CHAPTER 26

Securing Computers

In this chapter, you will learn how to

- Explain the threats to your computers and data
- Describe key security concepts and technologies
- Explain how to protect computers from network threats

Your PC is under siege. Through your PC, a malicious person can gain valuable information about you and your habits. He can steal your files. He can run programs that log your keystrokes and thus gain account names and passwords, credit card information, and more. He can run software that takes over much of your computer processing time and use it to send spam or steal from others. The threat is real and right now. Worse, he's doing one or more of these things to your clients as I write these words. You need to secure your computer and your users from these attacks.

But what does computer security mean? Is it an antivirus program? Is it big, complex passwords? Sure, it's both of these things, but what about the fact that your laptop can be stolen easily?

To secure computers, you need both a sound strategy and proper tactics. From a strategic sense, you need to understand the threat from unauthorized access to local machines as well as the big threats posed when computers go onto networks. Part of the big picture means to know what policies, software, and hardware to put in place to stop those threats. From a tactical in-the-trenches sense, you need to master the details, to know how to implement and maintain the proper tools. Not only do you need to install antivirus programs in your users' computers, for example, but you also need to update those programs regularly to keep up with the constant barrage of new viruses.

Analyzing Threats

Threats to your data and PC come from two directions: accidents and malicious people. All sorts of things can go wrong with your computer, from users getting access to folders they shouldn't see to a virus striking and deleting folders. Files can be deleted, renamed, or simply lost. Hard drives can die, and optical discs get scratched and rendered unreadable. Accidents happen and even well-meaning people can make mistakes.

Unfortunately, a lot of people out there intend to do you harm. Add that intent together with a talent for computers, and you have a deadly combination. Let's look at the following issues:

- Unauthorized access
- Data destruction, accidental or deliberate
- Administrative access
- Catastrophic hardware failures
- Viruses/spyware

Historical/Conceptual

Unauthorized Access

Unauthorized access occurs when a person accesses resources without permission. Resources in this case mean data, applications, and hardware. A user can alter or delete data; access sensitive information, such as financial data, personnel files, or e-mail messages; or use a computer for purposes the owner did not intend.

Not all unauthorized access is malicious—often this problem arises when users who are randomly poking around in a computer discover that they can access resources in a fashion the primary user did not intend. Unauthorized access becomes malicious when outsiders knowingly and intentionally take advantage of weaknesses in your security to gain information, use resources, or destroy data!

One of the ways to gain unauthorized access is through intrusion. You might imagine someone kicking in a door and hacking into a computer, but more often than not it's someone sitting at a home computer, trying various passwords over the Internet. Not quite as glamorous, but still.…

Dumpster diving is the generic term for anytime a hacker goes through your refuse, looking for information. This is also a form of intrusion. The amount of sensitive information that makes it into any organization's trash bin boggles the mind! Years ago, I worked with an IT security guru who gave me and a few other IT people a tour of our office's trash. In one 20-minute tour of the personal wastebaskets of one office area, we had enough information to access the network easily, as well as to embarrass seriously more than a few people. When it comes to getting information, the trash is the place to look!

Social Engineering

Although you're more likely to lose data through accident, the acts of malicious users get the vast majority of headlines. Most of these attacks come under the heading of *social engineering*—the process of using or manipulating people inside the networking environment to gain access to that network from the outside—which covers the many ways humans can use other humans to gain unauthorized information.

This unauthorized information may be a network login, a credit card number, company customer data—almost anything you might imagine that one person or organization may not want a person outside of that organization to access.

Social engineering attacks aren't hacking—at least in the classic sense of the word—although the goals are the same. Social engineering means people attacking an organization through the people in the organization or physically accessing the organization to get the information they need. Following are a few of the more classic types of social engineering attacks.

NOTE It's common for social engineering attacks to be used together, so if you discover one of them being used against your organization, it's a good idea to look for others.

Infiltration

Hackers can physically enter your building under the guise of someone who might have a legitimate reason for being there, such as cleaning personnel, repair technicians, or messengers. They then snoop around desks, looking for whatever they can find. They might talk with people inside the organization, gathering names, office numbers, and department names—little things in and of themselves but powerful tools when combined later with other social engineering attacks.

Dressing the part of a legitimate user—with fake badge and everything—enables malicious people to gain access to locations and thus potentially your data. Following someone through the door, for example, as if you belong, is called *tailgating*. Tailgating is a common form of infiltration.

Telephone Scams

Telephone scams are probably the most common social engineering attack. In this case, the attacker makes a phone call to someone in the organization to gain information. The attacker attempts to come across as someone inside the organization and uses this to get the desired information. Probably the most famous of these scams is the "I forgot my user name and password" scam. In this gambit, the attacker first learns the account name of a legitimate person in the organization, usually using the infiltration method. The attacker then calls someone in the organization, usually the help desk, in an attempt to gather information, in this case a password.

> **Hacker:** "Hi, this is John Anderson in accounting. I forgot my password. Can you reset it, please?"
>
> **Help Desk:** "Sure, what's your user name?"
>
> **Hacker:** "j_w_Anderson"
>
> **Help Desk:** "OK, I reset it to e34rd3."

Certainly telephone scams aren't limited to attempts to get network access. There are documented telephone scams against organizations aimed at getting cash, blackmail material, or other valuables.

Phishing

Phishing is the act of trying to get people to give their usernames, passwords, or other security information by pretending to be someone else electronically. A classic example is when a bad guy sends you an e-mail that's supposed to be from your local credit card company asking you to send them your username and password. Phishing is by far the most common form of social engineering done today.

Data Destruction

Often an extension of unauthorized access, data destruction means more than just intentionally or accidentally erasing or corrupting data. It's easy to imagine some evil hacker accessing your network and deleting all your important files, but authorized users may also access certain data and then use that data beyond what they are authorized to do. A good example is the person who legitimately accesses a Microsoft Access product database to modify the product descriptions, only to discover that she can change the prices of the products, too.

This type of threat is particularly dangerous when users are not clearly informed about the extent to which they are authorized to make changes. A fellow tech once told me about a user who managed to mangle an important database when someone gave them incorrect access. When confronted, the user said: "If I wasn't allowed to change it, the system wouldn't let me do it!" Many users believe that systems are configured in a paternalistic way that wouldn't allow them to do anything inappropriate. As a result, users often assume they're authorized to make any changes they believe are necessary when working on a piece of data they know they're authorized to access.

Administrative Access

Every operating system enables you to create user accounts and grant those accounts a certain level of access to files and folders in that computer. As an administrator, supervisor, or root user, you have full control over just about every aspect of the computer. Windows XP, in particular, makes it entirely too easy to give users administrative access to the computer, especially Windows XP Home, which allows only two kinds of users: administrators and limited users. Because you can't do much as a limited user, most home and small office systems simply use multiple administrator accounts. If you need to control access, you really need to use non-Home versions of Windows.

System Crash/Hardware Failure

As with any technology, computers can and will fail—usually when you can least afford for it to happen. Hard drives crash, the power fails—it's all part of the joy of working in the computing business. You need to create redundancy in areas prone to failure (such as installing backup power in case of electrical failure) and perform those all-important data backups. Chapter 16, "Securing Windows Resources," goes into detail about using backups and other issues involved in creating a stable and reliable system.

Practical Application

EXAM TIP CompTIA considers security to be an extremely important topic, whether you're at the Essentials level or at Practical Application. Unlike other chapters, almost every single topic covered in the Practical Application section of this chapter *applies equally to the Essentials test*. In other words, you need to know everything in this chapter to pass either CompTIA A+ certification exam.

Physical Theft

A fellow network geek once challenged me to try to bring down his newly installed network. He had just installed a powerful and expensive firewall router and was convinced that I couldn't get to a test server he added to his network just for me to try to access. After a few attempts to hack in over the Internet, I saw that I wasn't going to get anywhere that way. So I jumped in my car and drove to his office, having first outfitted myself in a techy-looking jumpsuit and an ancient ID badge I just happened to have in my sock drawer. I smiled sweetly at the receptionist and walked right by my friend's office (I noticed he was smugly monitoring incoming IP traffic by using some neato packet-sniffing program) to his new server. I quickly pulled the wires out of the back of his precious server, picked it up, and walked out the door. The receptionist was too busy trying to figure out why her e-mail wasn't working to notice me as I whisked by her carrying the 65-pound server box. I stopped in the hall and called him from my cell phone.

Me (cheerily): "Dude, I got all your data!"

Him (not cheerily): "You rebooted my server! How did you do it?"

Me (smiling): "I didn't reboot it—go over and look at it!"

Him (really mad now): "YOU <EXPLETIVE> THIEF! YOU STOLE MY SERVER!"

Me (cordially): "Why, yes. Yes, I did. Give me two days to hack your password in the comfort of my home, and I'll see everything! Bye!"

I immediately walked back in and handed him the test server. It was fun. The moral here is simple: Never forget that the best network software security measures can be rendered useless if you fail to protect your systems physically!

Virus/Spyware

Networks are without a doubt the fastest and most efficient vehicles for transferring computer viruses among systems. News reports focus attention on the many virus attacks from the Internet, but a huge number of viruses still come from users who bring in programs on floppy disks, writable optical discs, and USB drives. The "Network Security"

section of this chapter describes the various methods of virus infection and what you need to do to prevent virus infection of your networked systems.

Security Concepts and Technologies

Once you've assessed the threats to your computers and networks, you need to take steps to protect those valuable resources. Depending on the complexity of your organization, this can be a small job encompassing some basic security concepts and procedures, or it can be exceedingly complex. The security needs for a three-person desktop publishing firm, for example, would differ wildly from those of a defense contractor supplying top-secret toys to the Pentagon.

From a CompTIA A+ certified technician's perspective, you need to understand the big picture (that's the strategic side), knowing the concepts and available technologies for security. At the implementation level (that's the tactical side), you're expected to know where to find such things as security policies in Windows. A CompTIA Network+ or CompTIA Security+ tech will give you the specific options to implement. (The exception to this level of knowledge comes in dealing with malicious software such as viruses, but we'll tackle that subject as the last part of the chapter.) So let's look at three concept and technology areas: access control, data classification and compliance, and reporting.

NOTE Part of establishing local control over resources involves setting up the computer properly in the first place, a topic covered in depth in Chapter 16, "Securing Windows Resources." The basic cornerstones of local control are authentication through user names and passwords and authorization through NTFS permissions. Groups are important for managing multiple users. Encryption is important, especially with a computer that might fall into the hands of a third party.

Access Control

Access is the key. If you can control access to the data, programs, and other computing resources, you've secured your systems. *Access control* is composed of four interlinked areas that a good security-minded tech should think about: physical security, authentication, users and groups, and security policies. Much of this you know from previous chapters, but this section should help tie it all together as a security topic.

Secure Physical Area and Lock Down Your System

The first order of security is to block access to the physical hardware from people who shouldn't have access. This isn't rocket science. Lock the door. Don't leave a PC unattended when logged in. In fact, don't ever leave a system logged in, even as a limited user. God help you if you walk away from a server still logged in as an administrator. You're tempting fate.

For that matter, when you see a user's computer logged in and unattended, do the user and your company a huge favor and lock the computer. Just walk up and press the WINDOWS LOGO KEY-L on the keyboard to lock the system. It works in all versions of Windows.

Authentication

Security starts with properly implemented *authentication*, which means in essence how the computer determines who can or should access it. And once accessed, what that user can do. A computer can authenticate users through software or hardware, or a combination of both.

Software Authentication: Proper Passwords It's still rather shocking to me to power up a friend's computer and go straight to his or her desktop, or with my married-with-kids friends, to click one of the parents' user account icons and not be prompted for a password. This is just wrong! I'm always tempted to assign passwords right then and there—and not tell them the passwords, of course—so they'll see the error of their ways when they try to log in next. I don't do it but always try to explain gently the importance of good passwords.

You know about passwords from Chapter 16, "Securing Windows Resources." Make sure you and your users use *strong passwords*: at least eight characters in length, including letters, numbers, and punctuation symbols. Don't let them write passwords down or tape them to the underside of their mouse pads either!

