



**National Institute of  
Standards and Technology**

Technology Administration  
U.S. Department of Commerce

Special Publication 800-69  
**Sponsored by the  
Department of Homeland Security**

---

# Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist

---

## **Recommendations of the National Institute of Standards and Technology**

---

Karen Kent  
Murugiah Souppaya  
John Connor



**NIST Special Publication 800-69**

**Guidance for Securing Microsoft Windows  
XP Home Edition: A NIST Security  
Configuration Checklist**

*Recommendations of the National  
Institute of Standards and Technology*

**Karen Kent  
Murugiah Souppaya  
John Connor**

---

**C O M P U T E R   S E C U R I T Y**

---

Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930

September 2006



**U.S. Department of Commerce**

Carlos M. Gutierrez, Secretary

**Technology Administration**

Robert C. Cresanti, Under Secretary of  
Commerce for Technology

**National Institute of Standards and Technology**

William Jeffrey, Director

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

**National Institute of Standards and Technology Special Publication 800-69  
Natl. Inst. Stand. Technol. Spec. Publ. 800-69, 175 pages (September 2006)**

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

## Acknowledgements

The authors, Karen Kent and Murugiah Souppaya of the National Institute of Standards and Technology (NIST) and John Connor of Booz Allen Hamilton, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge Elaine Barker, Tim Grance, and Larry Keys of NIST; Chan Lee, Steven Sharma, and Victoria Thompson of Booz Allen Hamilton; and Rob Campbell of Microsoft Corporation for their keen and insightful assistance throughout the development of the document.

The National Institute of Standards and Technology would also like to express its appreciation and thanks to the Department of Homeland Security for its sponsorship and support of NIST SP 800-69.

## Trademark Information

Microsoft, Windows, Windows XP, Windows 2000, Windows NT, Internet Explorer, Microsoft Office, Outlook, Outlook Express, and Microsoft Word are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

All other names are registered trademarks or trademarks of their respective companies.

## Table of Contents

<b>Executive Summary</b> .....	<b>1</b>
<b>1. Introduction</b> .....	<b>1-1</b>
1.1 Authority.....	1-1
1.2 Purpose and Scope.....	1-1
1.3 Audience.....	1-2
1.4 Document Structure.....	1-2
1.5 Quick Start.....	1-3
<b>2. The Need to Secure Windows XP Home Edition Computers</b> .....	<b>2-1</b>
2.1 The Roles of Computers.....	2-1
2.2 Common Threats.....	2-2
2.3 Security Protections.....	2-4
2.4 Threat Environments.....	2-5
2.5 Summary.....	2-6
<b>3. Overview of Security Protections</b> .....	<b>3-1</b>
3.1 Reducing Weaknesses.....	3-1
3.1.1 Software Updates.....	3-1
3.1.2 User Accounts and Sessions.....	3-5
3.1.3 Networking.....	3-9
3.1.4 File Extensions and Associations.....	3-12
3.1.5 Services.....	3-13
3.2 Protecting Privacy.....	3-14
3.2.1 Web Browsers.....	3-15
3.2.2 Files.....	3-17
3.3 Stopping Attacks.....	3-19
3.3.1 Malware Protection.....	3-20
3.3.2 Personal Firewalls.....	3-22
3.3.3 Content Filtering.....	3-24
3.3.4 Popup Blocking.....	3-25
3.3.5 Security Software Suites.....	3-25
3.3.6 Application Configuration.....	3-26
3.3.7 Data Execution Prevention.....	3-28
3.4 Preserving Data.....	3-28
3.4.1 Backup or Restore Wizard.....	3-29
3.4.2 Files and Settings Transfer Wizard.....	3-29
3.4.3 Third-Party Backup and Restore Utility.....	3-30
3.4.4 Third-Party Remote Backup Service.....	3-30
3.4.5 File Copy to Media.....	3-30
3.5 Summary.....	3-30
<b>4. Installing Windows XP Home Edition</b> .....	<b>4-1</b>
4.1 Prepare for the Installation.....	4-2
4.2 Back Up Data Files and Configuration Settings.....	4-3
4.3 Install Windows XP Home Edition.....	4-6
4.4 Secure the Computer.....	4-9
4.5 Restore the Data Files and Configuration Settings.....	4-10

4.6	Summary.....	4-11
<b>5.</b>	<b>Securing a New Windows XP Home Edition Installation.....</b>	<b>5-1</b>
5.1	Prepare to Secure the Computer .....	5-1
5.1.1	Gather Needed Materials .....	5-1
5.1.2	Set the Default View for Control Panel .....	5-2
5.1.3	Identify Service Pack Currently in Use .....	5-2
5.2	Update Windows XP Home Edition .....	5-4
5.2.1	Configure a Personal Firewall .....	5-4
5.2.2	Connect the Computer to the Network .....	5-5
5.2.3	Activate Windows .....	5-7
5.2.4	Apply Updates .....	5-7
5.2.5	Configure the Computer for Automatic Updates.....	5-11
5.3	Install and Configure Additional Security Software .....	5-12
5.3.1	Malware Protection.....	5-12
5.3.2	Content Filtering .....	5-12
5.3.3	Personal Firewall.....	5-13
5.4	Alter the Windows XP Home Edition Configuration .....	5-14
5.4.1	User Accounts and Sessions.....	5-14
5.4.2	Networking.....	5-16
5.4.3	Files and Folders .....	5-20
5.5	Document the Installed Software Applications.....	5-21
5.6	Summary.....	5-25
<b>6.</b>	<b>Securing an Existing Windows XP Home Edition Installation.....</b>	<b>6-1</b>
6.1	Prepare to Secure the System .....	6-1
6.2	Assess the Computer's Security .....	6-1
6.2.1	Identify Installed Programs .....	6-1
6.2.2	Identify Running Applications and Startup Programs .....	6-3
6.2.3	Check Security Software Configuration.....	6-3
6.3	Identify and Remove Malware .....	6-4
6.3.1	Malware Scanning Options.....	6-4
6.3.2	Removing Malware.....	6-5
6.4	Secure the Computer.....	6-8
6.5	Summary.....	6-8
<b>7.</b>	<b>Securing User Accounts and Settings.....</b>	<b>7-1</b>
7.1	Secure User Accounts and Files.....	7-1
7.1.1	Set a strong password for each account .....	7-1
7.1.2	Make the user's folder private .....	7-1
7.1.3	Modify settings for file associations and extensions.....	7-2
7.2	Configure E-mail Clients .....	7-2
7.3	Configure Web Browsers .....	7-3
7.4	Configure Instant Messaging Clients .....	7-3
7.5	Configure Office Productivity Suites .....	7-3
7.6	Summary.....	7-4
<b>8.</b>	<b>Maintaining and Monitoring a Computer's Security .....</b>	<b>8-1</b>
8.1	Perform Backups and Restore Data As Needed .....	8-1
8.2	Perform Administrative Maintenance .....	8-1
8.2.1	Apply Updates .....	8-1

8.2.2	Check the Status of Security Software .....	8-2
8.2.3	Create New User Accounts .....	8-3
8.2.4	Delete Old System Restore Points .....	8-3
8.2.5	Create New System Restore Points .....	8-4
8.2.6	Review Shared Folders .....	8-4
8.2.7	Synchronize the Computer's Clock .....	8-5
8.2.8	Retire Unneeded User Accounts .....	8-6
8.3	Perform User Maintenance .....	8-6
8.3.1	Change Windows XP Home Edition Password Regularly .....	8-7
8.3.2	Delete Unneeded Files .....	8-7
8.3.3	Clear Web Browser Information .....	8-7
8.4	Identify Security Issues .....	8-8
8.5	Investigate Unusual Behavior .....	8-10
8.5.1	Seek Expert Assistance.....	8-11
8.5.2	Recover from a Failure or Compromise .....	8-17
8.6	Prepare a Computer for Retirement.....	8-19
8.7	Summary.....	8-20

## List of Appendices

<b>Appendix A— Essential Security Settings .....</b>	<b>A-1</b>
Step 1: Set the Default View for Control Panel .....	A-3
Step 2: Ensure a Personal Firewall Is Enabled.....	A-3
Step 3: Apply Updates .....	A-5
Step 4: Configure the Computer for Automatic Updates.....	A-8
Step 5: Install and Configure Antivirus/Antispyware Software .....	A-9
Step 6: Set Up Limited User Accounts.....	A-9
<b>Appendix B— Advanced Security Settings .....</b>	<b>B-1</b>
B.1 Configure Data Execution Prevention .....	B-1
B.2 Disable Default User Accounts .....	B-1
B.3 Disable Unneeded Networking Features .....	B-3
B.4 Protect Temporary Files.....	B-4
B.5 Disable Unneeded Services.....	B-4
B.6 Modify File Associations .....	B-6
<b>Appendix C— Directions for Securing Applications .....</b>	<b>C-1</b>
C.1 Antivirus Software .....	C-1
C.1.1 AVG Free Edition for Windows 7.1 .....	C-1
C.1.2 Avira AntiVir PersonalEdition Classic Version 7 .....	C-3
C.1.3 avast! 4 Home Edition, Version 4.6 .....	C-3
C.2 Antispyware Software .....	C-4
C.2.1 Ad-Aware SE Personal 1.06.....	C-4
C.2.2 Microsoft Windows Defender (Beta).....	C-4
C.2.3 Spybot - Search & Destroy 1.4 .....	C-5
C.3 Personal Firewalls.....	C-6
C.3.1 Windows Firewall.....	C-6
C.3.2 ZoneAlarm 6.1 .....	C-6
C.4 E-mail Clients.....	C-7
C.4.1 Eudora 7 .....	C-7



C.4.2	Microsoft Outlook Express 6.....	C-8
C.4.3	Mozilla 1.7.12 .....	C-8
C.4.4	Thunderbird 1.5 .....	C-9
C.5	Web Browsers.....	C-10
C.5.1	Firefox 1.5.....	C-10
C.5.2	Microsoft Internet Explorer 6 .....	C-10
C.5.3	Mozilla 1.7.12 .....	C-11
C.6	Instant Messaging Clients.....	C-13
C.6.1	AOL Instant Messenger (AIM) 1.0.3 .....	C-13
C.6.2	Windows Messenger 4.7 .....	C-13
C.6.3	Yahoo! Messenger 7 .....	C-14
C.7	Office Productivity Suites .....	C-14
C.7.1	Microsoft Office 2003.....	C-14
C.7.2	OpenOffice 2.0 .....	C-16
<b>Appendix D— Tools.....</b>		<b>D-1</b>
<b>Appendix E— Glossary .....</b>		<b>E-1</b>
<b>Appendix F— Acronyms .....</b>		<b>F-1</b>
<b>Appendix G— Resources.....</b>		<b>G-1</b>
G.1	Print Resources .....	G-1
G.2	NIST Documents and Resources .....	G-1
G.3	Microsoft Web-Based Resources .....	G-1
G.3.1	Windows XP Home Edition Resources .....	G-2
G.3.2	Windows XP Home Edition Security Resources .....	G-2
G.4	Other Web-Based Windows XP Home Edition Resources .....	G-3
<b>Appendix H— Index.....</b>		<b>H-1</b>

## List of Figures

Figure 3-1.	Automatic Updates Configuration Options .....	3-2
Figure 3-2.	File Association Mappings.....	3-13
Figure 3-3.	Web Browser History Screen .....	3-16
Figure 3-4.	Folder Sharing Properties.....	3-19
Figure 3-5.	Security Center.....	3-20
Figure 5-1.	System Properties .....	5-3
Figure 5-2.	Microsoft Update .....	5-10
Figure 5-3.	Automatic Updates Configuration.....	5-11
Figure 5-4.	Wireless Networking Security Properties .....	5-18
Figure 5-5.	Viewing Installed Program Names .....	5-21
Figure 5-6.	Running Tasks.....	5-22
Figure 5-7.	Startup Programs .....	5-23

Figure 5-8. Windows Defender .....	5-24
Figure 8-1. Security Center Status Reporting .....	8-3
Figure 8-2. Shared Folders .....	8-4
Figure 8-3. Microsoft Baseline Security Analyzer Report .....	8-10
Figure 8-4. History from System Information Utility .....	8-15
Figure 8-5. Event Viewer .....	8-16
Figure 8-6. Windows Advanced Options Menu.....	8-18
Figure A-1. Flowchart for Applying Essential Recommendations .....	A-2
Figure A-2. Microsoft Update .....	A-7
Figure A-3. Automatic Updates Configuration .....	A-8
Figure B-1. Disabling User Account at the Command Prompt.....	B-2
Figure B-2. Disabling Unneeded Networking Features.....	B-3
Figure B-3. Disabling Unneeded Services .....	B-5

### List of Tables

Table 3-1. Comparison of Update Methods .....	3-4
Table D-1. Windows XP Home Edition Tools .....	D-1

## Executive Summary

In today's computing environment, there are many threats to home computers, including those running Microsoft Windows XP Home Edition. These threats are posed by people with many different motivations, including causing mischief and disruption, committing fraud, and performing identity theft. The most common threat against Windows XP Home Edition computers is malware, such as viruses and worms. Users of home computers should ensure that they are secured properly to provide reasonable protection against threats. Accordingly, this document provides guidance to people on improving the security of their own home computers (desktops or laptops) or others' home computers that run Windows XP Home Edition. The recommendations draw on a large body of vendor knowledge and government and security community experience gained over many years of securing personal computers.

Users of Windows XP Home Edition need to be aware of the threats that their computers face and the security protections available to protect their computers so that they can operate their computers more securely. Security protections are measures used to thwart threats. Examples of common security protections are antivirus software, password-protected user accounts, and automatic software updates and patches. Security protections cannot prevent all attacks, but they can greatly reduce the opportunities that attackers have to gain access to a computer or to damage the computer's software or information. Securing a Windows XP Home Edition computer effectively and maintaining its security requires a combination of security protections; if one protection fails or is ineffective against a particular threat, other protections are likely to prevent the threat from succeeding. Security protections should be updated on a regular basis because new threats occur on a regular basis.

Implementing the following recommendations should help people to improve the security of Windows XP Home Edition computers.

