transfers to your computer's memory and may replicate itself further, spreading the infection. These viruses can be spread beyond the infected system as soon as the infected file or program is passed to another computer. The simplest of these viruses work by overwriting part of the program they are infecting. These can thankfully be caught early, because the program rarely continues to work as it should. More sophisticated versions hide their presence by saving the program or file's original instructions so that these are executed even after infection. This type may not be noticed until it is too late and enters the attack phase.

Good anti-virus software will automatically check any files being transferred to and from a computer; any anti-virus software should at least scan attachments of incoming e-mails automatically (even if the option can be turned off).

The intricate details of each anti-virus program vary, but all share the basic responsibility of identifying virus-laden files using *virus signature files*: a unique string of bytes that identifies the virus like a fingerprint. They view patterns in the data and compare them to traits of known viruses captured "in the wild" to determine if a file is infected, and in most cases are able to strip the infection from files, leaving them undamaged. When repairs are not possible, anti-virus programs will quarantine the file to prevent accidental infection, or they can be set up to delete the file immediately.

In the case of new viruses for which no antidote has been created, some anti-virus programs also use heuristic scanning. *Heuristic scanning* allows the anti-virus programs to flag suspicious data structures or unusual virus-like activity even when there is no matching virus definition. If the program sees any funny business, it quarantines the questionable program and broadcasts a warning to you about what the program may be trying to do (such as modify your Windows Registry). The accuracy of such methods is much lower, however, and often a program with this running may err on the side of caution. This can result in confusing false positive results.

If you and the software think the program may be a virus, you can send the quarantined file to the anti-virus vendor, where researchers examine it, determine its signature, name and catalog it, and release its antidote.

Virus Definition Files

Anti-virus software usually works by checking a file for certain patterns of binary code. The patterns used to identify viruses are stored in what is known as a *virus definition file*. When a new virus comes out, the virus definition file needs to be updated to include the new pattern.

The importance of keeping these definition files updated cannot be overstated. Basically, anti-virus software without updated definition files is useless.

Most anti-virus software will update these files automatically (or at least have the option to do so). The update of the definition files is usually achieved by having the software connect via the Internet to the vendor's Web site, and then downloading and installing the latest virus definition files. This is why it is important to purchase anti-virus software from an established company. Imagine you bought anti-virus protection and then six months later the company went bankrupt; you would have nowhere to get your virus definition updates. If you do not have anti-virus software, then check out these anti-virus products from established developers:

- McAfee VirusScan (www.mcafee.com).
- Norton Anti-virus (www.symantec.com).

Figure T1.17 displays an example of Norton Anti-virus after it has completed a virus scan of a hard drive.

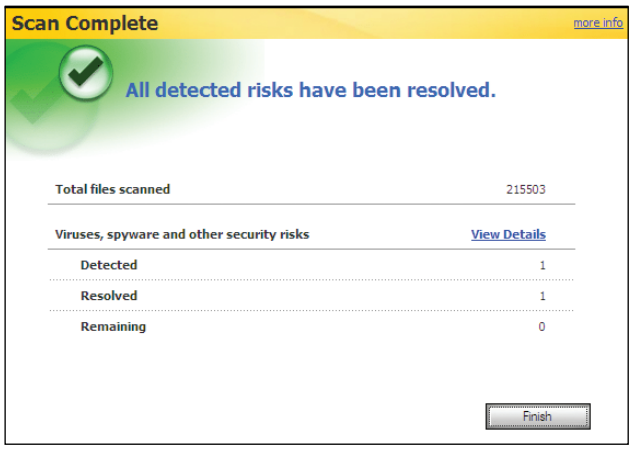


FIGURE T1.17
Norton Anti-Virus

CELL PHONE VIRUSES

Cabir, the world's first known cell phone virus, was found on the cell phone of a private user in 2004; however, it did not get very far. Cabir infected only a small number of Bluetooth-enabled phones and carried out no malicious action—a group of malware developers created Cabir to prove it could be done. *Malware*, short for malicious software, is designed specifically to damage or disrupt a system, such as a virus. The group's

next step was to send it to anti-virus researchers, who began developing a solution to a problem that promises to get a lot worse.

Cell phone viruses are at the threshold of their effectiveness. At present, they cannot spread very far and they don't do much damage, but the future might see cell phone bugs that are as debilitating as computer viruses.

A cell phone virus is basically the same thing as a computer virus—an unwanted executable file that "infects" a device and then copies itself to other devices. However, whereas a computer virus or worm spreads through e-mail attachments and Internet downloads, a cell phone virus or worm spreads via Internet downloads, MMS (multimedia messaging service) attachments, and Bluetooth transfers. The most common type of cell phone infection now occurs when a cell phone downloads an infected file from a PC or the Internet, but phone-to-phone viruses are on the rise.

Current phone-to-phone viruses almost exclusively infect phones running the *Symbian* operating system. The large number of proprietary operating systems in the cell phone world is one of the obstacles to mass infection. Cell phone virus writers have no Windows-level market share to target, so any virus will affect only a small percentage of phones.