It's not just access to Windows that you need to think about. There's always the temptation for people to hack the system and do mean things, such as changing CMOS settings, opening up the case, and even stealing hard drives. Any of these actions render the computer inoperable to the casual user until a tech can undo the damage or replace components. All modern CMOS setup utilities come with a number of tools to protect your computer, such as drive lock, intrusion detection, and of course system access passwords such as the one shown in Figure 26-1. Refer to Chapter 7, "BIOS and CMOS," to refresh yourself on what you can do at a BIOS level to protect your computer.

Figure 26-1 CMOS access password request

Hardware Authentication Smart cards and biometric devices enable modern systems to authenticate users with more authority than mere passwords. *Smart cards* are credit-card-sized cards with circuitry that can identify the bearer of the card. Smart cards are relatively common for such tasks as authenticating users for mass transit systems, for example, but are fairly uncommon in computers. Figure 26-2 shows a smart card and keyboard combination.

People can guess or discover passwords, but forging someone's fingerprints is a lot harder. The keyboard in Figure 26-3 authenticates users on a local machine by using fingerprints. Other devices that will do the trick are key fobs, retinal scanners, and PC cards for laptop computers. Devices that require some sort of physical, flesh-and-blood authentication are called *biometric devices*.

Figure 26-2 Keyboard-mounted smart card reader being used for a commercial application (*photo courtesy of Cherry Corp.*)

Figure 26-3 Microsoft keyboard with fingerprint accessibility

NOTE How's this for full disclosure? Microsoft does not claim that the keyboard in Figure 26-3 offers any security at all. In fact, the documentation specifically claims that the fingerprint reader is an accessibility tool, not a security device. Because it enables a person to log on to a local machine, though, I think it falls into the category of authentication devices.

Clever manufacturers have developed key fobs and smart cards that use radio frequency identification (RFID) to transmit authentication information so users don't have to insert something into a computer or card reader. The Privaris plusID combines, for example, a biometric fingerprint fob with an RFID tag that makes security as easy as opening a garage door remotely! Figure 26-4 shows a plusID device.

NTFS, not FAT32!

The file system on a hard drive matters a lot when it comes to security. On a Windows machine with multiple users, you simply must use NTFS or you have no security at all.

Figure 26-4
plusID (*photo courtesy of Privaris, Inc.*)

Not just primary drives but also any secondary drives in computers in your care should be formatted as NTFS, with the exception of removable drives such as the one you use to back up your system.

When you run into a multiple-drive system that has a second or third drive formatted as FAT32, you can use the *CONVERT* command-line utility to go from FAT to NTFS. The syntax is pretty straightforward. To convert a D: drive from FAT or FAT32 to NTFS, for example, you'd type the following:

```
CONVERT D: /FS:NTFS
```

You can substitute a mount name in place of the drive letter in case you have a mounted volume. The command has a few extra switches as well, so at the command prompt, type **a /?** after the CONVERT command to see all of your options.

Users and Groups

Windows uses user accounts and groups as the bedrock of access control. A user account is assigned to a group, such as Users, Power Users, or Administrators, and by association gets certain permissions on the computer. Using NTFS enables the highest level of control over data resources.

Assigning users to groups is a great first step in controlling a local machine, but this feature really shines once you go to a networked environment. Let's go there now.

User Account Control Through Groups

Access to user accounts should be restricted to the assigned individuals, and those who configure the permissions to those accounts must remember the Principle of Least Privilege discussed in Chapter 16, "Securing Windows Resources": Accounts should have permission to access only the resources they need and no more. Tight control of user accounts is critical to preventing unauthorized access. Disabling unused accounts is an important part of this strategy, but good user account control goes far deeper than that. One of your best tools for user account control is groups. Instead of giving permissions/rights to individual user accounts, give them to groups; this makes keeping track of the permissions assigned to individual user accounts much easier. Figure 26-5 shows me giving permissions to a group for a folder in Windows Vista. Once a group is created and its permissions set, you can then add user accounts to that group as needed. Any user account that becomes a member of a group automatically gets the permissions assigned to that group. Figure 26-6 shows me adding a user to a newly created group in the same Windows Vista system.

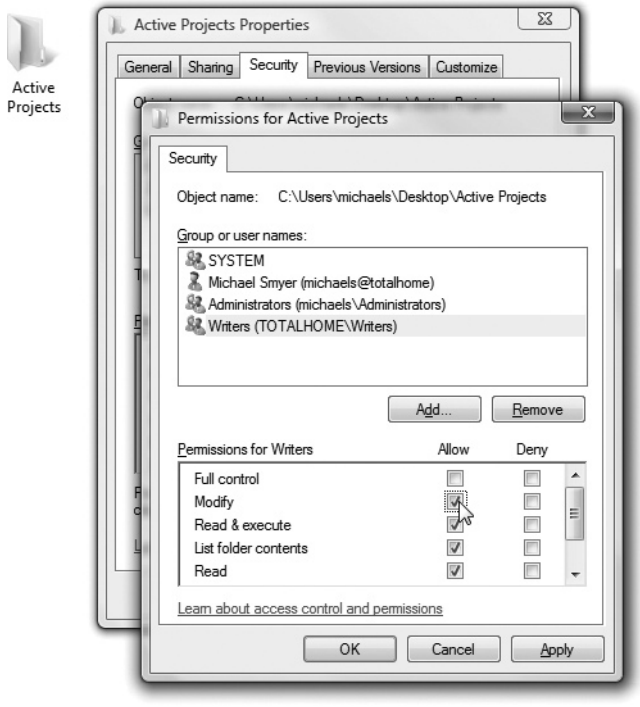


Figure 26-5 Giving a group permissions for a folder in Windows Vista

Groups are a great way to achieve increased complexity without increasing the administrative burden on network administrators, because all network operating systems combine permissions. When a user is a member of more than one group, which permissions does that user have with respect to any particular resource? In all network

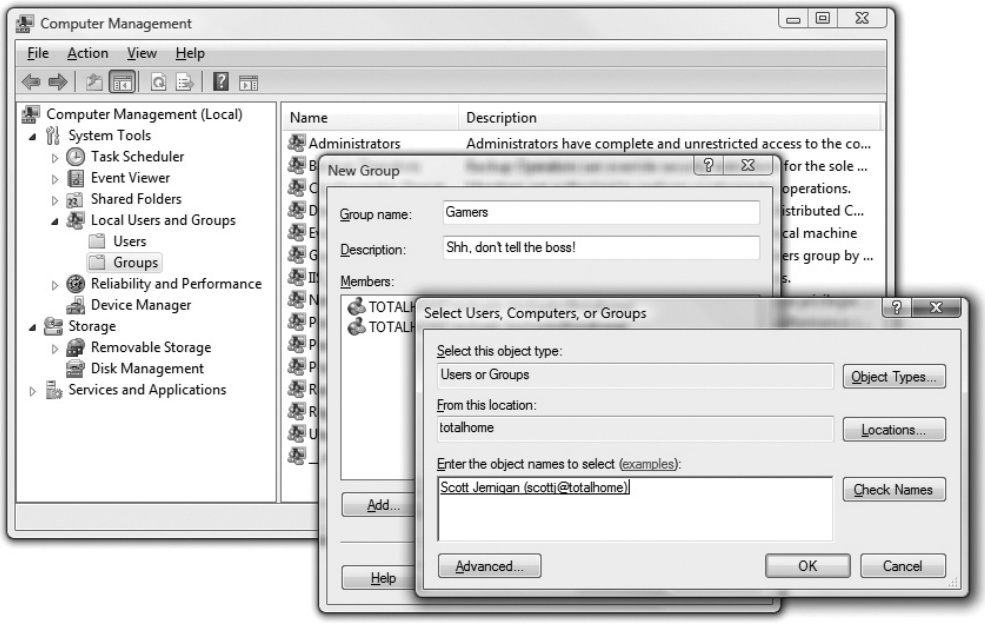


Figure 26-6 Adding a user to a newly created group in Windows Vista

operating systems, the permissions of the groups are *combined*, and the result is what you call the *effective permissions* the user has to access the resource. As an example, if Rita is a member of the Sales group, which has List Folder Contents permission to a folder, and she is also a member of the Managers group, which has Read and Execute permissions to the same folder, Rita will have both List Folder Contents *and* Read and Execute permissions to that folder.

Watch out for *default* user accounts and groups—they can become secret backdoors to your network! All network operating systems have a default Everyone group that can be used to sneak into shared resources easily. This Everyone group, as its name implies, literally includes anyone who connects to that resource. Windows gives full control to the Everyone group by default, for example, so make sure you know to lock this down!

All of the default groups—Everyone, Guest, Users—define broad groups of users. Never use them unless you intend to permit all of those folks to access a resource. If you use one of the default groups, remember to configure them with the proper permissions to prevent users from doing things you don't want them to do with a shared resource!

All of these groups and organizational units only do one thing for you: They let you keep track of your user accounts, so you know they are only available for those who need them, and they can only access the resources you want them to use.

Security Policies

Although permissions control how users access shared resources, there are other functions you should control that are outside the scope of resources. For example, do you want users to be able to access a command prompt on their Windows system? Do you want users to be able to install software? Would you like to control what systems a user can log into or at what time of day a user can log in? All network operating systems provide you with some capability to control these and literally hundreds of other security parameters, under what Windows calls *policies*. I like to think of policies as permissions for activities as opposed to true permissions, which control access to resources.

A policy is usually applied to a user account, a computer, or a group. Let's use the example of a network composed of Windows XP Professional systems with a Windows 2003 Server system. Every Windows XP system has its own local policies program, which enables policies to be placed on that system only. Figure 26-7 shows the tool you use to set local policies on an individual system, called *Local Security Settings*, being used to deny the user account Danar the capability to log on locally.

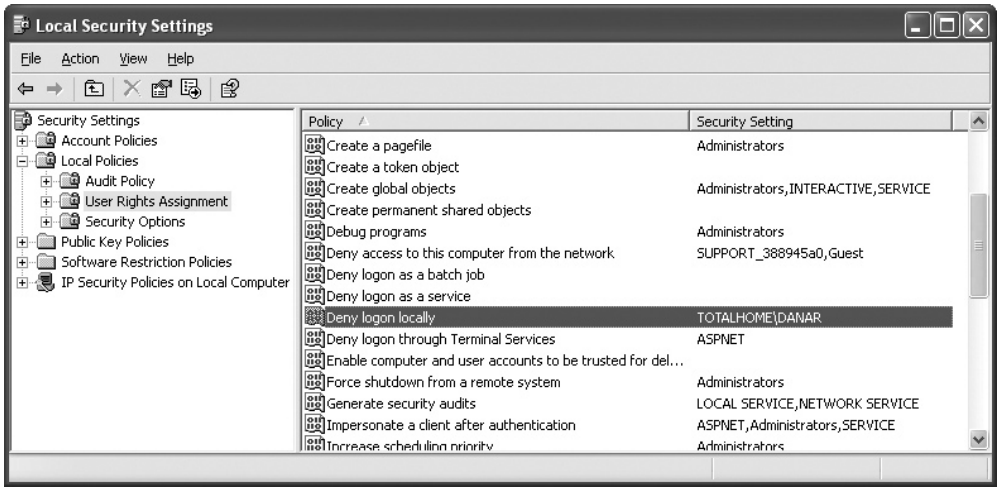


Figure 26-7 Local Security Settings

Local policies work great for individual systems, but they can be a pain to configure if you want to apply the same settings to more than one PC on your network. If you want to apply policy settings *en masse*, you need to step up to Windows Active Directory domain-based *Group Policy*. By using Group Policy, you can exercise deity-like—Microsoft prefers to use the term *granular*—control over your network clients.

Want to set default wallpaper for every PC in your domain? Group Policy can do that. Want to make certain tools inaccessible to everyone except authorized users? Group Policy can do that, too. Want to control access to the Internet, redirect home folders, run scripts, deploy software, or just remind folks that unauthorized access to

the network will get them nowhere fast? Group Policy is the answer. Figure 26-8 shows Group Policy; I'm about to change the default title on every instance of Internet Explorer on every computer in my domain!

