

eSecurity Guide

for Small Business



Microsoft®
Your potential. Our passion.™

Winter 2004

© 2004 Microsoft Corporation. All rights reserved. Microsoft, Outlook, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.



Dear Small Business Owner:

Today, computers and the Internet are indispensable tools for achieving business success, but they can make us vulnerable to new and serious threats. While larger companies have security experts at their disposal, small business owners are often left wondering how they can provide or increase the security of their information systems.

Thus, I am delighted to introduce the eSecurity Guide for Small Business—a security guide developed by Microsoft Small Business. Although the topic of information security can seem unwieldy and overly technical, this guide does an excellent job of outlining steps required to achieve a reasonable level of IT security that are not overly difficult, expensive, or beyond the ability of anyone savvy enough to be running their own business.

Sincerely,

Donald Wilson
President & CEO
Association of Small Business Development Centers

Small Business Development Centers

America's Small Business Development Center (SBDC) network is a partnership program uniting private enterprise, government, higher education, and local nonprofit economic development organizations. The SBDC network is the US Small Business Administration's largest economic development program, utilizing Federal, State, and private funds to provide management and technical assistance to help Americans start, run, and grow their own businesses. SBDCs are located in all 50 states, the District of Columbia, Puerto Rico, the US Virgin Islands, Guam, and American Samoa. With nearly 1000 centers across the nation, the SBDC program meets the in-depth counseling and training needs of more than 650,000 small businesses annually in face-to-face counseling and training events. In addition, the SBDCs assist hundreds of thousands more through fax-on-demand and email requests for information. Since its creation by Congress in 1980, SBDCs have served more than 11 million small business owners and aspiring entrepreneurs. The network's partnership programs and activities serving the small business sector have contributed significantly to economic growth locally, state wide, and across the nation.

The Association of Small Business Development Centers (ASBDC) is specifically provided for in the Small Business Act and represents America's Small Business Development Center network. All the SBDC host institutions located in the 50 states, the District of Columbia, Puerto Rico, the US Virgin Islands, Guam, and American Samoa are members of ASBDC.

To learn more about the ASBDC, visit www.asbdc-us.org.

Microsoft Small Business

Microsoft Small Business is an online resource designed specifically to address the needs of the small business by demystifying technology and helping Small Business get the most out of its software. To learn more, please go to www.microsoft.com/smallbusiness.



Contents

- 5** Is This Guide Right for You?
- 6** Why Security Matters
- 7** Finding the Right Consultant
- 8** When Bad Things Happen to Good Companies
 - Viruses
 - Email Spoofing and Identity Theft
 - Stolen Computers
 - War Driving
 - Confidential Information
 - Criminal Hacking
- 11** 22 Questions That Can Help Protect Your Business
- 14** Introduction to Criminal Hacking, Viruses, and Malicious Activities
 - Networks, Internets, and the Internet
 - Viruses, Worms, Trojan Horses, Spam, and Hoaxes
 - Why Software Is Vulnerable
 - Common Security Threats Against Networks
- 17** Ten Steps to Better Security
 - Step 1: Use an Internet Firewall
 - Step 2: Get Computer Updates
 - Step 3: Use Up-to-Date Antivirus Software
 - Step 4: Use Strong Passwords
 - Step 5: Ensure Physical Security
 - Step 6: Browse the Web Defensively
 - Step 7: Use Email Safely
 - Step 8: Back Up and Restore Regularly
 - Step 9: Connect Remote Users Securely
 - Step 10: Lock Down Wireless Networks
- 28** Taking Special Care of Notebook Computers
- 29** How to Write a Security Plan
 - Audit
 - Plan
 - Execute
 - Monitor and Repeat
- 30** How to Write a Security Policy
- 32** Sample Security Plan: Adventure Works
 - Introduction
 - Objectives
 - Circulation
 - Project Team
 - Audit Results
 - Security Plan
 - Resources and Budget
- 39** Information Online
- 41** Glossary

Is This Guide Right for You?

Computer security is a growing concern for businesses of all sizes.

Computer security issues range from viruses to automated Internet attacks to outright theft, and the cost of these issues takes the form of lost information and lost time. Security issues pop up in news articles every day, and most small business owners understand that they should take steps to better secure their business. Increasing security can seem complicated, though, and it's often difficult to figure out where to start and just what measures you can take. This guide answers those questions.

If you own a small business or are responsible for directing the computing and security policies for a small business, this guide is for you. It is written with business people in mind. While the subjects we cover are sometimes technical, we have done our best to present the issues in everyday language that examines the issues, then shows you where you can find more technical information when you need it.

This guide breaks down the major security threats that your business faces and features a quiz that introduces concepts and shapes the way you think about your own security practices. You'll find a list of the top 10 steps you can take to increase security (see the sidebar, "10 Easy Steps to Better Security") and advice for creating a comprehensive security plan of your own. We have even included a sample security plan for a fictitious company named "Adventure Works."

While many of the steps outlined in this guide are steps that you can take yourself, don't be afraid to ask for professional support if you need it. There are many qualified technology and security consultants available to help. Be sure to read the sidebar, "[Finding the Right Consultant](#)," for information about where to look and what questions to ask.

10 Easy Steps to Better Security

1. Use an Internet firewall.
2. Get computer updates.
3. Use up-to-date antivirus software.
4. Use strong passwords.
5. Ensure physical security.
6. Browse the Web defensively.
7. Use email safely.
8. Back up and restore regularly.
9. Connect remote users securely.
10. Lock down wireless networks.

"52,658 computer vulnerabilities were publicly released in 2002."
—Computer Emergency Response Team Coordination Center (CERT/CC)

Why Security Matters

One of the biggest problems in computer security is that people have trouble believing that anything bad can happen to them—until it does.

The truth is that bad things do happen, and they happen more often than you might think. Surveys conducted by the Computer Security Institute and the Federal Bureau of Investigation (FBI) estimate that 90 percent of corporations and government agencies detected computer security breaches in 2002. Of those corporations and agencies, 80 percent acknowledged that these breaches resulted in financial losses.

Many small business owners believe that they do not need to worry much about security. “After all,” they reason, “who would want to target my business when there are so many bigger targets out there.” While it is true that small businesses are not directly attacked as often as larger organizations, there are three reasons why small businesses should be concerned. The first reason is that small businesses often end up as part of larger attacks, such as mass worm outbreaks or efforts to harvest credit card numbers. The second reason is that because security is becoming tighter than ever at larger companies, small business networks look increasingly tempting to attackers. And the third reason is that this logic assumes that all attacks come from the outside.

“General Internet attack trends are showing a 64 percent annual rate of growth.”
—Cooperative Association for Internet Data Analysis (CAIDA)

Regardless of how or why your business is attacked, recovery usually takes significant time and effort. Imagine if your computer systems were unavailable for a week. Imagine if you lost all the data stored on all the computers in your company. Imagine if your worst competitor was able to obtain a list of your customers, along with sales figures and sales notes. How long would it take before you noticed? What would these breaches cost your company? Could you afford these losses?

It seems like common sense. You wouldn’t leave your building unlocked at night. The same is true with information security, and a few simple steps can make you a lot less vulnerable. Technology experts have a way of making basic security seem like a huge and difficult issue. Luckily, securing your business is easier than you might think.

Of course, there is no way to guarantee 100 percent security. As the old saying goes, “You can make a door only so strong before it’s easier to come through the wall.” However, you can achieve a reasonable level of security and be prepared in case breaches do happen. Properly weighing risks and consequences against the cost of prevention is a good place to start.



Finding the Right Consultant

Finding the right consultant can be trying, but good support makes technology easier to manage and ensures that you get the best possible advice and implementation.

Where Do You Start?

Ask your colleagues, suppliers, and peers whom they use. Ask your local Chamber of Commerce or local Small Business Development Center (SBDC) for their input.

What Are You Looking For?

Evidence of experience is essential. You're looking for someone who can help you now but also be a long-term partner. Look for evidence of the ability to grow and develop as a company and support businesses bigger than yours. Use the following checklist to select the right company.

Experience

- Does the consultant have a Certified Information Systems Security Professional (CISSP) engineer on staff? If they have a CISSP on staff, you should feel good about the consultant's level of security expertise.
- Does the consultant have a Microsoft Certified System Engineer (MCSE) or Microsoft Certified Systems Administrator (MCSA) on staff? MCSEs are specialized in understanding how to design, implement, and administer security for a Microsoft Windows Server 2003 network and using Microsoft Internet Security and Acceleration (ISA) Server. MCSAs are specialized in understanding how to administer network environments.
- Does the consultant have a CompTIA Security+ Certification, which measures competencies for managing security.

Services

- Which of the following security services does the consultant provide?
 - a) Antivirus
 - b) Hardening servers (i.e., ensuring all settings for a system are at their most secure)
 - c) Hardening client/desktop computers
 - d) Perimeter security
 - e) Intrusion detection
- Do they provide security audits? Across which platforms?
- Do they provide 24x7 remote or on-site security support?
- What levels of support will they provide? Look for a service level agreement that sets out how quickly they will respond to problems and the level of after-sales support they offer.
- Can they provide it or recommend reputable trainers?
- Will they have the resources to grow with you in the future?

Approach

- Does the consultant apply consistent patterns and practices in their operations? Ask to see a framework for their process.
- Can they commit to a specific schedule and budget for a given project? Will they be able to do the work with their own staff, or will they have to subcontract?
- What is their fee structure? Depending on the project, it is possible to agree on a flat fee, an hourly or daily rate, or an ongoing retainer. Are they willing to break down their cost structure

and allocate costs to different stages or activities? You want accurate, exact, and precise information before any work is commissioned.

- How do they approach documentation? They should supply you with a proposal for the work, including a budget, a timetable, and a reasonable specification. The proposal should be in plain English.
- If their proposal is satisfactory, you should have a written contract specifying what is going to be done and by whom. Make sure to include dates, deadlines, equipment, costs, and so on. Even if you do not have a formal contract drawn up by attorneys, make sure that the details of the work are written down and agreed to in some form.

Where Next

There are two detailed guides to writing a security plan. Microsoft maintains a guide at www.microsoft.com/technet/archive/security/bestprac/bpent/bpentsec.asp. The Internet Engineering Task Force (IETF) also maintains a guide at www.ietf.org/rfc/rfc2196.txt to help you design a plan that works with your partners.

To find a Microsoft Certified or Gold Certified Partner, visit directory.microsoft.com. From there, click the *Services* tab and select *Security Systems – Design, Deployment, and Integration* from the *Service you require* drop-down list, or click the *Software* tab and select a Microsoft or third-party security product.

When Bad Things Happen to Good Companies

Your business may be at risk on a daily basis. The following stories illustrate threats with real-world examples and results. Don't panic, though. This guide explains how to assess threats and take preventative measures. You'll find more about how attackers operate in the section [“An Introduction to Criminal Hacking, Viruses, and Malicious Activities.”](#)

Viruses

In April 2003, Internet users around the world received emails containing pornography from friends and relatives. Others found Internet access terminated because they were accused of sending spam emails. Still others found themselves signed up to newsletters they didn't want.

As accusations flew, people realized that a new virus known as 'Klez' was responsible. The virus used several tricks that helped it spread quickly. First, it fooled users into thinking that infected emails were sent by real people by using addresses from the infected users' own address books. This trick had the added effect of clogging up email systems with unnecessary warnings, replies, and recriminations.

Later versions of Klez made users' own files the vehicle for infection. Klez trawled through an infected computer's hard disks, infecting documents, then forwarding them to other users by email.

Klez exploited a problem in the Microsoft Outlook email software that had been discovered and fixed years earlier with free, downloadable updates from Microsoft. Antivirus software developers became aware of the virus and updated their detection software within hours, yet Klez raged for several months.

Email Spoofing and Identity Theft

“I'm a big fan of eBay. I've been using it for years as a sales outlet for some of my merchandise. Recently, I got an official-looking eBay message letting me know



that my service was about to be suspended. I clicked the link in the email, went to what I thought was an eBay site, filled in some personal information, and submitted it. Only later did I realize that something was wrong. I went to the eBay Web site and figured out that I'd been tricked into sending my personal information to some unknown source.”

Sending email that looks like it comes from someone else is an old trick known as email spoofing. For the most part, email spoofing is used to get you to open a simple piece of spam because you think it's from someone legitimate—an annoying but fairly harmless activity.

A different type of email spoofing, such as the example above, is known as “phishing” and is more dangerous. Typically, an attacker sends an email that looks very much like it comes from an official source (such as eBay or Microsoft). Links in the email take you to a Web site that also looks like the real thing. However, the site is just a front, and the goal of the scam is to trick you into giving away personal information, sometimes for spam lists, sometimes so that the perpetrators can steal your account information or even your identity.

Stolen Computers

“I was getting my boarding pass at the airport. I had my notebook bag right by my feet. I thought I was taking good care of it, but I didn't feel a thing when it was stolen.” A stolen computer can fetch up to 50 percent of its retail price.

This story is repeated thousands of times a year, and it doesn't end when the notebook computer is replaced. Lose a notebook computer and you often lose vital, even confidential, information.

Given the number of computers stolen every year, it is surprising how few users bother to encrypt their data or use strong passwords that prevent unauthorized access. It is also surprising how few small businesses train their staff on basic security measures.

War Driving

A war driver is a new breed of criminal hacker. Anyone with a notebook computer, an inexpensive wireless network card, freely downloaded software, and an antenna made from something as simple as a can of potato chips can hack into wireless networks in homes and companies from hundreds of feet away.

Most wireless networks are completely unsecured. Indeed, many manufacturers of wireless devices leave encryption turned off by default. Users tend not to enable **wireless encryption** or use any other added security measures, making it a pretty easy task for anyone with a wireless setup to find and exploit the connection. War driving is more than a geek prank. Some intruders seek to access files and damage systems. Fortunately, securing a wireless network is relatively easy, and the majority of war drivers can be deterred or deflected by a few simple steps.

Confidential Information

James worked for a successful advertising firm. His computer had a problem, so he called his technical support person. The technician arrived quickly, logged into the network using an administrator password, and fixed the problem. Under pressure to get to the next job, the technician scuttled off as soon as he finished. He did not, however, log out of the system. James, being curious, decided to look around a bit. He quickly found a spreadsheet with information on the salaries of all his coworkers. He made a mental note to ask for a substantial pay increase.

Luckily for his employer, James was only after a raise. Imagine if he had been a disgruntled employee bent on revenge. Would you like your entire staff to know how much you are paid or have access to the entire company's payroll information? What

would that information be worth to your competitors?

Technology can help prevent instances like this, but technology is only part of the answer. The best hardware and software are not enough if you don't also have good policies, procedures, and training in place.

Criminal Hacking

Jill, the manager of a small commercial Web site that sells niche software, was pleased with her new site, which was a big improvement on the old one. The company now had its own Web server and broadband connection, and they no longer had to pay someone else to host the site. Jill went home content on Friday night.

