THE INFORMATION WORKERS' SECURITY HANDBOOK

M

The Information Workers' Security Handbook

Topic Checklist

I want to know more about how the Internet works.
Go to this section: The Global Network of Networks: the Internet

I want to know how a typical business network works.
Go to this section: A Typical Business Network

What security risks are posed by networks?
Go to this section: The Security Risks Posed by Networks

I want to know more about e-mail exploits.
Go to this section: E-mail Exploits

I want to know more about remote access threats.
Go to this section: Remote Access Threats

What are the costs of security breaches to businesses and individuals?
Go to this section: The Consequences of Security Breaches

I want to know more about viruses, worms, Trojans and malicious executable programs.
Go to this section: Malware

How do attackers crack passwords?
Go to this section: Password Cracking

I want to know more about unwanted e-mail (spam).
Go to this section: Unwanted E-mail (spam)

What is phishing?
Go to this section: Phishing and Electronic Identity Theft

What is social engineering?
Go to this section: Social Engineering

How can I protect against viruses and malware?
Go to this section: Protecting Against Viruses and Malware

How can I protect against spyware and adware?
Go to this section: Protecting Against Spyware and Adware

How can I protect against Web exploits?
Go to this section: Making Web Browsing More Secure

How can I protect against social engineers and phishers?
Go to this section: Defending Against Social Engineers and Phishers

What should I do to protect my password and log on securely?
Go to this section: Protecting Your Password and Logging on Securely

How can I protect sensitive data?
Go to this section: Protecting Your Sensitive Data

Contents

Introduction

Today's information workers depend on computers and networks to perform many of their job duties. In the past, IT departments have focused on helping you become more productive and providing easier access to the data and network resources you need. As business networks have become more complex and interconnected, a new priority has emerged: securing the computer systems you use and the information that is stored on them and on the network.

Most computer users are aware of the risks involved in network computing today. These risks include:

- Viruses and other malicious code (sometimes known as *malware*).
- Intrusions by those who want to access the information on your system for unlawful purposes such as electronic identity theft, theft of trade secrets, and blackmail.
- Hack attacks by those who want to destroy your data and/or crash your computer.

Unfortunately, much of the available documentation either oversimplifies these issues or discusses them in highly technical jargon that can be confusing. Typical business computer users need to know what the risks are, how exploits work, and how to protect themselves and their computers.

This document provides, in plain language, the needed background information on how computer networks work and the specific security risks they face. It also provides real-world actions you can take to better secure your own computer and help preserve the security of the network as a whole. This document focuses on the needs of information workers whose computers are an integral part of their job duties, but who are not trained as technology professionals. If you use a computer that connects to a business network —either on-site or remotely—and connects to the Internet, this handbook is for you.

This document assumes users' computers are running the Microsoft® Windows® XP Professional operating system except where otherwise specified.

Note: This document was published in November 2004. For up-to-date security information, see the Microsoft Security Home Page at http://www.microsoft.com/security/default.mspx.

The Nature of Networks

A computer network is a group of computers and peripheral devices that are connected together and that communicate with each other through cable wires, phone lines, wireless connections, or some other medium. Networked computers can share files, exchange messages, access common printers and scanners, share an Internet connection, and more.

Networked computers communicate with each other using *protocols,* which are sets of rules that govern how the communication takes place. Most networks today use the Transmission Control Protocol/Internet Protocol (TCP/IP), the protocol that is used to communicate over the global Internet. It is a very powerful and robust protocol that allows millions of computers to communicate with each other all over the world.

Networks make it easy for workers to collaborate on projects. Organizations and individuals can make all types of information available, either to a limited group of computers and users or to the entire world. Such information can exist on internal file servers, external file transfer protocol (FTP) servers, or internal or external Web servers.

How Networks Work

There are two basic types of computer networks:

- **Peer-to-peer or workgroup networks,** in which all computers on the network function more or less as equals. Each computer has resources (such as data files) stored on it and may have peripheral devices (such as printers) connected to it that can be shared with other computers on the network. The user of each computer controls that computer's resources and can allow or deny access to them, usually by using passwords.
- **Client-server networks,** in which resources are stored on computers designated as servers that are accessed by computers referred to as clients or workstations. Servers typically run special operating system software, such as Windows 2000 Server or Windows Server™ 2003. Client workstations run operating systems such as Windows 2000 Professional or Windows XP. Windows –based client-server networks are organized into entities called *domains* that function as security boundaries. Network administrators can centrally manage the network's security and access to its resources using servers that are called *domain controllers.*

Peer-to-peer networks work well for small networks that only contain a few computers, such as home or small business networks. There is no need for a network administrator because control is decentralized – that is, resources are spread out among all the computers on the network and controlled by the administrator of each computer. Every computer can act as a server, sharing its files and peripherals with others. Every computer can also act as a client, accessing the resources of other computers. This configuration is not very secure, because many different people are equally responsible for securing the network's resources and they are not usually trained as network administrators.

Client-server networks are more appropriate for larger networks. If your business network has more than ten to fifteen computers, it is probably a client-server network. One or more dedicated network administrators control all network resources, which makes this a centralized security model. This configuration makes the network more secure, but may also make it more difficult for you to access the resources you need on other computers on the network.

In addition to being categorized as peer-to-peer or client-server, networks are often categorized based on the geographic area they span. The most common categories include:

- Local area networks (LAN) and wireless LANs (WLAN).
- Wide area networks (WAN).

Note: Other network types are more limited in area. These include home area networks (HAN), family area networks (FAN) and personal area networks (PAN). You might also hear terms such as MAN (metropolitan area network, which covers an area larger than a LAN but smaller than a WAN – typically about the size of a city), SAN (storage area network, which connects servers to data storage devices over fibre channel or other fast technologies) and even DAN (desk area network, which refers to the interconnection of devices that make up a multimedia workstation).

Local Area Networks (LANs and WLANs)

LANs cover a defined geographic area that can be as small as a single room or as large as a university or corporate campus. A LAN is usually owned or controlled by a single organization. Resources and users within the LAN are often referred to as internal resources or users. Users within a LAN usually have more access to internal resources, because there is often a firewall (a security barrier that is discussed later in this document) between the LAN and external users.

Access and communications between computers on the same LAN is fast, because they are usually (but not always) connected through Ethernet cables made of twisted pairs of copper wires. Ethernet typically provides data transfer speeds from 10 megabits per second (Mbps) to one or more gigabits per second (Gbps). These speeds are many times faster than a typical WAN or Internet connection.

Note: Other technologies sometimes used for cabled LANs instead of Ethernet include Token Ring, which uses a slightly different type of copper wire cabling (and is slower than Ethernet) and Fiber Distributed Data Interface (FDDI), which uses optical fiber cabling.

One building can be wired so that all computers in it are on the same LAN, or there can be many separate LANs, one for each floor or each office suite. However, the key point is that all computers on a LAN are connected to each other by cable or some other method.

An increasingly popular alternative to Ethernet cable for local area networks is wireless technology. Computers on wireless LANs (WLAN) communicate over the airwaves by using radio signals. WLANs eliminate the need to lay cable in hard-to-reach locations, and allow users of portable computers to move around within the building or campus, even outdoors, and still stay connected to the network. There are special security risks with both wired and wireless LANs, which are discussed later in this document.

Wide Area Networks (WANs)

As the name implies, WANs span greater distances than LANs. They operate over regular phone lines, ISDN (Integrated Services Digital Network) lines and dedicated leased lines (T-1, T-3, OC-3, OC-12). WANs can also be connected wirelessly, via satellite or cellular transmissions. Data transfer speeds on WANs range from less than 10 Kbps using some cellular technologies to 2.488 Gbps over OC-48 lines. Typical business WAN connections are in the range of 1.5 Mbps (T-1) to 45 Mbps (T-3). The following table shows relative transfer rates for different WAN link types.

Table 1: Data Transfer Rates for Different WAN Link Types

WAN link type	Data transfer rate	Typical cost/mo.	Comments
Analog phone lines	Up to 56 Kbps	$15-30 for phone line; $8-20 for ISP	Lowest cost, most widely available, not suitable for server hosting or high bandwidth applications.
Digital phone lines (ISDN, IDSL)	64 Kbps to 144 Kbps; same speed down and up	$50-80 for phone line; $25-100+ for ISP	May be the only relatively high speed, low cost link available in some areas.
Consumer Broadband (ADSL, cable Internet)	256 Kbps to 10 Mbps, typically 1.5 to 3 Mbps downstream; upstream usually throttled to 128-256 Kbps	$25-$60 for combined line and ISP	High speed, low cost. Not suitable for server hosting due to upstream throttling; not available in some areas.
Business Broadband (ADSL, SDSL, cable)	1.5 Mbps to 5 Mbps or more; upstream 256 Kbps to 768 Mbps	$75-200 for combined line and ISP	Higher upstream speeds may allow server hosting; not available in many areas.
T-1 (E-1 in Europe)	1.5 Mbps both ways (T1) 2.048 Mbps both ways (E1)	$300-1000+	High reliability, guaranteed uptime, suitable for server hosting; widely available.
T-3 (E-3 in Europe)	44.736 Mbps (T3) 34.368 Mbps (E3)	$10,000-15,000+	High reliability, guaranteed uptime; suitable for large businesses or ISPs.
OC-3 OC-12 OC-48	155.52 Mbps 622.52 Mbps 2.488 Gbps	Prohibitively expensive, up to several hundred thousands of dollars per month	Optical carriers; suitable for ISP backbone or very large enterprise network.

Note: One way to achieve greater WAN speed is to aggregate the bandwidth from two or more lines. For example, two aggregated T-1 lines (sometimes called “bonded”) can provide a transfer rate of about 3 Mbps.

WANs are often used to link two or more LANs together. For example, a dedicated leased line might connect the LAN at an organization's main office to the LAN at its branch office. Many WANs provide for redundant connections; that is, there are multiple paths that data can take to get from one point to another, as shown in the following figure. Each line represents a T-1 line connecting two offices. This design results in *fault tolerance;* if the line between the main office and the Oklahoma City office went down, those two offices could still communicate with each other by going through the Shreveport office.

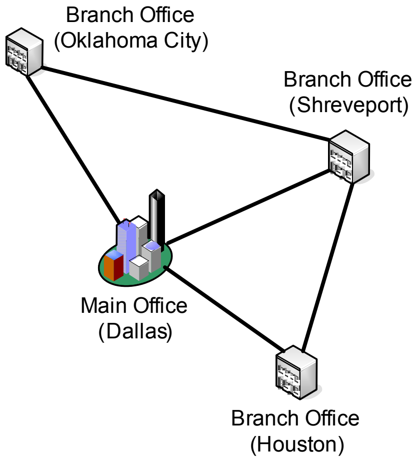


Figure 1
Redundant physical connections create fault tolerance, so that if one link goes down, communications can still take place

WANs are also used to link a LAN to an Internet service provider (ISP). The Internet is, in fact, the largest and most redundant WAN in the world.