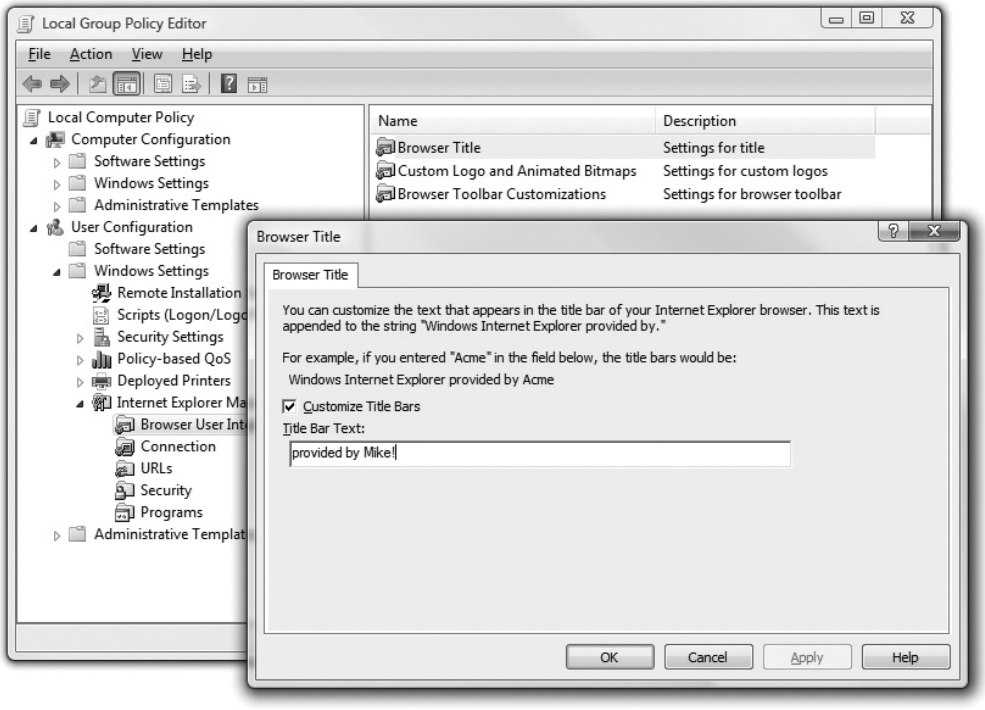


Figure 26-8 Using Group Policy to make IE title say "provided by Mike!"

That's just one simple example of the settings you can configure by using Group Policy. You can apply literally hundreds of tweaks through Group Policy, from the great to the small, but don't worry too much about familiarizing yourself with each and every one. Group Policy settings are a big topic on most of the Microsoft certification tracks, but for the purposes of the CompTIA A+ exams, you simply have to be comfortable with the concept behind Group Policy.

Although I could never list every possible policy you can enable on a Windows system, here's a list of some commonly used ones:

- **Prevent Registry Edits** If you try to edit the Registry, you get a failure message.
- **Prevent Access to the Command Prompt** Keeps users from getting to the command prompt by turning off the Run command and the MS-DOS Prompt shortcut.

- **Log on Locally** Defines who may log on to the system locally.
- **Shut Down System** Defines who may shut down the system.
- **Minimum Password Length** Forces a minimum password length.
- **Account Lockout Threshold** Sets the maximum number of logon attempts a person can make before being locked out of the account.
- **Disable Windows Installer** Prevents users from installing software.
- **Printer Browsing** Enables users to browse for printers on the network, as opposed to using only assigned printers.

Although the CompTIA A+ exams don't expect you to know how to implement policies on any type of network, you are expected to understand that policies exist, especially on Windows networks, and that they can do amazing things to control what users can do on their systems. If you ever try to get to a command prompt on a Windows system only to discover the Run command is dimmed, blame it on a policy, not the computer!

Data Classification and Compliance

Larger organizations, such as government entities, benefit greatly from organizing their data according to its sensitivity—what's called *data classification*—and making certain that computer hardware and software stay as uniform as possible. In addition, many government and internal regulations apply fairly rigorously to the organizations.

Data classification systems vary by the organization, but a common scheme classifies documents as public, internal use only, highly confidential, top secret, and so on. Using a classification scheme enables employees such as techs to know very quickly what to do with documents, the drives containing documents, and more. Your strategy for recycling a computer system left from a migrated user, for example, will differ a lot if the data on the drive was classified as internal use only or top secret.

Compliance means, in a nutshell, that members of an organization or company must abide by or comply with all of the rules that apply to the organization or company. Statutes with funny names such as Sarbanes-Oxley impose certain behaviors or prohibitions on what people can and cannot do in the workplace.

From a technician's point of view, the most common compliance issue revolves around software, such as what sort of software users can be allowed to install on their computers or, conversely, why you have to tell a user that he can't install the latest application that may help him do the job more effectively because that software isn't on the approved list. This can lead to some uncomfortable confrontations, but it's part of a tech's job.

The concepts behind compliance in IT are not, as some might imagine at first blush, to stop you from being able to work effectively. Rather they're designed to stop users with not quite enough technical skill or knowledge from installing malicious programs or applications that will destabilize their systems. This keeps technical support calls down and enables techs to focus on more serious problems.

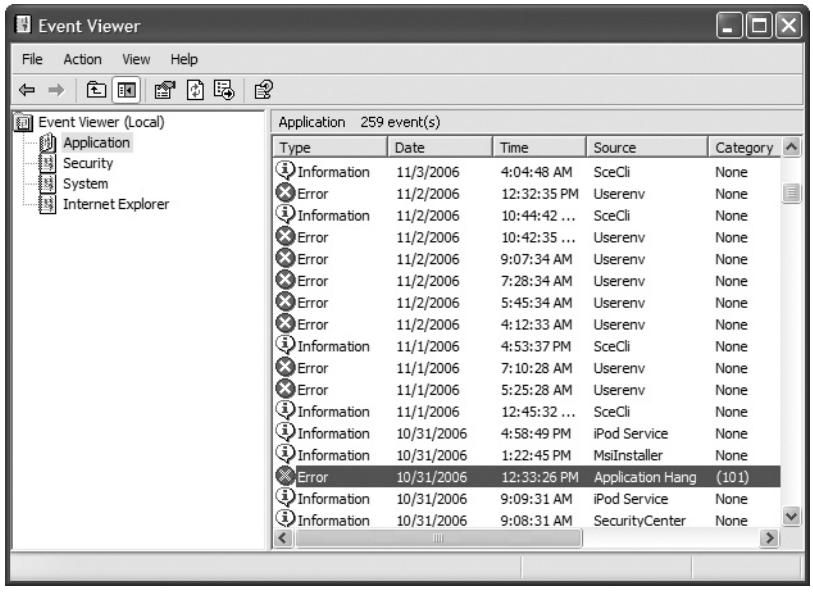
Reporting

As a final weapon in your security arsenal, you need to report any security issues so a network administrator or technician can take steps to make them go away. You can set up two tools within Windows so that the OS reports problems to you: Event Viewer and Auditing. You can then do your work and report those problems. Let's take a look.

Event Viewer

Event Viewer is Window's default tattletale program, spilling the beans about many things that happen on the system. You can find Event Viewer in Administrative Tools in the Control Panel. By default, Event Viewer has three sections: Application, Security, and System. If you've downloaded Internet Explorer 7, you'll see a fourth option for the browser, Internet Explorer (Figure 26-9). As you'll recall from Chapter 17, "Maintaining and Troubleshooting Windows," the most common use for Event Viewer is to view application or system errors for troubleshooting (Figure 26-10).

Figure 26-9
Event Viewer



One very cool feature of Event Viewer is that you can click the link to take you to the online Help and Support Center at Microsoft.com, and the software reports your error (Figure 26-11), checks the online database, and comes back with a more or less useful explanation (Figure 26-12).

Auditing

The Security section of Event Viewer doesn't show you anything by default. To unlock the full potential of Event Viewer, you need to set up auditing. *Auditing* in the security