**Users should eliminate any known weaknesses in their Windows XP Home Edition computers because attackers will attempt to take advantage of them.**

Known weaknesses should be eliminated through a combination of several methods, including the following:

- Installing Windows XP Home Edition Service Pack 2 (SP2) and applying software updates to the computer on a regular basis, including Windows XP Home Edition and software applications
- Limiting access to the computer through separate password-protected user accounts for each person
- Limiting network access by disabling unneeded networking features, limiting the use of remote access utilities, and configuring wireless networking securely
- Disabling services that are not needed.

**Users should configure their Windows XP Home Edition computers to use a combination of software and software features that are designed specifically to stop attacks, particularly malware.**

Every Windows XP Home Edition computer should use antivirus software, antispyware software, and a personal firewall at all times, and they should be kept up-to-date. Other helpful software includes spam and Web content filtering and popup blocking. Users can also change settings on common applications such as e-mail clients, Web browsers, instant messaging clients, and office productivity suites to stop some attacks.

**Users or administrators of Windows XP Home Edition computers should periodically perform backups that duplicate data from the computer onto another medium.**

Performing regular backups helps to ensure that user data is available after an unfortunate event such as an attack against the computer, a hardware failure, a natural disaster, or human error. User data should be backed up periodically, such as weekly or monthly. There are several options for performing backups on Windows XP Home Edition computers, including utilities built into Windows XP Home Edition, and third-party utilities and remote backup services.

**Users or administrators of Windows XP Home Edition computers that connect to the Internet should ensure that they are protected properly from Internet-based threats.**

The five most important protections that should be used for all Windows XP Home Edition computers connecting to the Internet are as follows:

- Applying updates to the operating system and major applications (e.g., e-mail clients, Web browsers) regularly, preferably through automated means that check for updates frequently
- Using a limited user account for typical daily use of the computer
- Running up-to-date antivirus software and antispyware software that is configured to monitor the computer and applications often used to spread malware (e.g., e-mail, Web) and to quarantine or delete any identified malware
- Using a personal firewall that is configured to restrict incoming network communications to only that which is required
- Performing regular backups so that data can be restored in case an adverse event occurs.

## 1. Introduction

### 1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

---

---

### 1.2 Purpose and Scope

This document seeks to provide advice primarily to experienced Windows XP administrators on securing Windows XP Home Edition computers for home users, such as telecommuting Federal civilian agency employees, from common threats such as malware, and keeping the computers secure. This document gives general guidance on workstation security as well as Windows XP Home Edition-specific guidance. Although some of the guidance presented in this document may be applicable to multiple versions of Windows XP, the guidance is specifically intended for Windows XP Home Edition computers running Service Pack 2.<sup>1</sup>

This document is published by NIST as recommended guidance for Federal agencies, in support of the NIST Security Configuration Checklists Program for IT Products.<sup>2</sup> Agencies can take advantage of the contents of this publication in different ways. For example, they could make telecommuting employees aware of its existence so that the employees can use it to secure the home computers from which they telecommute. Another example is reusing portions of it in training and awareness activities for telecommuting employees. The document may also be used by private sector organizations or individuals in securing personal computers.

---

<sup>1</sup> Portions of the guidance in this document might be applicable to other versions of Windows XP, but the guidance has not been tested on any versions of Windows XP other than Windows XP Home Edition. Also, because some versions of Windows XP offer functionality that Windows XP Home Edition does not, the guidance presented in this document would be incomplete for other Windows XP versions.

<sup>2</sup> For more information on the program, see NIST Special Publication (SP) 800-70, *Security Configuration Checklists Program for IT Products*, available at <http://checklists.nist.gov/>.

NIST recommends that organizations wanting to use Windows XP for organization-issued telecommuting computers should deploy Windows XP Professional instead of Windows XP Home Edition. Unlike Windows XP Home Edition, Windows XP Professional can be centrally managed and integrated with Microsoft Active Directory architectures, and it also provides additional security controls that can be enabled to enforce organizational policies, such as password, audit, patch management, and encryption policies.<sup>3</sup> However, NIST recognizes that there are many personal home computers running operating systems such as Windows XP Home Edition that are used by telecommuters to interact with organizations' information systems. This publication has been produced to help these telecommuters ensure that their personally owned Windows XP Home Edition computers are secure.

Windows XP Home Edition computers may need to protect the confidentiality or integrity of Federal information in storage (e.g., file encryption) or in transit (e.g., virtual private networks [VPN], secure access to Web pages). Such computers must use Federal Information Processing Standards (FIPS) approved cryptographic algorithms specified in FIPS or in NIST Recommendations and contained in validated cryptographic modules. The Cryptographic Module Validation Program (CMVP) at NIST coordinates FIPS testing.<sup>4</sup>

---

---

### 1.3 Audience

This document has been created for IT professionals (particularly Windows XP system administrators and information security personnel) who may need to help secure others' Windows XP Home Edition computers within home offices. Portions of the document are intended for Windows XP Home Edition users; these portions assume that readers have experience as Windows XP users, but not as administrators of Windows XP Home Edition computers.

---

---

### 1.4 Document Structure

Throughout this guide, filenames, menu items, and options are indicated through bold text (e.g., **Add or Remove Programs**, **Automatic Updates**, **Remember my password**). The remainder of this document is organized into seven major sections, followed by eight appendices.

- Section 2 explains the need to secure Windows XP Home Edition computers from common threats such as malware (e.g., viruses, worms) using a variety of countermeasures, also known as security protections.
- Section 3 presents an overview of the types of security protections that are most important for securing Windows XP Home Edition computers.
- Section 4 provides guidance on installing Windows XP Home Edition onto a computer.

---

<sup>3</sup> See NIST SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist* ([http://csrc.nist.gov/itsec/download\\_WinXP.html](http://csrc.nist.gov/itsec/download_WinXP.html)) for more information on Windows XP Professional computer security.

<sup>4</sup> The CMVP Web site is located at <http://csrc.nist.gov/cryptval/>. FIPS 140-2, *Security Requirements for Cryptographic Modules*, is available at <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>. Other FIPS publications are available at <http://csrc.nist.gov/publications/fips/index.html>.

- Section 5 discusses how to secure Windows XP Home Edition after it has been installed onto a computer but before that installation has been used.
- Section 6 explains how to secure a previously used installation of Windows XP Home Edition.
- Section 7 gives recommendations for securing each user account on a Windows XP Home Edition computer.
- Section 8 provides guidance on maintaining the security of a Windows XP Home Edition computer that has already been secured.
- Appendix A presents step-by-step instructions for performing the actions most essential to securing a Windows XP Home Edition computer.
- Appendix B contains step-by-step instructions for implementing advanced security recommendations on Windows XP Home Edition computers.
- Appendix C provides step-by-step directions for securing several common types of applications.
- Appendix D provides a summary of tools that may be helpful in configuring, managing, and monitoring Windows XP Home Edition security settings.
- Appendix E contains a glossary of selected terms used in the document.
- Appendix F lists acronyms used in this document.
- Appendix G lists print and online resources that may be helpful references for securing Windows XP Home Edition computers.
- Appendix H contains an index for the document.

---

---

## 1.5 Quick Start

This document is intended to be used by readers with various levels of Windows XP Home Edition experience and security knowledge, who are faced with different situations in securing computers. For example, one reader might be securing a brand-new computer, while another reader wants to secure a computer that has been in daily use for years. Not all sections of this guide will apply to every situation. The items below provide general recommendations as to which sections of the guide should be read, based on the reader's experience and goals. Readers who are unsure about the relevance or appropriateness of a particular section should read its introduction and summary to determine if the section is applicable to their situation.

**Users should back up all data and verify the validity of the backups before implementing any of the recommendations or suggestions in the guide. Readers with little or no Windows XP Home Edition experience should seek assistance in applying the recommendations to their computers. Although the recommendations presented in this guide have been tested thoroughly, every computer's existing configuration and environment is unique, so**

**changing settings could have unforeseen consequences, including loss of data and loss of Windows or application functionality.**

Sections 2 and 3 talk in detail about Windows XP Home Edition security concepts and capabilities; this is background information for other sections that provide step-by-step directions for securing computers, and also serves as general reference material. Readers who want to have a better understanding of security should read Sections 2 and 3 first. Readers who just want to secure computers without necessarily understanding the significance of each action should skip Sections 2 and 3.

Readers should carefully read and follow the step-by-step security directions listed for the appropriate goal from the following list:<sup>5</sup>

- **Build or Rebuild a Windows XP Home Edition Computer.** This is for readers that want to install or reinstall Windows XP Home Edition on a computer. Such readers should use the following sections:
  - Section 4 on installing Windows XP Home Edition
  - Section 5 on securing a new computer or installation
  - Section 7 on securing user accounts and settings
  - Section 8 on computer maintenance and monitoring.
- **Secure a New Windows XP Home Edition Computer.** This is for readers that have a new computer with Windows XP Home Edition or an existing computer with a new installation of Windows XP Home Edition. Such readers should use the following sections:
  - Section 5 on securing a new computer or installation
  - Section 7 on securing user accounts and settings
  - Section 8 on computer maintenance and monitoring.
- **Secure an Existing Windows XP Home Edition Computer.** This is for readers who want to improve security for a Windows XP Home Edition computer that has already been in use. Such readers should use the following sections:
  - Section 6 on securing an existing computer
  - Section 5 on securing a new computer or installation
  - Section 7 on securing user accounts and settings
  - Section 8 on computer maintenance and monitoring.

For Windows XP Home Edition users and other readers who do not necessarily have the time or expertise to follow all of the instructions in these sections, Appendix A contains

---

<sup>5</sup> Securing a home network is outside the scope of this publication. Guidance on home network security is provided in NIST SP 800-46, *Security for Telecommuting and Broadband Communications*, which is available at <http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf>.



instructions for the most essential security protections for Windows XP Home Edition computers.

- **Understanding of Windows XP Home Edition Security.** Readers who are seeking a deeper understanding of Windows XP Home Edition security should read the entire document, skimming any parts that contain familiar content.

**This page has been left blank intentionally.**

## 2. The Need to Secure Windows XP Home Edition Computers

In today's computing environment, there are many threats to home computers. These threats are posed by people with many different motivations, including causing mischief and disruption, committing fraud, and performing identity theft. Users of home computers can increase their security to provide better protection against these threats. The goal of this guide is to provide guidance to users on how to improve the security of their home computers (desktops or laptops) that run Windows XP Home Edition. This guide draws on a large body of vendor knowledge and government and security community experience gained over many years of securing computers.

*Because of differences in the security features available on various Windows versions, the guidance in this document is only applicable to Windows XP Home Edition systems. It should **not** be applied to any other versions of Windows XP, including Windows XP Professional, Windows XP Tablet PC Edition, and Windows XP Media Center Edition, or to any versions of Windows other than XP. Portions of the guidance in this document might be applicable to other versions of Windows XP, but the guidance has not been tested on any versions of Windows XP other than Windows XP Home Edition. Also, because some versions of Windows XP offer functionality that Windows XP Home Edition does not, the guidance presented in this document would be incomplete for other Windows XP versions.*

This section of the guide explains the need to secure home computers running Windows XP Home Edition. It describes common threats against Windows XP Home Edition computers that are likely to affect or attempt to affect users. This section also discusses the roles that Windows XP Home Edition computers can play, such as personal use and business use, and introduces the idea of threat environments, such as a home environment, office environment, or wireless network hotspot. This section then introduces the concept of security protections, which are ways of counteracting threats within a particular environment.

---

---

### 2.1 The Roles of Computers

Every computer has at least one role, such as the following:

- **Personal Use.** The computer is used to browse the Web, check e-mail, use instant messaging and peer-to-peer file sharing services, play network games, play audio and video content, and perform other personal tasks. Although the information on the computer is primarily personal, it may also include sensitive information such as financial data from balancing bank accounts, paying bills and making purchases online, doing online banking, and using tax preparation software.
- **Business Use.** The computer is used by a telecommuter to connect back to the employer's network and computers. The information processed by the computer is primarily corporate data.

- **Home Network Use.** The computer provides services to other computers on a home network. For example, the computer may be used as a file and print server, a multimedia server (e.g., music jukebox), or a gateway for sharing an Internet connection. The information processed by the computer varies based on the roles of the other computers on the home network.

Many computers have more than one role, and might even have multiple roles simultaneously. For example, a computer could be used to check personal e-mail while it is also connected to an employer's network. Thinking about roles is important because a computer that performs more important functions or contains more important data than another computer might need stronger protection from threats.

---

---

## 2.2 Common Threats

The most common threat against Windows XP Home Edition computers is malware.<sup>6</sup> *Malware*, also known as *malicious code*, refers to a computer program that is covertly placed onto a computer with the intent to compromise the privacy, accuracy, or reliability of the computer's data, applications, or operating system. Common types of malware threats include the following:

- **Viruses**, which are designed to self-replicate—make copies of themselves—and distribute the copies to other files, programs, or computers
- **Worms**, which are self-replicating programs that are completely self-contained and self-propagating
- **Malicious mobile code**, which is malicious software that is transmitted from a remote system to be executed on a local system, typically without the user's explicit instruction
- **Trojan horses**, which are non-replicating programs that appear to be benign but actually have hidden malicious purposes
- **Rootkits**, which are collections of files that are installed onto computers to alter their functionality in a malicious and stealthy way, including installing and hiding other types of malware.

Malware threats can infect computers through many means, including e-mail, Web sites, file downloads and file sharing, and instant messaging. Malware can disrupt a computer in many ways, such as the following examples:

- Destroying data, such as e-mails or word processing documents
- Causing computers to crash or reboot repeatedly
- Using a computer's resources, such as disk space, processing power, and network bandwidth
- Exposing personal data to others, such as e-mailing personal documents to others and collecting financial information viewed in a Web browser

---

<sup>6</sup> For more information on malware, see NIST Special Publication (SP) 800-83, *Guide to Malware Incident Prevention and Handling*, which is available for download at <http://csrc.nist.gov/publications/nistpubs/>.

- Attacking other computers, such as sending out many e-mails to infect other computers or performing a denial of service attack against a commercial Web site.