On Monday morning when Jill got back to work, it was a different story. Over the weekend, criminal hackers had gained access to the Web server, deleted her carefully crafted site, and replaced it with pornography. In addition, hundreds of thousands of people had been avidly downloading pictures from the site over the weekend. Her bandwidth usage had shot through the roof, and the company was facing a bill for thousands of dollars. Jill's boss had already started to receive emails from customers complaining about the site.

An antivirus software developer reported earlier this year that corporate servers receive, on average, 30 attacks a week. Most of these attacks are from dedicated amateur attackers known as "script kiddies," who, without much knowledge, use tools that are freely available on the Internet to probe networks for weaknesses. These tools scan the Internet randomly looking for vulnerable systems, then exploit any weak-

Nicholas Negroponte, founder of the Massachusetts Institute of Technology (MIT) Media Lab, was entering a secure building when a security guard asked him to state the value of the notebook computer he was carrying. Negroponte replied, "Roughly \$1 to \$2 million." Although the replacement value of the computer itself was only a couple of thousand dollars, the value of the information it contained was much greater.

nesses they find. With such tools available, a small anonymous company is potentially as much at risk as a well-known multinational corporation.

Many of these tools exploit known vulnerabilities that can be easily updated. For example, in 2001, a group of script kiddies calling themselves the *Smoked Crew* used a well-known and previously updated vulnerability in Web server software to deface Web sites belonging to Intel, Gateway, Disney, and The New York Times. An update to fix the vulnerability was available long before the attack, but many administrators had simply not installed it. Taking sensible precautions in general, and using up-to-date software in particular, would have easily prevented the attack.

Backing Up

Kevin was the managing director of a growing architectural firm. With 30 employees and a number of multinational clients, the company relied on its email system to keep in touch and to track client requests. Then, one afternoon, the email server had a catastrophic hardware failure, and the data became corrupted.

“No problem,” thought Kevin, “our support guy has a backup, so we can just restore it from that.” In fact, the company had an elaborate tape library and dutifully kept offsite copies of its critical backups. It was only after a day’s work of trying to restore the email system from the backup tapes that they realized the data hadn’t been properly backed up. They had never noticed the problem and had never tested to see whether restoring the data worked properly. They did not have any kind of disaster recovery plan in place.

“In December 2002, one online spam-prevention service measured upwards of 5,000,000 unique spam attacks.” —CAIDA

Information security isn’t just about getting the right hardware and software; it is about getting the processes right and concentrating resources on business-critical systems.



22 Questions That Can Help Protect Your Business

This quiz is intended as an education and diagnostic tool to help you start thinking about security as it pertains to your small business. The correct answers and the number of points awarded are noted in parenthesis after the choice.

General Knowledge

1. What is a firewall?
 - a. A method of protecting a computer network against unauthorized access from the Internet (1 point)
 - b. A solid brick enclosure around a server room
2. Why do software developers issue updates for their software?
 - a. They really enjoy staying in touch with their customers
 - b. Thousands of attackers constantly try to find previously unknown vulnerabilities and the software companies want to protect users against these threats (1 point)
3. Which of the following are attacks a criminal hacker might use?
 - a. Spoofing
 - b. Tampering
 - c. Repudiation
 - d. Information disclosure
 - e. Denial of Service (DoS)
 - f. Elevation of privilege
 - g. All of the above (1 point)
4. Have you or your business suffered any of the following? (1 point each because now you're a veteran)
 - a. Computer theft
 - b. Unauthorized disclosure of information by staff or outsiders
 - c. Loss of critical data that wasn't backed up
 - d. Virus infection
 - e. Any kind of hacking or electronic intrusion

Plans, Policies, and People

5. Does someone on your staff oversee security issues?
 - a. Yes (1 point)
 - b. No
6. When did you last review and update your security policy?
 - a. Within the past three months (2 points)
 - b. Within the past year (1 point)
 - c. What's a security policy?
7. Is there a manager responsible for ensuring ongoing compliance with a security policy?
 - a. Yes (1 point)
 - b. No
8. Do you carry out regular audits of computer and software inventory?
 - a. Yes (1 point)
 - b. No
9. Does your company have up-to-date policies covering the following? (1 point each)
 - a. Acceptable use policy
 - b. Remote access policy
 - c. Information protection policy
 - d. Virus protection policy
 - e. Password policy
 - f. Perimeter security policy
10. Do you teach employees how to spot and address email hoaxes?
 - a. Yes (1 point)
 - b. No

Physical Security

11. What physical security measures do you take to protect your desktop PCs? (1 point each)
 - a. Good locks, alarms, and physical barriers
 - b. Visitor access control
 - c. PCs locked securely to desks
 - d. Serial numbers of components recorded
 - e. Computers not visible from the street on the ground floor
 - f. Monitors not facing windows from any floor
12. What physical security measures do you take to protect your servers? (1 point each)
 - a. Kept in a secure room
 - b. Access restricted to authorized personnel
 - c. Adequate fire protection
 - d. Serial numbers of components recorded
 - e. Backup power source
 - f. Kept in a locked rack with access restricted to only the subset of people who need access to the systems in that particular rack
13. What security measures do you take to protect your notebook computers? (1 point each)
 - a. Transported in padded but nondescript bags
 - b. Secured by a cable lock when unattended
 - c. Components security marked
 - d. Encrypted data on the notebook computer
14. What physical security measures do you take to protect software and backups? (1 point each)
 - a. Application master disks and license documents kept securely
 - b. Backups stored in a fireproof safe or in a secure offsite location
15. Do you have a maintenance contract for your computer equipment?
 - a. Yes (1 Point)
 - b. No
16. When interviewing security or information technology (IT) consultants and new staff members, do you examine their background and qualifications?
 - a. Yes (1 Point)
 - b. No

Information Security

17. Have you ever opened a file in an email from someone you didn't know because it looked interesting?
 - a. Yes
 - b. No (1 point)
18. Which of the following defenses do you have operating on your business network: (1 point each)
 - a. Software updates installed as they become available
 - b. Virus definitions updated on a regular basis
 - c. Firewall installed and correctly configured
 - d. Centrally enforced strong password policy
 - e. Web browsing and email usage policy enforced
 - f. Secure connections for remote users
 - g. Secure wireless network
 - h. Regular backups
19. Do you regularly back up your data?
 - a. No
 - b. Yes (1 point)
 - c. Bonus point: And you test restoring the data periodically
20. Do you regularly test your backups by restoring them and verifying the restored data?
 - a. No
 - b. Yes (1 point)
21. Are you running the latest versions of Microsoft Internet Explorer and Microsoft Outlook?
 - a. No
 - b. Yes (1 point)
22. Do you use encryption on your wireless network?
 - a. No
 - b. Yes (1 points)

Quiz Results

- Less than 10** Seriously consider studying security issues and putting together a plan (or hiring someone else to do so).
- 11 to 20** You know you need security, but you don't have the skills, time, or confidence to do something about it. You are at serious risk, and you need to take steps to protect your business.
- 21 to 30** You are like many people. You have good intentions and have taken some measures but are mostly just hoping that something bad won't happen to you. There are steps you can take now that will transform your security from "barely adequate" to "good enough."
- 31 to 40** You're doing pretty well. Look through this guide and see if there's anything you've missed. There may be a few tricks you've overlooked and some risks you haven't considered.
- 41 to 50** You've done a great job. It's probably worth scanning this guide to see if there's anything you've overlooked. Don't forget about the need to keep reviewing your security and updating your plans.
- Over 50 points** You could probably write a guide of your own.

“Internet-related fraud was the subject of 55 percent of the more than half-million complaints filed in 2003, up from 45 percent a year earlier. The median loss for victims of Internet-related fraud was \$195.” —Federal Trade Commission (FTC)



Introduction to Criminal Hacking, Viruses, and Malicious Activities

“Time is precious. Life’s too short to worry about computers.” We agree. But to understand the threats that exist and how to handle those threats, you need to know some technical stuff. Don’t worry—we’ll keep it to a minimum.

Networks, Internets, and the Internet

One computer on its own is a beautiful thing—a technical marvel. But it’s good to communicate. Link two or more computers together using network cards and cables (or a wireless setup) and you have a local area network (LAN). All the computers on the network can share data and email as well as access shared resources like printers, modems, or broadband Internet connections. Link two or more LANs together and you have a wide area network (WAN). For example, you might link two offices in different locations with a dedicated leased line.

An internet (note the small “i”) is a network of networks. Information from any computer in any given network can travel over the internet to any computer on any other network, with the internet acting as a sort of common carrier. Think of an internet as a highway system linking local road systems together.

The Internet (note the capital “I”) is a global internet. All computers on the Internet communicate using standard protocols so that information from any computer on the Internet can reach any other computer on the Internet. This is where the trouble occurs. Until you connect with a public network, you are reasonably safe from external threats. Hooking up to the public Internet is like publishing your name, address, and phone number and saying, “Hey look, we have computers here.”

Packets

Information typically travels across networks in packets. A packet is a chunk of data plus an address and other information that tells the network where to deliver that data. Everything going over the Internet is broken down into packets: Web pages, email, down-



loads, everything. Think of it like taking a circus on the road. You can’t take the whole circus in one vehicle. You have to break it up, package it into separate vehicles, tell each vehicle where it’s going, and put the circus back together when all the vehicles arrive at their destination. Like vehicles on a road, packets share physical connections and travel in streams. Big data is broken down into a series of packets and reassembled at the destination. As packets travel over the Internet, they are effectively exposed to eavesdropping by the public.

Ports and Addresses

Each computer on a network is assigned a unique number called an IP address. The IP address uniquely defines that computer on the network and provides directions for packets to reach their destinations. IP addresses work a lot like a street addresses. Part of the address identifies the network segment of the destination computer, and part of the address identifies the actual computer.

While an IP address refers to a computer and the network segment on which that computer exists, the individual applications on that machine must also be identifiable. Think of it like an apartment number attached to the street address: The street address denotes the apartment building, and the apartment number denotes the actual apartment. The IP address denotes the

computer, and the port number denotes the program on that computer. Each program on a computer that must send and receive data over the network is assigned a special port number. When packets of information are received at a particular port number, the computer knows which application gets the packet. For example, port 80 is the port for Web servers (which host the Web sites you use your Web browser to explore), and port 25 is the port that is used to send email. Packets are addressed to a specific port at a specific IP address.

Firewalls

A firewall blocks traffic over specified ports. This doesn't mean that you can't access services on other people's computers, just that outsiders can't get into yours. Some firewalls examine the packets that flow in and possibly out of the network to make sure that they are legitimate; they can also filter out suspicious packets. Firewalls hide the identities of computers within your network to make it harder for criminal hackers to target individual machines (Figure 1).

Servers

A server is really just another computer attached to a network but one that is designated to perform some special function, such as share a printer, store files, or deliver Web pages. Remember that if your notebook or desktop computer is connected to the Internet, it is also a kind of server and, without a firewall, is capable of receiving unwanted traffic from the Internet.

Viruses, Worms, Trojan Horses, Spam, and Hoaxes

Email is the conduit for billions of messages per year, and an increasing proportion of those messages are not pleasant. One email security firm scanned 413 million

emails in August 2003. Three percent contained a virus, 52 percent were spam, and a small but troubling percentage contained some kind of pornographic image. There are five main email threats:

- **Viruses** are programs designed to replicate themselves and potentially cause harmful actions. They are often hidden inside innocuous programs. Viruses in emails often masquerade as games or pictures and use beguiling subject lines (e.g., "My girlfriend nude") to encourage users to open and run them. Viruses try to replicate themselves by infecting other programs on your computer.
- **Worms** are like viruses in that they try to replicate themselves, but they are often able to do so by sending out emails themselves rather than simply infecting programs on a single computer.
- **Trojan horses** are malicious programs that pretend to be benign applications. They don't replicate like viruses and worms but can still cause considerable harm. Often, viruses or worms are smuggled inside a Trojan horse.
- **Spam**, or unsolicited commercial email, wastes bandwidth and time. The sheer volume of it can be overwhelming, and it can be a vehicle for viruses. Much of it is of an explicit sexual nature, which can create an oppressive working environment and, potentially, legal liabilities if companies do not take steps to stop it.
- **Hoax emails**, such as fake virus warnings, chain letters, or implausible free offers, waste readers' time. Hoax emails often contain viruses or Trojan horses and can lead to identity theft.



Figure 1: Attacks are blocked on closed ports, while open ports allow traffic through.

Why Software Is Vulnerable

Software developers do not set out to write unsafe programs. For example, a typical operating system is the product of tens of thousands of hours of work and consists of millions of lines of code. A simple bug or oversight can provide an unexpected backdoor into an otherwise secure system. It is impossible to write bug-free software. Of course, that doesn't mean developers should give up trying to do so.

Then there are the bad guys. Bank robber Willie Sutton once said, "I rob banks because that's where the money is." It's the same with software. The more

successful and widespread a piece of software is, the more likely attackers are to target it.

There is a continual struggle between attackers exploiting weaknesses and developers seeking to eliminate those weaknesses. It's the same with locksmiths and burglars, alarm manufacturers and car thieves. This is why software developers release updates that fix known vulnerabilities and why you should install those updates.

Common Security Threats Against Networks

Attackers have different motivations—profit, mischief, glory—but they all work in similar ways. There are a number of basic threats all of which are capable of infinite variation:

- **Spoofing.** There are a couple of kinds of spoofing. IP spoofing means creating packets that look as though they have come from a different IP address. This technique is used primarily in one-way attacks (such as Denial of Service attacks). If packets appear to come from a computer on the local network, it is possible for them to pass through firewall security (which is designed to protect against outside threats). IP spoofing attacks are difficult to detect and require the skill and means to monitor and analyze data packets. Email spoofing means forging an email so that the *From* address does not indicate the true address of the sender. For example, a round of hoax email messages circulated the Internet in late 2003 that were made to look as though they carried notice of official security updates from Microsoft by employing a fake email address from Microsoft.
- **Tampering.** Tampering consists of altering the contents of packets as they travel over the Internet or altering data on computer disks after a network has been penetrated. For example, an attacker might place a tap on a network line to intercept packets as they leave your establishment. The attacker could eavesdrop or alter the information as it leaves your network.
- **Repudiation.** Repudiation refers to the ability of a user to falsely deny having performed an action that other parties cannot prove otherwise. For example, a user that deleted a file can successfully deny doing so if no mechanism (such as audit records) can prove otherwise.
- **Information disclosure.** Information disclosure consists of the exposure of information to individuals who normally would not have access to it.
- **Denial of Service.** DoS attacks are computerized assaults launched by an attacker in an attempt to overload or halt a network service, such as a Web server or a file server. For example, an attack may cause a server to become so busy attempting to respond that it ignores legitimate requests for connections. In 2003, massive DoS attacks were orchestrated against several major businesses on the Web, including Yahoo and Microsoft, in an attempt to clog the servers.
- **Elevation of privilege.** Elevation of privilege is a process by which a user misleads a system to grant unauthorized rights, usually for the purpose of compromising or destroying the system. For example, an attacker might log in to a network using a guest account, then exploit a weakness in the software that lets the attacker change the guest privileges to administrative privileges.