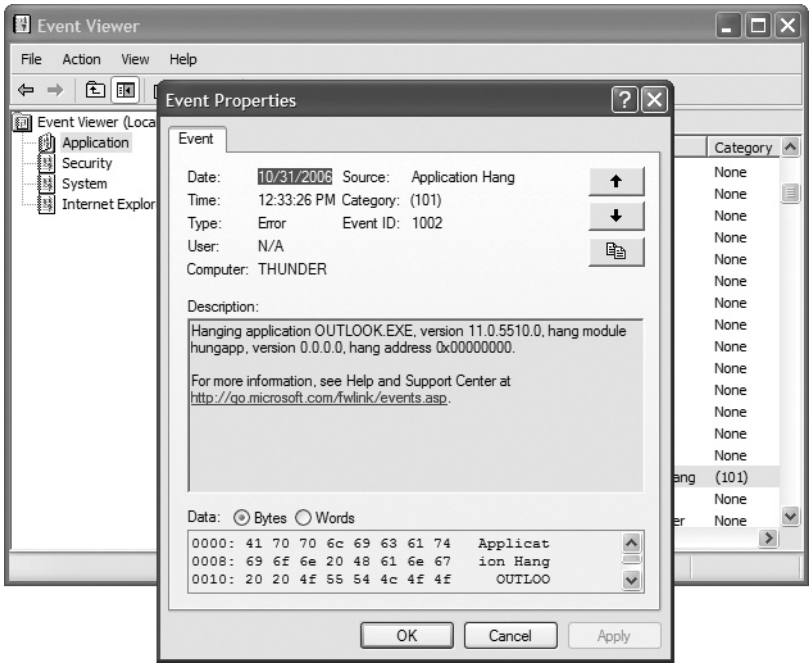


Figure 26-10 Typical application error message

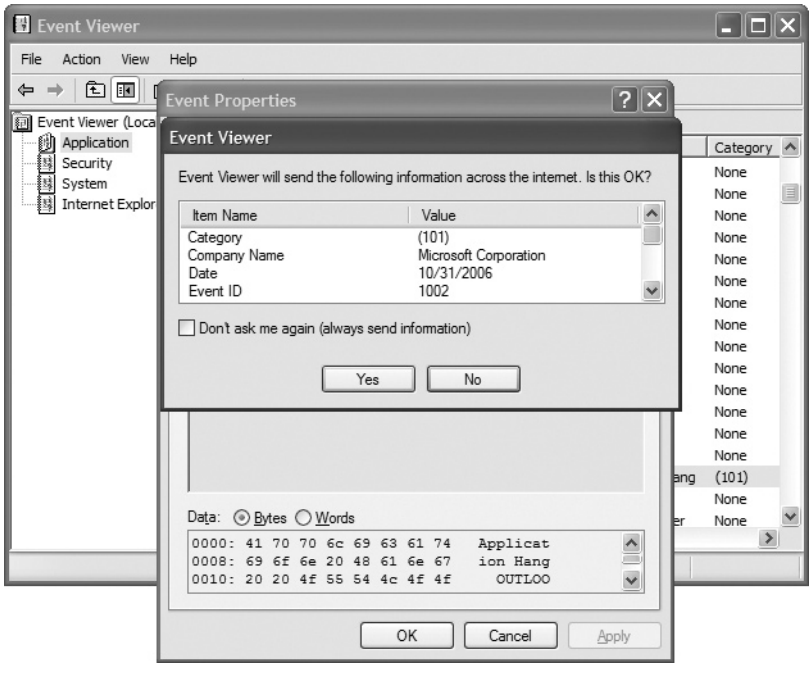


Figure 26-11 Details about to be sent

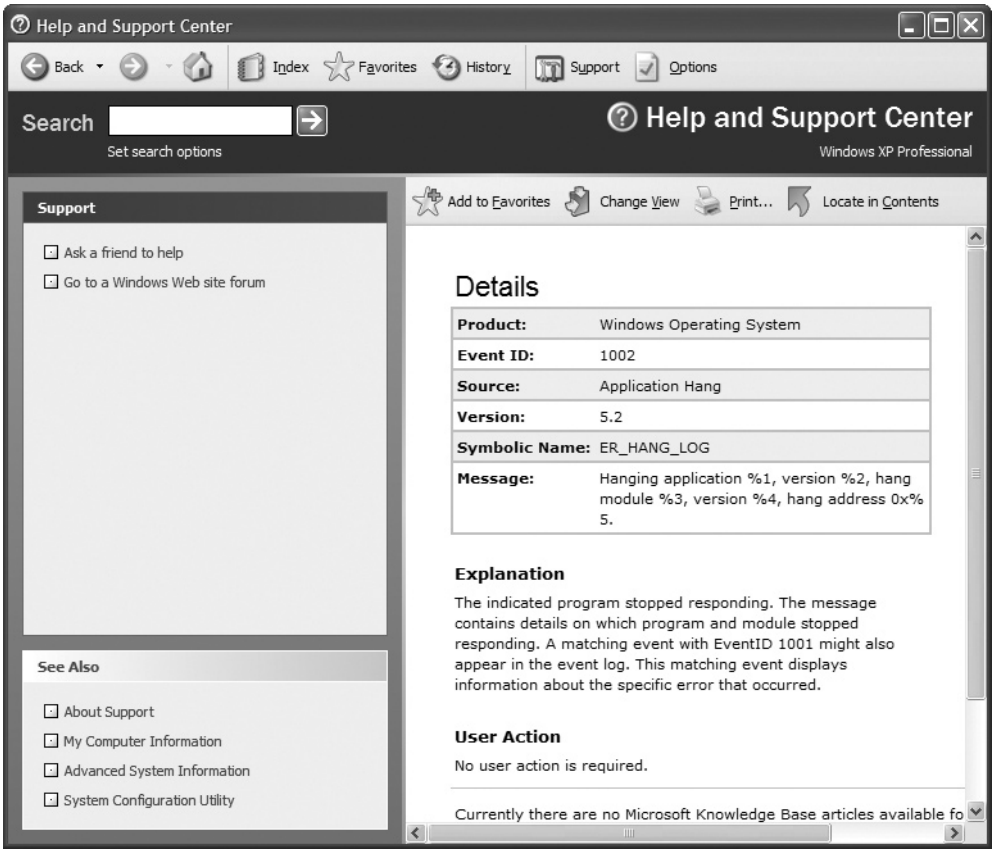


Figure 26-12 Help and Support Center being helpful

sense means to tell Windows to create an entry in the Security Log when certain events happen, for example, a user logs on—called *event auditing*—or tries to access a certain file or folder—called *object access auditing*. Figure 26-13 Shows Event Viewer tracking logon and logoff events.

The CompTIA A+ certification exams don't test you on creating a brilliant auditing policy for your office—that's what network administrators do. You simply need to know what auditing does and how to turn it on or off so you can provide support for the network administrators in the field. To turn on auditing at a local level, go to Local Security Settings in Administrative Tools. Select Local Policies and then click Audit Policies. Double-click one of the policy options and select one or both of the checkboxes. Figure 26-14 shows the Audit object access dialog box.

NOTE Event Viewer stores log files in %SystemRoot%\System32\Config.

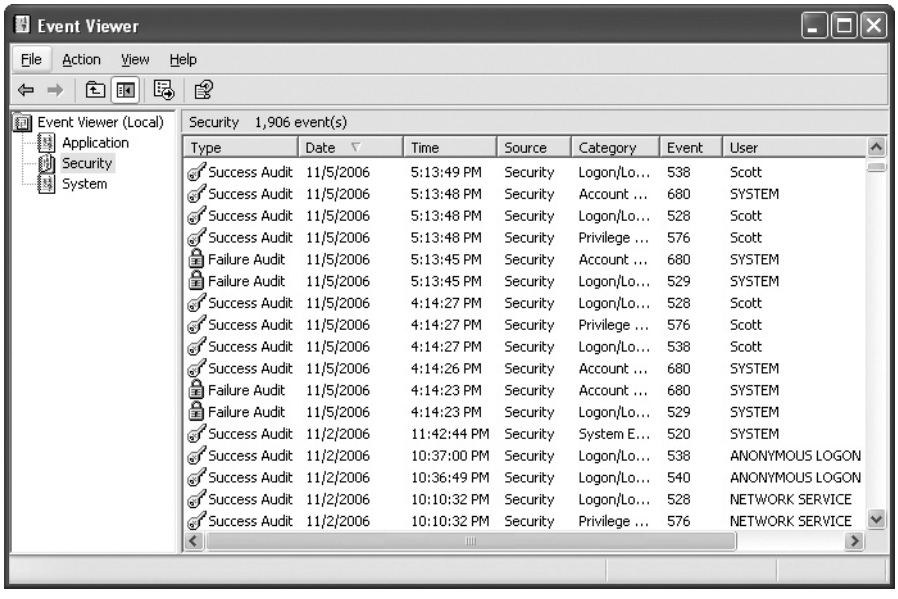


Figure 26-13 Event Viewer displaying security alerts

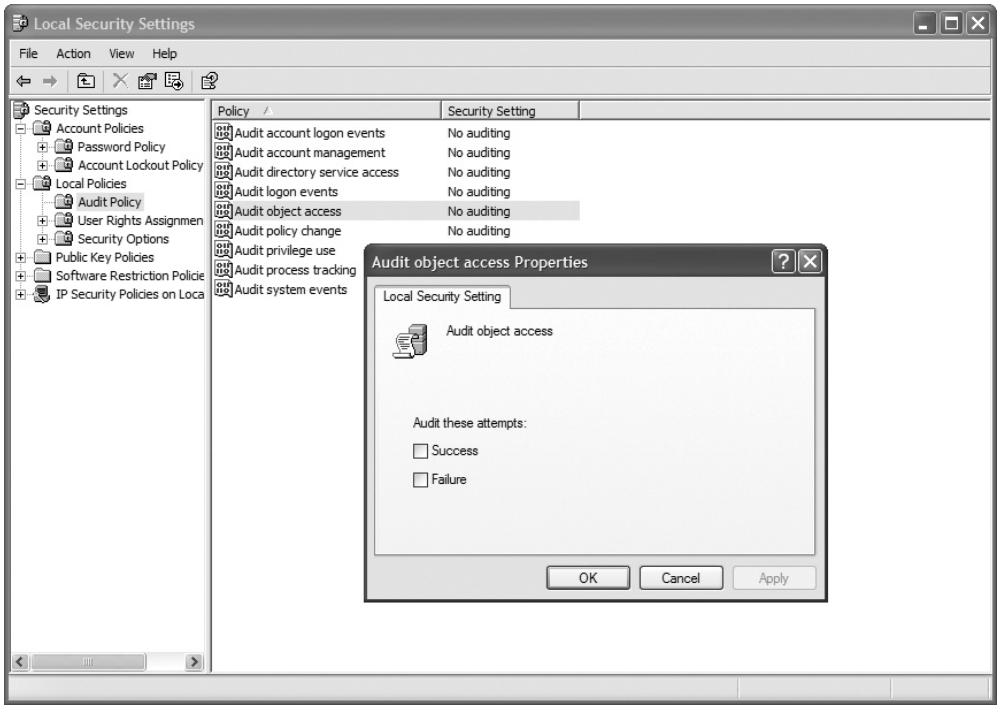


Figure 26-14 Audit object access, with the Local Security Setting dialog box open in the background

Incidence Reporting

Once you've gathered data about a particular system or you've dealt with a computer or network problem, you need to complete the mission by telling your supervisor. This is called *incidence reporting*. Many companies have pre-made forms that you simply fill out and submit. Other places are less formal. Regardless, you need to do this!

Incidence reporting does a couple of things for you. First, it provides a record of work you've accomplished. Second, it provides a piece of information that, when combined with other information you might or might not know, reveals a pattern or bigger problem to someone higher up the chain. A seemingly innocuous security audit report, for example, might match other such events in numerous places in the building at the same time and thus show that conscious, coordinated action rather than a glitch was at work.

Network Security

Networks are under threat from the outside as well, so this section looks at issues involving Internet-borne attacks, firewalls, and wireless networking. This content is the security bread and butter for a CompTIA A+ technician, so you need to understand the concepts and procedures and be able to implement them properly.

Malicious Software

The beauty of the Internet is the ease of accessing resources just about anywhere on the globe, all from the comfort of your favorite chair. This connection, however, runs both ways, and people from all over the world can potentially access your computer from the comfort of their evil lairs. The Internet is awash with malicious software—*malware*—that is, even at this moment, trying to infect your systems. Malware consists of computer programs designed to break into computers or cause havoc on computers. The most common types of malware are grayware, spam, viruses, Trojan horses, and worms. You need to understand the different types of malware so you can combat them for you and your users successfully.

Grayware

Programs that intrude unwanted into your computing experience but don't actually do any damage to your systems or data—what's called *grayware*—can make that computing experience less than perfect. On most systems, the Internet Web browser client is the most often used piece of software. Over the years, Web sites have come up with more and more ways to try to get you to see what they want you to see: their advertising. When the Web first got underway, we were forced to look at an occasional banner ad. In the past few years, Web site designers have become much more sophisticated, creating a number of intrusive and irritating ways to get you to part with your money in one form or another.

There are basically three irritating grayware types: pop-ups, spyware, and adware. *Pop-ups* are those surprise browser windows that appear automatically when you visit a Web site, proving themselves irritating and unwanted and nothing else. *Spyware*, meanwhile,

defines a family of programs that run in the background on your PC, sending information about your browsing habits to the company that installed it on your system. *Adware* is not generally as malicious as spyware, but it works similarly to display ads on your system. As such, these programs download new ads and generate undesirable network traffic. Of the three, spyware is much less noticeable but far more nefarious. At its worst, spyware can fire up pop-up windows of competing products on the Web site you're currently viewing. For example, you might be perusing a bookseller's Web site, only to have a pop-up from a competitor's site appear.

Pop-Ups Getting rid of pop-ups is actually rather tricky. You've probably noticed that most of these pop-up browser windows don't look like browser windows at all. They have no menu bar, button bar, or address window, yet they are separate browser windows. HTML coding permits Web site and advertising designers to remove the usual navigation aids from a browser window so all you're left with is the content. In fact, as I'll describe in a minute, some pop-up browser windows are deliberately designed to mimic similar pop-up alerts from the Windows OS. They might even have buttons similar to Windows' own exit buttons, but you might find that when you click them, you wind up with more pop-up windows instead! What to do?

The first thing you need to know when dealing with pop-ups is how to close them without actually having to risk clicking them. As I said, most pop-ups have removed all navigation aids, and many are also configured to appear on your monitor screen in a position that places the browser window's exit button—the little *X* button in the upper-right corner—outside of your visible screen area. Some even pop up behind the active browser window and wait there in the background. Most annoying! To remedy this, use alternate means to close the pop-up browser window. For instance, you can right-click the browser window's taskbar icon to generate a pop-up menu of your own. Select Close, and the window should go away. You can also press ALT-TAB to bring the browser window in question to the forefront and then press ALT-F4 to close it.

Most Web browsers have features to prevent pop-up ads in the first place, but I've found that these types of applications are sometimes *too* thorough. That is, they tend to prevent *all* new browser windows from opening, even those you want to view. Still, they're free to try, so have a look to see if they suit your needs. Applications such as Ad-Subtract control a variety of Internet annoyances, including pop-up windows, cookies, and Java applets, and are more configurable—you can specify what you want to allow on any particular domain address—but the fully functional versions usually cost at least something, and that much control is too confusing for most novice-level users.

Spyware Some types of spyware go considerably beyond the level of intrusion. They can use your computer's resources to run *distributed computing* applications, capture your keystrokes to steal passwords, reconfigure your dial-up settings to use a different phone number at a much higher connection charge, or even use your Internet connection and e-mail address list to propagate itself to other computers in a virus-like fashion! Are you concerned yet?

Setting aside the legal and ethical issues—and there are many—you should at least appreciate that spyware can seriously impact your PC's performance and cause problems

with your Internet connection. The threat is real, so what practical steps can you take to protect yourself? Let's look at how to prevent spyware installation and how to detect and remove any installed spyware.

How does this spyware get into your system in the first place? Obviously, sensible people don't download and install something that they know is going to compromise their computers. Makers of spyware know this, so they bundle their software with some other program or utility that purports to give you some benefit.