Infected files usually show up disguised as applications such as games, security patches, add-on functionalities, and, of course, pornography and free stuff. Infected text messages sometimes steal the subject line from a message you have received from a friend, which increases the likelihood of you opening it, but opening the message is not enough to get infected. You have to choose to open the message attachment and agree to install the program, which is another obstacle to mass infection. The installation obstacles and the methods of spreading limit the amount of damage the current generation of cell phone virus can do.

Installing a Personal Firewall

A *firewall* is a barrier to keep destructive forces away from your property. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next.

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into a computer. If an incoming packet of information is flagged by the filters, it is not allowed through.

Say that you work at a company with 500 employees. The company has hundreds of computers that are all connected. In addition, the company will have one or more connections to the Internet through something like T1 or T3 lines. Without a firewall, all of those hundreds of computers are directly accessible to anyone on the Internet. An outsider can probe those computers and try to make connections to them. If one employee makes a mistake and leaves a security hole, hackers can get to the machine and exploit the hole.

With a firewall in place, the landscape is much different. A company should place a firewall at every connection to the Internet (for example, at every T1 line coming into the company). The firewall can implement security rules. For example, one of the security rules inside the company might be "out of the 500 computers inside this company, only one of them is permitted to receive public FTP traffic. Allow FTP connections only to that one computer and prevent them on all others."

A company can set up rules like this for FTP servers, Web servers, Telnet servers, and the like. In addition, the company can control how employees connect to Web sites, whether files are allowed to leave the company over the network, and so on. A firewall gives a company tremendous control over how people use the network.

A variety of firewall software applications are available, including ZoneAlarm (www.zonealarm.com), which is free for download. Microsoft has improved the

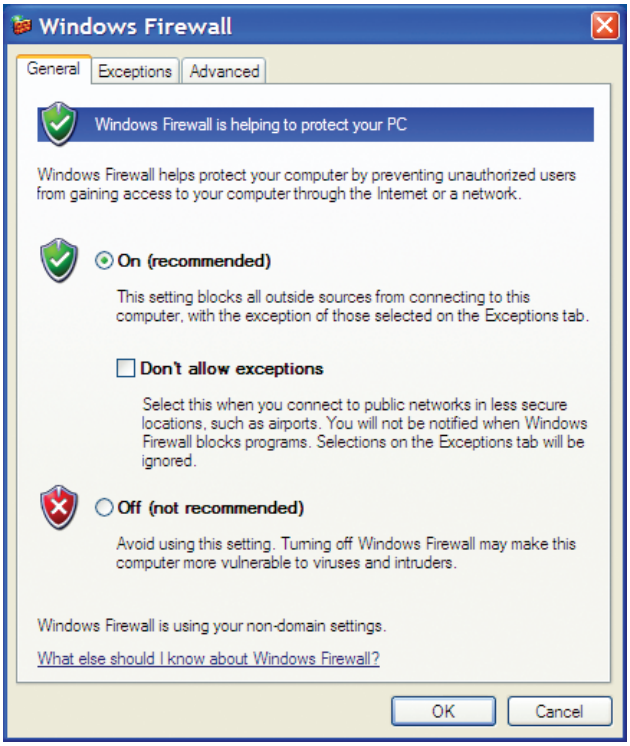


FIGURE T1.18
Windows Firewall Settings

firewall software in Windows XP Service Pack 2, which is turned on by default. However, some computer manufacturers and network administrators might turn it off.

TO OPEN WINDOWS FIREWALL

1. Click **Start** and then click **Control Panel**.
2. Click **Windows Firewall** (see Figure T1.18).

Figure T1.19 displays a list of some things firewalls do and do not do.

It Does	It Does Not
Help block computer viruses and worms from reaching a computer.	**Detect or disable computer viruses and worms** if they are already on a computer.
Ask for your permission to block or unblock certain connection requests.	**Stop you from opening e-mail with dangerous attachments**.
Create a record (a security log) that records successful and unsuccessful attempts to connect to a computer. This can be useful as a troubleshooting tool.	**Block spam or unsolicited e-mail** from appearing in an e-mail inbox. However, some e-mail programs can help do this.

FIGURE T1.19
What Windows Firewall Does and Does Not Do

PLUG-IN SUMMARY

This plug-in covered a number of things to do to keep your personal computer running effectively and efficiently, such as:

- Creating strong passwords.
- Performing good file management.
- Implementing effective backup and recovery strategies.
- Using Zip files.
- Writing professional e-mails.
- Stopping spam.
- Preventing phishing.
- Detecting spyware.
- Restricting instant messaging.
- Increasing PC performance.
- Using anti-virus software.
- Installing a personal firewall.