Most attackers use the processing power of computers as their weapon. They might use a virus to spread a DoS program to hundreds of thousands of computers. They might use a password-guessing program to try every word in the dictionary as a password. Of course, the first passwords they check are “password,” “let-mein,” “opensesame,” and a password that is the same as the username.

Attackers have programs that randomly probe every IP address on the Internet looking for unprotected systems and, when they find one, have port scanners to see whether there are any ports open for attack. If they find an open port, they have a library of known vulnerabilities they can use to try to gain access. For more deliberate attacks (e.g., industrial espionage), a combination of technology and social engineering is most effective. For example, inducing members of staff to reveal confidential information, rifling through trash in search of revealing information, or simply looking for passwords written on notes by monitors are all options. For a complete glossary of security related terms, please see the [Glossary](#).

“The number of known viruses surpassed 70,000 in January 2002.” — CAIDA

Ten Steps to Better Security

This section outlines the basic security measures that every company should take to protect itself. Refer to the [Glossary](#) and the section “[Introduction to Criminal Hacking, Viruses, and Malicious Activities](#)” for information on anything that seems too technical. These steps assume that you have a security policy in place that defines security requirements, conditions, and standards. See the sidebar “[Creating a Security Policy](#)” for more information.



Step 1: Use an Internet Firewall

Summary

Prevent outsiders from breaking into your network from the Internet by installing a hardware-based firewall. Further, protect individual computers by enabling the Microsoft Internet Connection Firewall, a feature of Windows XP Professional.

What

Hardware firewalls are an essential first line of defense that protect your local network from outside attacks by screening out unwanted communication. Think of a hardware firewall as a paranoid switchboard operator who allows calls only from people you say are okay and tells everybody else “you’re in a meeting.” Hardware firewalls block all traffic between the Internet and your network that isn’t explicitly allowed. They can also hide the addresses of the computers behind the firewall, making the individual computers on your network invisible to outsiders.

Software firewalls, such as the Internet Connection Firewall built into Windows XP Professional, work similarly to hardware firewalls but protect only the computer on which they are running. They offer a good backup defense to hardware firewalls but on their own are not adequate protection for a network.

Why

Criminal hackers can find your network and potentially target individual machines from the Internet, even if they don’t know you exist. It’s like dialing random numbers in the phone book. If you have an always-on connection, such as a cable modem, chances are that your network is being randomly probed or attacked several times each day. Armed with a valid computer address, these attackers can exploit vulnerabilities in software (especially software that isn’t kept up-to-date with the latest updates) or crack passwords to gain access to the network. A firewall isn’t sufficient on its own to guarantee security, but it is a good first line of defense.

How

Hardware firewalls are connected between the private computers on your network and the public Internet connection (refer to [Figure 1](#)). All traffic between the private network and the Internet pass through the firewall, so a hardware firewall protects your entire network. The firewall examines each incoming and outgoing packet and accepts it or rejects it based on predefined rules. For example, your firewall might be configured to accept a particular kind of email traffic and Web traffic but reject all other types of traffic.

Hardware firewalls are often integrated into the router or DSL/cable modem supplied by your Internet service provider (ISP) to connect your network to the Internet. Check with your supplier to see if this is the case. If your ISP just supplies a modem, you can purchase inexpensive hardware router/firewalls from companies such as LinkSys, Microsoft, D-Link, and NetGear. The nice thing about using a combination router/firewall is that in addition to providing firewall protection for your network, the device also lets you network multiple computers and share an Internet connection.

Hooking up a hardware firewall to your network is actually a pretty simple procedure. The firewall just connects between the cable/DSL modem and the computers on the network. Configuring the firewall is not much more complicated than connecting it. Most hardware firewalls provide for a simple Web-based connection so that you can configure them using your Web browser. By default, firewalls are set to block all incoming traffic from the Internet; configuring a firewall will be a matter of deciding what, if any, traffic you want to allow. Of course, if you have anything more complicated than a simple network, you can always consult a security or technology professional for guidance.

Software firewalls run on a particular computer and examine only that traffic coming into or leaving that computer. If you have a single computer connected to the Internet, you can use a software firewall. The Internet Connection Firewall built into Windows XP Professional is a powerful software firewall and it's free, but it's not quite as configurable as some of the other commercial software firewalls available. Users of previous versions of Windows should consider a commercial software firewall from vendors such as McAfee, Symantec, or ZoneLabs.

To enable Internet Connection Firewall on a computer running Windows XP Professional, click *Start*, then click *Control Panel*. In the Control Panel applet, click *Network and Internet Connections*, then click *Network Connections* to display all network connections configured on the computer. Right-click the connection you use for Internet access (typically a modem or a LAN connection to a router), then select *Properties*. In the Properties dialog box, click the *Advanced* tab. Select the *Protect my computer and network by limiting or preventing access to the computer from the Internet* option, then click *OK* (Figure 2).

Note: A firewall can sometimes block activities that you want to allow, such as instant messaging or hosting multiplayer games. If this happens, don't turn off the firewall. Instead, open just the ports that are required by the software you are running. Refer to www.microsoft.com/security/protect/ports.asp for further instructions.

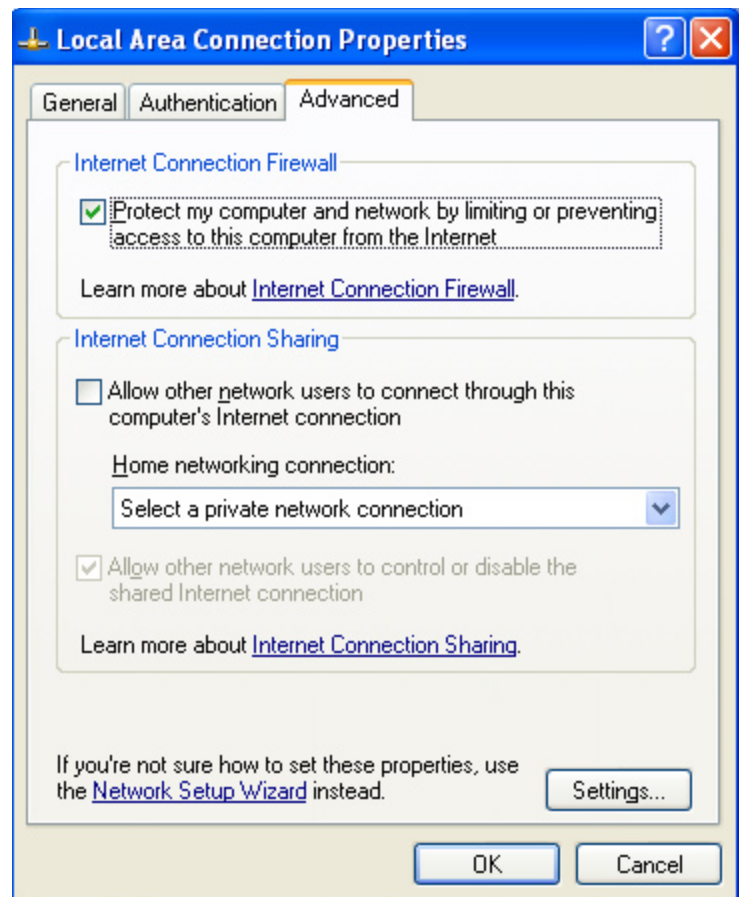


Figure 2: Enabling Internet Connection Firewall in Windows XP Professional

What a Firewall Does NOT Do

It is important to remember that a firewall is only the first line in your security defense. No matter how effective it is, a firewall does not protect against:

- malicious traffic that does not travel through the firewall
- attacks that are initiated after a network has been compromised (e.g., if an attacker is able to exploit vulnerabilities in your operating system software, if the computer has been accessed from inside the company)
- traffic traveling over legitimate channels
- many viruses, including those that might seek to open a loophole in your security

Where Next

For firewall software, visit www.networkassociates.com/us/index.asp, www.symantec.com, or www.zonelabs.com.

For information about how firewalls work, go to www.microsoft.com/security/protect and www.microsoft.com/technet/security/topics/network/firewall.asp.

To test your vulnerability, go to www.grc.com (follow the links for the Shields Up program) or securityresponse.symantec.com (click the Check for Security Risks link). The

www.grc.com site also provides an amazing amount of information about the world of Internet security.

For an excellent introduction to the world of criminal hackers, including interviews and useful background reading, visit www.pbs.org/wgbh/pages/frontline/shows/hackers.

Step 2: Get Computer Updates

Summary

Download and install the latest updates for your software so you can stay one step ahead of the bad guys.

What

Attackers find and exploit bugs and loopholes in popular software, mostly for the thrill of doing it, sometimes for profit or just to cause mischief. When Microsoft discovers a vulnerability in its software, it releases an update for people to download over the Internet. Over time, the fundamental architecture of computer systems becomes more robust and secure. For example, Microsoft Windows XP Professional is inherently more secure than Windows 95 or Windows 98.

Why

Many virus infections and attacks occur unnecessarily. Many times, updates exist that will prevent a problem, but users fail to install them.

How

It is easy to download and install the latest updates for Microsoft (and for many other) products. For Windows XP Professional, go to www.windowsupdate.com, click *Scan for updates*, and the Web site automatically downloads and installs what you need to be current. (For information about updates via email, see the sidebar, “Microsoft Security Update by Email.”) If you have an always-on broadband connection, you can take advantage of a feature called Automatic Updates in many newer versions of Windows, including Windows XP Professional. You can have Windows monitor for available updates, download them, then install them—all automatically and all in the background.

To enable the Automatic Updates feature, right-click *My Computer* and choose *Properties*, click the *Automatic Updates* tab, then select the *Keep my computer up to date* check box (Figure 3). Then, choose how Windows should scan for and download updates.

If you are using Microsoft Office, it is important that you keep it up-to-date, as well. Security updates and other downloadable add-ins are available at office.microsoft.com/officeupdate.

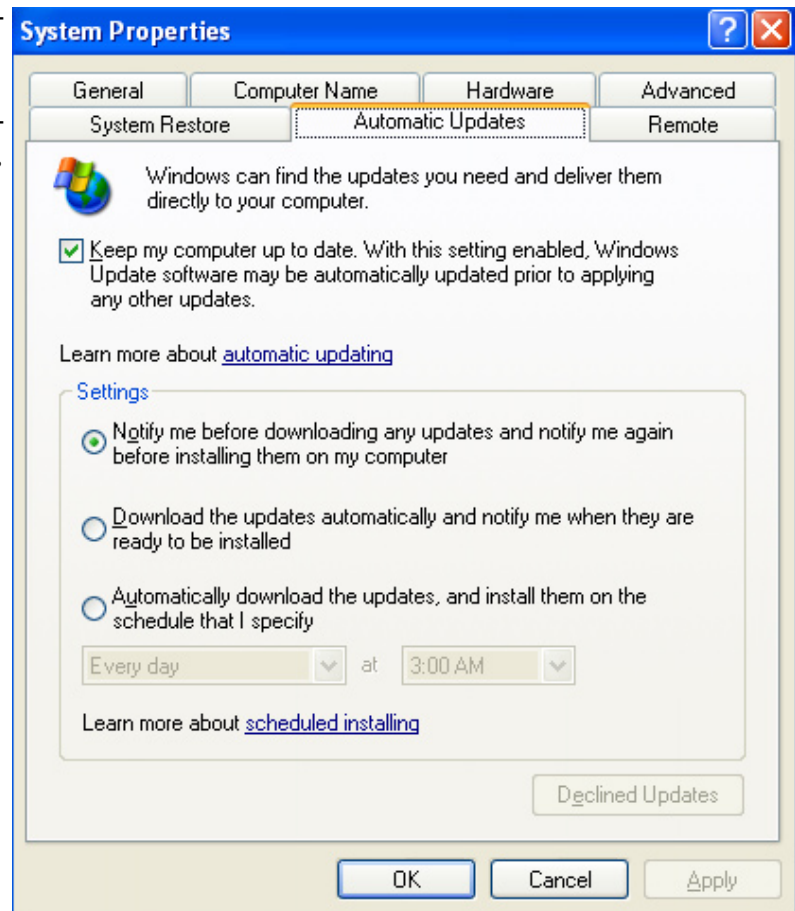


Figure 3: Enabling Automatic Updates in Windows XP Professional

Where Next

- www.windowsupdate.com
- office.microsoft.com/officeupdate (click *Check for updates*)
- www.microsoft.com/security

Microsoft Security Update by Email

Microsoft Security Update is a free email alert service geared toward home users and small businesses. Microsoft uses this service to notify subscribers when an important security bulletin or virus alert is released and to make users aware that they might need to take action to guard against a circulating threat. Microsoft Security Update is an important safeguard to help ensure that users are aware of current threats. For more information and to sign up, visit www.microsoft.com/security and click the Stay Secure banner.

Step 3: Use Up-to-Date Antivirus Software

Summary

Prevent virus infections by installing antivirus software and updating it regularly. Don't open suspect files. Use the security features built into Microsoft Outlook. Consider upgrading your email software to Outlook 2003 and using the built-in Junk Email filtering feature.

What

Viruses (and their counterparts, worms and Trojan horses) are malicious programs that infect computers. The infection starts when a user runs an infected program or script, usually from an email attachment or downloaded from a Web site. Viruses can also be embedded in Web pages and in emails formatted to look like Web pages (e.g., HTML-format emails). Embedded viruses simply run when the page or email is viewed. Often, these files are enticing or deliberately misleading. Once infected, a PC can spread the virus quickly to other users.

Why

Different viruses have different effects. Some viruses delete or change files. Other viruses consume computer resources. Some allow outsiders to access your files. All viruses take time to eradicate and, if passed on to friends, customers, or colleagues, can be embarrassing.

How

Here are four simple measures that dramatically reduce the risk of virus infections:

- *Buy and install antivirus software and keep it up-to-date.* You should install antivirus software on every computer on a network. This software works by scanning the contents of incoming emails (and files already on your computer), looking for virus signatures. If the software finds a virus, the software simply deletes or quarantines it. A virus signature is like a unique DNA sequence in the virus's computer code. Because there are hundreds of new viruses each month, all antivirus software must be updated regularly with the latest signature definitions so that the software can catch the latest viruses. Antivirus software without the latest virus signatures is no good. Look for software that automatically downloads the latest definitions and program updates from the Internet. If you have an always-on broadband connection, you can set most software up to scan for and download new virus definitions in the background. If you use a dial-up connection, be sure to check periodically for new updates yourself. As an additional line of defense, you can also install software on an email server so that every piece of email coming into a company is scanned. Some ISPs provide automatic virus filtering to their clients.
- *Don't open suspect files.* The golden rule is to not open any files attached to an email from an unknown, suspicious, or untrustworthy source, no matter how enticing the email may seem. Be just as careful when visiting suspect Web sites or downloading files from the Internet. It is better to be safe than sorry. Download only from sites you trust. Most antivirus products scan all files that are stored to your hard drive, no matter where they come from (e.g., a Web site, email, a floppy drive, over the network). Make sure that automatic protection is enabled in your antivirus software. Be aware that hoax emails about viruses (along with chain letters and other correspondence) are almost as common as viruses themselves. Check with a trusted source, such as the manufacturer of the antivirus software you use, before forwarding one of these emails to other people. Educate other users to be similarly circumspect.
- *Use the security features built into Outlook and Outlook Express.* Microsoft Office Small Business Edition 2003 prevents viruses with a trio of features. First, each program supports macro security that, when properly configured, prevents macro viruses from running on your computer. Second, Outlook 2003 blocks dangerous attachments so that you don't accidentally or unknowingly run a virus that you receive in an email message. Third, Outlook 2003 includes enhanced support for third-party antivirus products, making it more likely that your antivirus software works properly.