What kind of benefit? How about free access to MP3 music files? A popular program called Kazaa does that. How about a handy *e-wallet* utility that remembers your many screen names, passwords, and even your credit-card numbers to make online purchases easier and faster? A program called Gator does that, and many other functions as well. How about browser enhancements, performance boosters, custom cursor effects, search utilities, buddy lists, file savers, or media players? The list goes on and on, yet they all share one thing: they're simply window-dressing for the *real* purpose of the software. So you see, for the most part, spyware doesn't need to force its way into your PC. Instead, it saunters calmly through the front door. If the graphic in Figure 26-15 looks familiar, you might have installed some of this software yourself.

Figure 26-15 Gator Corporation's acknowledgment warning

Some spyware makers use more aggressive means to get you to install their software. Instead of offering you some sort of attractive utility, they instead use fear tactics and deception to try to trick you into installing their software. One popular method is to use pop-up browser windows crudely disguised as Windows' own system warnings (Figure 26-16). When clicked, these may trigger a flood of other browser windows, or may even start a file download.

The lesson here is simple: *Don't install these programs!* Careful reading of the software's license agreement before you install a program is a good idea, but realistically, it does little to protect your PC. With that in mind, here are a couple of preventive measures you can take to keep parasitic software off of your system.

Figure 26-16 A spyware pop-up browser window, disguised as a Windows alert

If you visit a Web site and are prompted to install a third-party application or plug-in that you've never heard of, *don't install it*. Well-known and reputable plug-ins, such as Adobe's *Shockwave* or *Flash*, are safe, but be suspicious of any others. Don't click *anywhere* inside of a pop-up browser window, even if it looks just like a Windows alert window or DOS command-line prompt—as I just mentioned, it's probably fake and the Close button is likely a hyperlink. Instead, use other means to close the window, such as pressing ALT-F4 or right-clicking the browser window's icon on the taskbar and selecting Close.

You can also install spyware detection and removal software on your system and run it regularly. Let's look at how to do that.

Some spyware makers are reputable enough to include a routine for uninstalling their software. Gator, for instance, makes it fairly easy to get rid of their programs; just use the Windows Add/Remove Programs applet in the Control Panel. Others, however, aren't quite so cooperative. In fact, because spyware is so—well, *sneaky*—it's entirely possible that your system already has some installed that you don't even know about. How do you find out?

Windows comes with Windows Defender, a fine tool for catching most spyware, but it's not perfect. The better solution is to back up Windows Defender with a second spyware removal program. There are several on the market, but two that I highly recommend are Lavasoft's Ad-Aware (Figure 26-17) and PepiMK's Spybot Search & Destroy.

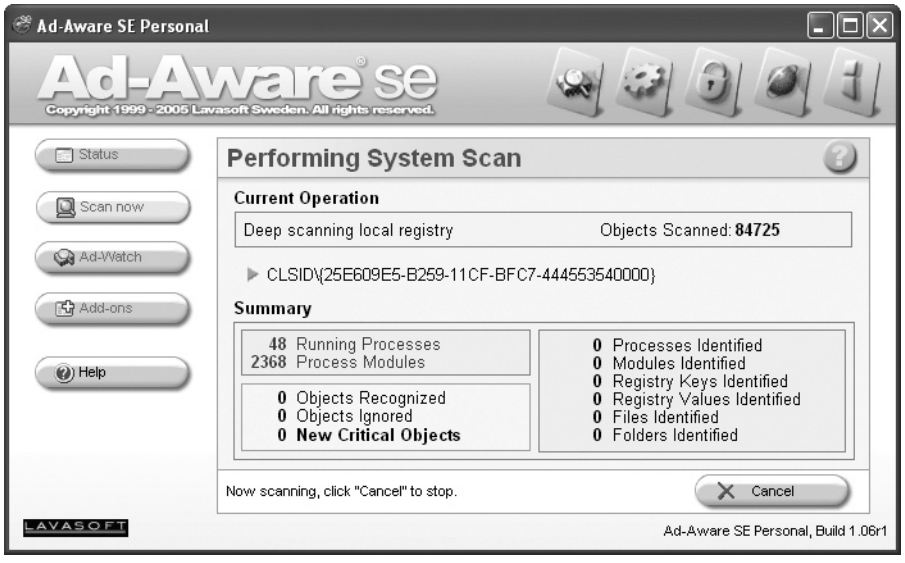


Figure 26-17 Lavasoft's Ad-Aware

Both of these applications work exactly as advertised. They detect and delete spyware of all sorts—hidden files and folders, cookies, Registry keys and values, you name it. Ad-Aware is free for personal use, while Spybot Search & Destroy is shareware (Figure 26-18). Many times I've used both programs at the same time because one tends to catch what the other misses.

Spam

E-mail that comes into your Inbox from a source that's not a friend, family member, or colleague, and that you didn't ask for, can create huge problems for your computer and you. This unsolicited e-mail, called *spam*, accounts for a huge percentage of traffic on the Internet. Spam comes in many flavors, from legitimate businesses trying to sell you products to scammers who just want to take your money. Hoaxes, pornography, and get-rich-quick schemes pour into the Inboxes of most e-mail users. They waste your time and can easily offend.

You can use several options to cope with the flood of spam. The first option is defense. Never post your e-mail address on the Internet. One study tested this theory and found that *over 97 percent* of the spam received during the study went to e-mail addresses they had posted on the public Internet.

Filters and filtering software can block spam at your mail server and at your computer. AOL implemented blocking schemes in 2004, for example, that dropped the average spam received by its subscribers by a large percentage, perhaps as much as 50 percent. You can set most e-mail programs to block e-mail from specific people—good to use if someone is harassing you—or to specific people. You can block by subject line

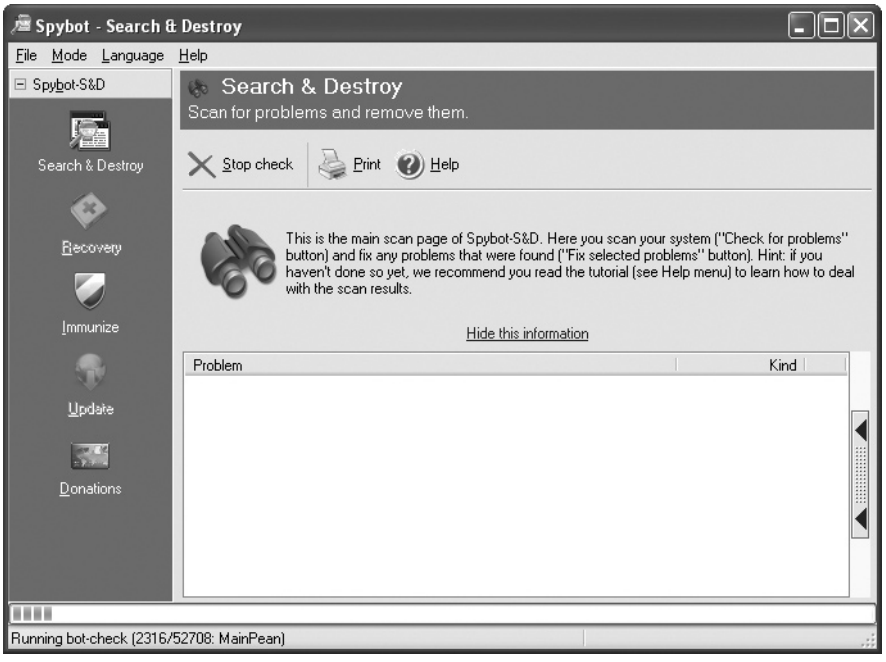


Figure 26-18 Spybot Search & Destroy

or keywords. Most people use a third-party anti-spam program instead of using the filters in their e-mail program.

Viruses

Just as a biological virus gets passed from person to person, a computer *virus* is a piece of malicious software that gets passed from computer to computer (Figure 26-19). A computer virus is designed to attach itself to a program on your computer. It could be your e-mail program, your word processor, or even a game. Whenever you use the infected program, the virus goes into action and does whatever it was designed to do. It can wipe out your e-mail or even erase your entire hard drive! Viruses are also sometimes used to steal information or send spam e-mails to everyone in your address book.

EXAM TIP Be sure to know the difference between viruses and spyware. Too many people use the terms interchangeably, and they're very different things.

Trojans

Trojans are true, freestanding programs that do something other than what the person who runs the program thinks they will do, much as the Trojan horse did in antiquity. An example of a *Trojan virus* is a program that a person thinks is an antivirus program

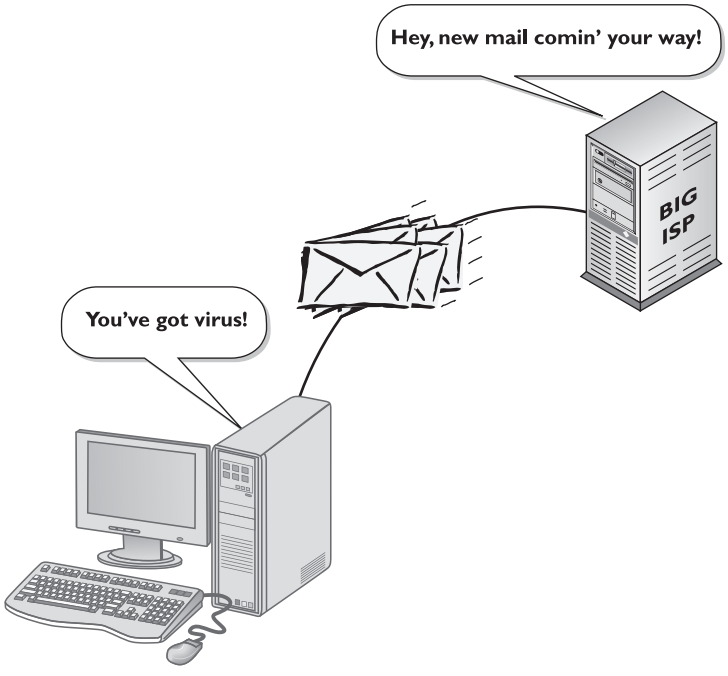


Figure 26-19
You've got mail!

but is actually a virus. Some Trojans are quite sophisticated. It might be a game that works perfectly well, but causes some type of damage when the user quits the game.

Worms

Similar to a Trojan, a *worm* is a complete program that travels from machine to machine, usually through computer networks. Most worms are designed to take advantage of security problems in operating systems and install themselves on vulnerable machines. They can copy themselves over and over again on infected networks and can create so much activity that they overload the network by consuming bandwidth, in worst cases even bringing chunks of the entire Internet to a halt.

You can do several things to protect yourself and your data against these threats. First, make sure you are running up-to-date virus software—especially if you connect to the Internet via an always-on broadband connection. You should also be protected by a firewall, either as part of your network hardware or by means of a software program. (See the sections on antivirus programs and firewalls, later in this chapter.)

Because worms most commonly infect systems through security flaws in operating systems, the next defense against them is to make sure you have the latest security patches installed on your version of Windows. A *security patch* is an addition to the operating system to patch a hole in the operating system code. You can download security patches from the Microsoft Update Web site (Figure 26-20).