MAKING BUSINESS DECISIONS

1. Third-Party Backup Utilities

Because of the importance of data backup, numerous companies produce specialized backup software. Backup utilities offer advanced features in the following areas to differentiate it from the Windows Backup utility and from software included with CD and DVD burners:

- Support for all current media types, including all DVD formats, Zip disks, Pen storage, and so on.
- Highly specific backup selections, combinations of files and folders in any location.
- On-the-fly compression of files, to provide reduced file sizes in the backup.
- Automatic comparisons of data after the backup, taking a number of forms.
- Support for multi-CD or multi-DVD backups, with a single backup spanning as many discs as necessary.
- Detailed backup schedulers.
- Detailed methods of including or excluding file types.
- Backup from remote computers.

In addition, some backup utilities now include the technology known as *ghost imaging*, or just plain *ghosting*. A ghost image captures the entire hard drive, backing it up to the point where you can restore your entire system from it.

Search the Internet to find different third-party utilities that perform backup, restore, and ghosting. List the features and prices of each.

2. Spybot Search & Destroy

Debuting in 2002, Spybot Search & Destroy has gained the reputation as one of the best stand-alone spyware detectors, monitors, and removers in the business. Spybot Search & Destroy is available free, although the Web site (www.safer-networking.org) asks for a donation to defray

development costs. Download and install the latest version of Spybot (www.safer-networking.org/en/download/index.html). Run the application to scan for spyware, adware, hijackers, and other malicious software. Installation is simple and fast (although you should create a Restore Point with System Restore before doing so, in case you want to reverse the process). Note how many references to spyware and adware the application finds.

3. Firewall Utilities

You have a good range of excellent choices when it comes to firewall protection. In addition to commercial products such as Symantec, McAfee, and Trend Micro, which include firewall protection as part of their security suites or as stand-alone products, Microsoft has a firewall that ships as part of SP1 and SP2.

Perhaps the best known of the stand-alone firewall utilities is ZoneAlarm (www.zonealarm.com), which offers its firewall as a free product as well as a purchasable product, ZoneAlarm Pro, with additional features (including e-mail security).

Other firewall products operate similarly to those already mentioned. Kerio Personal Firewall (www.kerio.com) makes your desktop invisible to outside intruders, blocks pop-up windows and banner ads, and detects a wealth of hacker intrusions. Kerio specializes in enterprise-level products, and its desktop firewall products take advantage of that specialization. Tiny Software (www.tinysoftware.com), recently acquired by industry giant Computer Associates, offers Tiny Firewall, which watches all network activity, establishes intrusion protection as you work, and offers a tool called Track `n' Reverse, which lets you see any changes to your files or your registry and reverse them so that your system is as it was before. Think of this as a kind of System Restore at the microlevel.

Another full-featured product is Sygate Personal Firewall (www.sygate.com), available as a free download for the Standard version or by purchase for the Pro version. Sygate's product offers an especially usable interface and an out-of-the-box configuration that makes it easy for even beginners to get a firewall established.

Download one of the free firewall products mentioned above and try them.

4. Testing Your Setup

How do you know you are actually safe?

- To test your firewall, visit Gibson Research Corporation (www.grc.com) and follow the links to ShieldsUp! This site runs numerous free, fast online tests of common vulnerabilities.
- Another free online tester can be found at www.pcflank.com.
- You can also test your browser's vulnerabilities by using the Browser Security Test (bcheck.scanit.be/bcheck).
- GFi will send a free series of e-mail messages to you with attachments intended to expose holes in your e-mail software (gfi.com/emailsecuritytest).
- Microsoft has a free, heavy-duty Baseline Security Analyzer (www.microsoft.com/technet/security/tools/mbsahome.mspx) available for download. It is intended to detect common security misconfigurations and missing security updates on your computer systems.

5. Scanning from the Web

It is not actually necessary to purchase an anti-virus package if all you want to do is check your PC's current virus situation. Increasingly, anti-virus vendors are offering scanning of your PC directly from their Web sites, a process that tends to take a bit longer than local scanning but which has four major benefits:

1. You can successfully scan a PC that does not have the latest virus definition files installed locally.
2. You are always assured of the most up-to-date virus scan possible.

3. You can scan PCs on which, for whatever reason, you cannot install anti-virus software.
4. You can get a second opinion to see if the results are different from those of your installed anti-virus program.

Go to Trend Micro's Housecall, the online free virus scan corresponding to their PC-cillin product (www.trendmicro.com). You need to agree to a download of an ActiveX control to have the virus-scanning software start; this is one of two apparent strikes against this method of virus checking. Since some of the fear surrounding spyware is precisely the vulnerability of your PC to software placed on your hard drives from outside, it seems counterintuitive from a security standpoint to allow an ActiveX control to install itself on your PC and then allow that control to scan all the files on your system.

[1]www.microsoft.com/presspass/press/2003/nov03/11-17ComdexAntiSpamPR.mspx, accessed on February 2, 2006.
[2]www.microsoft.com/athome/security/email/aboutspam.mspx, accessed on February 22, 2006.