If you use Microsoft Outlook Express, you may need to make a few changes. First, if you are running a version older than 6.0, upgrade to the latest version (www.microsoft.com/windows/ie). Second, increase security in Outlook Express by turning on its ability to block certain types of file attachments. Here's what to do: Select *Tools, Options*, then click the *Security* tab. Select the *Do not allow attachments to be saved or opened that could potentially be a virus* option, then click *OK*.

- *Block spam.* Spam is unsolicited commercial email and it's on the rise. Around half of all email being sent around the world is spam. Some of it carries viruses. Some of it is offensive. The average employee spends

about an hour a day dealing with email, so spam has a clear impact on productivity. Outlook 2003 features automatic spam protection. To enable this protection, select *Tools, Options*, then click *Junk Email* and choose your desired level of protection (Figure 4).

Where Next

For general information about viruses, visit www.microsoft.com/security/protect and www.microsoft.com/security/antivirus.

For antivirus products, visit www.symantec.com, www.mcafee.com, ca.com/smb, and www.trendmicro.com/en/home/us/smb.htm.

For an online database of known Internet hoaxes, visit hoaxbusters.ciac.org or www.symantec.com/avcenter/hoax.html.

For an informative explanation of how spam works, visit www.message-labs.com/viruseye/research/default.asp.

Step 4: Use Strong Passwords

Summary

Don't make it easy for the bad guys to access secure systems by using easily guessed or easily cracked passwords. Educate users to select strong passwords and change them regularly.

What

A password is the most common way of authenticating your identity. Authentication relies on something you know (e.g., a secret word or phrase), something you are (e.g., a fingerprint or iris scan), or something you have (e.g., a smart card or a physical key). Passwords are most common because they are the easiest to use. However, they are also the most easily misused.

Why

Attackers use automated tools to guess and find simple passwords in minutes. Social pressure or fraud (often referred to as social engineering) can persuade users to divulge their passwords. For example, an attacker might call your receptionist pretending to be a security consultant in the middle of an emergency and ask for his or her password for tracking or debugging purposes. The best security in the world is irrelevant if someone has your password.

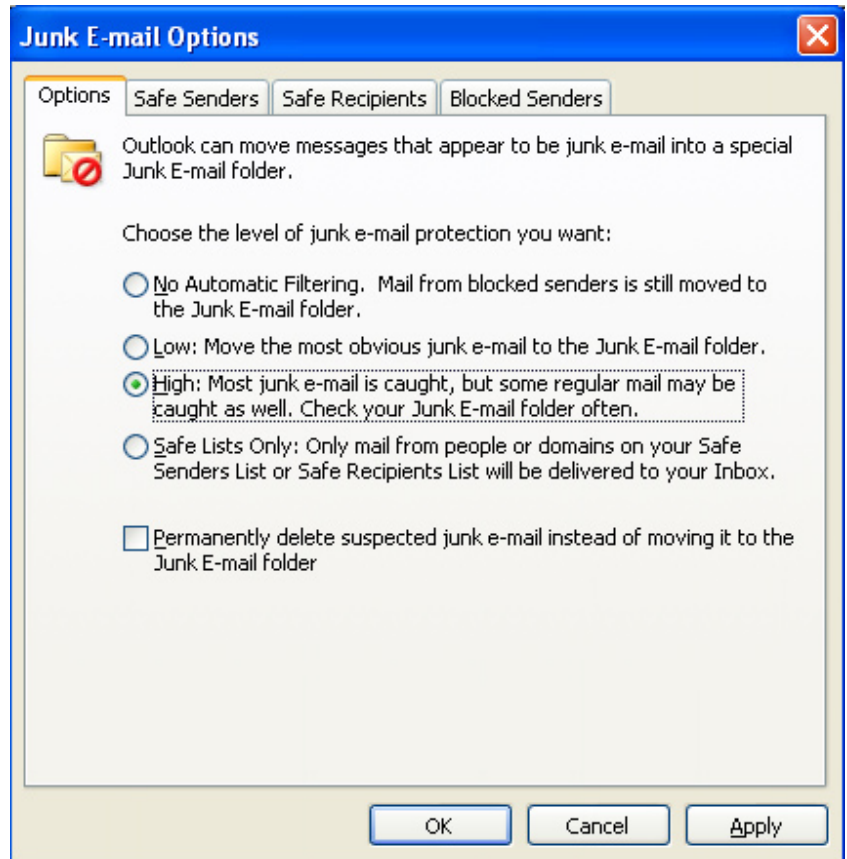


Figure 4: Enabling Spam Protection in Outlook 2003

How

First, you must understand why some passwords are weak. Consider the following:

- Using no password at all is not a good practice, mostly because it makes it easy for other employees to just walk up to an unsecured computer and log on.
- Using your real name, your username, or your company name makes for an easy-to-guess password.
- Using a common word makes you vulnerable to automated “dictionary attacks.”
- Common passwords such as “password,” “letmein,” and “1234” are easily guessed.
- Passwords that you write on a note near your computer are easy to find.
- A password you haven't changed in more than a couple of months may have been guessed or cracked without your knowing about it.

- A password that someone else knows is always an added vulnerability.
- A password that uses commonly known substitutions for letters, such as replacing ‘i’ with ‘!’, replacing ‘s’ with ‘\$’ or ‘5’, replacing ‘o’ with ‘0’, and so on. Modern password crackers take these substitutions into account, and using them in your password does not improve the strength of the password at all. Effectively speaking, if a substitution makes sense to you, it probably makes sense to a password cracker, too.

Conversely, a strong password has the following characteristics:

- It should be at least eight characters long, and longer is better.
- It should use a combination of lower-case and upper-case letters, numbers, and symbols (e.g., ` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : “ ; ‘ < > ? , . / or a space character).
- It is changed regularly (every 90 days is okay, but we recommend every 42 days) and is significantly different from previous passwords. (Passwords that increment, such as Password1, Password2, Password3, are not strong.)

Following these rules, an example of a strong password might be J*p2leO4>F.

Of course, a password you can’t remember is no use at all. There are some tricks that can make strong passwords more memorable:

- In Windows 2000 and Windows XP, you can use a passphrase such as “I had 5 chicken tacos for lunch.”
- You could also pick a phrase, then use only the first character of every word, such as Msi5Yold! (My Son is 5 years old!).
- Another trick is to take short, simple words and join them together with numbers and symbols (e.g., Tree+34+Pond).

You should decide on a password policy that balances security with practicality. Enforcing a tough policy on all users often encourages them to write down their passwords. You could also create different policies for different types of users and systems. For example, you might insist on stronger passwords for administrators or human resources (HR) personnel.

Any policy also needs to take into account the risk of social engineering and human weakness. Encourage users to think of their passwords in the same way they would think of a key to the office: Don’t leave it lying around, and don’t share it with anyone.

It is also sensible to set up screensavers so that systems require passwords to get back in. Doing so prevents people from wandering away from their desks and leaving their computer logged in.

Where Next

To configure a password policy in Windows Server 2003 (or Small Business Server 2003), go to www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/password_grouppolicy.asp.



Step 5: Ensure Physical Security

Summary

Keeping your office computers safe and preventing physical access to workstations and documents is a vital part of creating a secure computing environment.

What

Locks, alarms, lockable filing cabinets, visitor logging, computer restraints, and asset tagging

Why

Not all catastrophes are caused by outside attackers working over the Internet. Sometimes, a casual break-in can be more damaging. Even the best firewalls can’t keep out someone who is sitting at your server or a local workstation.

How

Here’s a step-by-step guide and checklist for ensuring the physical security of your business information and computers:

1. Establish a security perimeter around the area using (as appropriate) walls, self-shutting doors, lockable doors, alarms, and security curtains.
2. Make sure that points of access from the outside are manned and that visitors are identified and logged as they come and go.
3. Where possible, use additional barriers to restrict access to sensitive areas (such as server rooms or employee records). Review who has access to what on a regular basis. You should permit only authorized users to enter these areas. Visitors should be escorted. Staff should be encouraged to question unescorted strangers in secure areas.
4. When picking a location for a server room or other vital area, consider risks such as fire and flooding. If necessary, consider installing fire extinguishers.
5. Lock your doors and windows when they're not in use.
6. Test alarms regularly.
7. Initiate a "clear-desk" policy so that people can secure sensitive or valuable materials when they are not working on them.
8. Mark computers and their major components with information that identifies your company, the location of the computer, and the user.
9. Log the serial numbers of computers and components so they can be identified and recovered if stolen. Etch the serial numbers onto hidden areas of the computer case with a knife or other sharp implement, if possible.
10. Encourage users to pick up their documents from printers and photocopiers promptly. Set up secure printers for printing confidential information.
11. Make sure that your policies for staff cover what equipment can be taken off-site. Sign valuable items out to individuals and make them responsible for their return.

For information about securing notebook computers, see the sidebar, "Taking Special Care of Notebook Computers."

You should also consider performing a complete risk assessment in conjunction with your insurance company, a local crime prevention officer, and even independent advisors or security consultants.

Where Next

www.cybercrime.gov

www.gocsi.com

Step 6: Browse the Web Defensively

Summary

Ensure that you browse the Web safely.

What

You must educate employees about the ways in which they can minimize the risks of browsing the Web.

Why

Web pages can contain programs. These programs are usually innocent and useful (e.g., animations and pop-up menus) but can sometimes contain viruses. Also, allowing employees to view questionable content at the office can cause legal problems. Finally, bandwidth is often a consideration for small businesses and limiting the Internet activities allowed can help preserve this valuable commodity.

How

There are a number of precautions you can implement to help make Web browsing a safer activity for your employees. Consider the following steps:

- *Do not go to Web sites you cannot trust.* One way to implement this precaution is to discourage employees from using their work computers for idle browsing. Ask them to go only to sites necessary for their work.
- *Do not browse Web sites directly from a server.* Always use a workstation computer.
- *Consider using a router/firewall that lets you filter Web addresses or installing Web-filtering software.* Companies like Websense and Secure Computing offer products that filter Internet use based on many different criteria.
- *Create a Web policy handout to distribute to employees.* Indicate whether employees are allowed to browse the Web for personal use or only for increasing business productivity. If you want to allow personal use during lunch or off-hours, indicate that in the policy. Inform employees whether Web use is monitored and whether they can have expectations of privacy with regard to Internet usage. Don't be afraid to spell out unacceptable behavior in no uncertain terms—indicate behaviors like downloading offensive content, threatening or violent

behavior, illegal activities, commercial solicitations (non-business related), and so on. Provide two copies to employees—one for them to keep and one for them to sign and return to you.

Where Next

For more detailed instructions and background information, visit www.microsoft.com/windows/ie/using/howto/security/settings.asp.

For Web-filtering software, visit www.securecomputing.com and www.websense.com.

Step 7: Use Email Safely

Summary

Learn to spot email hoaxes, and take general email precautions.

What

Viruses, spam, and hoaxes can make using email a little frustrating, but you can make yourself much safer with a few simple precautions. Some of these precautions involve setting up your email software correctly, some involve using third-party software, and some involve teaching yourself and your staff how to spot potential problems.

Why

Email is a vital communications tool for most businesses. However, because email is the most-used Internet service, it makes a tempting target for attackers. Learn how to enjoy the benefits of email and minimize its risks.

How

Newer email client software has evolved to be more secure in response to the growing number of risks presented in email messages. However, you'll still need to take a few precautions:

- *Keep your email (and other) software up-to-date.* Program updates often include vital fixes for security issues. If you are using Microsoft Outlook, be sure to visit office.microsoft.com/officeupdate/regularly. Click Check for Updates, then let the site scan your computer and suggest updates. You should also keep Windows updated with the latest security updates. If you are using other email software, visit the manufacturer's site for updates.
- *Install antivirus software and keep it up-to-date.* Use a reputable vendor's antivirus software that works with your email software, and make sure you download new virus definitions regularly.

- *Filter junk email.* If you are using Outlook 2003, turn on its Junk Email filtering. If you are using earlier versions of Outlook (or other software), consider upgrading to Outlook 2003 or using a third-party antispyware software package.
- *Don't open suspicious attachments.* Do not open attachments to email messages that you did not explicitly request. The safest course of action is to respond to the sender and confirm the attachment's content.
- *Don't respond to spam.* Often, a piece of junk email has a link or an address included that claims it will have you removed from the spammer's mailing list. However, responding to spam usually just lets the spammer know that you have an active, valid email address. Ignore the spam and delete it.
- *Never give out passwords, credit card numbers, or other personal information in response to an email message.* If a valid business needs your information, they will not ask for it via email. Instead, they will ask you to submit it on a secure Web site. If you receive an email message and are not sure whether it is from a valid source, the first thing you should do is open Microsoft Internet Explorer and type in the address of the company (do not click the link in the email message). Once you are in the company's real Web site, you can probably find out whether they really need any information from you.

Where Next

For general information about email security and viruses, visit www.microsoft.com/security.

To research possible hoaxes, visit www.symantec.com/av-center/hoax.html, and hoaxbusters.ciac.org.

Step 8: Back Up and Restore Regularly

Summary

Back up regularly as a vital insurance policy. Test your backups by restoring them periodically to ensure proper procedures.

What

There are two parts to consider when creating a good backup solution: the backup hardware and the backup procedures. Having a fast, high-capacity backup device is no good if you don't back up all your data frequently. There are two basic kinds of backup: a full backup and an incremental backup. A full backup makes a complete copy of the selected data onto

another medium. An incremental backup just backs up the data that has been added or changed since the last full backup. Using a full backup augmented by incremental backups is quicker when backing up and takes less space. However, restoring data after a crash takes longer because you must first restore the full backup, then restore each incremental backup in turn. In a typical full/incremental backup solution, you might perform a full backup once a week and a faster incremental backup each day. Depending on the amount of data you need to back up and the times you have available for performing the backup, you may be better off just performing a full backup every night.

This solution is certainly simpler to keep up with and makes restoring much easier.

Just creating a good backup solution does not go far enough, though. You must test your backups regularly by actually restoring data to a test location. This ensures that your backup media and your backed-up data are in good shape. Practicing the restoration process also helps identify potential pitfalls in the process and provides a level of confidence that will come in handy during a real crisis.

Why

Backups are the last line of defense against hardware failure, floods or fires, the damage caused by a security breach, or just accidental deletion of data. Ask yourself what would happen if you lost all your critical business data. How long would it take you to recover? How much disruption and delay would occur?