*One form of malware is known as a zombie or a bot. A **bot** is a program installed onto a computer that causes it to attack other computers, typically without the knowledge of the computers' users. Through the use of automated tools, attackers can coordinate the actions of thousands of bots at once (known as a **botnet**) to launch massive attacks against Web sites and other computers.*

*Spyware*—malware specifically intended to violate a user's privacy—has become a major concern.<sup>7</sup> Although privacy-violating malware has been in use for many years, it became much more widespread in 2003 and 2004, with spyware invading many computers. Spyware can monitor a person's Web browser use and report personal behavior and related information to others, such as marketing firms. Some forms of spyware are specifically designed to assist in conducting financial fraud, such as collecting credit card numbers and bank account numbers. Spyware can also cause the same disruptions to computers as standard malware, such as crashes and data destruction.

In addition to malware and spyware, other common threats against Windows XP Home Edition computers include the following:

- **Phishing.** *Phishing* attacks involve the use of fraudulent e-mails and Web sites that look very similar to the legitimate sources, with the intent of committing financial fraud. These attacks trick users into revealing important information, such as bank account numbers, credit card numbers, PIN numbers, and financial Web site usernames and passwords. An example of a phishing attack is a spam message that appears to come from a bank—it uses the bank's name, logo, slogans, and other information and graphics to attempt to look legitimate. The message asks the user to update her personal information by clicking on a URL. This URL actually directs the user to a phony Web site that looks like the bank's real Web site.<sup>8</sup> Thinking that the Web site is legitimate, the user types in her username and password, then her bank account number; the Web site gives this information to the attacker.<sup>9</sup>
- **Scanning Tools.** Attackers use a variety of automated tools that send a series of messages to other computers to try to learn more about them. These tools, known as *scanners*, can check hundreds or thousands of computers an hour to identify good targets for future attacks. A

<sup>7</sup> Examples of spyware include *keystroke loggers* (also known as keyloggers), which monitor and record keyboard usage (e.g., usernames and passwords; financial information such as credit card numbers, social security numbers, and personal identification numbers [PIN]), and *tracking cookies*, which are small data files that hold information about the use of Web sites and are misused to track a user's Web browsing activities for questionable reasons without the user's knowledge or consent.

<sup>8</sup> A term often used in conjunction with phishing is pharming. Although both involve the use of deceit to gain access to personal information, they are performed differently. In *pharming*, an attacker actually takes control of a URL, such as the address of a Web site. Users enter the correct Web site URL into their Web browsers but are taken to a phony Web site run by the attacker. Users then enter passwords, PIN numbers, and other sensitive information, which the attacker collects.

<sup>9</sup> Should a user accidentally reveal sensitive information to an unknown Web site, the user should immediately contact the organization associated with the sensitive information (in this example, the bank) to prevent malicious parties from misusing the information to commit fraud.

computer connected directly to the Internet is scanned constantly; if the computer is not protected, attackers could gain information from the scans that would help them in planning attacks against the computer.

- **Attack Tools.** Many attackers use automated tools that send various types of attacks to other computers. Attack tools are sometimes used in conjunction with scanning tools; an attacker first scans computers to find ones that are good targets, then launches attacks against those targets. Because many attack tools are fully automated and run for extended periods, computers connected directly to the Internet need protection against these attacks at all times.

---

---

## 2.3 Security Protections

*Security protections*, also known as *security controls*, are measures against threats that are intended to compensate for the computer's security weaknesses, also known as *vulnerabilities*. Threats attempt to take advantage of these vulnerabilities. Some vulnerabilities can be eliminated through security protections, such as a feature in an application that automatically downloads and installs new versions of the application that have corrected previous errors. For vulnerabilities that cannot be eliminated, security protections can prevent attacks from taking advantage of them, such as antivirus software stopping an infected email from being opened by a user. No matter how many security protections are used, it is simply not possible to provide 100% protection against attacks because of the complexity of computing. A more realistic goal is to use security protections to give attackers as few opportunities as feasible to gain access to a computer or to damage the computer's software or information.

Security protections can be grouped into the following three categories:

- **Technical.** A *technical protection* is a way of configuring a computer to restrict the actions that can be performed within the computer and to monitor the actions that are performed. A commonly used technical protection is a username and password, which limit access to a computer, service, or other resource.
- **Operational.** An *operational protection* is one that involves the actions performed by the computer's users. For example, antivirus software checks a user's files, e-mails, and Web browsing for malware and quarantines or deletes any malware to prevent it from infecting the computer and causing damage. Other examples of operational protections are making backup copies of users' files, keeping a computer and its media (e.g., CDs) in a locked room, and learning how to use a computer securely (e.g., how to handle e-mail so as to avoid infecting a computer with malware).
- **Management.** A *management protection* involves oversight of the security of computers. Most types of management protections are focused on computers within an organization, but a few apply to individual computers, such as performing periodic reviews of their security and identifying vulnerabilities.

Securing a computer effectively usually requires a combination of security protections from all of these categories. If one protection fails or is ineffective against a particular threat, other protections are likely to prevent the threat from succeeding. Relying on only a few protections can lead to serious security breaches. For example, a lack of physical security protections could

make it easy for a computer to be stolen. Omitting training and awareness protections is unwise because users that are not aware of good security practices could inadvertently circumvent other protections. Users also need to be aware of the threats that their computers face and the capabilities of the security protections on their computers so that they can operate their computers more securely. Some operational protections such as antivirus software are always needed because they can recognize and respond to known and predictable threats within the computer automatically. Unfortunately, although many protections are very beneficial, they also make computers less convenient and more difficult to use. For example, passwords provide protection, but they can also be hard to remember.

Because most management protections are not applicable to individual Windows XP Home Edition computers used at individuals' homes, the focus of this guide is technical and operational protections. This guide also provides limited information on the relevant management protections, primarily performing periodic vulnerability assessments. Operational protections for physical security are not addressed in this guide; however, users should be aware of the physical risks against their computers and ensure that their computers are adequately protected. Examples of physical risks are theft, power disruptions, and water.

---

---

## **2.4 Threat Environments**

Every computer resides in an environment that exposes it to certain types of threats. For example, a desktop computer connected directly to the Internet from a house, and a desktop computer on a large organization's internal network, are likely to be exposed to different types and quantities of threats. The large organization probably uses additional security protections not present in the home computing environment; these protections block many threats from ever reaching the organization's desktop computer. In a home environment, it is not feasible from a cost perspective to have the same level of security protections. Also, most of the security protections used by a large organization require extensive technical expertise to configure and manage them effectively.

This guide assumes that the Windows XP Home Edition computers being secured are in home environments, and that they are either connected directly to the Internet or are part of a small office/home office (SOHO) network that is connected to the Internet. The recommendations presented in this guide focus on typical threats found in home environments. Many Windows XP Home Edition computers (particularly laptops) are also used in mobile environments such as a coffee shop wireless network hotspot, a university network, or a hotel wireless network. Computers that are used in multiple environments are typically exposed to a wider variety of threats than computers used in a single environment, and are more likely to spread malware from one environment to another (e.g., from a store's wireless hotspot to a home network). Also, mobile computers are more likely to be lost or stolen, which could lead to the disclosure of sensitive information on the computer. Accordingly, this guide presents additional recommendations for securing mobile computers.

## **2.5 Summary**

In today's computing environment, there are many threats to home computers. The motivations for these threats include causing disruption, committing fraud, and performing identity theft. Users need to secure their home computers to provide better protection against these threats, especially the most common one, malware. Security protections are measures used to thwart threats. Security protections cannot prevent all attacks, but they can greatly reduce the opportunities that attackers have to breach a computer's security. Securing a computer effectively requires a combination of security protections; if one protection fails or is ineffective against a particular threat, other protections are likely to prevent the threat from succeeding. Users also need to be aware of the threats that their computers face and the capabilities of the security protections on their computers so that they can operate their computers more securely.



## 3. Overview of Security Protections

As described in Section 2, *security protections* are measures that thwart threats. This section provides an overview of the types of security protections that are most important for securing Windows XP Home Edition computers. For each control type, the section provides a brief description of the protection, explains what types of threats it protects against, discusses its relative strengths and weaknesses, and recommends how it should be used. People should strive to secure their computers to a reasonable degree using a combination of technical and operational protections, such as antivirus software, Windows XP Home Edition configuration settings, and user education and security awareness activities. Because new vulnerabilities in Windows XP Home Edition and applications are discovered on an ongoing basis, it is important that many protections are not only used, but also updated on a regular basis.

---

---

### 3.1 Reducing Weaknesses

One of the most important parts of securing a Windows XP Home Edition computer is eliminating known weaknesses, because attackers will attempt to take advantage of them. This section makes recommendations for eliminating weaknesses using five types of techniques: updating software, restricting access to user accounts and sessions, limiting network access to the computer, protecting files and folders from unauthorized access, and disabling unneeded services.

---

#### 3.1.1 Software Updates

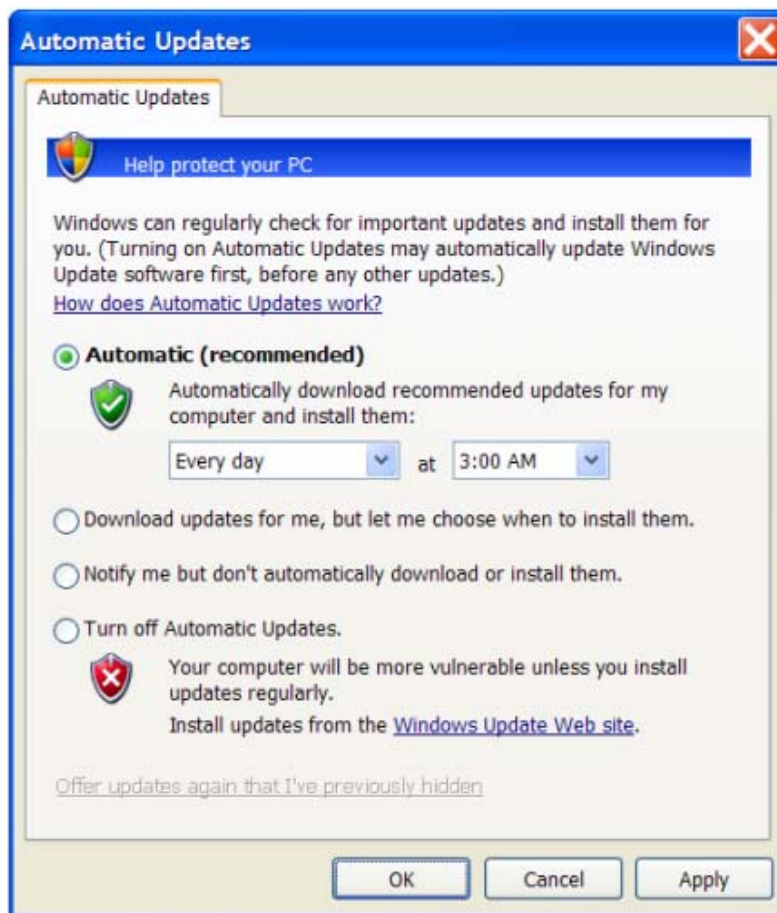
As described in Section 2, many threats take advantage of vulnerabilities in operating systems such as Windows XP Home Edition and applications such as e-mail clients and Web browsers. Microsoft and other software vendors release updates for their software to eliminate vulnerabilities. Accordingly, users should ensure that software updates are applied to their Windows XP Home Edition computers on a regular basis. Windows XP Home Edition and most popular applications provide built-in mechanisms to update themselves automatically. This section describes these update features. Section 5.2 provides detailed directions on implementing the recommendations presented in this section.

##### 3.1.1.1 Keep Microsoft Software Updated

Microsoft releases updated code for Windows XP Home Edition-related security issues through three mechanisms. A *hotfix* takes care of a specific problem. A *security rollup* is a collection of hotfixes. A *service pack* (SP) is a major upgrade to the operating system that resolves dozens of functional and security problems and often introduces new features or makes significant configuration changes to computers. Microsoft provides two ways of distributing hotfixes, security rollups, and service packs to individual computers: Automatic Updates and Microsoft

Update (formerly known as Windows Update).<sup>10</sup> Microsoft also makes service packs for Windows XP Home Edition available on CD.<sup>11</sup>

Automatic Updates is a built-in feature of Windows XP Home Edition. To function properly, it must be enabled from an administrative account. Once enabled, it can be run from any user account. It automatically checks the Microsoft update servers for Windows XP Home Edition and Microsoft application updates. Automatic Updates has a prioritization feature that ensures the most critical updates are installed before less important updates. As shown in Figure 3-1, Automatic Updates provides four configuration options to users.



**Figure 3-1. Automatic Updates Configuration Options**

<sup>10</sup> A comparison of Automatic Updates and Microsoft Update is available at <http://update.microsoft.com/microsoftupdate/v6/about.aspx>.

<sup>11</sup> Microsoft offers a free CD with Windows XP SP2; more information is available at [http://www.microsoft.com/windowsxp/downloads/updates/sp2/cdorder/en\\_us/default.msp](http://www.microsoft.com/windowsxp/downloads/updates/sp2/cdorder/en_us/default.msp). Microsoft also offers a network installation package that can be used to distribute large service packs to multiple Windows XP computers on a single network. The package for Windows XP SP2 is available for download at <http://www.microsoft.com/downloads/details.aspx?FamilyID=049c9dbe-3b8e-4f30-8245-9e368d3cdb5a&displaylang=en>.

Generally, it is best to configure the computer to download and install updates automatically, unless bandwidth usage is a concern. Downloading updates could adversely affect the functionality of a computer that is connected to the Internet on a slow link. In this case, it would be preferable for Automatic Updates to be configured to notify the computer's administrator that new patches are available. The administrator should then make arrangements to download and install the patches at the next possible time when the computer is not needed for other functionality.

Windows XP Home Edition also offers an **Install updates and shutdown** option as part of its Shut Down dialog box. Administrators can configure their computers to download updates automatically; when they shut down a computer, the option will appear and allow administrators to launch the update installation process.