The Global Network of Networks: The Internet

The Internet began as a joint project between the U.S. Department of Defense and major universities. It has evolved into a global commercial network connecting millions of computers and LANs to one another.

Individual users and organizations generally do not connect directly to the Internet “backbone,” because this type of connection is very expensive. The backbone network is made up of extremely fast fiber optic trunk lines. Network access points (NAP) connect to the backbone. ISPs connect to these NAPs, and individuals and organizations contract with the ISPs for Internet service. When a home user dials into an ISP or connects to an ISP over a broadband network, or a business connects to an ISP via a T-1 or T-3 line, the user’s computer and the business’s LAN become part of the ISP’s network.

Routers are devices that handle the tasks of getting data from one network to another and determining the best path for the data to take to reach its destination. Routers are used to join separate networks to each other and allow communications to pass between them, so they are also called gateways.

Computers on the Internet use the TCP/IP protocol, and every computer or router that is directly connected to an ISP has a unique identification number called an IP address. In the case of a LAN, not every computer on the internal network has to have a public Internet IP address. Instead, one computer (or a specialized computer device such as a firewall or proxy server) on the LAN can be directly connected to the ISP, and the other LAN computers can send and receive messages to and from the Internet through it, using a technology called network address translation (NAT). Computers on the Internet are also identified by names. The Domain Name System (DNS) translates names (for example, the name *www.microsoft.com* that you type into your browser to access a Web server) to IP addresses (for example, 207.46.130.108) that are understood by the Internet routers.

The Internet works through the interaction of client-server software. For example, your Web browser is a client program that can access Web pages stored on a computer running Web server software. Microsoft Outlook®, Outlook Express and other e-mail applications are client programs that can access mail messages stored on a computer running mail server software. Other Internet client programs you might have installed on your computer include Instant Messaging clients, FTP clients, newsgroup clients (often called news readers), Really Simple Syndication (RSS) clients, Internet Relay Chat (IRC) clients, Telnet clients, and peer-to-peer (P2P) clients, as well as client programs for connecting to online services such as MSN® or AOL.

Today, most home computers, business LANs and the computers on government and school networks are all interconnected through the Internet. This interconnectivity creates a powerful network that allows almost anyone to communicate quickly with almost anyone else. It also creates a significant security risk.

A Typical Business Network

A typical business network consists of one or more LANs with various types of servers, including some or all of the following:

- File servers where users store their data documents.
- Mail servers through which users send and receive e-mail.
- Web servers that host the organization's Web sites.
- Database servers that store information in easily queried format.
- Remote access and/or VPN servers through which employees and partners can connect to the LAN from home, while on the road, or from other remote sites.
- Authentication servers (domain controllers on Windows–based networks) that verify users’ credentials to log on to the network.

There are also many types of specialty servers, such as those that host e-commerce sites or live communications services and those that help administrators better manage the network. Sometimes one computer runs multiple server software applications and fills more than one server role.

Almost all business networks are connected to the Internet, usually through a T-1 or other dedicated leased line (but in the case of small businesses, sometimes through a broadband connection or even a dialup analog connection). Internet-connected business networks usually deploy a *firewall* between the Internet and the LAN. A firewall is a dedicated computer that runs special software that allows it to monitor incoming and outgoing LAN traffic and block or allow specific types of data traffic each way. The Microsoft Internet Security and Acceleration (ISA) Server is an example of a firewall. More information about firewalls is provided later in this document.

In addition to all these servers, business networks contain client computers, which are the workstations (desktop or portable computers) that employees use to perform everyday computing tasks. Word processing, spreadsheet calculations, accessing database information, composing and reading e-mail, and surfing the Web are all done on client computers. Some businesses use “thin" clients, which are low-powered computers that do not actually have application programs such as Microsoft Word or Excel installed on them. Users of thin clients connect to a terminal server that runs the applications. The application displays on the users’ screens, but it is actually running on the terminal server.

Business networks can range from a handful of Windows–based client computers connected in a simple peer-to-peer network to a complicated client-server network that spans multiple physical locations and multiple Windows–based domains, each with its own administrators and policies. The more complex a business network becomes, the greater the security risks it faces, and the more comprehensive its security policies must be.

The Security Risks Posed by Networks

The whole point of networking is to share, but allowing others to access a computer creates opportunities for those with malicious motives, too. Early networks were relatively secure because they were closed systems, and to do any damage you had to have physical access to a system that was wired to the LAN. Remote access and Internet connectivity have changed that. Wider availability and lower cost of broadband (DSL and cable) connections means that even home computers remain connected to the Internet 24 hours per day, which increases the opportunities for intruders to gain access.

Computer operating systems were originally designed for stand-alone computers, not networked ones, and security was not a priority. When networking became popular, operating systems and applications focused on easy accessibility instead of security. Because of this earlier focus on accessibility, security has to be retrofitted into many systems today. Modern operating systems such as Windows XP are designed with security in mind, but they still must operate using traditional networking protocols, which can result in security issues.

Access vs. Security

Users want easy access to network resources. Administrators want to keep the network secure. These two goals are at odds, because access and security are always on opposite ends of the continuum; the more you have of one, the less you have of the other.

For business networks, the key is to strike a balance so that employees are not frustrated and inconvenienced by security measures, while maintaining a level of protection that will keep unauthorized persons from gaining access. Specific security enforcement mechanisms are discussed later in this document.

Internal Security Threats

Internal security threats are those that come from within the organization or site, as opposed to those that come through the Internet or dial-up access. Internal threats include employees who deliberately attempt to steal data or introduce viruses or attacks on the network. Other internal threats are posed by outside workers (contract workers, janitorial services, people posing as utility company employees, and so on) who have physical access to the LAN computers. However, many internal threats are accidental. Employees may install or use their own software or hardware for their convenience, unaware that it poses a security risk to their computers and the entire network.

Unauthorized Software Installation

Installing unauthorized software programs (such as games to play during break time) on your computer at work may seem harmless or even beneficial (as with applications that make your job duties easier). However, software from unauthorized sources can create many problems. For example:

- Freeware and low-cost software downloaded from the Internet or distributed on floppy disks or CDs can contain viruses that will infect your system and spread to other computers on the network.

- Unauthorized software may be poorly written, intended for use with a different operating system, or have conflicts with currently installed software that can cause it to crash your computer or send unwanted messages on the network.
- Unauthorized software might be pirated (copied illegally), which could subject your organization to penalties in case of a software audit.

Unauthorized Hardware Installation

Bringing your own hardware devices to connect to your work computer is not a good idea, either. Many hardware devices, particularly those that allow data to leave the premises, create security issues.

Unauthorized Modems

Sometimes employees attempt to avoid their organization's firewall restrictions by bringing their own modems and attaching them to their business computers and phone lines, and then dialing into their personal ISPs. They may believe that doing this on their own time (during lunch or breaks) is okay. However, it creates a major security problem because the computer is still connected to the LAN while it is connected to the Internet through the modem. Without the firewall protections that are applied to data coming from the Internet to the LAN through the organization’s authorized Internet connection, all types of malicious code and attacks can penetrate and spread from the user’s computer throughout the LAN.

Unauthorized Wireless Access Points

Some employees may have wireless access points on their home networks, and appreciate the convenience of being able to walk around with their laptops or handheld computers and stay connected to the network. These employees might think it is a great idea to bring a WAP to work and plug it into the Ethernet ports in their offices, creating a wireless connection so they can take their laptops to the break room or wander around the halls with their handhelds and still access their e-mail or documents.

The problem is that wireless networks can be particularly vulnerable to attacks and intrusions because the signal can be picked up by anyone with a portable computer that is equipped with a wireless network interface card (NIC). Anyone else could also sit in the break room with a laptop and access the organization’s network through an unauthorized WAP.

Unauthorized Portable Storage Devices

Miniature so-called “thumb drives” and tiny flash memory card readers/writers can be easily plugged into a computer’s universal serial bus (USB) port and recognized as an additional drive. Files can be uploaded from the devices to the computer, and information can be downloaded from the computer to the drives.

Obviously, these devices provide an opportunity for viruses and other malicious code to be transferred to computers, either deliberately or accidentally. They also provide a way for employees to copy and take away files that should not leave the organization's network. Although they are very convenient for taking documents home to work on, they should never be used on your business network without the knowledge and permission of the IT department.

Unauthorized Printers

In a business environment where some of the data on the network is sensitive (which includes most business networks today), it is not just electronic copies of data that can pose a security threat. Printed data that falls into the wrong hands can be just as problematic. Some employees prefer to print their work because they are not comfortable proofreading it on screen, but if you haven’t been given access to a printer, it might be because printouts are prohibited for security reasons. Employees who install unauthorized printers and use them to print business files without permission put their organization at risk.

Note: If you do obtain permission to print your work, you should be careful to protect any printed material that could be sensitive or confidential (this topic is discussed later in this document). Keep track of the number of copies and ensure that they are kept in a locked file when you leave the office. Keep a log noting to whom (and when) you give copies, and shred documents that are no longer needed. Also be sure to shred or otherwise destroy any “bad” or extra printouts rather than just dumping them in the trash for anyone to find.

External Security Threats

External security threats are those that come from outside the LAN, usually over the Internet (but sometimes through dial-up connections to a remote access server on the LAN). These threats are the ones we usually think of when we talk about hackers, crackers, and network attackers. Such people can exploit flaws and characteristics of computer operating systems and software applications. They exploit the way various network communications protocols work to do a variety of things, including the following:

- Enter a system and access (read, copy, change or delete) its data.
- Crash a system and damage or destroy operating system and application files so they do not work.
- Plant viruses and worms that can spread to other systems across the local network.
- Use the system to launch attacks against other systems or other networks.

Operating System and Application Exploits

Computer operating systems are sophisticated programs that contain millions of lines of code. Just about every software program has some bugs (flaws in the code). Because of their size, operating systems often have many bugs. Attackers can write code to exploit bugs in both operating system and application software to gain access to a system. To use an analogy, think of a house that has a broken lock on the back door. The condition of the lock is a flaw that a burglar can use to gain access to the house.

Not all exploits are based on actual flaws in software code. In some cases, attackers just exploit the normal way the program works. To use another analogy, your home has vulnerable places that a burglar can exploit in order to break in. Glass windows are one such vulnerability, because even if you have great locks on them, a burglar can break the glass and enter the house. This does not mean that a house with windows is flawed.

According to the CERT Coordination Center at Carnegie Mellon University, there were more than 15,000 vulnerabilities reported between 1995 and the third quarter of 2004. This information is available on the CERT/CC Statistics page at www.cert.org/stats/cert_stats.html.