How

First decide on the hardware. Your solution depends on how much data you have and how much you want to spend. Reusable media like tapes are more expensive to buy initially but can be reused. Write-once media such as recordable CD-ROMs or DVDs are cheaper initially but can be used only once. The following table provides a rule-of-thumb guide.

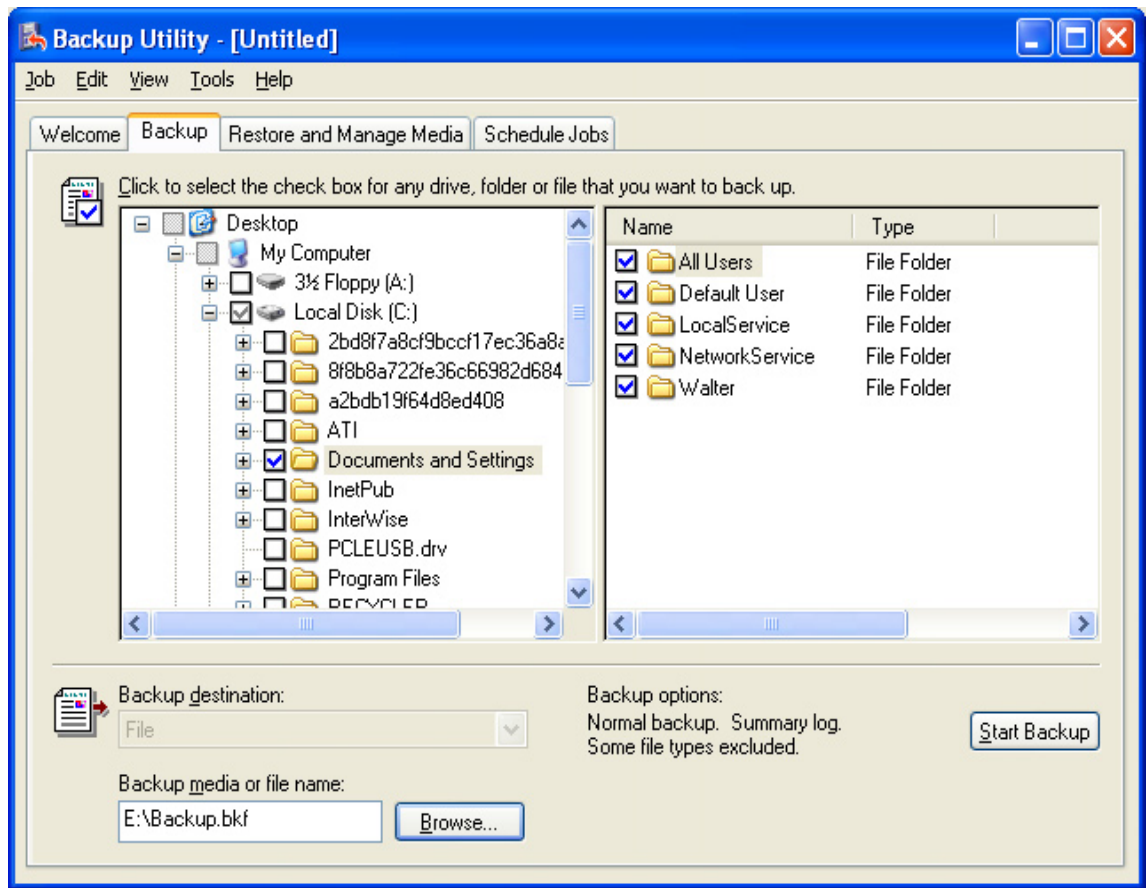


Figure 5: Microsoft Backup Utility for Windows XP Professional

| Total Size of Data | Suggested Medium |
|--------------------|---|
| Under 700MB | Recordable CDs |
| 700MB - 5GB | Recordable DVDs |
| 2GB - 12GB | Digital audio tapes (DATs) |
| Greater than 12GB | DAT carousels or higher capacity tape systems |

Most CD and DVD writers (the disc drives that can actually write CDs and DVDs) come with easy-to-use backup software. You simply select the data to back up, the location to which you're backing up, then start the backup. You can also schedule automated backups. Windows XP Professional comes with Microsoft Backup (Figure 5), which supports full and incremental backups of up to 4GB to spare disks and tapes. Windows Backup does not, however, support writeable CD or DVD drives.

Review what data is vital to your business and where it is stored. The data may be distributed across various computers or stored on a central server. It may reside in your company's email system. It may be in the form of databases or word processor documents. Create a simple map of where the data is located, and try to quantify its importance.

If data is stored on different computers, it makes sense to schedule a regular backup on each machine to consolidate the data in a single place (typically on a server). You can then back up the server for additional protection. For added security, store a copy of your backups at an offsite location (such as a safety deposit box) in case of catastrophic events like fires or natural disasters.

Identify the person responsible for backups. Have that person periodically test the integrity of backups by restoring some or all of the backed up data onto a test machine (make sure you don't overwrite existing data with the test data you are restoring).

Where Next

For more information about how to use Microsoft Backup, go to www.microsoft.com/windowsxp/home/using/howto/maintain/backup.asp.

Step 9: Connect Remote Users Securely

Summary

Make full use of encryption and authentication technologies when connecting to your network over the Internet.

What

It is useful for remote users (e.g., people working at home, or on the road) to access a company's network. Linking remote users and the network over the Internet is efficient because there is no need for dedicated (and expensive) leased lines. Dial-in users can connect to any local ISP rather than make a long-distance call back to the home office. There are several ways to achieve remote connections, but one of the most secure is using a virtual private network, or VPN (Figure 6). Encrypting the data as it travels over the public Internet stops outsiders being able to read it, and authenticating users ensures that only legitimate users can connect.

Why

Remote access to networks, including email, is an important business capability. At the same time, making your network available to outsiders is a security risk.

How

Setting up a VPN consists of three tasks. First, set up a VPN server on your company's network. (An existing computer can serve as the VPN server). Second, make sure that your firewall is set up to allow VPN traffic. Third, set the remote user's computer to connect through the Internet to the VPN server. Getting a VPN working properly can be tricky, so be prepared to spend some time researching it or to hire a security or technology consultant to set the VPN up for you.

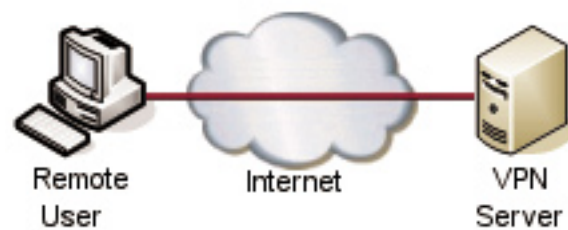


Figure 6: A VPN connection is a secure tunnel through the public Internet

Finally, use strong passwords (or even better, biometric or token-based authentication) to confirm the identity of users connecting to your network over the Internet.

Where Next

To learn more about remote access (including VPNs), visit www.microsoft.com/technet/security/topics/mobile/default.asp.

Step 10: Lock Down Wireless Networks

Summary

Implement basic security measures to make wireless networks less vulnerable to outside attacks and freeloaders.

What

Wireless networks, which are sometimes known as Wi-Fi or 802.11 networks, use a radio link similar to a cordless phone to connect computers. Because it allows computers to be connected to a network without physical cables, wireless networking makes setting up a network fast and flexible. Wireless networking can be used to link PCs, notebook computers, and PDAs to an access point that functions as a hub for all the computers connected to it.

Why

Wireless networks are more vulnerable than cabled networks. Anyone within radio range can, in theory, listen in or transmit data on your network. The point is that intruders don't need physical access to your hardware to do so. They can be war drivers in the parking lot snooping for secrets or neighbors just trying to catch a free ride on your Internet connection. Freely available tools allow intruders to "sniff" for insecure networks. Most manufacturers of wireless networking products turn off the security features by default, which makes wireless networks easier to set up but insecure.

How

The objective here is to make wireless networking as secure as possible on the assumption that someone is snooping. Although the Wi-Fi standard defines features such as encryption and access control, the way you set these features up varies by manufacturer. This advice seems a little technical because it is possible to say only what you need to do, not specifically how you do it. Therefore, you must refer to the documentation that comes with your hardware to set up the following defenses or get help from your local IT consultant. Figure 7 shows one possible means—the Microsoft Broadband Network Utility—of configuring a wireless network.

- *Turn on and use Wi-Fi Protected Access (WPA) encryption to prevent eavesdropping.* There are several encryption technologies used on wireless networks. Older equipment may offer only Wired Equivalent Privacy (WEP), a less robust encryption technology. If your hardware uses WEP, consider upgrading to hardware that offers WPA. When setting up encryption, be sure you use a strong password.
- *Use access points rather than ad hoc peer-to-peer networks.* Access points give you more control over who can access your network.
- *Restrict wireless access.* If your access point allows it, restrict wireless access to normal office hours or whenever you expect to use the network.

- *Use Media Access Control (MAC) filtering.* Each network card has a unique code called a MAC address. You can set access points to restrict access to certain trusted MAC addresses, which means that you can choose the specific computers (or other devices) that are allowed to access the network. Although an expert user can hack or deduce a MAC address, this simple precaution filters out some casual intruders.
- *Restrict the ability of users (and network administrators) to set up “quick and dirty” wireless networks, even temporarily.* Manage wireless networks carefully and continually. One rogue access point can undo all the good work you do securing the other access points.
- *Have security measures in place.* Make sure all your other security measures (e.g., strong passwords) are in place so that you have a good combination of defenses against intruders.

Where Next

For more information about the risks of wireless networks, go to www.wardriving.com.

See your manufacturer’s Web site for detailed security guidance.

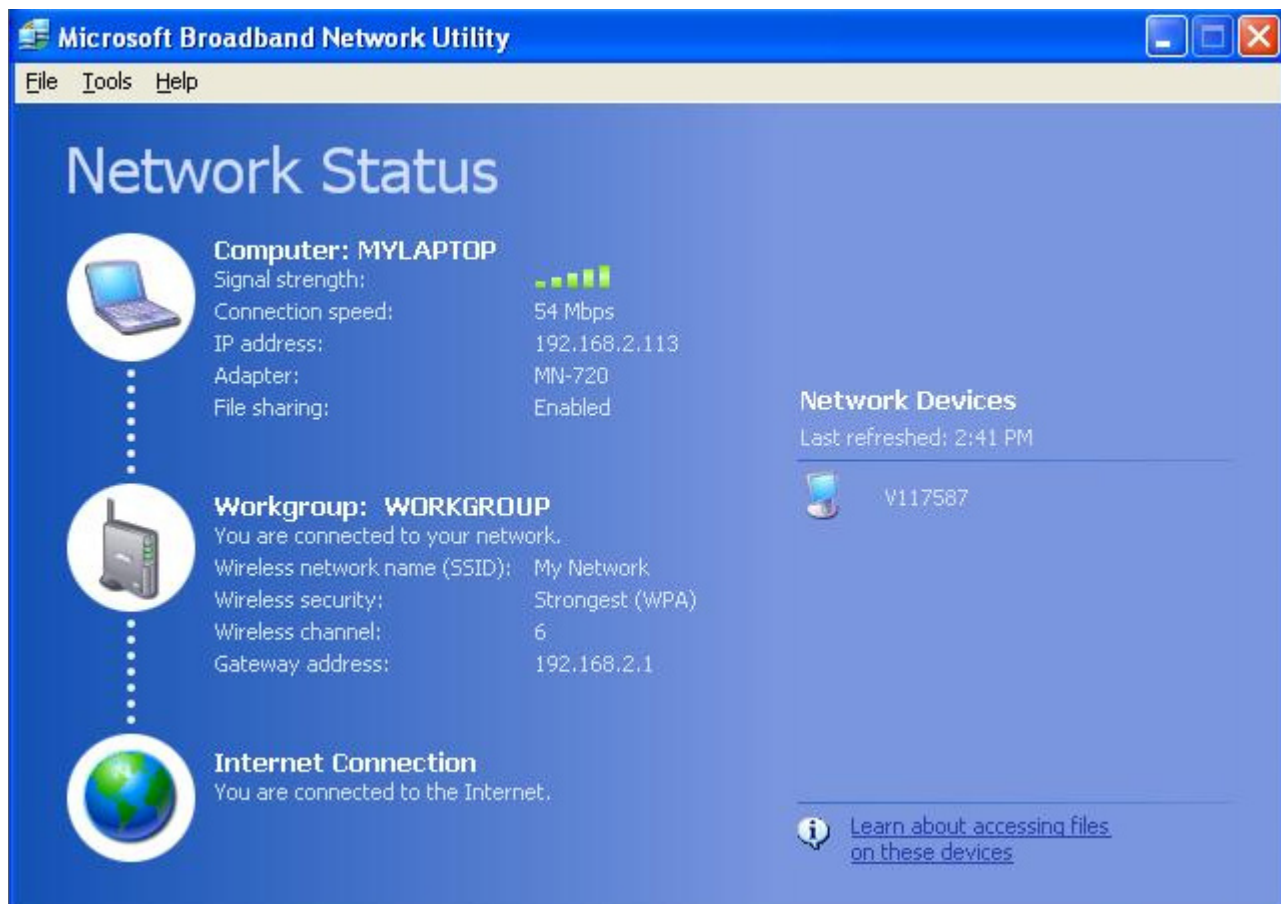


Figure 7: Configuring Wireless Settings

Taking Special Care of Notebook Computers

Notebook computers (or laptops) are a tempting target because they are easy to steal and to sell. Companies reported average losses of \$47,107 due to notebook thefts in 2002, according to the 2003 Computer Security Institute Computer Crime and Security Survey. Besides the hassle and cost of replacement, there is the risk that a stolen notebook computer contains hard-to-replace or confidential information. If thieves have a notebook computer, they will be able to access the data on it.



- *Use a strong password on your notebook computer.* Make sure you lock the workstation or shut down the notebook computer when it is unattended. You might also enable a screensaver and have Windows require a password to get back into the system.
- *Always keep the notebook computer within sight,* particularly in crowded public areas like train stations and airport security checkpoints. Also make sure it stays in your control at meetings and conferences. If you must leave a notebook computer unattended, lock the computer to a piece of furniture or something heavy using a cable lock. Kensington makes cable locks and other security devices for notebook computers. Visit Kensington's site at www.kensington.com.
- *When traveling, keep your notebook computer in your carry-on luggage and don't leave it in hotel baggage-hold rooms.* Don't carry notebook computers in cases stamped with a manufacturer's logo or cases that look too much like a notebook case; it just advertises what you're carrying.
- *Mark your notebook computer for identification purposes.* Keep a record of your notebook computer's serial number and all the software or accessories you use.
- *Be careful when carrying the notebook in your car.* Never leave your notebook computer or computer case in plain sight in your car.
- *Always keep a backup of all the work stored on your notebook computer before a trip and, if possible, continue to make backups of work you do on the road.* Emailing new documents home is one way to do this. Don't take sensitive files with you on a trip unless you actually need them.
- *Use the Windows XP Professional encrypting file system (EFS)* to secure confidential files and make it difficult for unauthorized users to open these files (even if they have physical access to them). Make sure to remove the encryption recovery key from the system. For advice on this process, go to support.microsoft.com/default.aspx?scid=kb;EN-US;223316.