Microsoft's Windows Update tool is handy for Windows users as it provides a simple method to ensure that your version's security is up to date. The one downside is that not

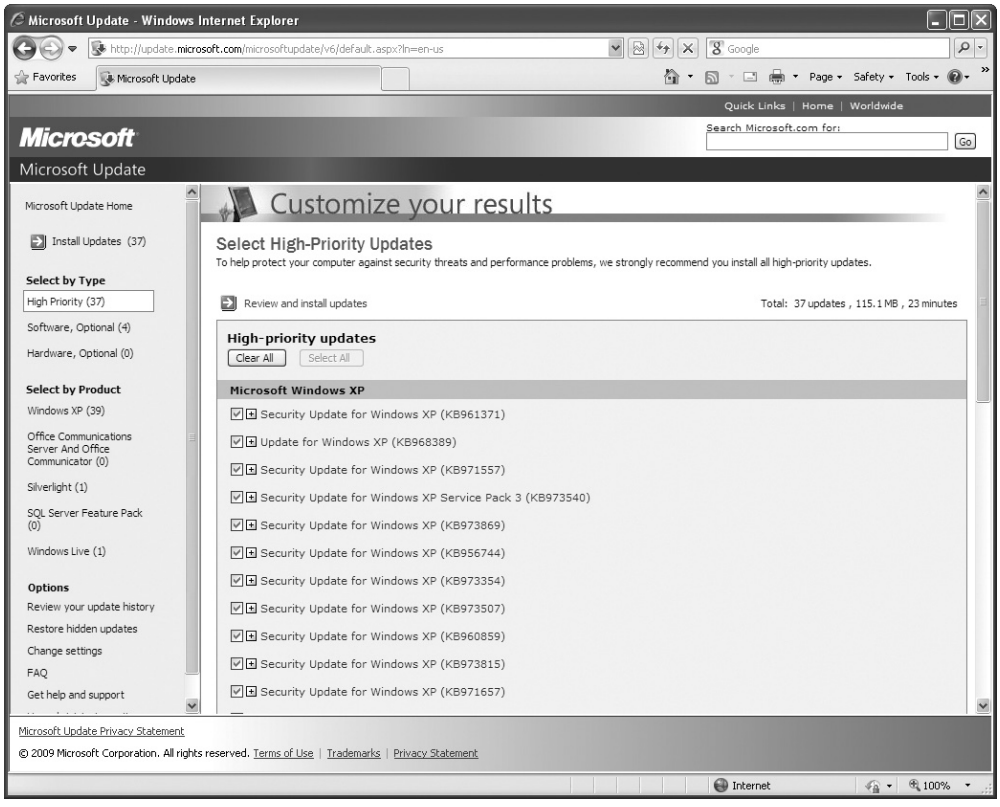


Figure 26-20 Microsoft Update

everyone remembers to run Windows Update. Don't wait until something goes wrong on your computer or you hear on the news that another nasty program is running rampant across the Internet. Run Windows Update weekly (or even better, automatically) as a part of your normal system maintenance. Keeping your patches up to date is called *patch management,* and it goes a long way toward keeping your system safe.

Virus Prevention and Recovery

The only way to protect your PC permanently from getting a virus is to disconnect from the Internet and never permit any potentially infected software to touch your precious computer. Because neither scenario is likely these days, you need to use a specialized antivirus program to help stave off the inevitable virus assaults. When you discover infected systems, you need to know how to stop the spread of the virus to other computers and how to fix infected computers.

Antivirus Programs

An *antivirus program* protects your PC in two ways. It can be both sword and shield, working in an active seek-and-destroy mode and in a passive sentry mode. When ordered to seek and destroy, the program scans the computer's boot sector and files for viruses and, if it finds any, presents you with the available options for removing or disabling them. Antivirus programs can also operate as *virus shields* that passively monitor your computer's activity, checking for viruses only when certain events occur, such as a program executing or a file being downloaded.

Antivirus programs use different techniques to combat different types of viruses. They detect boot sector viruses simply by comparing the drive's boot sector to a standard boot sector. This works because most boot sectors are basically the same. Some antivirus programs make a backup copy of the boot sector. If they detect a virus, the programs use that backup copy to replace the infected boot sector. Executable viruses are a little more difficult to find because they can be on any file in the drive. To detect executable viruses, the antivirus program uses a library of signatures. A *signature* is the code pattern of a known virus. The antivirus program compares an executable file to its library of signatures. There have been instances where a perfectly clean program coincidentally held a virus signature. Usually the antivirus program's creator provides a patch to prevent further alarms. Now that you understand the types of viruses and how antivirus programs try to protect against them, let's review a few terms that are often used when describing certain traits of viruses.

Polymorphics/Polymorphs A *polymorph virus* attempts to change its signature to prevent detection by antivirus programs, usually by continually scrambling a bit of useless code. Fortunately, the scrambling code itself can be identified and used as the signature—once the antivirus makers become aware of the virus. One technique used to combat unknown polymorphs is to have the antivirus program create a checksum on every file in the drive. A *checksum* in this context is a number generated by the software based on the contents of the file rather than the name, date, or size of that file. The algorithms for creating these checksums vary among different antivirus programs (they are also usually kept secret to help prevent virus makers from coming up with ways to beat them). Every time a program is run, the antivirus program calculates a new checksum and compares it with the earlier calculation. If the checksums are different, it is a sure sign of a virus.

Stealth The term "stealth" is more of a concept than an actual virus function. Most *stealth virus* programs are boot sector viruses that use various methods to hide from antivirus software. The AntiEXE stealth virus hooks on to a little-known but often-used software interrupt, for example, running only when that interrupt runs. Others make copies of innocent-looking files.

Virus Prevention Tips

The secret to preventing damage from a malicious software attack is to keep from getting a virus in the first place. As discussed earlier, all good antivirus programs include a virus shield that scans e-mail, downloads, running programs, and so on automatically (see Figure 26-21).

Figure 26-21 A virus shield in action

Use your antivirus shield. It is also a good idea to scan PCs daily for possible virus attacks. All antivirus programs include terminate-and-stay resident programs (TSRs) that run every time the PC is booted. Last but not least, know the source of any software before you load it. Although the chance of commercial, shrink-wrapped software having a virus is virtually nil (there have been a couple of well-publicized exceptions), that illegal copy of Unreal Tournament you borrowed from a local hacker should definitely be inspected with care.

Keep your antivirus program updated. New viruses appear daily, and your program needs to know about them. The list of virus signatures your antivirus program can recognize is called the *definition file*, and you must keep that definition file up to date so your antivirus software has the latest signatures. Fortunately, most antivirus programs update themselves automatically. Further, you should periodically update the core antivirus software programming—called the *engine*—to employ the latest refinements the developers have included.

Virus Recovery Tips When the inevitable happens and either your computer or one of your user's computers gets infected by a computer virus, you need to follow certain steps to stop the problem from spreading and get the computer back up safely into service. Try this five-step process.

1. Recognize
2. Quarantine
3. Search and destroy

4. Remediate
5. Educate

Recognize and Quarantine The first step is to recognize that a potential virus outbreak has occurred. If you're monitoring network traffic and one computer starts spewing e-mail, that's a good sign. Or users might complain that a computer that was running snappily the day before seems very sluggish.

Many networks employ software such as the open source PacketFence that automatically monitors network traffic and can cut a machine off the network if that machine starts sending suspicious packets. You can also quarantine a computer manually, by disconnecting the network cable. Once you're sure the machine isn't capable of infecting others, you're ready to find the virus and get rid of it.

Search and Destroy Once you've isolated the infected computer (or computers), you need to get to a safe boot environment and run your antivirus software. You can try Windows Safe Mode first, because it doesn't require anything but a reboot. If that doesn't work, or you suspect a boot sector virus, you need to turn to an external bootable source, such as a bootable CD or flash memory drive.

Get into the habit of keeping around an antivirus CD-R—a bootable, CD-R disc with a copy of an antivirus program. If you suspect a virus, use the disc, even if your antivirus program claims to have eliminated the virus. Turn off the PC and reboot it from the antivirus disc. (You might have to change CMOS settings to boot to an optical disc.) This will put you in a clean boot environment that you know is free from any boot-sector viruses. If you only support fairly recent computers, most have an option to boot to a USB flash drive, so you can put a boot environment on a thumb drive for even faster start-up speeds.

You have several options for creating the bootable CD-R or flash drive. First, some antivirus software comes in a bootable version, such as the avast! Virus Cleaner Tool (Figure 26-22).

Second, you can download a copy of Linux that offers a LiveCD option such as Ubuntu. With a LiveCD, you boot to the CD and install a complete working copy of the operating system into RAM, never touching or accessing the hard drive, to give you full Internet-ready access to many online antivirus sites. (You'll obviously need Internet access for those tools.) Kaspersky Labs provides a nice option at www.kaspersky.com.

You can download and burn a copy of the Ultimate Boot CD. It comes stocked with several antivirus programs, so you wouldn't need any other tool. Find it at www.ultimatebootcd.com. The only down side is that the antivirus engines will be out of date, as will their virus encyclopedias.

For those who like to create custom tools, you can make your own boot environment and stock it with the latest antivirus software of your choice. Use one of two preinstalled environment (PE) tools, BartPE and Windows PE.

BartPE is a third-party tool written by Bart Lagerweij that enables you to create a graphical bootable version of Windows XP, complete with software. You need a legitimate copy of Windows XP (Home or Professional) to create the bootable media,

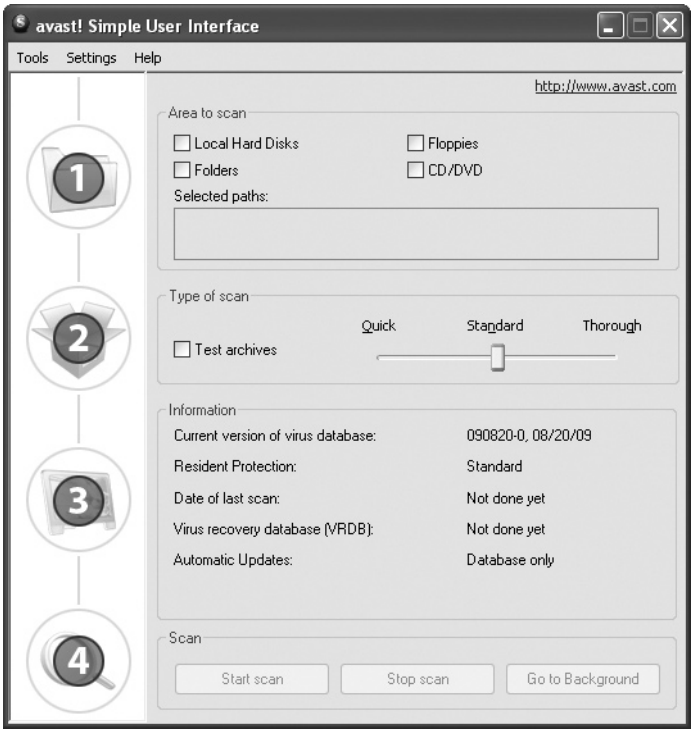


Figure 26-22 avast! Virus Cleaner Tool

as BartPE pulls from the Windows setup files. You can then add various plug-ins to get antivirus support. Find it here: hwww.nu2.nu/pebuilder.

Microsoft made available Windows PE 2.0 (Windows PE 3.0 for Windows 7 should be available by the time you read this) for Windows Vista for installation assistance on multiple computers. The boot environment created also enables you to run some software, though it's not as easy as the BartPE. Download Windows PE from Microsoft.

EXAM TIP You won't get asked about how to create a custom boot environment. You should know that you can, however, and that a bootable CD-R disc or thumb drive with antivirus tools is a must for any technician's toolkit.

Once you get to a boot environment, run your antivirus program's most comprehensive virus scan. Then check all removable media that were exposed to the system, and any other machine that might have received data from it or that is networked to the cleaned machine. A virus or other malicious program can often lie dormant for months before anyone knows of its presence.

E-mail is still a common source of viruses, and opening infected e-mails is a common way to get infected. Viewing an e-mail in a preview window opens the e-mail message and exposes your computer to some viruses. Download files only from sites you know to

be safe, and of course the less reputable corners of the Internet are the most likely places to pick up computer infections.

Remediate Virus infections can do a lot of damage to a system, especially to sensitive files needed to load Windows, so you might need to remediate formerly infected systems after cleaning off the drive or drives. *Remediation* simply means that you fix things the virus harmed. This can mean replacing corrupted Windows Registry files or even startup files.

If you can't start Windows after the virus scan is finished, you need to follow the steps outlined in Chapter 16, "Securing Windows Resources," to boot to the Recovery Console in Windows 2000/XP, or boot into a repair environment in Windows Vista.

Once in the Recovery Console, you'll have access to tools to repair the boot sector (or *boot blocks*, as CompTIA calls them) through the FIXMBR and FIXBOOT commands. You can run BOOTCFG to rebuild a corrupted BOOT.INI file. EXPAND will enable you to grab any replacement files from the Windows CAB files.