There are also exploits based on bad configuration. For example, Windows XP can be configured to allow logon without a password, or to require a password to log on. The former configuration can be exploited by hackers to access the system. To return to the previous analogy, the doors on your house can be configured as unlocked, locked with a deadbolt, or locked with only the default latch bolt that can be easily picked. If, for convenience, you lock only the latch bolt when you leave and not the deadbolt, this configuration could be exploited by a burglar who can slip a thin piece of plastic or metal between the door jam and door to disengage the lock.

An example of a common code exploit is the *buffer overflow* attack. Programs are often written with limits on the number of characters or bytes that can be entered in a particular field. The number is usually far greater than would ever be normally entered in that field. Hackers use buffer overflow attacks to deliberately exceed these limits and make the program crash.

Note: When flaws or vulnerabilities are discovered in programs, software vendors usually create fixes or patches that you can apply, just as you would install a new lock if you discovered the one on your back door was broken. Keeping your system updated with the latest patches and service packs is very important.

E-mail Exploits

Your e-mail program can be a point of vulnerability because it is where messages from many different sources enter your computer. Attackers do not have to worry about how to get in, because almost every system is configured to allow e-mail in. There are many ways e-mail can be used by attackers, including the following:

- A virus or other dangerous file can be sent with e-mail as an attachment. Any *executable* file (a file that is a program) is dangerous because programs can crash your computer, delete files, send messages to everyone in your address book without your permission, or create a *back door* through which hackers can access your computer later. All executable files can be dangerous. For more information, see the discussion of malicious executable files later in this document. Even graphics files, such as .jpg files, can exploit programs that process these files. According to reports from MessageLabs, which monitors approximately 50 million customer e-mails every day, more than five and half billion messages were scanned during the first six months of 2004, and one out of 12 carried a virus or worm. (See the article "Spammers and hackers in 'smart' virus attacks" at http://software.silicon.com/malware/0,3800003100,39123257,00.htm.)
- HTML e-mail can contain embedded scripts and ActiveX® controls that cause your computer to perform unwanted actions.
- Plain text e-mail can contain URL hyperlinks that, if clicked, take you to Web pages that contain embedded malicious code.
- The auto-response function of e-mail programs can be exploited to set up a feedback loop that results in a mail flood, which can overwhelm the mail servers.
- E-mail is often used for *social engineering* attacks in which fraudulent e-mail messages attempt to convince recipients to divulge passwords, credit card numbers and other sensitive information (also called *phishing*, because attackers send out hundreds or thousands of such messages, hoping for a few responses).
- E-mail is used to *spam* recipients with mass mailings of unwanted commercial e-mail. According to the MessageLabs Email Threats page at www.messagelabs.com/emailthreats/default.asp (click the **spam** tab and select **Last 12 months** in the drop-down box to select the view for the graph), in October 2004 more than 70% of e-mail messages scanned were spam.

Malicious Web sites

Web sites, like HTML mail, can include embedded scripts and ActiveX controls that can crash your computer, upload a virus, or capture your password or other information. Such actions are especially common on Web sites devoted to “warez” (pirated software) and pornography, but can occur on any Web site. Web site scripts can be used to cover the address bar on the browser with a spoofed (fake) URL so that you think you are at a legitimate site, and even to install software on your computer.

Instant Messaging

Instant Messaging (IM) chat programs provide a convenient way to communicate with others in real time, but attackers can exploit their features and make them a threat to the security of your computer and the network. The simplest exploits merely send messages containing links to malicious Web sites, or use the IM client's file sharing capability to send files that contain viruses and other malware.

Unencrypted IM traffic can be intercepted using so-called "man in the middle" attacks, which allow hackers to impersonate one of the parties to the IM conversation.

File Sharing and Downloads

P2P file sharing programs provide yet another entry point for viruses, worms and attackers. Devious employees could also use these programs to circumvent their organizations' security policies; for example, they could disguise sensitive Word documents as MP3 files and make them available to outsiders using P2P software. Even if no deception takes place, trading music and movie files on a P2P network may constitute copyright violation and subject the organization to legal sanctions.

Downloading files from Internet Web sites and FTP servers can also present security issues. The dangers of executable files and HTML documents have already been discussed, but even word processing documents can contain macros (small programs). The recently publicized .jpg exploit shows that even graphics files are not always safe.

Remote Access Threats

Remote access users are those who connect to an organization's network from off-site locations, including telecommuters and after-hours workers who connect from home, executives who travel and connect from hotel rooms, and sales or support people who connect from clients' and partners' networks. There are two basic types of remote access:

- **Dial-up remote access,** which uses a modem on the off-site computer to call a phone line that is connected to a special remote access server on the organization's LAN.
- **Virtual private networking (VPN),** in which both the off-site computer and a VPN server on the organization's LAN are connected to the Internet. Special protocols are used to create a "tunnel" or virtual network directly between the two systems through the Internet.

Remote access presents special security threats because the organization's network administrators do not have as much control over off-site computers as they have over those physically wired to the LAN. A significant risk is presented when off-site users can access the Internet through their own Internet connections at the same time they are accessing the LAN through VPN. This *split tunneling* renders the VPN and LAN susceptible to attacks from the Internet that bypass the LAN's firewall. The same risk is present if a user connects to a remote access server through a modem while connected to the Internet through a broadband connection.

Dial-up connections have a security advantage in that they do not traverse a public network (the Internet) and are therefore less susceptible to interception. VPN connections have a security advantage in that their communications are encrypted for privacy. VPN is usually the most cost-effective way to provide remote access, and is the most popular method.

The Consequences of Security Breaches

A security *breach* occurs when a computer system or network is compromised in such a way that data is accessed by unauthorized persons; network bandwidth is used by unauthorized persons; damage is done to data, applications or systems files; or an outage or denial or service is caused.

A breach can be deliberate or unintentional, and results can be relatively benign (for example, a teenage hacker reading a non-sensitive company file) or devastating (an entire network is disabled for hours or days, resulting in loss of worker productivity, loss of revenue, and loss of customers' confidence in the business).

Cost to Businesses

Costs to businesses of security breaches run into the millions of dollars every year. Tangible, measurable monetary costs can include the following:

- Labor and materials required for IT personnel to detect, repair, and contain the damage to breached resources.
- Loss of worker productivity while the system(s) or network is down.
- Lost business due to unavailability of e-commerce sites, customer information, or databases needed by sales personnel.
- Public relations costs to address questions from the press and public.
- Legal costs involved in collecting evidence and prosecuting an attacker.
- Legal costs incurred as a result of lawsuits if confidential client information is breached.
- Fines and penalties incurred if the breach violates regulatory requirements.
- Insurance premium increases.

According to case studies documented in the article "The Cost of Network Downtime" at http://telephonyonline.com/ar/telecom_cost_network_downtime/, just one hour of downtime can cost an organization up to $96,632. Intangible costs include loss of future potential business caused by publicity about the breach and loss of market share to competitors.

Consequences to Individuals

Because the impact of a security breach to the organization can be so great, most organizations take breaches very seriously. An employee who deliberately breaches security can expect disciplinary action up to and including termination of employment, and might even face a civil lawsuit or criminal prosecution.

Individuals who do not practice secure computing can also suffer personal consequences. If you store personal information on your computer, a security breach could allow hackers to discover your social security number, banking information, credit card numbers, or other credentials that could result in identity theft. An intruder could read your personal e-mail and divulge your private conversations to others. A malicious hacker could even plant pornographic images or other incriminating data on your computer that could incriminate you in the eyes of your organization or law enforcement.

Understanding the Threats

The term *computer security* is a broad one, and it involves protecting your system and network from many different types of threats. These threats include viruses and related malware, executable programs of all types, password cracking, electronic eavesdropping, spyware, hack attacks (including wireless exploits), spam (which often contains phishing links that result in identity theft), and social engineering attacks that rely more on “people” skills than technological skills.

Malware (Viruses, Worms, Trojans and Malicious Executable Programs)

Malware is an abbreviation for malicious software, and refers to programs that perform unwanted actions. These programs include viruses, worms, Trojans and other malicious executable programs. Also included are spyware and adware programs that are installed on a system without the user’s permission. These terms are explained in more detail in the following sections.

Viruses and Worms

Computer viruses and worms are small, unwanted programs that replicate themselves. Some are relatively harmless (for example, those that pop up a dialog box at a specified time or date). Others can do great damage by deleting files, crashing programs, or flooding networks with so much traffic that normal network communications become impossible.

Programs that replicate themselves by exploiting security vulnerabilities to spread across a network are called worms. By some definitions, viruses spread from one file to another within the same computer and worms are designed to spread from one computer to another. By other definitions, viruses require that the user do something (for example, click on a file or open an e-mail message) to get infected, whereas worms do not rely on human interaction to copy themselves. Another difference is that viruses attach themselves to other software programs (such as word processing programs, e-mail programs, or even operating systems), and worms reside in active memory and do not need a host program to attach themselves to.

Viruses and worms can be spread through e-mail attachments and HTML mail, online P2P file sharing services, instant messages, Windows file sharing, or files downloaded from Web sites, FTP sites, newsgroups, or other sources. They may lie dormant until a particular date or time or specific circumstances trigger them. Viruses and worms that are programmed to activate on a certain date or time are called *time bombs*. Those that are programmed to activate under certain conditions (for example, the tenth time you open a particular program) are called *logic bombs*.

Trojan Horses

Trojan horses (also called Trojans) do not infect other files or replicate, but are malicious programs that are disguised as legitimate software. They are often installed along with free software such as games or screensavers. Once installed, Trojans perform some malicious action, typically creating a back door that allows hackers to seize control of the computer or send passwords or other stored sensitive information to the hacker.

Malicious Executable Programs

Some programs perform unwanted actions (for example, deleting all Microsoft Word files) on your computer, but do not replicate themselves and do not allow others to access your system. Dangerous files include those with the .exe, .cmd, .bat, .js/.jse, .reg, .scr, .vb/.vbe/.vbs, and .wsf extensions. In addition, Microsoft Office files, such as Word .doc files and Excel .xls files, can contain *macros,* which are small programs that can perform malicious actions.

An example of a malicious program is dialer software that surreptitiously changes the settings of a modem's dialup connection so that it will call a 900 number or other expensive long-distance number.

Adware and Spyware

Adware refers to software products that display advertising. The adware may be part of a legitimate free software program, or it may be a separate program that is installed along with another program that you downloaded or bought. Sometimes you do not even have to explicitly install anything to get infested with adware; all you have to do is visit a Web site or open an HTML e-mail message. One type of adware is a *browser hijacker* program that changes your Web browser's home page.