How to Write a Security Plan

You need a plan. Security is not a one-off task but an overlapping mesh of technology, people, policies, and processes. A plan helps you coordinate the whole security effort and make sure there are no gaps. A plan also gives a sense of proportion and priority.



There are four steps to creating a good security plan: audit, plan, execute, and repeat. Before you begin these steps, though, your organization needs to develop a **simple security policy**. First, use the 22 questions and the 10-step plan earlier in this document as a checklist and apply them to all the computers in your business. Second, after you have completed the audit, prioritize action items according to the probability and likely impact of a problem. Third, taking each risk in turn according to its priority, decide how to transfer, mitigate, or avoid it (or, on consideration, live with it). Finally, put together a team, allocate resources and responsibilities, and carry out your plan. Ensure ongoing review and compliance.

A good plan today is better than a perfect plan tomorrow. By its nature, planning for security is a cyclical and repetitive process, never cut and dry, so it makes sense to execute a quick plan now and refine it later.

Audit

- Review your own skills and knowledge. Decide whether outside help or training is required, and find a consultant if necessary.
- Analyze your current state of security using our questionnaire, 10-step plan, and the Microsoft Baseline Security Analyzer. The MBSA is a free program that scans single systems or multiple systems across a network for common system misconfigurations and missing security updates. You can find the MBSA at www.microsoft.com/technet/security/tools.
- Identify assets that need to be protected, including hardware, software, data, documentation, and people. Also identify account information, administrative procedures, and legal compliance.

- Categorize your information according to its sensitivity on the following scale: public (Web site data), internal (marketing data), confidential (payroll), and secret (patents).
- Identify services that are required, such as remote access and email.
- Predict threats such as spoofing, tampering, repudiation, information disclosure, DoS, and elevation of privilege. Consider using trusted third parties to test exposure.
- Calculate exposure for each asset and service against each threat. Use the formula $\text{probability} \times \text{impact} = \text{exposure}$ to generate an ordered list of security priorities.

Plan

- Remember that the objective is not to eliminate all risk regardless of the cost but to minimize the risks as far as possible. There are three main trade-offs:
 - Functionality desired versus security required
 - Ease-of-use versus security
 - Cost of security versus risk of loss
- For each risk, plan how to transfer, avoid, mitigate, or (worst case) live with it.
- Create a plan that
 - includes a policy defining the organization's security requirements and acceptable use
 - has procedures for preventing, detecting, and responding to security incidents
 - gives a framework for enforcing compliance

-
- reflects the culture of the organization and the resources available for implementation
 - Create a plan for dealing with a security breach (e.g., a virus attack):
 - What are the goals and objectives in handling an incident?
 - Whom should be notified in case of an incident?
 - How will you identify an incident and determine how serious it is?
 - What should happen when an incident occurs?
 - Create a project team. Include senior management, legal and HR, training, and users. Give everyone clearly defined roles and responsibilities.
 - Create a project time line.
 - Write it all up and make sure everyone agrees to it.

Execute

- Communicate with staff and provide training where necessary.
- Test measures for technical adequacy and obtain participant feedback.
- Modify the plan, if necessary.
- Carry out the plan.

Monitor and Repeat

- Research new threats and include new risks as you become aware of them:
 - Subscribe to security bulletins.
 - Train administrators and users.
- Modify the plan when changes occur in personnel, the organization, hardware, or software.
- Conduct ongoing maintenance such as virus updates, new user training, and backups.

Creating a Security Policy

A security policy sets guidelines that define an organization's approach to security. A policy differs from a plan in that a plan is a call to action, while a policy defines the goals of a plan.

When we talk about a security policy, it's important to understand that your security policy will actually be a collection of a number of different policies. These policies might include policies on employee Web and email use, policies on administrative access, and policies on remote access. Above all, you must understand the two most important aspects of a good security policy:

- A policy is useful only if it is enforced. You should not create policies that are stricter or more complicated than you are willing to enforce.
- A policy is not set in stone but is a living document. A good policy must be allowed to grow so that it can accommodate new threats, new technology, and new ways of thinking.

Although each organization's security needs are unique, most security policies address a handful of common elements. The SANS Institute defines a number of elements that you should include in a good security policy:

- **Objectives.** This section clearly states the reason the security policy exists.
- **Scope.** This section identifies the people and systems affected by the policy.
- **Protected Assets.** This section identifies the assets that the policy protects. Mail servers, databases, and Web sites are common business assets that need to be protected. Think of this section as an expanded discussion of the objectives.

- **Responsibilities.** This section of the policy identifies the groups or individuals responsible for implementing the conditions of the policy.
- **Enforcement.** This section of the policy discusses the consequences for violating the policy.
- **Definitions.** This section of the policy defines terms and acronyms to ensure that everyone reading the policy will clearly understand what is being discussed.

Examples of policies include (but are not limited to) the following:

- **Acceptable Use Policy.** Defines the appropriate use of computing resources
- **Remote Access Policy.** Outlines acceptable methods for remotely connecting to the internal network
- **Information Protection Policy.** Provides guidelines to users on the processing, storage, and transmission of sensitive information
- **Virus Protection Policy.** Provides baseline requirements for the use of antivirus software as well as guidelines for reporting and containing virus infections
- **Password Policy.** Provides guidelines for how user-level and system-level passwords are managed and changed
- **Perimeter Security Policy.** Describes, in general, how perimeter security is maintained and by whom

For more information on security policies, visit www.sans.org.



Sample Security Plan: Adventure Works



Introduction

This plan was developed by Matthew, Managing Director of Adventure Works, in cooperation with other key members of the Adventure Works staff.

About Adventure Works

We are a 20-person firm specializing in high-adventure travel packages. Our staff includes designers, travel agents, sales and marketing personnel, and the administrative team that supports them. The staff also includes the senior management of the business: the co-founders, Matthew and Tanya, and the financial controller, Steve.

Objectives

This security plan is our first. My intention is to take a broad view of the security risks facing the firm and take prompt action to reduce our exposure. Everyone remembers the virus attack we had earlier this year, and we hope to avoid another disaster like that! However, I hope that by taking a wider view, we may foresee threats that we do not know about yet. So, this plan is also something of an insurance policy.

In writing this plan, I realize that we are limited in time, people, and (of course) cash. Our main priority is to continue to grow a successful business. We cannot hope for CIA-like security, and it wouldn't be good for our culture to turn Adventure Works into Fort Knox. The project team has weighed these constraints carefully in deciding what to do and has tried to strike a balance between practicality, cost, comfort, and security measures. We are all convinced, however, that doing nothing is not an option.

I am taking responsibility for leading this review and ensuring that all the action items are carried out. I am concerned about the risks we face, although having reviewed the plan, I am sure we can address them properly. This project has my full support and is a high priority for the business.

Circulation

Because this document contains important security information, it is confidential. You are requested to keep it under lock and key when not actually using it and, please, don't leave it lying around or make photocopies. We will not be emailing this document or storing it on the server—paper copies only, please. The following people are authorized to view this document:

- Matthew (Managing Director)
- Tanya (Operations Director)
- Steve (Financial Controller)
- Tracy (HR Manager)
- Jarndyce and Jarndyce (our lawyers)
- Jeremy, our outside security consultant

Project Team

The project team includes

- Tanya, project leader
- Steve
- Tracy
- Jeremy, advising our staff and carrying out some of the implementation

In addition, we consulted with members of staff from sales, marketing, and design to get their feedback about what they wanted and how the plan might affect them.

Audit Results

Skills and Knowledge

Our technology consultant, Jeremy, is familiar with the whole situation and will be our expert guide. However, we need to internalize as much of this knowledge as possible by doing as much of the work as we can. Doing so will also help us save money. Luckily, Steve is a bit of an amateur computer enthusiast. He has attended a security training course.

Each member of the project team has read the available security planning guides from Microsoft and the IETF in preparation. The company as a whole is reasonably technically literate, but (with one or two exceptions) they see computers as tools to get the job done and don't know much about how they work.

Our Network and Systems

- Desktops: Twenty-two (one per member of staff plus two old machines acting as print servers)
- Notebook computers: Six (one each for the directors, one for Steve, and three for the sales team)
- Printers: Two (one high-end plotter and one printer-fax combo unit for general use)
- Servers: One (running Microsoft Small Business Server 2003 and looking after files, the Internet connection, and email)
- Internet connection: 1.5Mbps cable modem connection

The server and several of the computers are linked by 100Mbps Cat5 Ethernet cables. The remainder are linked by an 802.11g wireless network with an access point. All computers run Windows XP Professional except for the two print servers and two admin machines, which run Windows 98.

Security Audit

We compared each machine against the checklist in the eSecurity Guide for Small Business. We also ran the MBSA. These actions produced the following results:

- Virus protection: Not present on six machines; not up-to-date on four machines; generally, most users were aware of viruses but were a bit unsure about what they could do to prevent them.
- Spam-filtering software: Many users have begun to complain about spam, but no protection is in place.
- Firewall: We thought the ISP's router included a firewall, but it doesn't; so, we don't have one.
- Updates: All the Windows XP Professional systems are up-to-date because they were automatically checking and downloading updates. However, several installations of Microsoft Office need updating, and the Windows 98 machines are not updated at all.
- Passwords: A random sampling found that most people aren't using passwords at all or had them written on Post-it notes. In particular, none of the notebook computers are password protected.
- Physical security: We had the insurance people in last year, so the window locks, doors, and alarms are pretty good. However, none of the computers has a serial number etched on its cases, and we didn't have a log of the serial numbers. We also noticed that everyone, including Tracy and the two directors, are using the same printer, which means that there is a risk of confidential documents being left there by accident.
- Notebook computers: All the notebook computers had shiny bags with big manufacturer logos. No security locks.
- Wireless networking: We're wide open here. It turns out that we just set the thing up and it worked, so nobody touched any of the settings. The wireless network is open to people who have wireless access capability to snoop on the network or freeload on the Internet connection.
- Web browsing: Everyone thinks that having fast Internet access is a great perk, but they are using it all the time and without much thought to the risks. We don't have a policy on acceptable use, and no one is taking any security measures.
- Backups: We back up data on the server to a DAT drive on a weekly basis, but we haven't tested restoring the data; unless people remember to copy local files to the server, those files aren't backed up, which is unsatisfactory.

Assets

Besides the physical property (e.g., computers), our main assets are

- our product designs and marketing collateral
- records of our contracts with suppliers and the specifications and change orders
- our email database and archive
- sales orders and the customer database
- financial information
- paper HR and legal records stored in various filing cabinets

All these assets are considered secret and should be accessible only on a need-to-know basis. In addition, they need to be protected and backed up as safely as we can manage.

Risks

We believe the risks break down into four main categories:

1. Hackers (viruses, worms, hijacking of our computer resources or Internet connection, and random malicious use). These are the risks that anyone using computers connected to the Internet faces. High risk, high priority.
2. External threats (rivals, disgruntled ex-employees, bad guys after money, and thieves). They are likely to use the same tools as hackers, but in deliberately targeting us they may also try to induce members of staff to supply confidential information or even use stolen material to blackmail or damage us. We need to protect our assets with physical and electronic security. High risk, high priority.
3. Internal threats. Whether accidental or deliberate, a member of staff may misuse his or her privileges to disclose confidential information. Low risk, low priority.
4. Accidents and disasters. Fires, floods, accidental deletions, hardware failures, and computer crashes. Low risk, medium priority.

Priorities

1. Hacker deterrence:
 - Firewall
 - Virus protection
 - Strengthening the wireless network
 - Installing Windows XP Professional on the four Windows 98 machines
 - Ensuring that all machines are regularly updated
 - User education and policies
2. Theft prevention:
 - Notebook computer security
 - Security marking and asset inventory
 - Moving the server into a secure, lockable room
 - Security locks for PCs and notebook computers
3. Disaster prevention:
 - More frequent backups with offsite storage
 - Ensure backup of users' local data
 - Offsite backup of critical paper documents
 - Regularly testing the backups by performing a restore
4. Internal security and confidentiality:
 - Strong password policy and user education
 - Secure printers for accounts, HR, and directors
 - Review security for filing cabinets and confidential documents

Security Plan

Action Items

1. Select, purchase, and install a hardware firewall (or ask our ISP or technology consultant to provide one).
2. Enable Internet Connection Firewall on the server.
3. Make sure that virus software is installed on all computers and that it is set to automatically update virus definitions.
4. Configure computers running Outlook 2003 to use Junk Email filtering. Select, purchase, and install spam-filtering software on the mail server, if necessary.
5. On the wireless network, disable service set identifier (SSID) broadcasting, choose and configure a sensible SSID, enable WPA encryption, enable MAC filtering, and configure the access point to allow traffic only from the PCs and notebook computers in the office.
6. Buy Windows XP Professional upgrades and install them on the four Windows 98 machines.
7. Review all machines to make sure that they are fully updated, and set them to automatically refresh those updates.
8. Buy new, nondescript notebook bags and notebook locks.
9. Security mark all PCs, notebook computers, and their components.
10. Log all serial numbers.
11. Buy and install desk security locks for PCs.
12. Find a suitable, lockable room for the server and move it there.
13. Review backup and restore procedures. Ensure that user data is either stored on the server or copied across regularly prior to backups. Implement daily backups. Ensure that a full backup goes offsite once a week. Ensure that the backup is password protected and encrypted. Review paper documents, and make photocopies for secure offsite storage of critical documents.
14. Configure Small Business Server 2003 and individual machines to enforce reasonably strong passwords. Discuss with users what would be an acceptable balance of convenience and security. (We don't want them writing down their new passwords.)
15. Configure workstations to log users out and require a password to log in again if the workstation is idle for more than five minutes.
16. Buy cheap printers for accounts, HR, and the two directors so that they can have private documents printed securely.

Policy Changes

Tracy will update the staff handbook to include new policies on

- acceptable use of email and the Internet
- use of passwords
- who can take company property away from the office

After she has completed a first draft, it will be reviewed by the directors and the company's attorneys before being rolled out.

User Education

We expect to give up to two hours of user training in small groups as a result of these changes. Training will cover

- the importance of security
- passwords
- notebook computer security
- virus prevention
- safe Internet browsing
- introducing the new staff policies
- assessing employees' understanding of the new policies
- periodically reviewing the practice of the new policies

Project Time Line and Responsibilities

The top three priorities—firewall, virus protection, and strengthening the wireless network—will receive urgent attention from our security consultant, Jeremy. The remaining tasks will be done by our own staff in order of priority.

We expect the top three priorities to be completed within a week and the remaining tasks within 30 days. Steve will be responsible for purchasing and implementing the technical changes. Tracy will be responsible for all the policy and training requirements. Tanya will oversee the project and be responsible for any other tasks that arise.

Response Planning

In the event of a security breach, we will contact Jeremy. His company has a one-hour response policy during office hours and a four-hour response policy at all other times to deal with serious incidents, such as virus infections. In addition, Steve will monitor the server and firewall regularly to make sure that no breaches have occurred.