With the Windows Vista repair environment, you have access to more repair tools, such as Startup Repair, System Restore, Windows Complete PC Restore, and the command prompt (Figure 26-23). Run the appropriate option for the situation and you should have the machine properly remediated in a jiffy.

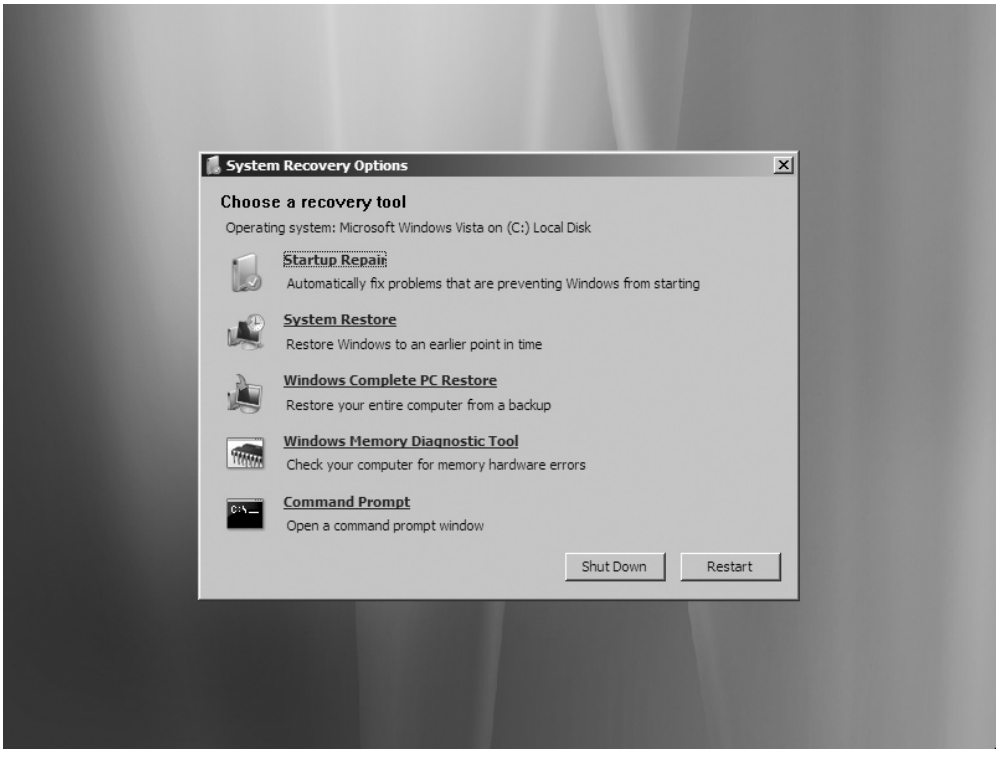


Figure 26-23 System Recovery options in Windows Vista

Educate The best way to keep from having to deal with malware and grayware is education. It's your job as the IT person to talk to users, especially the ones whose systems you've just spent the last hour cleaning of nasties, about how to avoid these programs. Show them samples of dangerous e-mails they should not open, Web sites to avoid, and the types of programs they should not install and use on the network. Any user who understands the risks of questionable actions on their computers will usually do the right thing and stay away from malware.

Finally, have your users run antivirus and antispyware programs regularly. Schedule them while interfacing with the user so you know it will happen.

Firewalls

Firewalls are an essential tool in the fight against malicious programs on the Internet. *Firewalls* are devices or software that protect an internal network from unauthorized access to and from the Internet at large. Hardware firewalls use a number of methods to protect networks, such as hiding IP addresses and blocking TCP/IP ports. Most SOHO networks use a hardware firewall, such as the Linksys router in Figure 26-24. These devices do a great job.

Figure 26-24 Linksys router as a firewall

Windows XP and later comes with an excellent software firewall, called the Windows Firewall (Figure 26-25). It can also handle the heavy lifting of port blocking, security logging, and more.

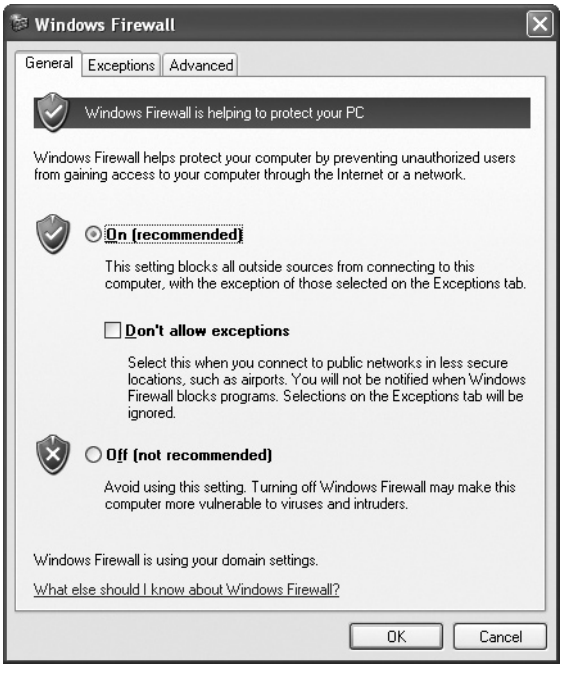


Figure 26-25
Windows Firewall

You can access the Windows Firewall by opening the Windows Firewall applet in the Control Panel. If you're running the Control Panel in Category view, click the Security Center icon (Figure 26-26) and then click the Windows Firewall option in the Windows Security Center dialog box. Figure 26-27 illustrates the Exceptions tab on the Windows Firewall, showing the applications allowed to use the TCP/IP ports on my computer.

Authentication and Encryption

You know from previous chapters that the first step in securing data is authentication, through a user name and password. But when you throw in networking, you're suddenly not just a single user sitting in front of a computer and typing. You're accessing a remote resource and sending login information over the Internet. What's to stop someone from intercepting your user name and password?

Firewalls do a great job of controlling traffic coming into or out of a network from the Internet, but they do nothing to stop interceptor hackers who monitor traffic on the public Internet looking for vulnerabilities. Worse, once a packet is on the Internet itself, anyone with the right equipment can intercept and inspect it. Inspected packets are a cornucopia of passwords, account names, and other tidbits that hackers can use to intrude into your network. Because we can't stop hackers from inspecting these packets, we must turn to *encryption* to make them unreadable.

Network encryption occurs at many levels and is in no way limited to Internet-based activities. Not only are there many levels of network encryption, but each

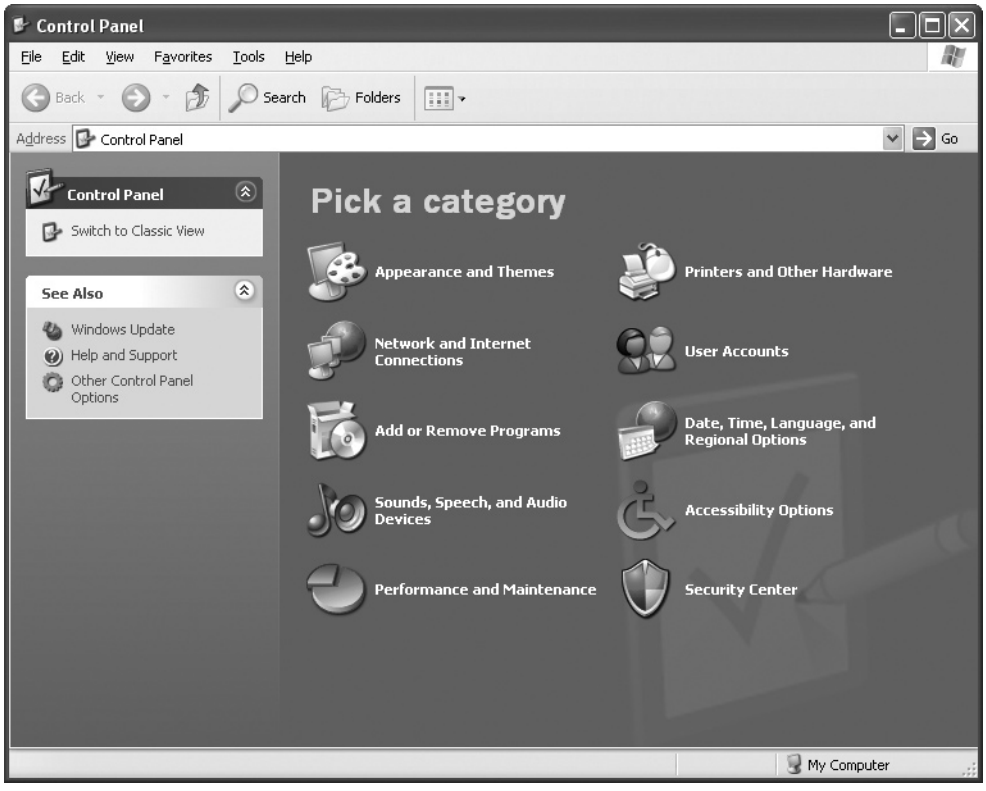


Figure 26-26 Control Panel, Category view

encryption level also provides multiple standards and options, making encryption one of the most complicated of all networking issues. You need to understand where encryption comes into play, what options are available, and what you can use to protect your network.

Network Authentication

Have you ever considered the process that takes place each time a person types in a user name and password to access a network, rather than just a local machine? What happens when this *network* authentication is requested? If you're thinking that when a user types in a user name and password, that information is sent to a server of some sort to be authenticated, you're right—but do you know how the user name and password get to the serving system? That's where encryption becomes important in authentication.

In a local network, authentication and encryption are usually handled by the NOS. In today's increasingly interconnected and diverse networking environment, there is a motivation to enable different network operating systems to authenticate any client

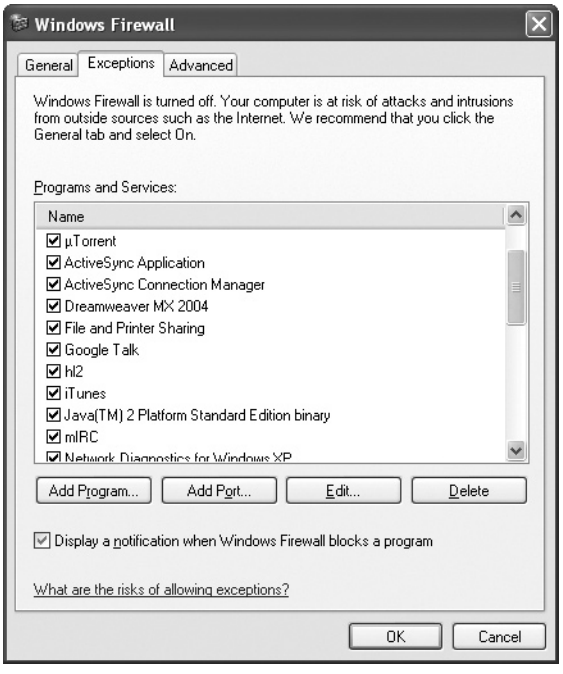


Figure 26-27 Essential programs (doesn't everyone need to run Half-Life 2?)

system from any other NOS. Modern network operating systems such as Windows and OS X use standard authentication encryptions such as MIT's *Kerberos*, enabling multiple brands of servers to authenticate multiple brands of clients. These LAN authentication methods are usually transparent and work quite nicely, even in mixed networks.

Unfortunately, this uniformity falls away as you begin to add remote access authentications. There are so many different remote access tools, based on UNIX/Linux, Novell NetWare, and Windows serving programs, that most remote access systems have to support a variety of authentication methods.

PAP *Password Authentication Protocol* (*PAP*) is the oldest and most basic form of authentication. It's also the least safe, because it sends all passwords in clear text. No NOS uses PAP for a client system's login, but almost all network operating systems that provide remote access service support PAP for backward compatibility with a host of older programs (such as Telnet) that only use PAP.

CHAP *Challenge Handshake Authentication Protocol* (*CHAP*) is the most common remote access protocol, by which the serving system challenges the remote client by asking the remote client some secret—usually a password. If the remote client responds appropriately, the host allows the connection.