A particularly insidious form of adware is *spyware*, which collects information about your system or your computer activities and transmits it to the program's developers for statistical and marketing purposes. For example, spyware may send a list of Web sites that you visited. When you install the software you *do* want, you may or may not be informed that the adware or spyware is also being installed. This information is often buried in a long, legalistic end user license agreement (EULA) which you must accept in order to install the original software. There are a number of free toolbar utilities that include adware and/or spyware. According to McAfee, there were more than 14 million adware and spyware programs that had been detected by the first quarter of 2004 (see "How to Prevent the Online Invasion of Spyware and Adware" at www.internetworldstats.com/articles/art053.htm).

An especially dangerous type of spyware is not intended to collect information for marketing, but is designed to log your keystrokes or save images of your screen so that someone else can monitor what you do on the computer. This type of spyware can be used for identity theft (see our discussion of electronic eavesdropping later in this document).

Note: "Cookies" are small text files placed on your computer by a Web site to retain information you have entered on the site so you will be recognized when you return to the site from that computer. Cookies are legitimate mechanisms that make Web surfing more convenient. For example, you can put an item in an online shopping basket on an Internet commerce site and it will still be there when you log on to the site again later. Cookies can also be used to track your Web activities and target specific advertising to you based on your activities.

Password Cracking

Most computer security mechanisms use user accounts and passwords to identify users and determine what permissions they have on a system or network. Passwords are also used to protect individual files, to access e-mail accounts, and to visit protected Web sites. In the case of administrative accounts or sensitive files, discovering passwords is like finding master keys, so it is no wonder that hackers spend a lot of time attempting to “crack” passwords. Although there are many ways to break into a system, the easiest way is to simply log on with a valid user name and password.

A common method of cracking a password is to simply guess it, based on commonly used passwords or personal information about the user, such as the name of a spouse, child, or pet, or a social security or phone number.

Other common password cracking techniques use software to launch *dictionary attacks* that quickly try out all the words in the dictionary or *brute force* attacks that try out all possible combinations of letters, numbers and symbols. Password cracking software is readily available on hacker sites and from newsgroups.

Passwords are also often cracked through social engineering techniques (see the discussion of this topic later in this document).

Electronic Eavesdropping

Interception of electronic communications can be done in a number of ways. Eavesdroppers who have physical access to the network can use protocol analyzer software (informally called *packet sniffers*) to capture individual packets of data and look inside them to piece together information and messages. Malicious programs can be disseminated through viruses or included in Web downloads to automatically e-mail copies of a user’s files to the attacker. Monitoring software can log Web sites that are visited, chat conversations, and every keystroke. Copies of your incoming and outgoing e-mail can be redirected to the attacker. There are literally hundreds of surveillance software products (some of them free) that can be used to intercept network communications.

Hack Attacks

There are literally hundreds of specific attacks that can be used to gain access to or bring down a computer system or network. Some, such as the man in the middle attack, are designed to intercept messages between two parties and modify them. Others exploit flaws or characteristics of protocols, operating systems, or applications to crash a system or take control of it.

Intrusion detection systems (IDS) are designed to monitor for suspicious activity that may indicate an attack. IDSs are discussed later in this document.

Denial of Service Attacks

Denial of service (DoS) attacks involve flooding a system or network with more data than it can handle, so the system crashes or network bandwidth is so clogged that legitimate communications cannot occur.

Distributed DoS (DDoS) attacks are more sophisticated. In such an attack, the attacker takes control of a number of computers over the Internet by secretly installing software on them that lets him control them remotely. Then he uses these *slave* or *zombie* computers to launch the DoS attack against another system or network. This approach keeps the attack from being traced to the real attacker. Unprotected systems are not only in danger of being the target of a DoS attack, but are also in danger of being used as an intermediary attacker in a DDoS attack.

There are a number of different technical methods for creating a denial of service. Names of common DoS/DDoS attacks include buffer overflow, SYN flood, teardrop attack, and Smurf attack. Unfortunately, hackers do not have to be highly skilled to launch attacks, because there are dozens of DoS/DDoS tools available on the Internet.

Port Scanning

A port is a logical point of connection that is used by network applications for communications between two computers. Ports are numbered, and different applications use different ports. For example, the Post Office Protocol (POP) that is used to download e-mail from an ISP's server uses port 110. There are 65,536 available ports on a typical computer system.

Port scanning is technically not an attack, but is often a precursor to an attack. Attackers use scanning software to discover which ports are open on a system, and then try to enter the system through an open port. You can (and should) block unnecessary ports with a firewall. Port scanning is analogous to a burglar knocking on doors to determine which houses are empty and thus available to be burglarized.

Spoofing

Spoofing is not an attack either, but a mechanism used by attackers to disguise the origin of an attack. IP spoofing involves forging the source IP address on data sent over the network so that it appears to come from a different computer or network. E-mail spoofing involves changing the header information on e-mail messages to make them appear to come from someone other than the true sender. Web spoofing involves attackers creating false copies of a Web site or entire Web which they control, so that victims are actually visiting the attacker's Web server when they think they are visiting a legitimate Web site on a different server.

Wireless Exploits

If you use wireless networking, you may be susceptible to some special exploits. Hackers can use all the attacks described earlier against wireless systems and networks, but they can also exploit the way wireless communications are sent over the airwaves to obtain access to a wireless network more easily.

Do not think that you are safe because your wireless equipment lists its range as 300 feet. Hackers can use high powered directional antennas attached to their wireless network cards to extend the range and intercept wireless communications from further away.

Wireless security precautions such as MAC address filtering, which lets you specify that only computers with particular physical addresses can connect to the wireless network, will not necessarily protect you from a determined hacker, either. A savvy hacker can intercept wireless communications between two legitimate computers on the wireless network and then spoof the MAC address of one of them to gain access to the network.

More information about wireless security is provided later in this document.

Unwanted E-mail (spam)

Unwanted e-mail is called by many names, including unsolicited commercial e-mail (UCE), unsolicited bulk e-mail (UBE), junk mail, and spam. Characteristics of this type of mail include:

- It is intended to persuade you to buy something or do something.
- It is sent by someone with whom you have no pre-existing relationship and is not in response to any request for information by you.
- It is sent in a mass mailing, with the same message going to dozens, hundreds, or even thousands of addresses.

Some UCE is sent by legitimate organizations in the belief that mass mailings are a viable marketing tool. Others make fraudulent claims, do not deliver the promised products after payment is received, or use questionable tactics such as fake return addresses and deliberate misspellings designed to circumvent junk mail filters.

Worse, some UCE is not distributed for the purpose of selling, but for the purpose of tricking recipients into divulging sensitive information that can then be used to steal from them. This moves it from the category of spam to the category of phishing, which is discussed in the following section.

UCE has become an enormous problem, filling up mailboxes and making it difficult for users to sort through it and find their legitimate e-mail and even overwhelming mail servers to the point of causing them to crash. The problem is so bad that federal and state legislatures have passed laws against *spamming* (for more information, there is a spam laws Web site at www.spamlaws.com/). However, these laws can be difficult to enforce because of jurisdictional issues when e-mail crosses international lines and deceptive practices that disguise the senders' true identities.

Phishing and Electronic Identity Theft

The most dangerous type of electronic mass mailing is sent by *phishers* who create messages that are designed to look as if they were sent from banks, mortgage companies, brokerage firms, ISPs, or other legitimate organizations with which the recipients may do business, such as Citibank, PayPal, or eBay.

These messages instruct you to respond with account numbers, passwords, social security numbers, or other sensitive information. Sometimes they direct you to log on to a Web site and fill out a form asking for sensitive information. These messages have forged return addresses and headers, and the Web sites usually have spoofed Web addresses to make them appear to be the sites of the organizations being impersonated. Often the messages say that your account will be suspended or your funds frozen unless you provide the information. If you respond with the requested information, it is used to access your accounts and/or steal your identity and set up new accounts in your name.

According to the Anti-Phishing Working Group (an organization committed to eliminating Internet scams and fraud), 1,974 different phishing attacks were reported in the month of July, 2004 alone, and the number of reported phishing attempts grew by 50% per month from May to July. You can view the July 2004 "Phishing Attack Trends Report" at http://antiphishing.org/APWG_Phishing_Attack_Report-Jul2004.pdf.

Phishing can be considered a variant of a hacking technique called social engineering, which is discussed in the next section. For more information, see the article "Phishing" at www.computerworld.com/securitytopics/security/story/0,10801,89096,00.html.

Social Engineering

This term is used by hackers to describe the art of persuading people to divulge information, such as account names and passwords, which will allow the hackers to access a system or network. These methods depend on people skills rather than technical skills, since they exploit human nature rather than software or hardware vulnerabilities.

A good social engineer is an accomplished actor who tries to charm or intimidate network users into giving him sensitive information. Common ploys include pretending to be an organization executive or member of the IT staff, a fellow worker, or a member of an outside organization, such as a network consultant or phone company employee. A survey by BBC News indicated that more than 70% of people who work with computers were willing to reveal their passwords and information that could be used to steal their identities. Information about the survey is available in the article "Passwords revealed by sweet deal" at http://news.bbc.co.uk/2/hi/technology/3639679.stm.

Kevin Mitnick was one of the most famous hackers of the 1980s and 1990s, and served five years in prison for breaking into telephone and computer systems. He now lectures and writes about computer security, and says that social engineering is one of the most dangerous hacking techniques because the best technology in the world cannot defend against it. This human factor is one of the most often overlooked threats to computer security.

More information about social engineering is available in "Social Engineering Fundamentals, Part I: Hacker Tactics" at www.securityfocus.com/infocus/1527 and in "Social Engineering Fundamentals, Part II: Combat Strategies" at www.securityfocus.com/infocus/1533.

Note: Hackers also use other non-technological methods to obtain information they need that do not even require good people skills. These methods include shoulder surfing (reading over your shoulder as you type your password), dumpster diving (retrieving information from the trash), and scavenger hunting (going through desk drawers, notepads, or briefcases for information).

Protecting Your Computer and Network

Understanding how networks and security threats work is only half the battle. In this section, we discuss what you, as an information worker, can do to protect yourself, your computer, and the networks to which it connects. Security measures you can put into practice include physically securing your systems, using software mechanisms to protect against exploits, and being aware of the human factor and how you can defend yourself against social engineers. This section reviews the special security issues involving wireless networks and discusses logon authentication, which serves as your first line of defense. It also examines the importance of keeping your operating system and applications updated with the latest security patches and service packs, and shows you how to take extra steps to protect sensitive data. Finally, it outlines how all these practices work as part of a multi-layered security plan.

Physical Security

The first step in securing your data is securing the hardware on which it is stored and by which it moves across the network. This step means limiting who is able to actually touch the computer, and what a person can do with it if they do gain on-site access.