Ongoing Maintenance and Compliance

Steve will be responsible for security on a day-to-day basis, with Tanya taking overall responsibility. Steve will continue his own self-education on the topic, subscribe to security bulletins from Microsoft and our anti-virus software supplier, and liaise with Jeremy on a regular basis to monitor compliance with the new policies.

On a monthly basis, Steve will make sure that Windows and our antivirus software are updated and that the backup and restore procedure is working properly. He will also be responsible for ensuring that new computer equipment is properly configured and up-to-date.

Tracy will be responsible for ensuring that new staff joining the company are fully trained in the company's security policies and procedures.

There will be a full, formal review of this plan in six months' time.

Resources and Budget

The following expenditure has been approved:

Software and Hardware

- Purchase antivirus software.
- Configure Outlook 2003 to filter junk mail.
- Install a hardware firewall.
- Upgrade the last four PCs to Windows XP Professional.
- Purchase security locks and new nondescript notebook bags.
- Check into additional backup media.

Professional Advice

- Jarndyce and Jarndyce to review our rewritten staff policies
- Jeremy for advice during the creation of this plan
- Jeremy for help with implementation

Internal Resources

Although we are not paying for our own staff directly, to be clear about the allocation of resources and the time that is available for this work, we have authorized the use of internal staff as detailed above.

Information Online

You should consider this guide a starting point for securing your business. The following sites provide additional technical information and security guidance.

For information about technology options and how they affect your business, visit
www.microsoft.com/smallbusiness
www.bcentral.com

For information about starting and running a small business, go to
www.asbdc-us.org
www.uschamber.com
www.sba.gov
www.entrepreneur.com

For business software and productivity solutions, go to
www.microsoft.com/office
www.microsoft.com/windows

For information about software and the law, go to
www.bsa.org

For explanations of technical terms, visit
www.howstuffworks.com
www.webopedia.com

For general information about security, visit
www.microsoft.com/security/protect
www.microsoft.com/security
www.bcentral.com/resources/security.asp
www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/hardsys/TCG/TC-GCH00.asp

For information about computer crime, visit
www.usdoj.gov/criminal/cybercrime
www.gocsi.com
www.kensington.com

For mobile networking and VPNs, go to
www.microsoft.com/technet/security/topics/mobile/default.asp

For information about backups, go to
www.microsoft.com/windowsxp/home/using/howto/maintain/backup.asp

For more detailed advice about writing a security plan, go to
www.microsoft.com/technet/archive/security/best-prac/bpent/bpentsec.asp
www.ietf.org/rfc/rfc2196.txt

For information on Internet filtering software, go to
www.websense.com
www.securecomputing.com

For more technical information, go to
www.microsoft.com/security
www.microsoft.com/technet/security
www.cert.org/tech_tips/home_networks.html
www.ja.net/documents/factsheets.html

For firewalls, go to
www.microsoft.com/technet/security/topics/network/firewall.asp
www.networkassociates.com/us/index.asp
www.symantec.com
www.zonelabs.com

For antivirus software and email security, go to
www.microsoft.com/security/antivirus
www.microsoft.com/security/partners/antivirus.asp
www.mailfrontier.com
www.messagelabs.com
www.symantec.com
us.mcafee.com/default.asp
hoaxbusters.ciac.org

To get the latest software updates for all versions of Windows and Microsoft Office, go to
www.windowsupdate.com
www.officeupdate.com

Windows Server 2003

For the Windows Server 2003 Security Guide, go to go.microsoft.com/fwlink/?LinkId=14845

For Threats and Countermeasures Guide: Chapter 1, Security Settings in Windows Server 2003 and Windows XP, visit go.microsoft.com/fwlink/?LinkId=15159

For the National Security Agency (NSA) Windows Server 2003 Security Guide, go to www.nsa.gov/snac/support/winserver03.htm

Windows 2000 Family:

For the Microsoft Windows 2000 Security Hardening Guide, visit www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/win2khg/06tmplts.asp

For the Microsoft Solution for Securing Windows 2000 Server, go to www.microsoft.com/technet/security/prodtech/windows/secwin2k/default.asp

For Overview: Windows 2000 Common Criteria Certification, visit www.microsoft.com/technet/security/issues/w2kccwp.asp

For the Microsoft Windows 2000 Security Configuration Guide, go to www.microsoft.com/technet/security/issues/W2kCCSCG/default.asp

Windows XP

For the Microsoft Windows XP Security Guide Overview, visit go.microsoft.com/fwlink/?LinkId=14839

Glossary

802.11 (a.) A standard for wireless networks that ensures interoperability between different manufacturers. 802.11 networks come in three variants: a, b, and g. 802.11b is the most common, while a and g are much faster. Usually cards capable of faster speeds are backwardly-compatible to the b standard.

access (n.) In respect to privacy, an individual's ability to view, modify, and contest the accuracy and completeness of PII collected about him or her. Access is an element of the Fair Information Practices.

Access point (n.) A wireless hub that links together different 802.11 network cards to form an "infrastructure" wireless network (as opposed to an ad hoc network).

access token (n.) A data structure that contains authorization information for a user or group. A system uses an access token to control access to securable objects and to control the ability of a user to perform various system-related operations on a local computer.

Ad hoc network (n.) A wireless network that links computers on a peer-to-peer basis rather than by routing traffic through a central access point.

Administrator (n.) A user who has sufficient access rights to allow him or her to manage the access rights of other users and carry out other high-level computer management tasks.

administrative vulnerability (n.) Failure to observe administrative best practices, such as using a weak password or logging on to an account that has more user rights than the user requires to perform a specific task.

anonymity (n.) A condition in which an individual's true identity is unknown.

antivirus software (n.) Software specifically designed for the detection and prevention of known viruses.

authentication (n.) The process for verifying that someone or something is who or what it claims to be.

In private and public computer networks (including the Internet), authentication is commonly performed through the use of logon passwords.

authorization (n.) In reference to computing, especially remote computers on a network, the right granted an individual or process to use a system and the data stored on it. Authorization is typically set up by a system administrator and verified by the computer based on some form of user identification, such as a code number or password.

Blaster Worm (n.) A family of worms that makes use of an exploit in DCOM RPC in Microsoft Windows 2000 and XP and does not require users to trigger it, (e.g., by running an executable file). It is not distributed by email and can easily be prevented through installation of the correct patches and/or a properly configured firewall

Broadband connection (n.) Broadband connections to the Internet differ from dial-up connections in two ways. First, they are much faster, typically 10 times faster than a modem. Second, they are usually always connected to the Internet, not just when they are in use. Examples of broadband connections include ADSL, cable modem, and fiber-optic leased lines.

BBBOnLine (n.) A privacy seal program established by the Better Business Bureau which certifies that certain Web sites conform to baseline privacy standards. Microsoft is a sponsor of BBBOnLine.

Bugbear Worm (n.) A mass-mailing worm that also spreads through network shares, the Bugbear worm and its variants attempt a variety of activities, including shutting down common firewall software programs.

buffer (n.) A region of memory reserved for use as an intermediate repository in which data is temporarily held before it is transferred between two locations or devices.

buffer overrun (n.) A condition that results from adding more information to a buffer than it was designed

to hold. An attacker may exploit this vulnerability to take over a system.

certificate (n.) An encrypted file containing user or server identification information, which is used to verify identity and to establish a secure link.

change management (n.) The practice of administering changes with the help of tested methods and techniques in order to avoid new errors and minimize the impact of changes.

choice (n.) An individual's ability to determine whether and how PII collected from him or her may be used, especially for purposes beyond those for which the information was originally provided. Choice is an element of the Fair Information Practices.

cipher (n.) An encryption method, typically using a predefined key and an algorithm to transform plaintext into ciphertext.

ciphertext (n.) Text that has been encrypted with an encryption algorithm and key.

clickstream data (n.) Information that users generate as they move from page to page and click on items within a Web site, usually stored in log files. Web site designers can use clickstream data to improve users' experiences with a site.

computer security (n.) The discipline, techniques, and tools designed to protect the confidentiality, integrity, and availability of data and systems.

Content Advisor (n.) A tool in Microsoft Internet Explorer that lets you control which sites users on your computer can visit. This is particularly helpful for parents who want to control the content their children view on the Web.

cookie (n.) A small data file that is stored on a user's local computer for record-keeping purposes and which contains information about the user that is pertinent to a Web site, such as user preferences.

COPPA (n.) The Children's Online Privacy Protection Act. A U.S. law that took effect on April 21, 2000, and requires parental consent for certain Web sites to knowingly collect personally identifiable information on children under the age of 13. Other countries may enact similar privacy laws in the future.

Cracking (v.) Finding a password by trying many combinations and words.

credentials (n.) Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names and passwords, smart cards, and certificates.

critical update (n.) A broadly released fix for a specific problem addressing a critical, non-security related bug.

cryptology(n.) The use of codes to convert data by using a key so that only a specific recipient will be able to read it. Cryptology is used to enable and ensure confidentiality, data integrity, authentication, and nonrepudiation.

DAT (n.) See digital audio tape

data transfer (n.) As a key principle of privacy, the movement of PII between entities, such as a customer list being shared between two different companies.

deceptive trade practices (n.) Misleading or misrepresenting products or services to consumers and customers. In the U.S., these practices are regulated by the Federal Trade Commission at the federal level and typically by the Attorney General's Office of Consumer Protection at the state level.

decryption (n.) The process of converting encrypted content back into its original form

denial of service (DoS) attack (n.) A computerized assault launched by an attacker to overload or halt a network service, such as a Web server or a file server. For example, an attack may cause the server to become so busy attempting to respond that it ignores legitimate requests for connections.

Dial-up connection (n.) A dial-up connection uses a modem (or sometimes an ISDN terminal adaptor) to connect to an ISP. Usually, these connections are quite slow and open only while the user is actually online.

Digital audio tape (DAT) (n.) Used to store data, a DAT can store up to 24GB of data (assuming optimal compression).

digital certificate (n.) See certificate.

digital rights management (DRM) (n.) A technology that provides persistent protection to digital data using encryption, certificates, and authentication. Authorized recipients or users must acquire a license in order to consume the protected material—files, music, movies—according to the rights, or business rules, set by the content owner.

digital signature (n.) Data that is bundled with a message or transmitted separately and is used to identify and authenticate the sender and message data. A valid digital signature also confirms that the message has not been tampered with.

disclosure (n.) A component of the notice principle, wherein a company should make available its data handling practices, including notices on how it collects, uses, and shares PII.

download (v.) To transfer a copy of a file from a remote computer to a requesting computer by means of a modem or network.

elevation of privileges (n.) The process by which a user misleads a system to grant unauthorized rights, usually for the purpose of compromising or destroying the system.

encrypted data (n.) Data that has been converted from plaintext into ciphertext.

Encrypting File System (EFS) (n.) A file-based encryption technology that enables users to encrypt files and folders on an NTFS volume disk to keep them confidential.

encryption (n.) The process of converting data into ciphertext to prevent it from being understood by an unauthorized party.

enforcement (n.) A privacy principle which provides mechanisms for assuring compliance with the Fair Information Practices, recourse for individuals affected by non-compliance, and consequences for non-compliant organizations. Methods for enforcement include a review by independent third parties, such as BBBOOnline.

EU Data Protection Directive (n.) A European Union (EU) law stating that personal data from EU countries can only be transferred to non-EU countries that pro-

vide an acceptable level of privacy protection. An organization must inform individuals why information about them is collected, how to contact the organization with inquiries and complaints, the types of third parties to which the organization will disclose, and the options an organization provides to limit the disclosure of certain information. Proper notice and choice must be offered to allow an individual to opt in or opt out of providing specific information the organization plans on tracking. See also Safe Harbour Agreement.

Fair Information Practices (n.) The basis for privacy best practices, both online and offline. The Practices originated in the Privacy Act of 1974, the legislation that protects personal information collected and maintained by the U.S. government. In 1980, these principles were adopted by the Organization for Economic Cooperation and Development and incorporated in its Guidelines for the Protection of Personal Data and Transborder Data Flows. They were adopted later in the EU Data Protection Directive of 1995, with modifications. The Fair Information Practices include notice, choice, access, onward transfer, security, data integrity, and remedy.

filter (n.) A pattern or mask through which data is passed to separate specified items. For instance, a filter used in e-mail or in retrieving newsgroup messages can allow users to automatically discard messages from specific users.

firewall (n.) A combination of hardware and software that provides a security system, usually to prevent unauthorized access from outside to an internal network or intranet.

full file replacement (n.) A technology used in hotfixes that replaces the currently installed files with new files. Compare patching.

GLB (Graham/Leach/Bliley) Act (n.) A U.S. law containing financial provisions that require all financial institutions to disclose to consumer customers their policies and practices for protecting the privacy of non-public personal information. Non-public personal information includes any PII provided by a customer, resulting from transactions with the financial institution or obtained by a financial institution through providing products or services. Also known as the Financial Modernization Act of 1999.

globally-unique identifier (GUID) (n.) A 16-byte value generated from the unique identifier on a device, the current date and time, and a sequence number. A GUID is used to identify a particular device, component, user, or session.

HFNETCHK (n.) A command-line tool that enables an administrator to check the update status of all Windows NT 4.0, Windows 2000, and Windows XP computers on a network from a central location.

HIPAA (Health Insurance Portability and Accountability Act) (n.) A U.S. regulation that gives patients greater access to their own medical records and more control over how their personally identifiable health information is used. The regulation also addresses the obligations of health care providers and health plans to protect health information. In general, covered entities such as health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically have until April 14, 2003, to comply.

Honey pot (n.) A system designed to look like a regular network but that, in fact, monitors and traces unauthorized access.

hotfix (n.) A single cumulative package composed of one or more files used to address a problem in software. Hotfixes address a specific customer situation and may not be distributed outside that customer organization.

impersonation (n.) The ability of a process to run in a specified security context. For example, impersonation is used in Web applications to provide a secure user context for anonymous requests.

implicit profiling (n.) An information collection process in which the actions and behaviors of a user visiting a Web site are recorded as the user moves around in and interacts with the Web site.

implicit targeting (n.) An information delivery process in which existing user data is used to deliver tailored content to users who browse a Web site.

information disclosure (n.) The exposure of information to individuals who normally would not have access to it.

interactive logon (n.) The process of logging on to a local computer using a keyboard. Compare network logon.

Internet Service Provider (ISP) (n.) A company that provides access to the Internet.

Internet Content Rating Association (ICRA) (n.) An international nonprofit group that has developed a content advisory service for the Internet. ICRA's aim is to protect children from potentially harmful material on the Internet.

IPSec (Internet Protocol Security) (n.) IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices.

KB article (n.) A technical document in the Microsoft KnowledgeBase accessible through microsoft.com.

Kids Passport (n.) A .NET Passport service that helps Kids Passport-participating sites and services obtain parental consent to collect, use, and disclose a child's personal information. This service is used to support legal requirements such as COPPA or Korean Kids. See also COPPA, Microsoft Passport.

Klez (n.) A particularly destructive species of virus.
least privilege administration (n.) A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform.