Administrators can also manually update their computers by visiting the Microsoft Update Web site.<sup>12</sup> The site will first validate that the Windows XP Home Edition software installed on the computer is authentic and properly licensed. Next, it will check the computer to determine what security and functionality updates are available and produce a list of updates. The administrator can then select which updates should be installed at this time, and tell Microsoft Update to perform the installations. In addition to retrieving Windows XP Home Edition updates, Microsoft Update can also get security updates for other Microsoft products, such as Microsoft Office, and non-security updates for Microsoft software and for hardware. Administrators should run Microsoft Update when updating a new installation of Windows XP Home Edition, and should also run it periodically throughout the life of the system to acquire non-security updates, such as new hardware drivers. Even though these updates are not specifically intended to improve security, some might have security implications, such as adding new, stronger security features.

Table 3-1 compares the update methods described in this section, indicating under what circumstances each method might be appropriate.

---

<sup>12</sup> The Microsoft Update Web site is located at <http://update.microsoft.com/>. The site may only be used with the Internet Explorer Web browser. Windows XP Home Edition computers that are not fully updated may display the Windows Update Web site instead of the Microsoft Update Web site.

**Table 3-1. Comparison of Update Methods**

Goal	Low-Bandwidth Internet Connectivity	High-Bandwidth Internet Connectivity
Secure a new computer or a previously unsecured computer	<ol style="list-style-type: none"> <li>1. Order the Windows XP service pack CD from Microsoft.</li> <li>2. Apply the service pack from the CD.</li> <li>3. Apply the security rollups, hotfixes, and other security-related updates through Microsoft Update. Because of the amount of time needed to download them, it might need to be performed in multiple sessions.</li> <li>4. Apply non-security-related updates through Microsoft Update.</li> </ol>	<ol style="list-style-type: none"> <li>1. Apply all security-related updates through Microsoft Update.</li> <li>2. Apply all non-security-related updates through Microsoft Update.</li> </ol>
Install a new service pack onto a previously secured computer	<ol style="list-style-type: none"> <li>1. Order the Windows XP service pack CD from Microsoft.</li> <li>2. Apply the service pack from the CD.</li> </ol>	<ol style="list-style-type: none"> <li>1. Apply the service pack through Automatic Updates.</li> </ol>
Install a new security rollup, hotfix, or any other security update besides a service pack onto a previously secured computer	<ol style="list-style-type: none"> <li>1. Apply the updates through Automatic Updates. Because of the amount of time needed to download them, it might need to be performed in multiple sessions.</li> </ol>	<ol style="list-style-type: none"> <li>1. Apply the security updates through Automatic Updates.</li> </ol>
Install a non-security update, such as a new hardware driver	<ol style="list-style-type: none"> <li>1. Apply the update through Microsoft Update.</li> </ol>	<ol style="list-style-type: none"> <li>1. Apply the update through Microsoft Update.</li> </ol>

### 3.1.1.2 Keep Other Software Updated

In addition to keeping Microsoft software updated, it is important to keep other software applications on Windows XP Home Edition computers updated as well. For example, vulnerabilities are discovered in e-mail clients and Web browsers periodically; attackers can take advantage of these problems to infect computers with malware or perform other malicious acts. Also, security software such as antivirus and antispyware software needs to be kept up-to-date so that it can detect and stop the latest security threats. Administrators should check each third-party application on the computer to determine how it can be updated, then ensure that it is updated regularly. Updates are usually available through at least one of the following methods.

- **Automatic Update Feature.** Many software programs have a feature similar to Microsoft's Automatic Updates that automatically checks for, downloads, and installs updates from the software vendor. Administrators may need to enable this feature and set a frequency for update checks, such as daily or weekly.

- **Manual Update Feature.** Many software programs allow administrators to manually launch an update feature which checks for, downloads, and installs updates from the software vendor. Manual updates should be performed at least monthly, preferably weekly.
- **Separate Update Acquisition.** Some software programs do not have a built-in feature for acquiring updates. Administrators may need to visit the software vendor's Web site, find the appropriate Web page (usually the support, download, or security page), download the update, and then run it to install it onto the computer. In some cases, rather than applying an update to the application, administrators need to download and install a new version of the whole application instead.

Some applications offer updates at no charge, while others require an annual fee or other payment to receive updates (e.g., new antivirus software signatures). Most software vendors that charge a fee allow users to pay it through their Web site and receive updates within minutes of making the payment.

---

### 3.1.2 User Accounts and Sessions

Windows XP Home Edition computers can be configured to limit access through user accounts and passwords. This section describes ways in which users can take advantage of these configuration options to prevent unauthorized local and network access to the computer and its applications and data. Specific directions on implementing the recommendations described in this section are provided in Section 5.4.1.

#### 3.1.2.1 Use Separate Accounts for Each Person

A Windows XP Home Edition computer can be run with a single user account that multiple people use, or with separate user accounts for each person. From a security standpoint, it is strongly recommended that each person has a separate account.<sup>13</sup> On Windows XP Home Edition computers, the capability to have multiple user accounts is known as Personalized Login. Having an individual user account for each person allows personal data (e.g., each account has its own My Documents folder) and settings (e.g., Internet Explorer bookmarks and security settings) to be kept private from other users.<sup>14</sup> Also, should malware infect a computer, it might only be able to affect the files and settings of the current user, not other users, depending on what rights the current user has (as described in Section 3.1.2.4).

Windows XP Home Edition offers another feature closely related to Personalized Login called Fast User Switching (FUS).<sup>15</sup> It allows two or more users to be logged into the same Windows

---

<sup>13</sup> Microsoft has an overview of Windows XP Home Edition computer sharing features at <http://www.microsoft.com/windowsxp/evaluation/features/sharing.mspix>. Additional information on user account security is available at

[http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ua\\_c\\_account\\_types.mspix](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ua_c_account_types.mspix).

<sup>14</sup> Personal data is only kept private if the user account is protected with a password and the Windows XP Home Edition computer is using the NTFS filesystem

(<http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/xpsec.mspix>).

<sup>15</sup> Additional information on FUS is available at

[http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/fast\\_user\\_switching.mspix](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/fast_user_switching.mspix) and from Microsoft Knowledge Base articles 279765 (<http://support.microsoft.com/?id=279765>) and 294739 (<http://support.microsoft.com/?id=294739>).

XP Home Edition computer simultaneously, but only a single user session is active at any given time. The use of Fast User Switching is recommended on a computer where a user may need brief access to a computer that someone else is using, because it preserves security and privacy for both users. The person currently using the computer cannot gain access to the other user's session, assuming that each user account is protected with a password.

### 3.1.2.2 Protect Each Account with a Password

Whether a Windows XP Home Edition computer has a single shared account or multiple accounts, each account usually should have a password.<sup>16</sup> Without a password, unauthorized people could use the computer—not only people with physical access to the computer, but also possibly remote attackers contacting the computer through the Internet if the computer is not protected through a personal firewall and other technical controls. Windows XP Home Edition does not have any requirements for the quality of passwords, such as minimum password length, so users are responsible for understanding the desirable characteristics of passwords and selecting sufficiently strong passwords. Recommended practices include the following:<sup>17</sup>

- **Changing Passwords Regularly.** This is necessary because if a password is unknowingly revealed to an unauthorized person or uncovered by malware or other automated attacks, the password could be used without authorization for a long time. Users should change their passwords at least once every three months.
- **Selecting a Sufficiently Long Password.** Longer passwords are more difficult to guess than shorter passwords. The downside is that longer passwords are often more difficult for users to remember. Users should select passwords that are at least eight characters long.<sup>18</sup> Users should also consider using passphrases, which are long passwords usually composed of multiple words. Passphrases may be easier to remember than conventional passwords.
- **Creating a Complex Password.** This refers to the variety of characters within the password. For example, a password made of all lower case letters is a relatively simple password, while a password made of upper and lower case letters, digits, and symbols such as punctuation marks is a relatively complex password. The more complex the password is, the more difficult it will generally be for others to guess. Users should select passwords that contain digits and/or symbols in addition to letters.
- **Not Reusing Passwords.** Old passwords may have been compromised, or an attacker may have taken a long time to crack encrypted passwords. Reusing an old password could inadvertently give attackers access to the computer. Users should not reuse old passwords, nor should they create new passwords that are very similar to old passwords. For example, if the old password was “dahlia\*1”, the new password should not be “dahlia\*2”.

---

<sup>16</sup> If the computer has a single user, is located in a physically secure area, and is protected from unauthorized network access by sufficient technical controls (e.g., personal firewall), then it might be acceptable not to have a password.

<sup>17</sup> Microsoft provides guidance on passwords for small business users in the *Security Guide for Small Business*, which is available for download at <http://www.microsoft.com/smallbusiness/support/security-toolkit-pdf.mspx>.

<sup>18</sup> The Microsoft *Security Guide for Small Business* recommends a minimum password length of eight characters. The maximum password length in Windows XP Home Edition is 128 characters.

- **Not Using Password Hints.** Password hints can be very helpful to people in guessing others' passwords and using them to gain unauthorized access to a computer. Users should not use password hints unless their computers do not need protection from people with physical access to them.
- **Not Using Passwords for Other Accounts.** Users should not use the same password for multiple accounts, such as professional and personal e-mail accounts, instant messaging accounts, and e-commerce Web site accounts. If the password used for Windows XP Home Edition access is also used for other user accounts and an attacker learned one of the passwords, the attacker could then access the other accounts.

### 3.1.2.3 Disable Unneeded Default User Accounts

Default user accounts are often used in attacks against various types of computers, including Windows XP Home Edition. By disabling certain default Windows XP Home Edition user accounts, it will be more difficult for attackers to gain access to a computer; however, disabling some accounts can impair the functionality of the computer. The default user accounts are as follows:<sup>19</sup>

- **Administrator.** Attackers often attempt to use the default Administrator account on various operating systems. Windows XP Home Edition does have an account named Administrator, but it is only available for use when the computer is booted into Safe Mode. Since the account is inaccessible under normal circumstances and is needed for Safe Mode to work properly, the original Administrator account should not be disabled, and it should have a password set to prevent unauthorized access.<sup>20</sup> Windows XP Home Edition requires a separate administrative account to be created during the Windows XP Home Edition installation process. This account or other additional administrative accounts should be used instead of the original Administrator account when performing computer administration.
- **Guest.** In earlier versions of Windows, the Guest account was a common means by which to gain remote access to a computer through a network and launch additional attacks against the computer. In Windows XP Home Edition, the Guest account has strictly limited privileges. By default, it is disabled. When enabled, it can only access resources that have been specifically designated for remote sharing, such as folders and printers. If a computer does not share any of its resources, the Guest account is effectively made useless.
- **HelpAssistant.** This account is used only for Remote Assistance sessions, which are described in Section 3.1.3.2. The HelpAssistant account should be disabled unless the Remote Assistance feature is needed. By default, this account should already be disabled.<sup>21</sup>

---

<sup>19</sup> The HelpAssistant and Support\_388945a0 accounts are not visible from the User Accounts portion of the Control Panel. However, the accounts can be viewed and disabled from the Command Prompt.

<sup>20</sup> To ensure that the Administrator account can be accessed when needed, there should either be a current password reset disk for the Administrator account at all times, or the Administrator account's password should be written down and stored in a physically secure location. The password reset disk can be used for the Administrator account in Safe Mode.

<sup>21</sup> This account is disabled by default only on Windows XP Home Edition computers running Service Pack 2. For earlier versions of Windows XP Home Edition, this account is enabled by default.



- **Support\_388945a0.** This account is intended to assist in providing technical support within an enterprise environment. Therefore, it should be disabled for computers used in home and mobile environments. By default, this account should already be disabled. Computer vendors may install their own remote technical support accounts as part of their Windows XP Home Edition installations. Such accounts should also be disabled if possible.

#### 3.1.2.4 Use a Limited User Account for Daily Tasks

User accounts on Windows XP Home Edition computers can have full privileges or limited privileges. An account with full privileges, also known as an *administrative account*, is intended to be used only when performing computer management tasks, such as installing updates and application software, managing user accounts, and modifying Windows XP Home Edition and application settings. If a computer is attacked while an administrative account is in use, the attack will be able to do more damage to the computer. Therefore, user accounts should be set up to have limited privileges; such accounts are known as *daily use* or *limited user accounts* (LUA).<sup>22</sup> Users should not use administrative accounts for general tasks such as reading e-mail and surfing the Web because such tasks are common ways of infecting computers with malware. Malware is likely to do more damage to a computer if accessed using an administrative account than a limited user account.

The primary disadvantages of having separate administrative and limited user accounts are that limited users might not be able to run some applications, such as games and other applications designed for older operating systems, or to install applications, Windows XP Home Edition updates, and application updates. This could cause a significant delay in downloading and installing updates, as well as making other certain tasks less convenient for users. To help work around this problem, Windows XP Home Edition includes a Run As feature, which allows a person logged in as a limited user to perform individual administrative tasks. For example, by right-clicking on an Internet Explorer icon, a limited user can select the Run As option, which causes Internet Explorer to be run with administrative privileges after the limited user has provided a valid administrative username and password. The Fast User Switching feature provides another way to use a separate administrative account to perform a single task while still logged in to a computer with a limited user account.

#### 3.1.2.5 Protect User Sessions from Unauthorized Physical Access

In addition to the limitations on user accounts already described in this section, it is also important in some environments to provide protection against unauthorized physical access to Windows XP Home Edition computers. For example, if a computer is sitting unattended in an area that other people can access, someone could walk up to the computer and masquerade as the user, such as sending e-mail from the user's account, accessing the user's work, making purchases from Web sites, or accessing sensitive financial information stored on the computer. To prevent such events, a user can lock the current session by holding down the Windows logo key on the keyboard and then pressing the L key, or by pressing the Ctrl + Alt + Del keys simultaneously and then selecting **Lock Computer**. This essentially works the same way as Fast User Switching; the user needs to enter the account's password to regain access to the session.

---

<sup>22</sup> For a comparison of administrative and limited user accounts, see [http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ua\\_c\\_account\\_types.msp](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ua_c_account_types.msp).