Note: Because the goal of security is to protect your computers, network, and data from all types of damage and loss, physical security should also include protection from natural disasters and accidental damage in addition to deliberate acts. Physical security means installing smoke detectors to guard against fire damage, using uninterruptible power supplies (UPS) to protect against power surges and power loss, maintaining proper temperatures for computer operation, and keeping computers out of vulnerable areas (for example, away from glass surfaces and windows in earthquake or tornado-prone locations).

Physically Securing Desktop Computers

Desktop systems are easier to physically secure because they are larger, heavier, and consist of multiple components, which means they are more difficult to steal. Theft can occur, however, so systems containing sensitive information or connected to the network should be kept in locked offices when no one is there to oversee them. Cable lock systems (steel cables that attach the computer to the desk, floor, or wall) can be used to secure the computer case to a large structure. Computer cases should be locked so intruders cannot open them and steal the hard disks. Media that holds data (floppy disks, CDs, flash memory cards, tape backups) should be kept in locked cabinets to prevent theft.

Removing unneeded floppy disk drives, CD drives, and USB ports will keep unauthorized persons from uploading data, installing programs, or copying data. Installing removable hard disks that slide into nesting devices allows you to remove the disk when you leave the computer (similar to the way you can remove a car stereo's faceplate to prevent it from being stolen). These devices should also lock in place with a key so they cannot be removed without authorization. If the hard disk is removed, the computer's local data cannot be accessed. And because the operating system also resides on the removable disk, the computer cannot be used to access the network; it will not even start.

Server rooms and offices where computers with sensitive data are located should be protected by motion sensors after hours.

Physically Securing Laptop/Notebook/Handheld Computers

Portable computers can be even more vulnerable because it is so easy to steal the entire computer. A thief might then be able to access the data stored on the hard disk and log on to the organization's network remotely, if additional protective measures have not been taken (see the section on software security for portable computers later in this document).

Cable locks are even more desirable for laptops than for desktop computers. Many portable computers come with built in security slots for attaching these locks.

Alarm systems are available that can attach to portable computers. Once activated, these alarms will sound if they are not disarmed before the computer is moved. A variation on this concept is the transmitter-receiver system. The transmitter is kept on your person (for example, on your keychain) and the receiver is attached to the portable computer. If the two are separated by more than a small distance, the alarm sounds.

If you must leave a portable computer in a hotel room, lock it in the in-room safe or in a large locked piece of luggage that is stowed out of plain sight. If you must leave the computer in a car, lock it in the trunk and cable lock it to the trunk lid. If the vehicle is a hatchback, pickup, or SUV, cable lock the computer to the vehicle’s structure and cover it so it is not visible from outside.

Clearly engraving identifying information (but *not* your social security number or other personal information that could be used by identity thieves) may help to deter some thieves and make it easier for police to identify your computer if it is recovered.

Physically Securing Network Components

Network components (routers, hubs, switches, wireless access points, and cables) can all be points of vulnerability, but their security is often overlooked. A hacker who has physical access can plug a laptop into a hub and intercept network communications using packet sniffer software.

Because the twisted pair cabling used for most modern Ethernet networks is unshielded, the electromagnetic signals radiate from the cable and can be picked up by a properly equipped hacker who has access to only the cable. Exposed cables going through hallways, false ceilings, or in unlocked offices can present a security risk. Most information workers will not be responsible for securing network devices such as routers, hubs and switches, but you should be aware that the cabling in your office can also be “listened to” by savvy hackers. Making it as inaccessible as possible is a good security practice.

For an in-depth discussion of physical security of the network components, see Chapter 4 from Mastering Network Security (published by Sybex, Inc.) "Topology Security" on Microsoft TechNet at www.microsoft.com/technet/security/topics/network/topology.mspx.

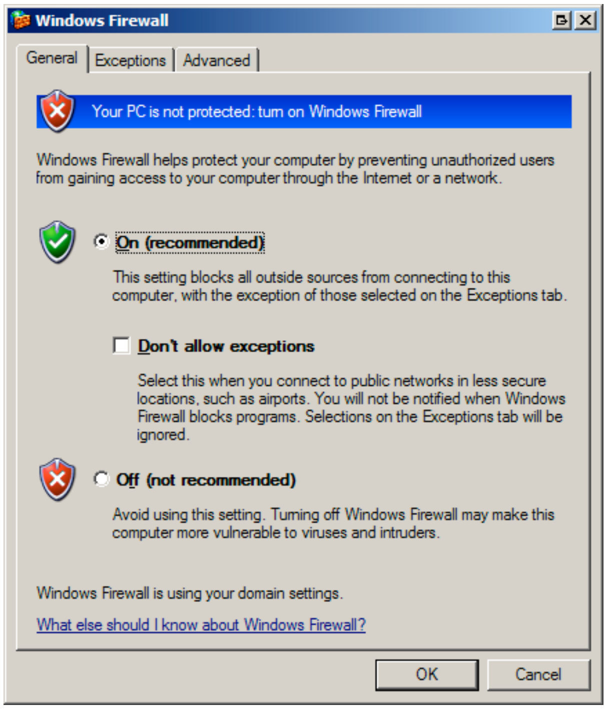
Software Security

Unfortunately, physically securing your systems and network components is not enough. Although many intrusions and attacks originate internally, many others come from outside the organization’s walls, over the Internet or through dial-up connections. Protecting against these threats requires special software or dedicated hardware/software combinations such as firewall appliances. Because there are so many different threats, there are also many different types of software security mechanisms.

Protecting Against Internet Intruders with Firewalls and IDS

A firewall operates between your computer or network and the Internet, and examines the data that attempts to move through it. The firewall can be set up to block or to allow particular types of data. A firewall that protects a whole LAN is called an *edge firewall*, a *perimeter firewall*, or sometimes a *network firewall*. Firewall software that is installed on a single computer to protect just that computer is called a *personal firewall* or a *host firewall*. For more information about the details of how firewalls work, see the article "How Firewalls Work" at http://computer.howstuffworks.com/firewall.htm.

Windows XP includes a built-in personal firewall called the Internet Connection Firewall. When you install Service Pack 2 (SP2), this firewall is replaced by Windows Firewall, which has increased functionality. SP2 also turns the firewall on by default. If you do not have other firewall software installed or if a network firewall is not protecting the network, you should always have the firewall enabled on your Windows XP computer. Third-party personal firewall software is available for older versions of the Windows operating system. For more information about Windows Firewall, see the article "Understanding Windows Firewall" at www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx.



Your PC is not protected: turn on Windows Firewall

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

Windows Firewall is using your domain settings.

What else should I know about Windows Firewall?

Figure 2

Windows Firewall in Windows XP SP2 is easy to access and configure through the Control Panel

Some personal firewalls allow you to block specific applications or protocols (for example, Telnet). Firewalls can also block outgoing data (for example, preventing a Trojan or virus from causing your computer to send out personal data without your permission. The firewalls built into some broadband routers are not very configurable; they protect the computers behind them from being seen on the Internet by using network address translation (NAT) to conceal private IP addresses of LAN computers.

Your organization's network probably uses a network firewall such as ISA Server. The organization may also install centrally managed host firewall software on all computers. To avoid potential conflicts, you should check with your network administrator before enabling or configuring personal firewall software on a computer on the organization's LAN.

A firewall may prevent you from using particular Internet applications or visiting certain Web sites. Firewalls are sometimes combined with proxy servers, which act as intermediaries between users' computers and Internet Web servers. They can also store copies of the Web sites you visit (called *caching*) so that when you or someone else on your LAN wants to visit that same site again, it can be downloaded more quickly from the proxy server (which is part of your local network) instead of from the Internet.

Some firewalls have built in intrusion detection system (IDS) functions. If a firewall is like a guard at the gate who keeps undesirable traffic out of your network, an IDS is like a burglar alarm that alerts you when someone without authorization tries to get in.

The IDS can recognize common attempted attack patterns and may be able to notify you via e-mail or pager if network activity resembles an attack. If not, it will log the information so you can track it later. More sophisticated IDS products are separate from the firewall. Like firewalls, IDS and IPS (intrusion prevention systems) can be either host−based (installed on your personal computer) or network−based (placed between the Internet and the LAN).

Protecting Against Viruses and Other Malware

Computer viruses do millions of dollars in damage every year, so it is absolutely essential that every computer that connects to a network have adequate virus protection. Antivirus software such as Symantec Norton Antivirus (information available at www.symantec.com/product/index.html), Trend Micro PC-cillin (information available at http://www.trendmicro.com/en/products/global/enterprise.htm) and Network Associates McAfee (information available at www.networkassociates.com/us/products/home.htm) are popular virus protection programs. For the complete Microsoft Antivirus Partners list, see www.microsoft.com/security/partners/antivirus.asp.

Installing antivirus software is not enough. New viruses are being written and released every day. According to Symantec's Internet Security Threat Report of July 2004, more than 4000 new viruses and worms were discovered during the first half of 2004. You must update the virus definition files that are used by the antivirus programs to detect viruses on a regular basis. (If you have an always-on connection, you should update weekly or even daily.) Most antivirus programs can be set to automatically connect to the Internet and download updates on a set schedule.

You should ensure that a full virus scan is set to run at a regular time. You should perform a full system scan at least once per week. You might want to schedule scanning for late at night or some other time when you will not be using the computer. You should also turn on auto-protect and e-mail protection features for continuous protection. It is especially important to have updated virus protection on any computer that you use to connect remotely to your organization's network (through a VPN or dialup connection).

Note: Many organizations already have antivirus software set up on their computers, so check first with the IT department before installing such software or changing the configuration of any existing antivirus program.

Protecting Against Spyware and Adware

If you notice any of the following symptoms, you may have adware or spyware installed on your computer:

- Noticeable slowdown in performance with no other explanation.
- Unusual software behavior, such as your Web browser's home page suddenly changing, new items appearing in your Favorites menu, or programs closing unexpectedly.
- Strange hardware behavior, such as the CD drive opening or unusual hard drive activity.
- Strange network behavior, such as indications by your modem lights that your computer is transmitting data when you are not doing anything online.
- Pop-up ads displaying when you are not surfing the Web.

Adware/spyware detection and removal software is becoming just as necessary as antivirus software. However, you must be careful when choosing anti-spyware tools (especially free ones), because some programs that claim to be spyware removal tools actually install their own spyware. Use only reputable anti-spyware scanning and removal programs.

In addition to using these tools, there are ways to guard against the installation of adware and spyware. Be careful about installing free software, and always read the entire end user license agreement (EULA). Configure your browser security settings to prompt you before downloading programs or controls or running scripts.

Protecting Against Unwanted E-mail

Unwanted e-mail, like junk mail in physical mailboxes, probably can never be completely eliminated. However, there are several things you can do to reduce the amount of spam you receive, including general spam protection practices, using spam filtering services or software, and using sender verification systems.