Local area network (LAN) (n.) A local computer network for communication between computers.

local attack (n.) An attack that targets the computer to which the attacker is interactively logged on.

LoveBug Worm (n.) A mass-mailing worm that originated in Manila, Philippines on May 4, 2000. The worm sends itself to email addresses in the Outlook address book and also spreads to Internet chat rooms using mIRC. The worm is designed to overwrite common files on local and remote drives.

MAC (Message Authentication Code) (n.) An algorithm that allows a receiver to ensure that a block of data has retained its integrity from the time it was sent until the time it was received.

MAC filtering (n.) Each network card has a unique ID called a MAC. A wireless network access point can be configured to give access to specific network cards (and the computers in which they are installed) and exclude others on the basis of these MAC addresses.

mail bomb (n.) An excessively large amount of e-mail data sent to a user's e-mail address in an attempt to make the user's e-mail program crash or to prevent the user from receiving further legitimate messages.

mail relaying (n.) A practice in which an attacker sends e-mail messages from another system's e-mail server in order to use its resources and/or make it appear that the messages originated from the other system.

malicious user (n.) A person who has access to a system and poses a security threat to it, for example, someone who tries to elevate their privileges to gain access to unauthorized data.

Microsoft Baseline Security Analyzer (n.) A free tool from Microsoft that searches computers for known security vulnerabilities and suggests remedies. To download the Microsoft Baseline Security Analyzer, visit <http://www.microsoft.com/technet/security/tools>.

Microsoft Download Center (n.) A Microsoft Web site that provides product updates and security updates for Microsoft products.

Microsoft Passport (n.) A Web-based service that is designed to make signing in to Web sites fast and easy. .NET Passport enables participating sites to authenticate a user with a single set of sign-in credentials, alleviating the need to remember numerous passwords and user names.

Microsoft Security Bulletin (n.) A document that describes a specific security issue in a Microsoft product and directs the reader to a downloadable file that resolves the issue.

Microsoft Virus Alert (n.) An announcement that describes a specific virus, the impact of potential attacks on Microsoft software, and suggestions for preventing or recovering from such attacks.

network logon (n.) The process of logging on to a computer by means of a network. Typically, a user

first interactively logs on to a local computer, then provides logon credentials to another computer on the network, such as a server, that he or she is authorized to use. Compare interactive logon.

nonrepudiation (n.) The ability to identify who has performed various actions on a computer, so that users cannot deny responsibility for the actions they perform. Generally used in the sense of creating unimpeachable audit trails to identify the source of commercial transactions or malicious actions.

notice (n.) A privacy principle that requires reasonable disclosure to a consumer of an entity's PII collection and use practices. This disclosure information is typically conveyed in a privacy notice or privacy policy. Notice is addressed in Fair Information Practices.

onward transfer (n.) The transfer of PII by the recipient of the original data to a second recipient. For example, the transfer of PII from an entity in Germany to an entity in the United States constitutes onward transfer of that data. Onward transfer is addressed in Fair Information Practices.

opt in (v.) To explicitly consent to participate. Typically used in marketing programs and offerings, whereby an action (such as the use of personal information beyond the original, primary purpose for which it was collected) is not undertaken unless an individual explicitly consents. An element of choice (See Fair Information Practices).

opt out (v.) To explicitly decline to participate. Typically used in marketing programs and offerings, whereby an action (such as the use of personal information beyond the original, primary purpose for which it was collected) is undertaken unless an individual explicitly declines. An element of choice (see Fair Information Practices)

P3P (Platform for Privacy Preferences Project) (n.) An open privacy specification developed and administered by the W3C (World Wide Web Consortium) that, when implemented, enables people to make informed decisions about how they want to share personal information with Web sites.

password (n.) A string of characters entered by a user to verify his or her identity to a network or to a local computer.

patch (n.) See security update.

patching (n.) A method of updating a file that replaces only the parts being changed, rather than the entire file. Compare full file replacement.

permissions (n.) Authorization to perform operations associated with a shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

physical vulnerability (n.) Failure to provide physical security for a computer, such as leaving an unlocked workstation running in a workspace that is accessible to unauthorized users.

PII (personally identifiable information) (n.) Any information relating to an identified or identifiable individual. Such information may include name, country, street address, e-mail address, credit card number, social security number, government ID number, IP address, or any unique identifier that is associated with PII in another system. Also known as personal information or personal data.

PIN (n.) Acronym for Personal Identification Number. A unique access code number assigned, as with automatic teller machine cards, to the authorized user.

plaintext (n.) A message that is not encrypted. Plaintext messages are also referred to as cleartext messages.

Port (n.) an assigned number that indicates to which application at a given IP address a data packet should be delivered. Each network service on a given computer has its own port, something like a telephone extension.

Port sniffer (n.) A hacker program designed to find open or unguarded ports.

PPTP (Point-to-Point Tunneling Protocol) (n.) PPTP provides security for transmission of sensitive information over unprotected networks such as the Internet.

principal (n.) See security principal.

privacy (n.) The control customers have over the col-

lection, use, and distribution of their personal information.

privacy compromise (n.) A scenario in which an unauthorized individual is able to gain access to personal or confidential information about another user.

privacy policy (n.) An organization's requirements for complying with privacy regulations and directives. The policy is expressed in a privacy statement.

privacy statement (n.) A document describing a company's position on privacy, detailing what information their Web site collects, with whom the data is shared, and how users can control the use of their personal data.

Privacy Wizard (n.) A software tool developed by Microsoft that helps businesses craft privacy policies (statements) based on widely accepted privacy principles. Currently, the Privacy Wizard is being updated to include support for P3P.

private fix (n.) An unofficial hotfix which may not be fully tested or packaged. It is released to the customer to verify that it solves the problem before final testing & packaging.

private key (n.) One of two keys in public key encryption. The user keeps the private key secret and uses it to encrypt digital signatures and to decrypt received messages.

privilege (n.) See user rights.

product vulnerability (n.) A security-related bug in a product that is addressed by a Microsoft security bulletin or a service pack.

proxy server (n.) A firewall component that manages Internet traffic to and from a local area network (LAN) and can provide other functions, such as document caching and access control.

public key (n.) One of two keys in public key encryption. The user releases this key to the public, who can use it to encrypt messages to be sent to the user and decrypt the user's digital signature. See also public key encryption. Compare private key.

public key encryption (n.) An asymmetric encryption scheme that uses a pair of keys for encryption:

the public key encrypts data, and a corresponding secret key decrypts it. For digital signatures, the process is reversed: the sender uses the secret key to create a unique electronic number that can be read by anyone possessing the corresponding public key, which verifies that the message is truly from the sender. See also private key, public key.

Public-key infrastructure (PKI) (n.) Generally, the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys.

QFE (quick fix engineering) (n.) A team within Microsoft that produces hotfixes. Most of these teams now refer to themselves as Sustained Engineering teams.

Quality of Service (QoS) (n.) A set of quality assurance standards and mechanisms for data transmission.

race condition (n.) A condition caused by the timing of events within a piece of software. Race conditions typically are associated with synchronization errors that provide a window of opportunity during which one process can interfere with another, possibly introducing a vulnerability.

remote attack (n.) An attack that targets a computer other than the one that the attacker is interactively logged on to. For example, an attacker can log on to a workstation and attack a server on the same network or on an entirely different one.

remote procedure call (RPC) (n.) A communication mechanism that allows a client and a server application to communicate with each other through function calls sent from the client to the server.

repudiation (n.) The ability of a user to falsely deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can prove otherwise.

role-based authorization (n.) A type of authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

rollup (n.) See update rollup.

Router (n.) A device that determines the next network point to which a data packet should be forwarded on its way to its destination. Routers are used to move packets around the Internet, and most broadband connections end with a router in your building that connects your LAN to the rest of the Internet.

sandbox (n.) A protective mechanism used in some programming environments that limits a program's access to system resources. A sandbox restricts a program to a set of privileges and commands that make it difficult or impossible for the program to cause any damage to the user's data.

safeguard (n.) A technology, policy or procedure that counters a threat or protects assets.

Safe Harbour Agreement (n.) An agreement between the U.S. and the European Union regarding the transfer of PII from the European Union to the United States, which is consistent with Fair Information Practices. Companies that register for Safe Harbour with the United States Department of Commerce, and abide by the agreement, are deemed by the European Union to provide adequate data protection for PII transferred from the European Union to the United States.

Safe Harbour Principles (n.) Seven principles agreed to by the United States and the European Union for the transfer of PII from the European Union to the United States, which a company must adhere to if it registers for Safe Harbour. The seven principles are categorized into the following subjects: (1) Notice; (2) Choice; (3) Access; (4) Onward Transfer; (5) Security; (6) Data Integrity; and (7) Enforcement. See also "Safe Harbour Agreement".

Script kiddies (n.) Inexperienced hackers who use publicly available tools.

secondary data uses (n.) Uses of personal information for purposes other than those for which the information was collected. The Fair Information Practices state that a person can provide personal information for a specific purpose without the fear that it may later be used for an unrelated purpose without that person's knowledge or consent.

Secure Sockets Layer (SSL) (n.) A protocol for establishing a secure communications channel to prevent the interception of critical information, such as credit card numbers on the World Wide Web.

security identifier (SID) (n.) A value that uniquely identifies each user, group, computer account, and logon session on a network.

Security plan (n.) A written plan that examines your company's current security practices, analyzes the company's weaknesses, and suggests a systematic approach to increasing the security of the company.

security principal (n.) An account holder that is automatically assigned a security identifier (SID) to control access to resources.

security push (n.) A sustained effort by an entire product team over a period of weeks or months to examine a product for security flaws. During a typical security push, team members are required to spend all their time looking for security flaws or fixing them.

security update (n.) A broadly released fix for a product-specific security-related vulnerability. Security vulnerabilities are rated based on their severity, which is indicated in the security bulletin as critical, important, moderate, or low.

sensitive data (n.) From the European Union perspective, PII regarding race or ethnic origin, political opinions, religious or philosophical beliefs, sex life or trade union membership. Within the U.S., sensitive information also includes information about health, finances, and children.

Server (n.) A computer that provides a service to other computers in a network.

service pack (n.) A cumulative set of all hotfixes, security updates, critical updates, and updates created and fixes for defects found internally since the release of the product. Service packs may also contain a limited number of customer requested design changes or features.

SID (n.) See security identifier.

smart card (n.) A credit card-sized device with an embedded microprocessor that is used with an access code to enable certificate-based authentication.

Sobig Worm (n.) Sobig.A and its variants spread through e-mail and network shares. This worm typically disguises e-mail messages with an @microsoft.

com address so that it appears they are coming from Microsoft, a tactic known as spoofing. Many of the addresses are valid addresses that are being spoofed for malicious purposes.

software update (n.) Any update, update rollup, service pack, feature pack, critical update, security update, or hotfix used to improve or fix a software product released by Microsoft Corporation.

software upgrade (n.) See upgrade.

spam (n.) Unsolicited commercial e-mail (UCE). Also known as junk e-mail.

spoof (v.) To make a transmission appear to come from a user other than the user who performed the action.

SSID (service set identifier) (n.) The name given to a wireless network that enables users to find the network.

STRIDE threat model (n.) A method of categorizing threat types. These threat types include: spoofing identity, tampering with data, repudiation, information disclosure, denial of service, and elevation of privilege.

strong password (n.) A password that provides an effective defense against unauthorized access to a resource. A strong password is at least six characters long, does not contain all or part of the users' account name, and contains at least three of the four following categories of characters: uppercase letters, lowercase letters, base 10 digits, and symbols found on the keyboard, such as !, @, and #.

tamper (v.) To maliciously modify data.

TCP/IP (n.) Transmission Control Protocol/Internet Protocol. The protocols, or conventions, that computers use to communicate over the Internet.

Third-Party Seal (n.) An online seal of approval, certifying that a Web site's privacy statement has been examined and tested (by organizations including BBBOnLine and TRUSTe) according to the Fair Information Practices.

throttling (n.) A method of preventing a denial of ser-

vice attack by limiting the number of requests that can be made to a system. Also called pooling.

token (n.) See access token.

transparency (n.) A standard that requires that the structure for processing personal information be in a fashion that is open and understandable to the individual whose data is being processed. It is a goal of the Fair Information Practices, which requires a company to inform users what personal information the company collects and how the data is used.

Transport Layer Security (TLS) (n.) A protocol that provides communications privacy and security between two applications communicating over a network. It also enables clients to authenticate servers or, optionally, servers to authenticate clients.

Trojan horse (n.) A computer program that appears to be useful but that actually does damage.

TRUSTe (n.) An online privacy seal program that certifies eligible Web sites and holds Web sites to a baseline privacy standard. It serves as a key privacy watchdog organization that is the mediator for MSN privacy disputes. TRUSTe plays an important enforcement role in the dispute and resolution of privacy issues.

update (n.) A broadly released fix for a specific problem addressing a non-critical, non-security related bug.

update (v.) To make a system or data file more current.

update rollup (n.) A cumulative set of hotfixes, security updates, critical updates and updates packaged together for easy deployment. A rollup targets a specific area such as security or component of the product such as Internet Information Services (IIS).

upgrade (n.) A software package that replaces an installed version of a product with a newer version of the same product. The upgrade process typically leaves existing customer data and preferences intact while replacing the existing software with the newer version.

upgrade (v.) To change to a newer, usually more powerful or sophisticated version of a product.

user profile (n.) Information about an individual that contains any of a variety of business-specific data elements, including configuration information for a specific user, such as desktop settings, persistent network connections, and application settings, or personally-identifiable information, Web site use, or other behaviors and demographics.

user rights (n.) Policies governing specified system tasks that a system administrator assigns to individual user accounts or administrative groups. For example, you must have been assigned the Shut down the system user right in order to shut down your computer.

virtual private network (VPN) (n.) A set of nodes on a public network such as the Internet that communicate among themselves using encryption technology so that their messages are as safe from being intercepted and understood by unauthorized users as if the nodes were connected by private lines.

virus (n.) Code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or data. Compare worm.

vulnerability (n.) Any product flaw, administrative process or act, or physical exposure that makes a computer susceptible to attack by a hostile user.

War chalking (v.) Using chalk symbols on walls to indicate the presence and configuration of an insecure wireless network.

War driving (v.) Locating insecure wireless networks by scanning for them with a portable computer and special software.

WEP (wired equivalent privacy) (n.) WEP data encryption is defined by the 802.11 standard to prevent eavesdropping and access to the network by malicious users.

Wi-Fi (a.) See 802.11.

Windows Update (n.) 1. An online extension of Microsoft Windows that enables a user to download files that are necessary to keep a computer up-to-date. 2. A Microsoft Web site maintained by the Windows product group for the purpose of providing updates.

WPA (Wi-Fi protection algorithm) (n.) A wireless encryption standard that was designed to improve on the features of WEP. WPA provides improved data encryption and user authentication.

worm (n.) A subclass of virus. A worm generally spreads without user action and distributes complete copies (possibly modified) of itself across networks. A worm can consume memory or network bandwidth, thus causing a computer to stop responding. Compare virus.