### 3.1.2.6 Protect Passwords

Another important task is to create a password reset disk, which can be used to regain access to the computer if a password is forgotten.<sup>23</sup> Without a password reset disk, a forgotten administrative password could necessitate reinstalling Windows XP Home Edition and all applications, as well as losing all data stored on the computer. Therefore, the administrator of a Windows XP Home Edition computer should create a password reset disk and update the disk each time the administrative password is changed. The administrator should also ensure that the password reset disk is stored in a physically secure location. Users can also create password reset disks for their individual accounts if desired; these should also be stored securely.

Although Windows XP Home Edition offers built-in capabilities to create a password reset disk, this feature requires the presence of a floppy disk drive and cannot be used on computers without such a drive.<sup>24</sup> If a password reset disk cannot be created, it is strongly recommended to write down the administrative password and store it in a physically secure location in case the password is forgotten. Users can also write down their own passwords and store them securely as well if desired.

---

## 3.1.3 Networking

A Windows XP Home Edition computer can be configured to limit network access; this can reduce the number of ways in which attackers can try to gain access to the computer. This section makes recommendations for configuring networking features to provide increased protection for the computer. Section 5.4.2 provides detailed directions for implementing the recommendations.

### 3.1.3.1 Disable Unneeded Networking Features

By default, Windows XP Home Edition includes several networking features that can provide communications and data sharing between computers. Most computers do not need to use all of these features. Because many attacks are network-based, Windows XP Home Edition computers should only use the necessary networking features, which should reduce the likelihood that the computer will be compromised or misused. On Windows XP Home Edition computers, the networking features that are the most likely candidates for being disabled are as follows:

- The **Quality of Service (QoS) Packet Scheduler**, which is designed to prioritize network traffic by application over slow network connections. For example, it could give e-mail communications priority over Web surfing. Unfortunately, most applications cannot use the QoS feature, so the QoS Packet Scheduler is beneficial in very few home user situations.
- The **File and Printer Sharing for Microsoft Networks** service, which allows other computers to connect to the local computer's file and printer shares. This service should only be enabled on the computer if the computer shares files or printers with other computers, or if

---

<sup>23</sup> More information on password reset disks is available from Microsoft Knowledge Base (MSKB) article 305478, located at <http://support.microsoft.com/kb/305478/>.

<sup>24</sup> Floppy disk drives are not present in many new computers, and it is anticipated that they will continue to decline in prevalence.

a particular application on the computer requires the service to be enabled. Disabling this service does not prevent users on the local computer from connecting to other computers' shared files and printers.

- **The Client for Microsoft Networks** service, which allows a Windows XP Home Edition computer to use folders and printers that are shared by other computers on the local network. This service should only be enabled if the computer needs to access shared folders and printers, or if a particular application on the computer requires the service to be enabled. Disabling this service does not prevent the local computer from sharing its folders or printers with other computers on the local network.

### 3.1.3.2 Limit the Use of Remote Access Utilities

The Remote Assistance (RA) feature of Windows XP Home Edition provides a way to get remote technical support assistance from a coworker, friend, or family member when running into problems with a computer.<sup>25</sup> Users in need of assistance can send an invitation to start an RA session through the Windows Messenger facility, e-mail requests, and via a Web e-mail service (filling out a form to request assistance). Unfortunately, if RA is configured improperly, unauthorized parties could use it to gain remote access to a computer. Therefore, RA should be disabled except when needed.

Some users also acquire third-party utilities that permit remote access to the computer from other computers. Although this may be convenient, it also increases the risk that the computer will be accessed by remote unauthorized parties. Therefore, such utilities should be enabled only when needed and configured to require authentication (e.g., username and password) before granting remote access.

### 3.1.3.3 Configure Wireless Networking to Support Security

Wireless networking transfers information through the air between a user's computer and a device known as a wireless access point (AP).<sup>26</sup> If improperly configured, wireless networking can cause sensitive information to be transmitted without adequate protection, exposing it to others in close geographic proximity. Recommendations for wireless network security are as follows:<sup>27</sup>

- **Use strong encryption to protect communications.** To provide a better solution for wireless security, an industry group called the Wi-Fi Alliance has created a series of product certifications called Wi-Fi Protected Access (WPA), which include the WPA1 and WPA2 certifications.<sup>28</sup> Computers with wireless network cards that support either WPA1 or WPA2

---

<sup>25</sup> An overview of Remote Assistance is available at <http://www.microsoft.com/windowsxp/using/helpandsupport/learnmore/remotearr/intro.mspx>.

<sup>26</sup> A user's computer can also wirelessly network with another user's computer through what is known as an ad hoc wireless network. However, there are known security risks with ad hoc networks, so this guide does not recommend their use.

<sup>27</sup> Additional information is available from MSKB article 309369, available at <http://support.microsoft.com/kb/309369/>.

<sup>28</sup> The WPA1 certification is also known as WPA. For more information on WPA2, see MSKB article 893357, *The Wi-Fi Protected Access 2 (WPA2)/Wireless Provisioning Services Information Element (WPS IE) Update for Windows XP with Service Pack 2 Is Available*, which is located at <http://support.microsoft.com/kb/893357/>.

can use their security features, such as using Advanced Encryption Security (AES) for encrypting network communications. Whenever available, users should choose 128-bit encryption or greater.

- **Limit access to only specific wireless network cards.** Some access points can be configured to allow only specific computers to have wireless network access. This is done by finding the media access control (MAC) address of each computer's wireless network card and entering the MAC address into a list on the access point. Because a MAC address should be unique to a particular network card, this can be helpful in preventing unauthorized parties from gaining wireless network access.
- **Require the use of a wired equivalent privacy (WEP) key.** A *WEP key* is a series of letters, digits, and other characters that is used to limit access to wireless networks. A wireless access point can be configured to require all computers attempting to connect to it to use a WEP key. When a computer attempts to join the wireless network, it must provide the same WEP key as the one stored in the access point. Users should set a WEP key that is long and complex, making it hard for others to guess. This should help to prevent people in close physical proximity to the access point from gaining unauthorized access to the wireless network.

Windows XP Home Edition offers a feature called Wireless Auto Configuration that can be set to automatically attempt to join any wireless networks it detects in an established list of preferred networks.<sup>29</sup> By default, Windows XP Home Edition computers with SP2 will not attempt to connect to any other networks automatically. This default setting should not be changed. However, if the preferred networks cannot be found, by default the computer will attempt to transmit identifier information to other wireless computers in the area using what is known as ad hoc networking. An attacker could take advantage of this to establish unauthorized communications with the computer. Windows XP Home Edition can be configured to prohibit the use of ad hoc mode, preventing such attacks from succeeding.

#### 3.1.3.4 Limit the Use of Internet Connection Sharing (ICS)

Internet Connection Sharing (ICS) allows a Windows XP Home Edition computer to share an Internet connection with other computers. ICS is most often used in SOHO environments when Internet access is available only through a dial-up modem in one computer. In such a situation, ICS can allow multiple computers to share the limited Internet connectivity. If a higher-bandwidth network is in use, such as DSL or cable modem service, it is generally easier to purchase an inexpensive router or other network hardware device and use it to share access among multiple computers. This allows each computer to access the Internet independently without relying on another computer running ICS, and reduces the burden on the computer that would have been running ICS. ICS should be disabled unless it is needed.

If ICS is used, the computer running ICS should use a personal firewall such as Windows Firewall. Not only can the firewall provide protection for the ICS computer, but it can also help

---

<sup>29</sup> For more information on Wireless Auto Configuration, see the article *Wireless XP Wireless Auto Configuration*, which is available from Microsoft TechNet at <http://www.microsoft.com/technet/community/columns/cableguy/cg1102.mspx>.

to protect the computers behind the ICS from attacks by external parties. Although ICS can provide network address translation (NAT) services to other computers, which essentially hide them from public view, NAT cannot protect computers against many types of threats.

---

### 3.1.4 File Extensions and Associations

The name of a file on a Windows XP Home Edition computer can have a *file extension* that is supposed to indicate the file's type. For example, the filename "readme.txt" has a file extension of ".txt", which is intended to mean that the file is a text file. By default, if a user double-clicks on a file called "readme.txt", Windows XP Home Edition attempts to open it in Notepad, which is a text editing program. If a user double-clicks on a file called "readme.html", by default Windows XP Home Edition will assume that the file is a Web page and attempt to open it in a Web browser. The mapping between a file extension and the software that attempts to run files with that extension is known as a *file association*. By default, Windows XP Home Edition has file associations for many common types of files. Figure 3-2 shows some of the default file associations.

Although file associations are a convenient feature, they also pose some risk. For example, if a person accidentally double-clicks on a piece of malware, it is likely that the malware will be executed and attempt to infect the computer because of Windows XP Home Edition's default file associations. To prevent this, users should consider changing the default file associations for files that are most likely to be used for malicious purposes and least likely to be used for legitimate purposes. A list of these associations is presented in Appendix B. Typically, the default file associations for these programs are changed so that files of those types are opened by the Notepad application; this effectively neutralizes malicious files of those types. The Folder Options area of Control Panel allows users to alter file associations.

Users should also alter another setting in Folder Options related to filenames. By default, Windows XP Home Edition does not display mapped file extensions. Because of this, files named "readme.txt" and "readme.exe" would both be displayed to users with just the filename "readme". Attackers can take advantage of the hidden file extensions to trick users into running malicious files.<sup>30</sup> To thwart this, users should disable the **Hide file extension for known file types** setting in Folder Options, which will cause file extensions to be displayed for nearly all types of files.<sup>31</sup> This is most beneficial for users who are familiar with file extensions, but it should also help other users.

---

<sup>30</sup> Microsoft describes how malware uses this technique at [http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prkd\\_tro\\_ecgm.asp](http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prkd_tro_ecgm.asp).

<sup>31</sup> Some file extensions will continue to remain hidden from users, even when the **Hide file extension for known file types** setting is disabled. One example is shortcut files, which have a .lnk extension.

Sections 5.4.3 and 7.1.3 provide specific directions for altering the Folder Options settings.

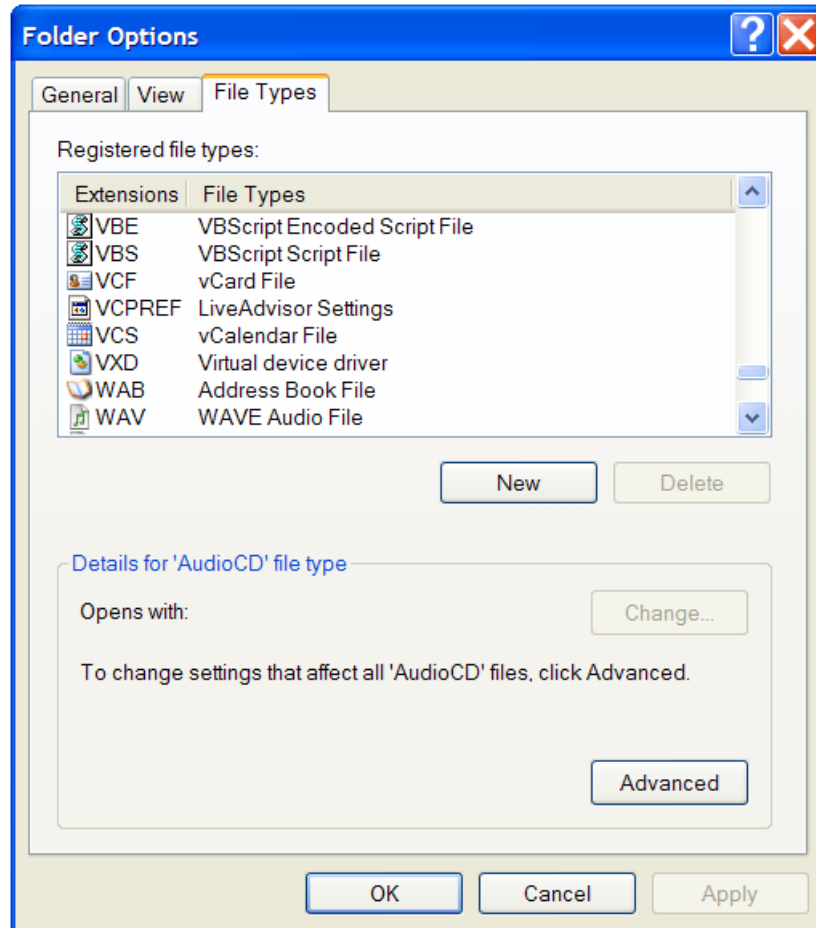


Figure 3-2. File Association Mappings

### 3.1.5 Services

By default, Windows XP Home Edition includes various built-in programs known as *services* that support the operations of the computer. Most computers do not need to use all of these services. Vulnerabilities are occasionally discovered in the services, so to reduce the possibility of successful attacks, Windows XP Home Edition computers should only have the necessary services enabled. On Windows XP Home Edition computers, the services that are the most likely candidates for being disabled are as follows:

- **ClipBook.** This service permits users to share copied text and graphics with other users. It should be disabled unless there is a specific desire to share data through the Clipbook instead of other means, such as e-mail or Shared Folders.
- **Infrared Monitor.** Some computers have infrared sensors that permit them to interact with other computers, printers, and other computing devices in close proximity without being

physically connected to each other. If there is no need to use a computer's infrared sensor, this service should be disabled.

- **NetMeeting Remote Desktop Sharing.** This service is used for online conferencing with other people through audio, video, chat, and other means. It should be disabled if it is not needed.<sup>32</sup>
- **Routing and Remote Access.** This service is only needed if the Internet Connection Sharing feature is needed, so it should be disabled if that feature is not being used.
- **Universal Plug and Play (UPnP) Device Host.** This service is used primarily to allow a Windows XP Home Edition computer to interact with UPnP-enabled consumer electronics devices connected to the same local network. Unless this functionality is needed, the UPnP service and the **SSDP Discovery Service** should both be disabled.<sup>33</sup>
- **Wireless Zero Configuration.** This service should be disabled on any computers that do not use wireless networking and enabled on any computers that do.

Appendix B.5 provides specific directions for disabling unneeded services.