General Spam Protection Practices

- Do not give out your e-mail address indiscriminately. Spammers often collect addresses from Web forms or buy them from organizations that collect the information. When you fill out online registrations (for example, many online news sites require that you register before you can read the stories), leave the e-mail address blank or provide an alternate address. For more information on how spammers harvest addresses, see "Spam Address FAQ -- How To Fight Back" at http://laku19.adsl.netsonic.fi/era/spam/faq/spam-addresses.html.
- Set up an alternate e-mail address that you can use for activities that require an e-mail address and that are likely to result in spam. There are many Web−based e-mail services that offer free e-mail accounts.
- If you post to newsgroups or public mailing lists, leave your e-mail address out of your signature line. Some users alter their addresses in such a way that humans can discern the correct address but *bots* (software programs that scavenge for addresses) can not. For example, they might insert extra letters or words that are obviously not part of the address: johnsmith@mycompany.removethis.com. This technique is called address *munging*. For more information, see "Address Munging FAQ: Spam-Blocking Your Email Address" at http://members.aol.com/emailfaq/mungfaq.html.

- Do not reply to junk messages, even if they contain an address to write to requesting removal from the mailing list. This is a trick that is often used to verify that your e-mail address is valid.
- If a message is obviously spam (for example, if the Subject: line reads “Cheap V*i*a*g*r*a”), do not open it. HTML messages can run scripts or contain *beacons*, which report back to the sender that you opened the message, verifying that your address is valid.
- Report spam to services such as Spamcop at www.spamcop.net. These services compile lists of known spammers that can then be used by spam blocking software.

Using Spam Filtering Services and Software

A key factor in reducing the amount of unwanted e-mail that reaches your inbox is to use spam blocking software or services. Unwanted mail can be blocked in many ways, at many different levels. For example, you can enroll in services that route your e-mail through special servers so that it can be scanned for spam.

Spam can be blocked at the firewall level when it first enters the network, by edge firewalls that support *application layer filtering.* The incoming messages can be blocked by sender’s e-mail address or the Internet domain from which the message originates (useful for blocking known spammers) or by content (key words or phrases).

Many organizations and ISPs that run their own mail servers perform spam filtering at the server level. You can also run spam filtering software on your client computer to catch any spam that makes it past the firewall and/or server filters. Client filtering software typically places spam in a junk mail folder in your mailbox.

The biggest problem with spam filtering is the risk of *false positives* (legitimate mail that was misclassified as spam). Good filtering software allows each user to check the mail that has been quarantined as spam so that they can ensure that no legitimate mail was lost. Some filtering software uses so-called “intelligent” methods to determine what is and is not spam; these methods include examining the messages you mark as spam and “learning” from them. Good filtering software also allows you to configure lists of sender addresses whose mail should never be marked as spam, as well as lists of known spammer addresses.

Using E-mail Sender Verification

To effectively combat spam, e-mail-borne viruses, and other abuse of the Internet e-mail system, there must be a way to prevent e-mail spoofing by verifying that the return addresses and headers on e-mail messages identify the true sender. There are technologies being developed that can accomplish this verification.

The Sender Policy Framework (SPF) involves having all Internet domain owners identify their mail servers that send mail in a registry of domain names maintained on special DNS servers. If all such mail servers were registered, header information could be checked and verified. The problem is that both administrators and users have to take action to make it work. Microsoft and others in the industry have developed the Sender ID Framework, which is based on SPF but has some technical differences. You can read more about it in the article "Sender ID Framework Overview" at www.microsoft.com/mscorp/twc/privacy/spam_senderid.mspx.

Another technological solution for verifying identity is to use digitally signed e-mail. Digital signatures use public key cryptography. Every user has a *key pair*, one that is made public and one that is kept private. If the sender of a message encrypts the message with his private key, anyone can decrypt it because the public key is widely available. In addition, all recipients can be assured that only the sender who had possession of the private key could have sent it. Public key technology is based on digital certificates that are issued by *certification authorities*, which are trusted entities that vouch for the key holder’s identity. The process works similarly to the issuance of a driver’s license or government ID card; the issuing entity verifies the applicant’s identity and then issues a document that other entities trust to identify that person.

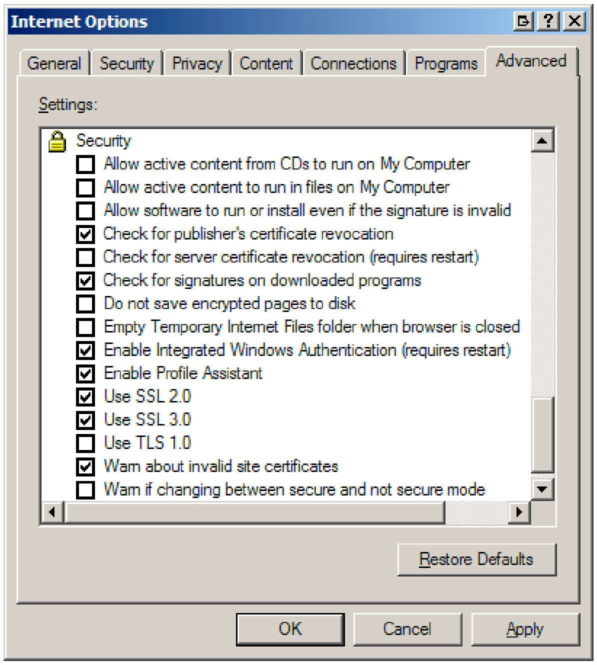
Making Web Browsing More Secure

Many exploits, malware programs, spam schemes, and phishing scams make use of the Web to collect information. Early Web pages consisted of just text and graphics, but now sophisticated Web sites use programming embedded in the Web pages to create amazing special effects. These capabilities also create security issues.

You can make Web browsing more secure by doing a few simple things:

- Keep all security patches and service packs for your Web browser and operating system up to date. For example, SP2 for Windows XP increases Internet Explorer’s security and adds pop-up blocking and add-on management.
- Configure your browser’s security settings for safe browsing.
- Configure your browser’s privacy settings to avoid unwanted cookies and pop-up ads.
- Be careful about which Web sites you visit. Sites devoted to illegal or questionable subjects, such as hacker sites, sites for downloading pirated music or software, and pornographic sites are most likely to contain malicious code.
- Enable checking of digital signatures on drivers and other programs you download.
- Do not conduct financial transactions or send private information over the Web unless the site is secure (which is usually indicated by a dialog box or a “lock” icon in the browser’s status bar).
- Configure your browser to not automatically download ActiveX controls, or run scripts, Java applets, or other code. If you want to be able to run code on some sites, configure the browser to prompt you before doing so.

As shown in the following figure, popular Web browsers such as Internet Explorer 6 have many security settings that you can configure.



Security

- ☐ Allow active content from CDs to run on My Computer
- ☐ Allow active content to run in files on My Computer
- ☐ Allow software to run or install even if the signature is invalid
- ☑ Check for publisher's certificate revocation
- ☐ Check for server certificate revocation (requires restart)
- ☑ Check for signatures on downloaded programs
- ☐ Do not save encrypted pages to disk
- ☐ Empty Temporary Internet Files folder when browser is closed
- ☑ Enable Integrated Windows Authentication (requires restart)
- ☑ Enable Profile Assistant
- ☑ Use SSL 2.0
- ☑ Use SSL 3.0
- ☐ Use TLS 1.0
- ☑ Warn about invalid site certificates
- ☐ Warn if changing between secure and not secure mode

Figure 3

You can adjust the security settings for your Web browser software to make Web browsing more secure

You can test your Web browser software for common vulnerabilities and determine its encryption strength at the following Web sites:

- The Scanit Browser Security Test page at http://bcheck.scanit.be/bcheck/
- The Qualys Free Browser Checkup page at http://browsercheck.qualys.com/
- The Verisign Browser Check page at www.verisign.com/advisor/check.html

Software Security for Portable Computers

The best defense for portable computers is theft prevention, but there are ways to minimize the impact if your portable does get stolen. Setting a startup password is a first step, although thieves may be able to defeat this by resetting the password or using a master password that is designed to let the original equipment manufacturer (OEM) bypass user-set passwords.

You should not use features that allow you to remember passwords on laptop computers. Although it is convenient not to have to type in your passwords each time, it is very inconvenient when a thief is able to log on to your computer, log on to the network, and access your e-mail and data files.

Note: If you have used your portable computer to access your organization's network and it is stolen, you should immediately report the theft to the IT department, even if you own the computer personally. Your network passwords may need to be changed or your account deactivated.

Biometric identification systems that use fingerprint scans or voice recognition in addition to passwords will help keep thieves from breaking into your portable computer. Some handheld computers, such as the iPAQ 5555, now include such systems.

Software such as CompuTrace from Absolute Software (information available at www.absolute.com/public/main/default.asp), ZTrace Gold from zTrace Technologies (information available at www.ztrace.com/zTraceGold.asp), and LapTrak from Secure-It, Inc. (information available at www.secure-it.com/products/laptrak/index.htm) can be installed on your portable computer to track its location by causing it to "call home" when a thief uses it to connect to the Internet.

Any important data stored on a portable computer's hard disk should be encrypted. More information about using encryption to protect sensitive data is provided later in this document.

Defending Against Social Engineers and Phishers

There are really only two steps involved in protecting yourself against social engineers who try to charm, intimidate, or trick you into giving them information or against phishers who try to steal your personal information:

- Being aware of what is happening
- Just saying no

You should be suspicious of people who ask you for your account name and password, computer name, IP address, employee ID number, or other information that could be misused. You should be especially suspicious if they attempt to charm you or intimidate you. Refer them to the IT department. If they claim to be *from* the IT department, hang up and call back to verify this information or check it out with your supervisor. If they claim to be a manager or officer in your organization and you do not recognize their name, voice, or face, explain that you are concerned about protecting the security of the network and that you need to verify their identity before you can give them sensitive information.

If you receive e-mail that claims to be from your bank, ISP, or an organization with whom you do business that requests information about your account, do not respond via e-mail or a Web page. Instead, call the organization and ask if the e-mail request is legitimate (do not use any telephone number listed in the e-mail; look up the number separately). Most organizations do *not* use e-mail for such correspondence. Do not click on links contained in e-mail messages to visit an organization's Web site. Instead, manually type in the URL for the organization's home page and navigate from there to your account logon site.

Protecting Your Password and Logging on Securely

Hackers who know your password do not have to resort to technological exploits; they can log on and do anything that you can do on the computer or network. Keeping your password secret is one of the most important things you can do to protect against security breaches.

Tips for Creating Strong Passwords

The first step in password security is creating strong passwords that cannot be easily guessed or deduced. Tips for creating strong passwords include the following:

- Do not use personal information for your password. Social security numbers, driver's license numbers, phone numbers, birth dates, spouse names, and pet names are all factual information that can be found out by others.
- Do not use words that are in the dictionary, including words in foreign languages. Dictionary attacks try these words and combinations of them.
- Do use a combination of uppercase and lowercase letters, numbers and symbols.
- Do not substitute numbers for letters to make words (for example, s0ph1st1cated). Hackers are aware of this trick.