MS-CHAP *MS-CHAP* is Microsoft's variation of the CHAP protocol, using a slightly more advanced encryption protocol. The version of MS-CHAP that comes with Vista is version 2 (MS-CHAP v2).

Configuring Dial-up Encryption

It's the server, not the client, that controls the choice of dial-up encryption. Whoever configures the dial-up server determines how you have to configure the dial-up client. Microsoft clients handle a broad selection of authentication encryption methods, including no authentication at all. On the rare occasion when you have to change your client's default encryption settings for a dial-up connection, you'll need to journey deep into the bowels of its properties. Figure 26-28 shows the Windows Vista dialog box, called Advanced Security Settings, where you configure encryption. The person who controls the server's configuration will tell you which encryption method to select here.

Figure 26-28 Setting dial-up encryption in the Windows Vista Advanced Security Settings dialog box

Data Encryption

Encryption methods don't stop at the authentication level. There are a number of ways to encrypt network *data* as well. The choice of encryption method is dictated to a large degree by the method used by the communicating systems to connect. Many networks consist of multiple networks linked together by some sort of private connection, usually some kind of telephone line such as ISDN or T1. Microsoft's encryption method of choice for this type of network is called *IPSec* (derived from *IP security*). IPSec provides transparent encryption between the server and the client. IPSec also works in VPNs, but other encryption methods are more commonly used in those situations.

Application Encryption

When it comes to encryption, even TCP/IP applications can get into the swing of things. The most famous of all application encryptions is Netscape's *Secure Sockets Layer* (*SSL*) security protocol, which is used to create secure Web sites. Microsoft incorporates SSL into its more far-reaching *HTTPS* (HTTP over SSL) protocol. These protocols make it possible to create the secure Web sites people use to make purchases over the Internet. You can identify HTTPS Web sites by the *HTTPS://* included in the URL (see Figure 26-29).

Figure 26-29 A secure Web site

To make a secure connection, your Web browser and the Web server must encrypt their data. That means there must be a way for both the Web server and your browser to encrypt and decrypt each other's data. To do this, the server sends a public key to your

Web browser so the browser knows how to decrypt the incoming data. These public keys are sent in the form of a *digital certificate*. This certificate is signed by a trusted authority that guarantees that the public key you are about to get is actually from the Web server and not from some evil person trying to pretend to be the Web server. A number of companies issue digital certificates to Web sites, probably the most famous being VeriSign, Inc.

Your Web browser has a built-in list of trusted authorities. If a certificate comes in from a Web site that uses one of these highly respected companies, you won't see anything happen in your browser; you'll just go to the secure Web page, where a small lock will appear in the lower-right corner of your browser. Figure 26-30 shows the list of trusted authorities built in to the Firefox Web browser.

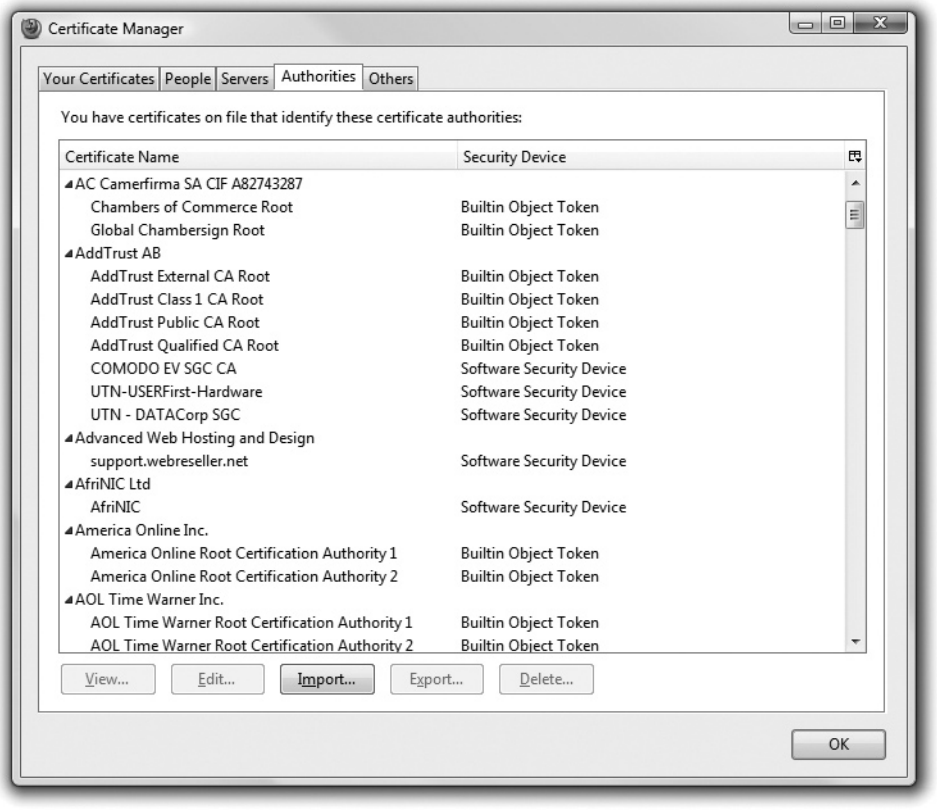


Figure 26-30 Trusted authorities

However, if you receive a certificate from someone *not* listed in your browser, the browser will warn you and ask you if you wish to accept the certificate, as shown in Figure 26-31.

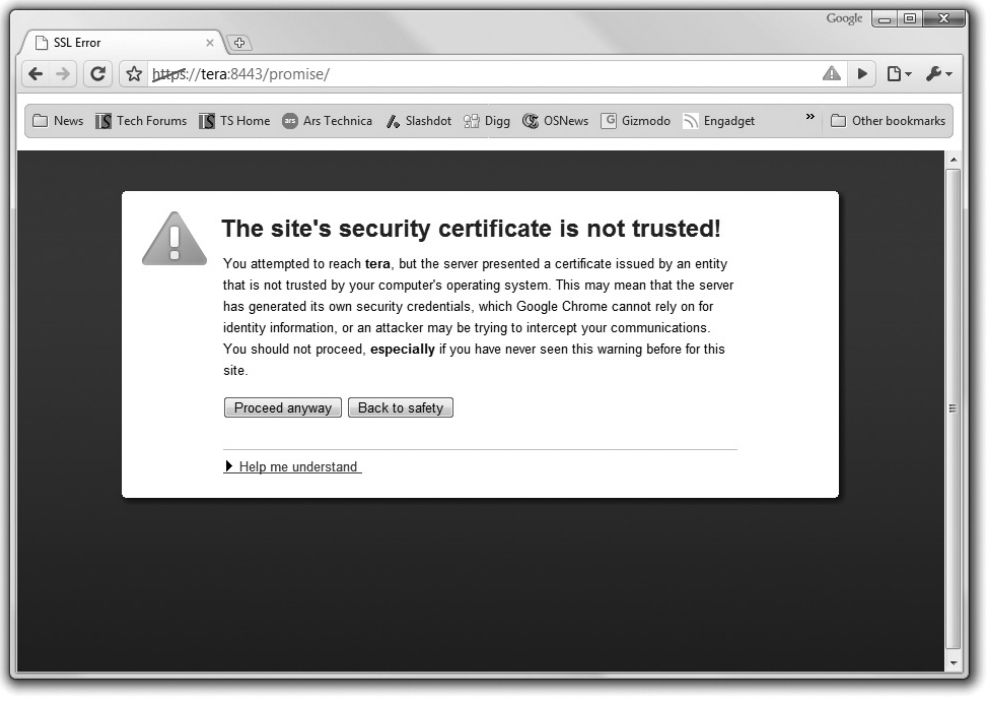


Figure 26-31 Incoming certificate

What you do here is up to you. Do you wish to trust this certificate? In most cases, you simply say yes, and this certificate is added to your SSL cache of certificates. However, an accepted certificate may become invalid, usually because of something boring; for instance, it may go out of date or the public key may change. This never happens with the "big name" certificates built in to your browser—you'll see this more often when a certificate is used, for example, in-house on a company intranet and the administrator forgets to update the certificates. If a certificate goes bad, your browser issues a warning the next time you visit that site. To clear invalid certificates, you need to clear the SSL cache. The process varies in every browser, but in Internet Explorer, go to the Content tab under Internet Options and click the *Clear SSL state* button (Figure 26-32).

Figure 26-32 The Internet Options Content tab

Wireless Issues

Wireless networks add a whole level of additional security headaches for techs to face, as you know from Chapter 24, "Wireless Networking." Some of the points to remember or to go back and look up are as follows:

- Set up wireless encryption, at least WEP but preferably WPA or the more secure WPA2 and configure clients to use them.
- Disable DHCP and require your wireless clients to use a static IP address.
- If you need to use DHCP, only allot enough DHCP addresses to meet the needs of your network to avoid unused wireless connections.
- Change the WAP's SSID from default and disable SSID broadcast.
- Filter by MAC address to allow only known clients on the network.
- Change the default user name and password. Every hacker has memorized the default user names and passwords.
- Update the firmware as needed.
- If available, make sure the WAP's firewall settings are turned on.

Chapter Review Questions

1. What is the process of using or manipulating people to gain access to network resources?
   - **A.** Cracking
   - **B.** Hacking
   - **C.** Network engineering
   - **D.** Social engineering
2. Which of the following might offer good hardware authentication?
   - **A.** Strong passwords
   - **B.** Encrypted passwords
   - **C.** NTFS
   - **D.** Smart cards
3. Which of the following tools would enable you to stop a user from logging on to a local machine but still enable him to log on to the domain?
   - **A.** AD Policy
   - **B.** Group Policy
   - **C.** Local Security Settings
   - **D.** User Settings
4. Which type of encryption offers the most security?
   - **A.** MS-CHAP
   - **B.** PAP
   - **C.** POP3
   - **D.** SMTP
5. Zander downloaded a game off the Internet and installed it, but as soon as he started to play, he got a Blue Screen of Death. Upon rebooting, he discovered that his My Documents folder had been erased. What happened?
   - **A.** He installed spyware.
   - **B.** He installed a Trojan.
   - **C.** He broke the Group Policy.
   - **D.** He broke the Local Security Settings.
6. Which of the following should Mary set up on her Wi-Fi router to make it the most secure?
   - **A.** NTFS
   - **B.** WEP

C. WPA

D. WPA2

7. What tool would you use to enable auditing on a local level?

A. AD Policy

B. Group Policy

C. Local Security Settings

D. User Settings

8. John dressed up in a fake security guard uniform that matched the uniforms of a company and then walked in with some legitimate employees in an attempt to gain access to company resources. What kind of attack is this?

A. Administrative access

B. Data destruction

C. Spoofing

D. Tailgating

9. The first day on the job, Jill received a spreadsheet that listed approved software for users and clear instructions not to allow any unapproved software. What kind of policy must she follow?

A. Classification

B. Compliance

C. Group

D. Security

10. Edna wants to put a policy in place at her company with regard to virus prevention or at least limitation. What policies would offer the best solution?

A. Install antivirus software on every computer. Teach users how to run it.

B. Install antivirus software on every computer. Set the software up to scan regularly.

C. Install antivirus software on every computer. Set the software up to update the definitions and engine automatically. Set the software up to scan regularly.

D. Install antivirus software on every computer. Set the software up to update the definitions and engine automatically. Set the software up to scan regularly. Educate the users about sites and downloads to avoid.

Answers

1. **D**. Social engineering is the process of using or manipulating people to gain access to network resources.

2. **D**. Smart cards are an example of hardware authentication devices.
3. **C**. You can use Local Security Settings to stop someone from logging on to a local machine.
4. **A**. Of the choices here, MS-CHAP offers the most security.
5. **B**. Zander clearly installed a Trojan, a virus masquerading as a game.
6. **D**. Mary should set up WPA2 on her Wi-Fi router.
7. **C**. You can enable local auditing through Local Security Settings.
8. **D**. John just practiced tailgating on the unsuspecting company.
9. **B**. Jill needs to enforce compliance to help keep the tech support calls at a minimum and the uptime for users at a maximum.
10. **D**. The best policy includes updating the software engine and definitions, scanning PCs regularly, and educating users.