---

---

## 3.2 Protecting Privacy

Windows XP Home Edition computers may contain a wide variety of sensitive user data, such as personal correspondence, financial information, and healthcare information. If more than one person may be using a computer, or the computer is at risk of being used by unauthorized people (e.g., stolen from a public place), users may be concerned about protecting the privacy of their data on the Windows XP Home Edition computer.

The primary location for user data on a Windows XP Home Edition computer is the directories where users store their files. However, data may also reside in other locations. For example, the Recycle Bin holds deleted files. If multiple people use the computer with the same shared user account, they can access each others' files in the Recycle Bin unless each person empties the recycle bin after deleting files, or the users configure Windows XP Home Edition to delete files immediately without storing them temporarily in the Recycle Bin. A disadvantage of these settings is that if a person decides later that a file should not have been deleted, it has already been purged from the computer.

The most important method of protecting privacy on a Windows XP Home Edition computer that is used by multiple people is to have each person use a separate limited user account with a password to access the computer. Each account is automatically set up with a separate personal folder (as described in Section 3.1.2), Recycle Bin, temporary directory, and other resources, as well as separate configuration settings (e.g., desktop, Web browser). Each account also has a separate history of user actions, such as recently opened files, recently accessed Web pages, and frequently used applications. This section recommends protective measures for users' Web browsers and files.

---

<sup>32</sup> More information on NetMeeting is available at <http://www.microsoft.com/windows/netmeeting/>.

<sup>33</sup> For more information on UPnP, see the article *Universal Plug and Play in Windows XP*, which is available at <http://www.microsoft.com/technet/prodtechnol/winxp/evaluate/upnpxp.msp>.

People who are installing Windows XP Home Edition or configuring new computers should consider privacy when configuring each computer and its applications. For example, every Windows XP Home Edition computer has a short text identifier known as a Computer Name. This name might be visible to other computers on the same network, which could cause privacy concerns. For example, if the computer is named after its owner, and it then joins a wireless hotspot network, other people on that network might learn the owner's name. Also, many applications ask for a user's name or initials during setup or initial use; this information might be embedded in documents without the user realizing this is occurring. Accordingly, people who are installing, configuring, or using computers and applications should keep privacy considerations in mind when supplying any personal information.

---

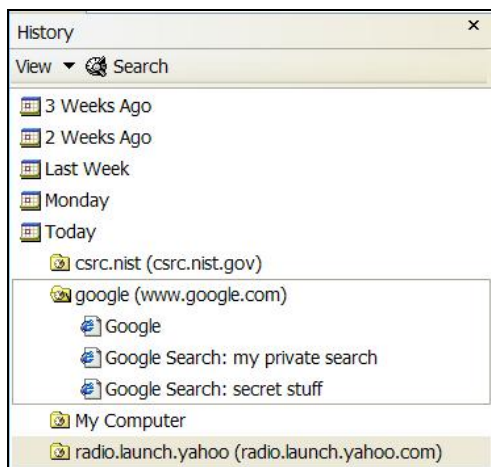
### 3.2.1 Web Browsers

Web browsers may be used to access just about any type of information imaginable on Web sites, as well as to use services such as online banking and shopping. Web browsers are also frequently used to send and receive e-mail and to use newsgroups. As part of their normal operations, Web browsers store different types of information related to using Web sites. If multiple people use a single computer, particularly using the same user account, each user might be able to gain access to Web browser usage-related information regarding the others. Web browsers store different types of information in different places, including the following:

- **History Files.** A *history file* records all the Web sites that were visited recently, generally in the last two or three weeks, and also records the individual Web pages accessed at each site. Figure 3-3 shows a history window from Microsoft Internet Explorer. (The history windows offered by other Web browsers are similar in appearance and functionality.) Users can review the Web site history manually or perform searches for keywords. On Windows XP Home Edition computers, the history file includes not only Web activity, but also the names and locations of files opened on the computer by applications such as Microsoft Word and Adobe Reader.
- **Browser Cache Files.** To make Web browsing faster, browsers store Web pages that have been accessed in a cache on the local Windows XP Home Edition computer. The next time the page is needed, the Web browser can check to make sure the local copy of the page is still current, then display the local copy instead of downloading another copy from the remote Web site. Users that can access the folder holding the cache can look at the content of the files it contains. Web browsers typically have options that allow the user to clear the browser cache, deleting all the files.
- **Cookies.** Many Web sites place cookies on users' computers; a *cookie* is a small file that stores information for a Web site. A *persistent cookie* stays on a computer to allow a Web site to identify the Web site's user. Unfortunately, if someone else uses the same user account on the computer, some Web sites that use cookies may think that the two people are really the same person. The Web sites might then allow the second person to gain access to the first person's information on the Web sites. Persistent cookies may also store sensitive information such as passwords or account numbers that could be accessed by other people using the same computer. Another type of cookie, a *session cookie*, is only valid for a single Web site session. Session cookies do not usually contain personal information. Most Web



browsers can be configured to permit all session cookies and to permit persistent cookies to be set only for the same Web site that the user visited (*first-party cookies*), not for the Web sites of advertisers and others (*third-party cookies*). This balances the preservation of users' privacy with the functionality that cookies can provide for Web site usage.



**Figure 3-3. Web Browser History Screen**

Web browsers usually offer easy ways to delete the history file entries, browser cache files, and cookies. Although this supports user privacy, it may also make the computer less user-friendly. Deleting browser cache files means that all Web pages and page elements previously accessed have to be downloaded again, which could significantly slow Web page access at first (especially for dial-up users). Deleting cookies means that Web sites forget the preferences specified by users. Erasing a history file does not simply clear the history listing; it also wipes out the list of recently visited Web sites typically shown from the Web browser's address bar. Many Web browsers attempt to preserve the privacy of individual users by storing information separately, but this might work only if each person uses a separate, password-protected user account.

Windows XP Home Edition offers a feature known as Stored User Names and Passwords.<sup>34</sup> This feature permits users to store authentication information—usernames and passwords—for remote operating systems (e.g., virtual private networking, dial-up access) and Web sites.<sup>35</sup> For example, when a user is prompted to enter a username and password to access a particular Web site, the prompt window includes a dialog box labeled **Remember my password**. If the user accepts the prompt and has the computer store the authentication information, anyone who gains

<sup>34</sup> For more information on how this is implemented in Windows XP Home Edition, and how it differs from Windows XP Professional, see MSKB article 281660, available at <http://support.microsoft.com/kb/281660/>.

<sup>35</sup> For more information, see the Microsoft article *Stored User Names and Passwords Overview* at [http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/key\\_concepts\\_overview.mspx](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/key_concepts_overview.mspx).



unauthorized access on that computer as the user (e.g., walking up to an unattended workstation) would then be able to use all resources to which the stored credential grants access.<sup>36</sup>

*Passwords should be stored only in environments in which there is a minimal physical threat, or where the password has trivial value (e.g., for a demo on a public Web site). Many Web browsers also offer the ability to store usernames and passwords, and the recommendations listed here for the Stored User Names and Passwords feature apply to Web browser password management as well.*

---

## 3.2.2 Files

People often want to share files among computers because of the convenience. However, a person typically does not want to share all of their files—for example, preventing others from accessing files containing financial records and personal correspondence. This section explains how Windows XP Home Edition computers can be configured to protect files that should remain private and share files that should be available to others. Directions on implementing these recommendations are provided in Section 5.4.3.

### 3.2.2.1 Protecting Files

As described in Section 3.1.1, having a separate user account for each person causes a My Documents folder to be created for each user. **By default, other users can see the contents of this folder.** Users can easily change this so that the contents are kept private: files placed in this folder will not be accessible by other users of the computer. Although using a private My Documents folder is a helpful measure to protect files, the files in it are still at risk. For example, if the password for the user's account is compromised, or the user uses the computer when it is infected with malware, the files could be exposed to unauthorized parties. Also, anyone with access to an administrative account on the computer can reset the password for a user account and gain access to it and its files. Windows XP Home Edition does not provide stronger mechanisms for file protection.

If protecting sensitive information in files is a concern, users should install third-party products onto Windows XP Home Edition computers to provide file encryption capabilities.<sup>37</sup> File encryption products are specifically designed to keep sensitive data private and unreadable by unauthorized users. Some products encrypt individual files and protect the files no matter where they are placed (e.g., e-mail attachment, CD-ROM). Other products encrypt many files collectively and protect each file only as part of that collection; if a file is copied or moved

---

<sup>36</sup> If any usernames and passwords have accidentally been stored, they can be removed from the **Control Panel**. Double-click on the **User Accounts** icon and click on the appropriate user account. Under the **Related Tasks** pane, click on **Manage my network passwords**. For each stored password, select it and click the **Remove** button. When all stored passwords have been removed, click **Close**, and then close the **User Accounts** window and the **Control Panel**.

<sup>37</sup> Windows XP Professional systems include the Encrypting File System (EFS), a file encryption feature. However, EFS can only encrypt files that are stored on the local Windows XP Professional system. If there is a need to protect files no matter where they are located, such as stored on CDs or e-mailed to others, then third-party encryption software would need to be used instead of EFS. Third-party encryption software is also needed if the user wants to decrypt files that were encrypted on another computer and provided to the user through e-mail, removable media, or other means.

elsewhere, it is no longer protected by encryption. Before using any third-party encryption product, users should carefully read the supporting information for the product and seek assistance from others with experience as needed. File encryption can be very effective at protecting sensitive data from access, modification, or deletion by malware and unauthorized parties, particularly for computers at high risk of theft. However, file encryption can also cause files to be inaccessible, such as a user that forgets an associated password or loses encryption keys. Also, if a computer is compromised by malware or another form of attack, then all activity on the computer might be monitored, including the decrypted files as they are used and modified by their owners, and any passwords used to encrypt or decrypt files.

*Another measure that supports the protection of information is having a separate directory for temporary files for each user. Temporary files are created by applications such as word processors as part of their normal operations, and they may contain sensitive information. If an application fails to close properly, temporary files may be left on the computer instead of being deleted automatically. To prevent users from accessing others' temporary files, each user should have a separate temporary directory. By default, Windows XP Home Edition provides a temporary directory for each user within the user profile's directory.*

### 3.2.2.2 Sharing Files

The Shared Folders feature of Windows XP Home Edition causes folders called Shared Documents and Shared Pictures to be accessible by all users on the computer, but not remote users.<sup>38</sup> This allows users to share files without sharing user accounts or permitting other users to access their personal folders.<sup>39</sup> Unfortunately, Shared Folders cannot be configured to limit access to some users; all users can read and modify all files in the shared folders. If more restrictive sharing is needed, such as permitting all users to read but not modify files, users should create their own folders and share them.<sup>40</sup> Figure 3-4 shows the available security settings for a folder. A disadvantage of using a custom share is that it cannot be set up for just local users of the computer; it must also be available to users on other computers.

The Simple File Sharing feature of Windows XP Home Edition, which is always enabled, allows only the Guest account to be used to gain access to the computer through the network. This means that attackers cannot gain remote access by guessing passwords to other accounts, such as the Administrator account.

---

<sup>38</sup> The Shared Folders feature is always enabled unless the filesystem is not formatted as NTFS.

<sup>39</sup> More information on Windows XP file sharing is available from MSKB article 304040, *How to Configure File Sharing in Windows XP*, available at <http://support.microsoft.com/kb/304040/>.

<sup>40</sup> If more restrictive sharing is needed, such as allowing only some users to have access, or allowing some users to have read access while others have read and modify access, alternate solutions need to be used. One possibility is to use a third-party encryption program that prevents access to the files without knowing a password or possessing a cryptographic key; another possibility is to store the files on removable media (e.g., flash drive, CD) and store the media in a protected place that only the appropriate people can access.

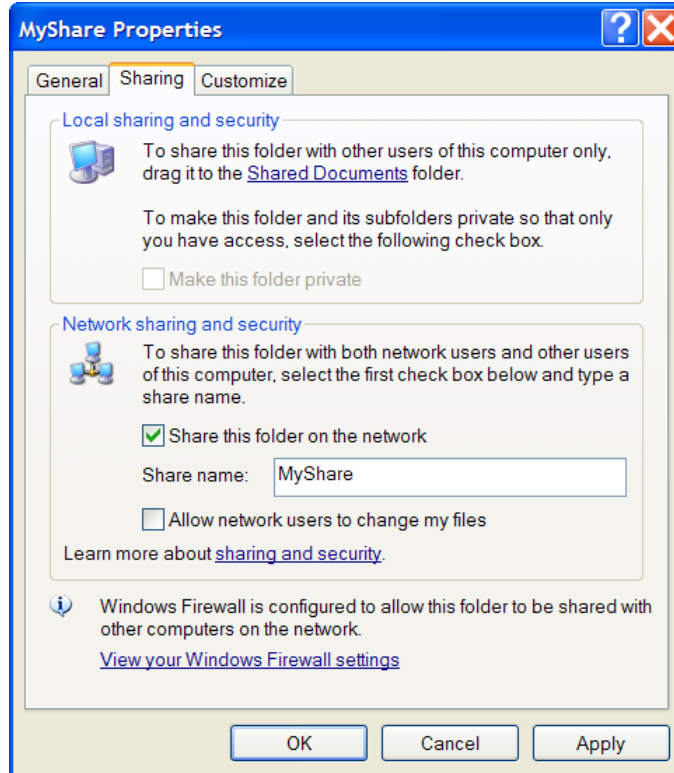


Figure 3-4. Folder Sharing Properties

---



---

### 3.3 Stopping Attacks

This section describes software and software features that are designed specifically to stop some local attacks and most network attacks against a computer, such as malware, spyware, and automated scanning and attack tools. As explained in Section 2, there is no 100% solution to computer security; although having multiple layers of defense provides a much stronger solution than a single layer of defense, it is simply not possible to thwart every single attack. Windows XP Home Edition computers should use a combination of software and software features that will stop some local attacks and most network attacks, particularly malware. Software described in this section includes antivirus software, personal firewalls, spam and Web content filtering, and popup blocking. Users can also change a few settings on common applications such as e-mail clients and Web browsers to stop some attacks.