- Generally, longer passwords are harder to crack because a brute force attack must try more combinations before finding a correct one. Windows XP allows up to 128 character passwords, although the Welcome screen only displays 12 characters at the password prompt. You can switch to the classic logon screen, or just keep typing the characters after the password field appears to stop accepting them.
- Do not use sample passwords that you see in security articles or books, even if they are exceptionally complex.
- Do use a combination of letters, numbers, and symbols that have meaning to you so you – but no one else – will be able to easily remember the password. For example, mfc!rB&G might mean “my favorite colors (!) are Blue and Green” to you, but to anyone else it looks like a random combination of characters.
- Do select a password that you can type quickly, to minimize the chance of someone discovering it by watching over your shoulder when you type it. However, do not use common key sequences such as qwerty.

Keeping Passwords Secure

After you create a strong password, you must keep it secure. Tips for keeping passwords secure include the following:

- Never share your password with anyone else.
- Do not write your password down. This is the reason why you need to create a password that is easy for you to remember. If you disregard this advice and do write it down, keep the written copy in a locked off-site container.
- Do change your password on a regular basis, even if your network policies do not require you to do so. Always change your password if you suspect it might have been compromised (for example, if someone was standing over you when you typed it).
- Do not use the same password for multiple purposes. For example, some people might use the same number combination for their ATM PIN, network logon password, e-mail password, and for all protected Web sites. If this password is cracked, all of your accounts and activities will be compromised.
- Do not save your password(s) in a file on your computer that can be read by others.
- Do not use features that allow you to remember passwords for critical applications or sensitive Web sites.

Multiple Factor Authentication

Passwords are the most common way to identify yourself or *authenticate* to a computer or network server. However, there are other ways. The most secure identification methods use multiple factor authentication, which means you have to provide two or more of the following:

- Something you know (a password or passphrase).
- Something you have (a card or token).
- Something you are (unique physical characteristics).

Smart cards are credit card-sized devices that have a magnetic strip or embedded chip that holds identification information such as a digital certificate. To log on to a network or computer, you slide the card through or insert it into a card reader. *Tokens* are physical keys, often implemented as small USB devices that can be carried on a key ring and inserted into a USB port to be read. In addition to inserting the card or token, you usually must also enter a PIN or password. This approach means even if someone steals your card or token, it will not work without the password; and even if someone discovers your password, it will not work without the physical device.

Biometric authentication refers to physical characteristics such as fingerprints, voice patterns, retinal patterns, and facial structure.

Keeping Your System Updated

Remember that operating systems and applications can have security vulnerabilities, and that hackers enjoy discovering and exploiting such vulnerabilities. When vulnerabilities are discovered (either by hackers or by legitimate testing processes), software vendors typically release add-on software to eliminate the vulnerabilities.

Keeping your system and applications updated is critical to the security of your computer and network.

Patches, Hotfixes, Service Packs and Critical Updates

Software releases that address particular security vulnerabilities are called *patches* or *hotfixes.* They should be downloaded and applied as quickly as possible after a vulnerability is discovered so that it cannot be exploited.

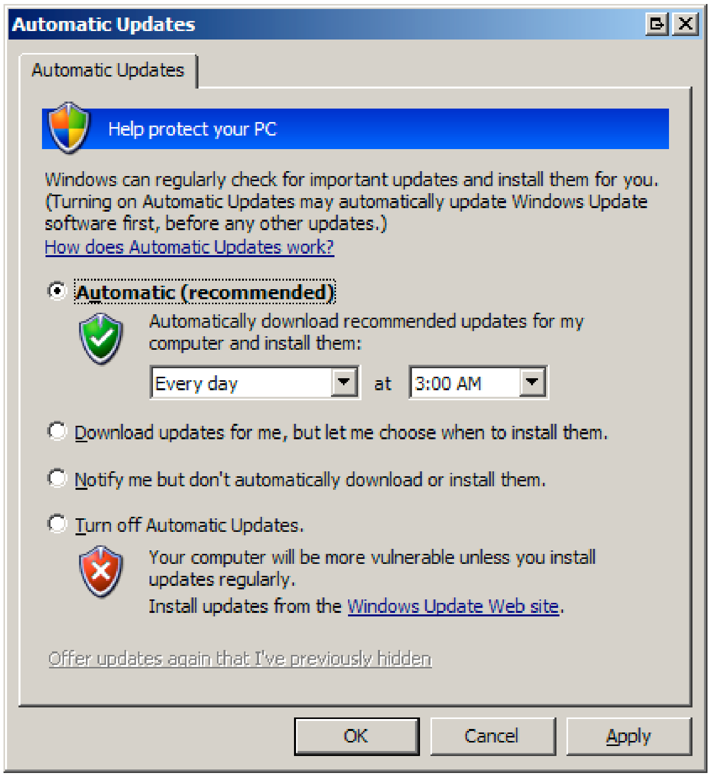
Service packs are released at longer intervals. They usually contain an accumulation of multiple fixes for different security issues, and may also add new features or components to the operating system or application.

Software vendors release many updates that are optional. You can apply them if you are having a particular problem or if you want the particular features that they add. *Critical updates* are those that address serious problems and should be applied to all affected systems.

How to Keep your System Up to Date

Microsoft makes it easy to keep their software up to date with the automatic update feature that is built into Windows XP. If your computer is connected to the Internet through your organization's LAN or other always-on connection (such as cable or a DSL broadband connection), Windows XP can automatically check for available updates and download and install them for you.

The automatic update feature is configured through the Control Panel and can be set to do everything automatically. It can also be configured to download updates automatically but let you choose when to install them, or to notify you when there are updates but not download or install them without your permission. The **Automatic Updates** configuration screen is shown in the following figure.



Help protect your PC

Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)

How does Automatic Updates work?

● Automatic (recommended)

Automatically download recommended updates for my computer and install them:

Every day at 3:00 AM

○ Download updates for me, but let me choose when to install them.

○ Notify me but don't automatically download or install them.

○ Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.

Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden

Figure 4

Windows XP Automatic Updates makes it easy to keep your system updated with all available patches, fixes, and service packs

You can also check for updates by visiting the Windows Update Web site at http://windowsupdate.microsoft.com. To update Microsoft Office programs, see Office Update on the Microsoft Office Online page at http://office.microsoft.com/en-us/officeupdate/default.aspx.

To update third-party software products, visit the software vendors' Web sites. Some third-party products will automatically check for updates when you run them if you are connected to the Internet.

Note: Some organizations' IT policies specify that updates and patches only be installed by the IT department. Organizations may delay deploying service packs and other updates because of conflicts with proprietary software. Do not download or install software of any kind, including updates, and do not change the automatic update settings on any computer owned by the organization without the knowledge and permission of the IT department.

Protecting Your Sensitive Data

An important aspect of security is protecting sensitive data from being read, changed, copied, or destroyed by unauthorized persons. Protection is especially important in today's business world, where trade secrets can be worth millions of dollars, client confidentiality must be safeguarded, and government regulations often mandate that particular information not be disclosed.

What is Sensitive Data?

Sensitive data is any information that should be viewed and manipulated only by trusted parties. For practical purposes, the sensitive data that you might have stored on your computer or that you might access on the network can be divided into two categories: sensitive business data and sensitive personal data.

Sensitive Business Data

Sensitive business data includes any information related to the business or organization that could cause harm to the organization, its clients, its partners or any individual if it were deleted or made available to unauthorized users. Such information includes, but is not limited to, the following:

- Clients' or business partners' personal information collected in the course of doing business, such as names, addresses, phone numbers, social security numbers, financial information, medical records, legal matters, and account numbers.
- Employees' personal information, including salary information (unless the organization is a public entity), disciplinary records, employment history, medical history, and criminal history.
- Financial information about the organization (other than that required to be disclosed by law), business strategies, and future business plans.
- Trade secrets, research and development information, and patent plans.

Sensitive Personal Data

Sensitive personal data you might have stored on your computer or on the network includes:

- Your home address and telephone number.
- Social security number, driver's license number and other identification numbers.
- Bank account information and credit card information (if you perform financial transactions online).
- Medical information such as health insurance claims and correspondence with health care providers.
- Legal information.
- Internal employee information.

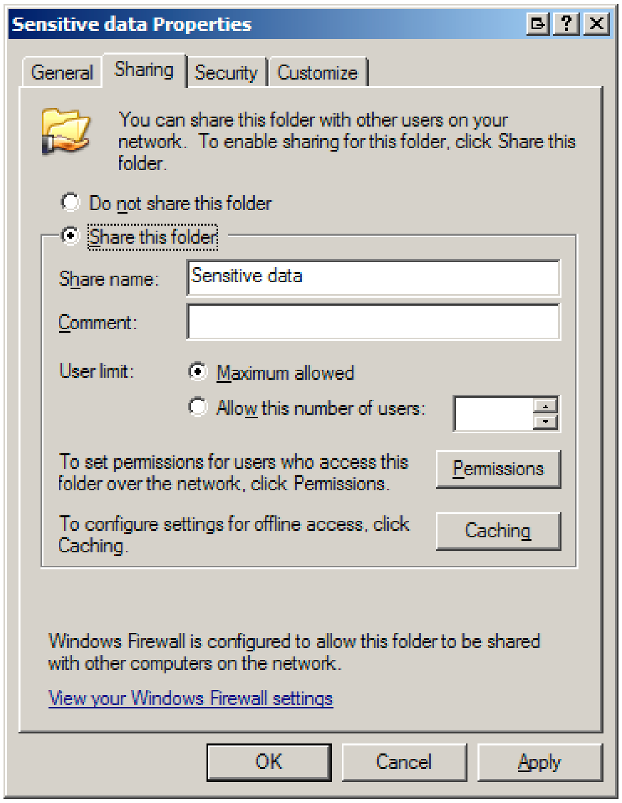
Access Controls

One way to protect sensitive data is by setting access controls on files or folders. There are two types of access controls you can place on the data stored on your computer: *share level protection* that applies only to data that you share on the network, and *file level protection* that applies to data whether it is shared on the network or accessed by another user who logs on to your computer locally.

Share Level Protection

You can control who has access to your data from the network by setting *shared folder permissions* in Windows XP. This capability allows you to place sensitive documents that need to be shared on the network with some people (but not others) into folders and designate which users or groups can access those folders, and also what level of access each can have. That is, a particular user can be given permission to read only, to make changes, or to take full control. By default, when you share a folder, everyone on the network has read permissions. It is very important to change this setting for sensitive data that should only be viewed by certain people.

You set shared folder permissions using the **Sharing** tab on the folder's **Properties** sheet, as shown in the following figure. These permissions can only be set on folders, not individual files.



You can share this folder with other users on your network. To enable sharing for this folder, click Share this folder.

○ Do not share this folder

● Share this folder

Share name: Sensitive data

Comment:

User limit: ● Maximum allowed

○ Allow this number of users:

To set permissions for users who access this folder over the network, click Permissions.

To configure settings for offline access, click Caching.

Windows Firewall is configured to allow this folder to be shared with other computers on the network.

View your Windows Firewall settings

Figure 5
You can set shared folder permissions to control who can access your data from the network and their level of access

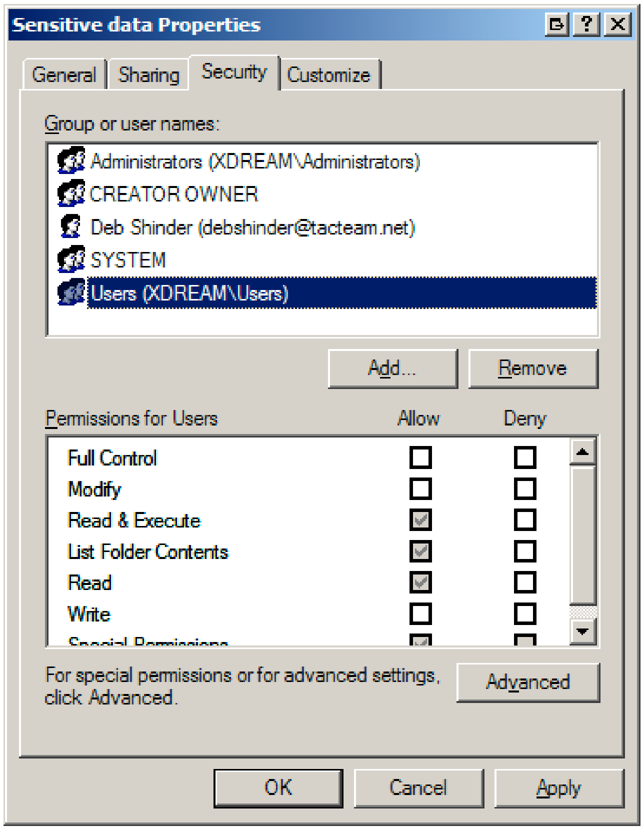
The **Permissions** button is used to specify the users and groups that will have access.

File Level Protection

If there are other people who log on to your computer, shared folder permissions will not affect them. To control their access to your data, you need to set *file security* *permissions,* which are also sometimes called *NTFS permissions* (because to use them the data must be on a partition that is formatted with the NTFS file system). These permissions also apply to people accessing the data across the network, in addition to any shared folder permissions that are set.

You can set file security permissions on both files and folders from the **Security** tab on the file's or folder's **Properties** sheet.

As shown in the following figure, file level permissions are more complicated than shared folder permissions. There are a number of different levels of access that you can give to each user or group.



Group or user names:

- Administrators (XDREAM\Administrators)
- CREATOR OWNER
- Deb Shinder (debshinder@tacteam.net)
- SYSTEM
- Users (XDREAM\Users)

Permissions for Users	Allow	Deny
Full Control	☐	☐
Modify	☐	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☐	☐
Special Permissions	☑	☐

For special permissions or for advanced settings, click Advanced.

Figure 6
You can set file level permissions to control who can access your files or folders from the network or from the local computer

Using Data Encryption

In addition to setting access control permissions on your files and folders, you should consider encrypting documents that contain sensitive information. Windows XP includes built-in data encryption technology called the Encrypting File System (EFS). When you encrypt a file or folder with EFS, other users who log on to the computer with their own user accounts will not be able to read the file (or the documents in the folder), even if they otherwise have permission to access it. Similarly, users who try to access the file from the network will not be able to access it.

You can share encrypted files and folders with other users by adding their user accounts to the encryption permissions. Encrypting a file or folder with EFS is as easy as checking a box in the file or folder's **Advanced Attributes** properties.

Using IP Security

EFS protects data that is stored on disk, but it does not protect data that is traveling across the network. A hacker with a sniffer program can intercept data and look inside the packets to read the information within them.

Computers running Windows XP and Windows 2000 support the IP Security protocol (IPsec), which can be used to encrypt data as it travels on the network so that hackers will not be able to read it if they intercept the packets. Both your Windows XP computer and the server with which it is communicating must be configured to use IPsec. Configuration is done using Windows XP's Group Policy. IPsec configuration should be done by your network administrator.

Understanding Computer Forensics and Data Destruction

An often overlooked aspect of computer security involves data that remains on your computer after you think it is gone. The practice of recovering data from a computer is called *computer forensics,* a term that is usually associated with recovering data that constitutes evidence in a criminal or civil court case.

Recovery of "Deleted" Data

How is data recovered? When you press the DELETE key or drag a file to the Recycle Bin, you might think that is the end of it – but that is not the case. Deleting e-mail usually just moves it to another folder, and even after you empty the Deleted Items folder, it usually goes into the Recycle Bin, where it can still be easily found and restored with a few clicks of the mouse.

Even after you empty the Recycle Bin, data is still not really gone – because deleting data does not erase the data from the disk. Deleting data just removes the pointers to the file from the file system's table and marks the space where it is stored as reusable. Until new data is written to that same location on the disk, the information is still there and can be recovered with special data recovery software. Even after other data is written over it, fragments of the data can still sometimes be recovered because of the way the drive heads write to the disk. If there is an *offset* in which the new 1s and 0s do not exactly line up with the old ones, the old data may still be discernable. Even formatting the disk does not guarantee that all data is gone.

Where Data Exists

Data is located in many different places, including the following:

- Your Web browser's cache (Temporary Internet Files) and history folder can reveal what Web sites you have visited, as can the cookies folder and the Favorites list.
- The My Downloads folder can reveal files that you have downloaded.
- Your e-mail program's temporary folder can contain copies of file attachments that you have received with e-mail.
- Word processing programs create temporary files while you are working that may not be deleted when you delete the main file. Many other application programs also create temporary files.
- The Windows clipboard can show data that you have cut from documents.
- Your Instant Messenger (IM) program may be set to log your conversations to a file. Its contact or "buddy" list will reveal persons with whom you communicate.
- Your My Recent Documents folder shows what files you have worked on.
- Media Player software's history and playlists can reveal what audio and video files you have played.

- Your contacts list can reveal persons with whom you exchange e-mail, as can the address autocomplete feature in your e-mail program.
- Your calendar program may reveal your activities for past days.
- Information you have deleted may still exist in memory (if the computer has not been turned off) or in virtual memory (the page file or swap file on the hard disk).
- Copies of e-mail messages you have sent or received may still exist on the server or on the sender's or recipient's computer.
- Backup tapes may contain copies of files even though you have deleted the originals.

How to Destroy Electronic Data

If you are concerned about deleted data that may still exist on your computer, you can do things such as manually delete temp files, empty cache and history files, prune contact lists, delete old calendar entries, and configure Windows not to save document histories.

An easier alternative is to use one of many third-party evidence elimination programs that can automate the process of removing data from common hiding places.

Complete elimination of data with 100% assurance that it cannot be recovered requires destruction of the media on which it is stored. Government agencies and organizations that must ensure data does not remain generally use incineration, pulverization, or destruction of the hard disk or other media with acid.

Using Wireless Networks Securely

Wireless networks are, by nature, less secure than wired networks. However, there are a number of steps you can take to make your wireless communications more secure, including the following:

- When you set up a wireless access point (WAP), immediately change the default SSID (network identifier or network name) and the default administrator password.
- Turn off SSID broadcasting on the WAP.
- Enable encryption with either WEP or WPA. WPA encryption is stronger and more secure, so it is the encryption method of choice if your hardware (WAP and wireless NICs) and your operating system support it. Windows XP with SP2 supports WPA. WPA client software for Windows XP SP1 can be downloaded from the Microsoft Web site; for more information see Microsoft Knowledge Base article 826942, "Wireless update rollup package for Windows XP is available" at http://support.microsoft.com/kb/826942. Whichever encryption method you use, set an encryption key (password) that is not easy to guess. Change the key on a regular basis or any time you suspect it might have been compromised.
- Enable MAC address filtering and enter the physical addresses of computers that will be allowed to connect to the wireless network.
- Disable the Dynamic Host Configuration Protocol (DHCP) on the WAP and use a private IP addressing range that is outside the most common (192.168.x.x). This method prevents intruders from being assigned an IP address, and they will have to guess an address that is correct for your network.
- Disable Simple Network Management Protocol (SNMP) support on the WAP. This protocol can be used by hackers to gather information about your network.
- Do not use an overly powerful antenna that broadcasts beyond the range you need. Do not place the antenna close to a window; place it as close to the center of the area you want the network to cover as possible.

The Importance of Multi-Layered Security

As you can tell from this document, there are many different levels at which computer and network security can be implemented. The best security plan is a multi-layered one that creates circles of protection within one another, so that if one defense is penetrated, an intruder still has to get through more levels in order to do damage. Such an approach is called a defense-in-depth design.

A good security plan cannot rely on just one technology or solution. Compare this to an organization's physical security measures. Most organizations do not depend on just the locks on the buildings' doors to keep out burglars. They also set up perimeter security (a fence), and they might add external security measures such as a guard or guard dog and external and internal alarm systems. To protect special valuables, they may have "inner circle" safeguards such as a vault or safe.

Computer security should also be multi-layered, which means inclusion of more than one of the following:

- Physical security measures to keep intruders from gaining on-site access to workstations, servers and network components, and to keep portable computers from becoming available to unauthorized users.
- Firewalls at the Internet "edge" to protect computers on the LAN, and personal (host) firewall software to protect computers connected directly to the Internet.
- Intrusion detection/prevention systems to alert you to attempts to break into the computer or network.
- Passwords (and possibly card/token or biometric authentication) should be required to log on to computers and the network.
- Access controls (shared folder and file level permissions) for sensitive documents.
- Encryption for sensitive files and folders.
- IP Security (IPsec) to encrypt sensitive data as it traverses the network.
- Special security measures to protect wireless communications.

Conclusion

Protecting your computer from hackers, crackers, attackers, viruses, spyware, spam and other threats that exist because of network connectivity is a joint effort. It involves individual computer users, organizational IT departments and organizational policy-makers, and the Internet community as a whole. By putting good security practices into use, you not only protect your own computer and your local network, you also contribute to the overall security of the global network.

The first steps in making your computer and network more secure are to become aware of the threats, to learn how to recognize them, and to understand what you can do to protect against them. This document provided an overview of how networks work and an outline of the security risks that they entail, along with tips about what information workers can do to make using their computers a safer and more pleasant experience.