Windows XP Home Edition has a built-in utility called the Security Center, which is shown in Figure 3-5.<sup>41</sup> It provides a single interface for the status of the computer's antivirus software, personal firewall, and Automatic Updates feature. Security Center monitors these constantly to ensure that they are enabled properly and kept up-to-date.<sup>42</sup> If Security Center detects a problem

<sup>41</sup> More information on Security Center is available from the article *Windows Security Center—Managing the State of Security*, which is available at <http://www.microsoft.com/windowsxp/sp2/wscoverview.msp>.

<sup>42</sup> Not all antivirus software and personal firewalls may be capable of providing accurate status information to Security Center. If in doubt about the status of a particular security tool, check the status provided by that tool itself.

with one of these security tools, it notifies the user at login and displays a red icon in the taskbar to alert the user of the issue. This can be very helpful to users in identifying security software misconfigurations and failures quickly.



Figure 3-5. Security Center

Although security tools can stop many attacks, users also need to practice safe computing habits. One of the most common ways that computers are attacked is by users opening and executing files from unknown and untrusted sources. Users may download these files from Web sites, file sharing services, or other means, or they may be sent to users through e-mail, instant messaging, and other communications services. These files often contain malware, and users unknowingly infect their computers by trying to use these files. Users should be very cautious about any files that are coming from unknown and untrusted sources, and it is generally prudent to avoid such files.

---

### 3.3.1 Malware Protection

The most common tool for providing protection against malware is antivirus software, which is specifically designed to detect many forms of malware and prevent them from infecting computers, as well as cleaning computers that have already been infected. Windows XP Home

Edition does not have built-in antivirus software. Because malware is the most common threat against Windows XP Home Edition computers, and antivirus software is the most effective protective measure against malware, NIST strongly recommends that every Windows XP Home Edition computer use antivirus software at all times.<sup>43</sup> Also, because antivirus software is updated frequently by vendors (sometimes more than once a day) so it can identify the latest malware threats, NIST also strongly recommends that users keep their antivirus software up-to-date.<sup>44</sup> Antivirus software cannot provide complete protection against malware threats, so users still need to follow other good computing practices to help prevent malware infections, as described in Section 7.

There are many brands of antivirus software available, which offer similar functionality. NIST recommends configuring antivirus software to use several types of functions, including the following:

- Scanning critical operating system components such as startup files, system basic input/output system (BIOS), and boot records
- Performing real-time scans of each file as it is downloaded, opened, or executed, which is known as *on-access scanning*
- Monitoring the behavior of common applications, such as e-mail clients, Web browsers, file transfer and file sharing programs, and instant messaging software
- Scanning files for known viruses. Antivirus software on computers should be configured to scan all hard drives regularly to identify any file system infections, and optionally to scan other storage media as well. Users should also be able to launch scans manually as needed, which is known as *on-demand scanning*.
- Handling files that are infected. Antivirus software can do this in two ways: *disinfecting* files, which refers to removing malware from within a file, and *quarantining* files, which means that files containing malware are stored in isolation for future disinfection or examination. Disinfecting a file is generally preferable to quarantining it because the malware is removed and the original file restored; however, many infected files cannot be disinfecting. Accordingly, antivirus software should be configured to quarantine infected files and to attempt to disinfect them.
- Logging all significant events, such as the results of scans, the startup and shutdown of antivirus software, the installation of updates, and the discovery and handling of any instances of malware

---

<sup>43</sup> Microsoft provides its Windows Malicious Software Removal Tool for Windows XP Home Edition computers. It is distributed for free along with Windows XP Home Edition updates, as described in Section 3.1.1. This tool is a form of antivirus software that looks for and attempts to remove certain common threats. Because it does not contain a comprehensive list of known malware threats, it is not a substitute for a full-fledged antivirus software program; rather, it should be thought of as a supplement. More information on the Windows Malicious Software Removal Tool is available at <http://www.microsoft.com/security/malwareremove/default.aspx>.

<sup>44</sup> Microsoft recommendations for antivirus software are available at [http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prkd\\_tro\\_ecgm.asp](http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prkd_tro_ecgm.asp).

- Automatically downloading and installing updates from the vendor daily.

Most antivirus products can identify several types of malware, including viruses, worms, Trojan horses, and malicious mobile code.<sup>45</sup> Antivirus products offer varying levels of support for detecting spyware. Separate antispyware utilities should be used to supplement any antivirus products that do not have robust spyware handling capabilities. Unlike antivirus software, which attempts to identify many types of malware, antispyware utilities specialize in both malware and non-malware forms of spyware. Although some antispyware utilities specialize in a particular form of spyware, such as browser plug-ins, most can detect many types of spyware and offer similar features to antivirus software. The same updating and configuration recommendations made earlier in this section for antivirus software also apply to antispyware utilities.

Microsoft offers a free antispyware program for Windows XP Home Edition computers. The program, Microsoft Windows Defender, has not yet been finalized, but a preliminary test version of it known as a *beta* is available until the final version is ready.<sup>46</sup> The second test version of the software, known as Beta 2, cannot detect some common forms of spyware that other antispyware programs can, such as tracking cookies. Accordingly, users should use the second beta version of the program in conjunction with another antispyware program for better overall detection of spyware.

Section 5.3.1 provides additional information on recommended malware protection practices.

---

### 3.3.2 Personal Firewalls

A *personal firewall* is a software program that monitors communications between a computer and other computers (e.g., a Windows XP Home Edition computer and computers on the Internet) and blocks communications that are unwanted. When properly configured, a personal firewall limits the access that other computers have to the Windows XP Home Edition computer through the network. This can significantly reduce the exposure of the computer to network-based attacks such as worms. A personal firewall can also be used to protect shared resources (e.g., file and print shares) on a computer. Accordingly, a personal firewall should be installed and enabled on every Windows XP Home Edition computer.<sup>47</sup> Personal firewalls should be configured to log significant events, such as blocked activity, the startup and shutdown of the firewall software, and firewall configuration changes.

Although personal firewalls are one of the most important security controls for Windows XP Home Edition computers, they can be relatively difficult to configure correctly. If a personal firewall is configured to be too restrictive, it could prevent certain user applications or Windows XP Home Edition functions from working correctly. For example, a personal firewall might

---

<sup>45</sup> A *virus* is a program that self-replicates—makes copies of itself—by infecting files and distributing copies of itself to other files, programs, or computers. A *worm* is a self-replicating program that is completely self-contained and self-propagating. A *Trojan horse* is a program that appears to be benign but actually has a hidden malicious purpose. *Malicious mobile code* is software that is transmitted from a remote computer to be run on the local computer for malicious purposes, typically without the user's explicit instruction or knowledge.

<sup>46</sup> The Microsoft Windows Defender home site contains information on the software and also makes it available for download. The site is located at <http://www.microsoft.com/athome/security/spyware/software/default.aspx>.

<sup>47</sup> Microsoft recommendations on personal firewalls are available from the *Security Guide for Small Business*, which is available for download at <http://www.microsoft.com/smallbusiness/support/security-toolkit-pdf.aspx>.



prevent the use of Microsoft file and print services. On the other hand, if a personal firewall is configured to be too permissive, it could permit attacks to compromise the computer. Users should read all personal firewall documentation carefully to gain a solid understanding of how it should be configured. If it is not clear, users should seek expert guidance on configuring their personal firewalls.

Ideally, firewalls should deny all types of communications that have not specifically been approved by the administrator or users as being permitted. This is known as a *deny by default* configuration, because all communications that are not on the exception list are denied automatically. Most firewalls can be configured to allow communications based on lists of authorized applications, such as Web browsers contacting Web servers and e-mail clients sending and receiving e-mail messages. Activity involving any other application is either denied automatically, or permitted or denied based on the user responding to a prompt asking for a decision regarding the activity. For example, if a user runs a new application that was just installed on the computer, the firewall might ask the user if it is acceptable for that application to access the Internet. To prevent malware incidents, users should configure personal firewalls as deny by default, so that they permit only the communications desired by the users.

Windows XP Home Edition includes a personal firewall called Windows Firewall.<sup>48</sup> It can be configured to restrict all inbound communications—those initiated by other computers. Windows Firewall is enabled by default for each network interface, including wired and wireless network cards, dial-up modems, and virtual private networks (VPN). When configured properly, Windows Firewall can restrict access to Microsoft networking services so that remote computers and malware cannot reach them. Windows Firewall also supports the creation of multiple firewall profiles, so that a computer used in different environments (e.g., home network, wireless hotspot) can have a different personal firewall configuration for each environment.

There are many third-party personal firewall products available that can be used instead of Windows Firewall. Some of these products offer more robust capabilities, such as filtering and blocking unauthorized outbound communications—those initiated by malicious activity (e.g., malware) on the Windows XP Home Edition computer. This is particularly helpful in detecting that a computer has been compromised. For example, if a computer is infected with a worm, it is likely that the computer will try to initiate connections to other computers to spread itself. If a properly configured personal firewall is monitoring outbound communications, it should see the worm activity and stop it, both alerting the user to the problem and preventing other computers from becoming infected. Some third-party firewalls also offer other security controls, such as popup ad blocking or Web content filtering (which are described later in this section).

Windows XP Home Edition computers should only have a single personal firewall enabled. If two or more firewalls are enabled, they are likely to interfere with each other. For example, one firewall might block activity that the other firewall has been configured to allow, or one firewall might allow activity that the other one has been configured to block. This could slow the

---

<sup>48</sup> Windows Firewall was added to Windows XP in Service Pack 2. For more information on Windows Firewall, visit [http://www.microsoft.com/windowsxp/using/security/internet/sp2\\_wfintro.msp](http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.msp). Before SP2, the built-in firewall was called the Internet Connection Firewall (ICF). For more information on ICF, read Microsoft Knowledge Base (MSKB) article 320855, *Description of the Windows XP Internet Connection Firewall*, available at <http://support.microsoft.com/kb/320855/>.

performance of the computer and cause applications to stop functioning properly, as well as weaken the computer's security.

Section 5.2.1 has more detailed information on configuring personal firewalls.

In addition to using personal firewalls, many people use a small, inexpensive device called a firewall appliance or firewall router to protect the computers on their home networks from threats outside the network. A firewall appliance performs similar functions to a personal firewall, and it can provide protection for multiple computers on a home network. Even if each computer on a home network is using a personal firewall, a firewall appliance is still a valuable additional layer of security. Should a personal firewall on a computer malfunction, be disabled, or be misconfigured, the firewall appliance can still protect the computer from unauthorized network communications from external computers.<sup>49</sup> However, in most cases the firewall appliance cannot provide any protection for communications between computers on the home network. For example, if one computer becomes infected, the firewall appliance cannot prevent the infection from spreading to other computers on the home network because it has no control over their communications. Also, firewall appliances typically do not block any communications from the home network computers to external computers, so if a home network computer becomes compromised and is used to attack other computers, a firewall appliance probably cannot stop that attack.

---

### 3.3.3 Content Filtering

*Content filtering* is the process of monitoring communications such as e-mail and Web pages, analyzing them for suspicious content, and preventing the delivery of suspicious content to users. The two most common types of content filtering are as follows:

- **Spam Filtering Software.** Spam—unsolicited e-mail—is often used to deliver spyware and other forms of malware to users. Spam is also frequently used for performing phishing attacks. Spam filtering software analyzes e-mails to look for characteristics of spam, and typically places messages that appear to be spam in a separate e-mail folder. Because spam filtering is subjective, some spam will still reach users, and some desired e-mail messages will accidentally be classified as spam. Still, spam filtering software can significantly reduce the amount of spam that reaches users, leading to a corresponding decline in spam-triggered malware incidents. Many e-mail clients also offer some helpful spam filtering capabilities. Also, some ISPs offer spam filtering services for their e-mail users; in addition to identifying previously known spam, such services can also identify new spam that is sent to many customers at the same time.
- **Web Content Filtering Software.** Web content filtering software typically works by comparing a Web site address that a user attempts to access to a list of known bad Web sites. Although the primary purpose of Web content filtering software is to prevent access to materials that are considered inappropriate, many also contain lists of Web sites that are known as hostile, such as those that attempt to distribute malware to visitors or host phishing

---

<sup>49</sup> A detailed discussion of firewall appliances is outside the scope of this publication. Guidance on home network security is provided in NIST SP 800-46, *Security for Telecommuting and Broadband Communications* (<http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf>).



Web sites. Web content filtering software might inadvertently classify benign content as inappropriate, or vice versa.

From a Windows XP Home Edition security perspective, spam content filtering technologies are strongly recommended for all e-mail use, and Web content filtering technologies can also be helpful but are considered optional. Any content filtering products that are used should be kept up-to-date so that their detection is as accurate as possible. Section 5.3.2 provides more information on configuring spam and Web content filtering software.

---

### 3.3.4 Popup Blocking

Nearly all Web browsers support the use of *popup windows*, which are standalone Web browser panes that open automatically when a Web page is loaded or a user performs an action designed to trigger a popup window. Many popup windows contain advertising, but they are increasingly being used as a way to attack computers. Some popup windows are crafted to look like legitimate system message boxes or Web sites, and can trick users into going to phony Web sites, including sites used for phishing, or authorizing changes to their computers, among other malicious actions. For example, a popup window may tell a user that the computer is infected with spyware and to click on OK to disinfect it. By clicking on OK, the user unwittingly permits spyware or other types of malware to be installed on the computer.

To control popup windows, various third-party popup blocking utilities were created. Most Web browsers also offer popup blocking capabilities. Generally, these utilities and features prevent popup windows from opening, and indicate to the user that a popup window was blocked. If the user did not want the window to be blocked, he can then choose to permit that particular popup window or to permit all popup windows from a trusted Web site. Because popup windows can be a nuisance as well as a security risk, they should be blocked by default on Windows XP Home Edition computers, either by configuring Web browser features or by using third-party utilities. Section 7.3 provides general instructions on configuring popup blocking.

---

### 3.3.5 Security Software Suites

Sections 3.3.1 through 3.3.4 have described several types of software that can be helpful for protecting Windows XP Home Edition computers. Originally, each type of software was created as a separate, standalone product. As users needed to acquire more security products for their computers, vendors began creating security software suites that incorporate several types of security software in a single integrated product. For example, several vendors offer suites that include antivirus software, antispyware software, a personal firewall, a Web browser popup blocker, spam filtering, and Web content filtering. Some suites offer additional functions, such as managing Web browser cookies and identifying potential privacy issues within Web pages and e-mails.

Suites offer a few advantages over purchasing components separately. Generally, a suite costs much less than the individual components would. It is also more convenient to purchase and install a single product than several separate products. Updating and maintaining a suite is also simpler and quicker than doing so for several products. Another advantage of using a suite is that conflicts or incompatibilities between components are unlikely; when separate products are

used on the same computer, problems between products are more likely. The primary disadvantage of using a suite is that one or more suite components might not be as effective, easy to use, full-featured, or efficient as competing standalone products. However, in many cases, suites are easier to use than individual products because all suite components have the same user interface.

---

### 3.3.6 Application Configuration

Many attacks, particularly malware, take advantage of features provided by common applications such as e-mail clients, Web browsers, instant messaging clients, and office productivity suites. By default, applications often are configured to favor functionality over security. Accordingly, users should consider disabling unneeded features and capabilities from applications, particularly those that are commonly exploited by malware. Users should also consider configuring applications to filter content and stop other activity that is likely to be malicious. Examples of application settings to consider in malware incident prevention are listed below. Users should be aware that a single computer might have multiple Web browsers, e-mail clients, instant messaging clients, and office productivity suites installed, each of which may have different features and configuration settings. More details on configuration settings are available in Section 7.

#### 3.3.6.1 Web Browsers

- **Restricting Web browser cookies.** See Section 3.2.1 for additional information.
- **Preventing software installation within Web browsers.** Some Web browsers can be configured to prompt the user to approve the installation of software such as Web browser plug-ins. Some browsers can even prevent Web sites from installing software on the client. These settings are particularly helpful for preventing the installation of spyware within Web browsers.
- **Limiting mobile code execution.** Most Web browsers can be configured to allow, limit, or deny the use of certain types of mobile code (e.g., JavaScript, ActiveX, Java). Mobile code is a way for a remote computer, such as a Web site, to run programs on a user's local Windows XP Home Edition computer. Although limiting or denying mobile code use can provide stronger security, typically this interferes with needed Web browser functionality.
- **Blocking popup windows.** See Section 3.3.4 for information on this.

#### 3.3.6.2 E-Mail Clients

- **Preventing automatic loading of e-mail images.** Most e-mail clients can be configured not to load graphics contained within e-mails automatically. This is particularly helpful for thwarting e-mail-based Web bugs. With this configuration setting, the outline of an unloaded Web bug appears as a small box within the e-mail, and the user's activity cannot be tracked unless the user chooses to have the image loaded.
- **Limiting mobile code execution.** Most e-mail clients can be configured to permit only the required forms of mobile code. This can be effective at stopping some instances of malicious mobile code.

- **Setting default message reading format and sending format to plain text.** Most e-mail clients allow users to specify the default format for reading and sending e-mails. The most commonly used formats are plain text and HTML. Because malware, phishing, and other types of attacks often take advantage of features offered by HTML, it is preferable to set the default message format to plain text. This will cause e-mails to be displayed as text only, which means that pictures, hyperlinks, and other content provided through HTML are omitted or displayed only through alternative text. Also, sending e-mails as plain text is helpful to other users who are security-conscious and prefer to read e-mail messages in plain text.
- **Disabling automatic opening of e-mail messages.** Some e-mail-based malware may be activated and infect a computer when the malicious e-mail is opened. Many e-mail clients can be configured to open e-mail messages automatically. This can provide an easy way for malware to infect a computer. Accordingly, e-mail clients should be configured not to open e-mail messages automatically. This gives users an opportunity to identify and delete an e-mail that appears to be suspicious based on the sender, recipient, subject, and other identifying information that can be reviewed without opening the e-mail.
- **Enabling spam filtering.** Section 3.3.3 has additional information on this.

### 3.3.6.3 Instant Messaging Clients

- **Suppressing the display of e-mail addresses.** If the user's displayed name or supporting information includes an e-mail address, this may be harvested by malware or malicious users, then used in future attacks.
- **Restricting file transfers.** If the software can transfer files with other instant messaging users, it should be configured to prompt the user before permitting a file transfer to begin. File transfers are a common way to transfer malware to other computers and infect them.

### 3.3.6.4 Office Productivity Suites

- **Restricting macro use.** Applications such as word processors and spreadsheets often contain macro languages; macro viruses take advantage of this. Most common applications with macro capabilities offer security features that permit macros only from trusted locations or prompt the user to approve or reject each attempt to run a macro. The prompting feature can be very effective at stopping macro-based malware threats.
- **Limit personal information.** Many office productivity tools allow personal information, such as name, initials, mailing address, and phone number, to be stored with each document created. Although the most basic information (typically, name and initials) are often needed for collaboration features and edit tracking, information such as mailing addresses and phone numbers is not. Personal information becomes embedded within document files and may inadvertently be distributed with files to others. If privacy is a concern, then users should not enter any more personal information than necessary into the user settings of office productivity tools.
- **Use secured folders for application files.** Most office productivity applications allow users to define default locations for saving documents and holding temporary files, including auto-

save and backup copies of documents. This can be very helpful at protecting application files from unauthorized access by others. Users should also store their custom dictionary entries in a user-specific file stored in one of their protected folders.

---

### 3.3.7 Data Execution Prevention

Windows XP Home Edition offers a feature known as Data Execution Prevention (DEP). When enabled, this feature prevents software on the computer from performing certain actions that could cause problems. For example, DEP could stop certain types of malware from successfully infecting a computer. Different computers offer varying levels of support for DEP based on their processors. Because DEP limits what software can do, unfortunately there might be occasional conflicts between DEP and certain applications, causing those applications to malfunction. Accordingly, users should consider enabling DEP on their computers, and if DEP is enabled, users should monitor their computers for application conflicts and disable DEP if necessary. Appendix B.1 contains instructions for configuring DEP.

---

---

## 3.4 Preserving Data

A Windows XP Home Edition computer could stop functioning properly or have corrupted data due to several causes, including the following:

- Attack against the computer, such as malware
- Hardware, software, or power failure<sup>50</sup>
- Natural disaster, such as a fire or flood
- Human error.

To ensure that user data is available after an unfortunate event, users or administrators should periodically duplicate data from Windows XP Home Edition computers onto another medium, such as a CD-ROM or flash drive. This process is known as a *backup*. Transferring the data from the medium back to the computer is known as a *restore*. User data should be backed up periodically, such as weekly or monthly. Administrators may also wish to back up the Windows XP Home Edition files themselves occasionally, to assist in rebuilding the computer should Windows XP Home Edition need to be reinstalled. Users or administrators should also verify periodically that backups can be restored successfully; backing up a computer regularly may not be beneficial if the backups are corrupt or the wrong files are being backed up. Because backups may contain sensitive user data, backup media should be properly protected to prevent unauthorized access.

There are several options for performing backups and restores on Windows XP Home Edition computers. This section describes each option; additional details on implementing them are available in Section 4.2.

---

<sup>50</sup> An uninterruptible power supply (UPS) and surge protection device can provide temporary emergency battery power when the utility-provided power is unavailable.

---

### 3.4.1 Backup or Restore Wizard

Windows XP Home Edition CDs contain a program called the Backup or Restore Wizard. Although this program is not installed as part of Windows XP Home Edition by default, it is available to all Windows XP Home Edition users. The Backup or Restore Wizard automates most of the backup and restore processes. For example, during a backup the user is presented with several options, including backing up the current user's files and settings, backing up all users' files and settings, and backing up the whole computer. This allows the user to back up data and operating systems without having to manually indicate which files and directories should be backed up, if the user's files are where the backup program expects them to be. When a backup is performed, the result is a .bkf file (Backup.bkf by default). As the name indicates, the Backup or Restore Wizard can also be used to restore a backup from a .bkf file.

If a full backup is performed, the Automated System Recovery Wizard will prompt the user to insert a floppy disk, which is intended to be turned into a recovery disk that could be used with the .bkf file to restore the computer in case of failure. However, even though creating this recovery disk appears to be feasible, Automated System Recovery is not fully supported by Windows XP Home Edition.<sup>51</sup> It may be possible to create the recovery disk, but Windows XP Home Edition does not allow it to be used to recover the system from a failure. Therefore, the Automated System Recovery Wizard and other Windows XP Home Edition features and options related to Automated System Recovery should not be used.

When the Backup or Restore Wizard is run, it presents an option to select Advanced Mode.<sup>52</sup> This switches to the Backup Utility interface, which is not as user-friendly but provides greater customizability and more features. For example, the Backup Utility can be used to schedule backups. In general, only the most technically adept users and administrators are more likely to use the Backup Utility mode, while others are more likely to use the Backup or Restore Wizard mode.

---

### 3.4.2 Files and Settings Transfer Wizard

Another utility included with Windows XP Home Edition is the Files and Settings Transfer Wizard.<sup>53</sup> The wizard can back up files and settings for Windows XP Home Edition and applications. Examples of settings the wizard can back up include network configurations, desktop settings (e.g., wallpaper, screen resolution), e-mail client configuration, and Web browser bookmarks. The wizard can save the files and settings to removable media or a shared folder on another computer on the network.

---

<sup>51</sup> For more information, see MSKB article 302700 at <http://support.microsoft.com/kb/302700/>.

<sup>52</sup> For more information on Advanced Mode, see MSKB article 308422, *How to Use Backup to Back Up Files and Folders on Your Computer in Windows XP*, available at <http://support.microsoft.com/kb/308422/>, and article 309340, *How to Use Backup to Restore Files and Folders on Your Computer in Windows XP*, available at <http://support.microsoft.com/kb/309340/>.

<sup>53</sup> For more information, see the "Migrating to a Clean Installation of Windows XP" section of the *Step-by-Step Guide to Migrating Files and Settings*, available at <http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/mgrtfset.mspx>.

Unlike the Backup or Restore Wizard, the Files and Settings Transfer Wizard can only back up data for a single user at a time, and it cannot make a backup of the whole computer. In case of computer failure, a user would need to reinstall Windows XP Home Edition and all needed applications, in addition to restoring all users' backups performed by the Files and Settings Transfer Wizard. An advantage of using the Files and Settings Transfer Wizard is that it should require much less media storage space than the Backup or Restore Wizard.

---

### 3.4.3 Third-Party Backup and Restore Utility

There are various third-party utilities, known as backup utilities or drive imaging utilities, for backing up and restoring files and operating systems. If a third-party utility is to be used, it is important to first verify that it can properly back up and restore Windows XP-specific resources, such as the Windows registry, which stores configuration information for Windows XP Home Edition, applications, and users. The Backup or Restore Wizard built into Windows XP Home Edition uses a *shadow copy* backup technique when possible, which means that it essentially takes a snapshot of the computer and then perform a backup on that snapshot. This avoids problems with attempting to back up files that are currently in use, also known as *open files*. Third-party backup utilities used on Windows XP Home Edition computers should have good mechanisms for handling open files.

---

### 3.4.4 Third-Party Remote Backup Service

Commercial vendors offer remote backup services over the Internet. Users typically install an agent program on their Windows XP Home Edition computers and configure the agent to back up their data periodically over the Internet to remote storage. The use of such services is usually practical only for users with high-speed Internet connections. Because users are entrusting the security of their data to the remote backup service provider, users should research the security precautions performed by the provider, and should consider using third-party file encryption software on their computers to protect any sensitive information before sending it to the remote backup service provider.

---

### 3.4.5 File Copy to Media

In the simplest cases, no utility may be needed at all to perform a backup. For example, if a computer contains a few folders with data that should be backed up, and users do not want to have their custom settings preserved, it should be sufficient to copy files onto a writable CD or DVD, flash drive, or other removable media. Should the computer be damaged or require Windows XP Home Edition to be reinstalled, this backup method would preserve only those files specifically copied to the media. This backup method also relies on users to be aware of exactly where all of their files are located on the computer.

---

---

## 3.5 Summary

Security protections are measures that thwart threats. Windows XP Home Edition computers should be secured using a combination of technical and operational protections, such as antivirus software, Windows XP Home Edition configuration settings, and user education and security

awareness activities. Because new vulnerabilities in software are discovered on an ongoing basis, security protections should be updated on a regular basis.

One of the most important parts of securing a Windows XP Home Edition computer is eliminating known weaknesses, because attackers could attempt to take advantage of them. Five categories of methods for eliminating weaknesses are as follows:

- Limiting access to the computer through separate password-protected user accounts for each person, with different accounts for administrative and daily tasks (a limited user account)
- Applying software updates to the computer on a regular basis, including Windows XP Home Edition and software applications
- Limiting network access by disabling unneeded networking features, limiting the use of remote access utilities and Internet Connection Sharing, and configuring wireless networking securely
- Modifying default file associations and the display of default file extensions
- Disabling services that are not needed.

Another concern in securing a Windows XP Home Edition computer is protecting the privacy of user data, such as personal correspondence and financial information. The most important method of protecting privacy is to have each person use a separate password-protected user account. Each account has a separate personal folder, Recycle Bin, temporary directory, and configuration settings. The personal folder and the files within it can be protected from access by other users of the computer. Users can also share files with each other, including users on other computers on the local network.

Another important component of Windows XP Home Edition security is using a combination of software and software features that are designed specifically to stop attacks, particularly malware. Every Windows XP Home Edition computer should use antivirus software, antispyware software, and a personal firewall at all times, and they should be kept up-to-date. Other helpful software includes spam and Web content filtering and popup blocking. Users can also change settings on common applications such as e-mail clients, Web browsers, instant messaging clients, and office productivity suites to stop some attacks.

Users or administrators of a Windows XP Home Edition computer should periodically duplicate data from the computer onto another medium, such as a CD-ROM or flash drive. This process, known as a backup, helps to ensure that user data is available after an unfortunate event such as an attack against the computer, a hardware failure, a natural disaster, or human error. User data should be backed up periodically, such as weekly or monthly. There are several options for performing backups on Windows XP Home Edition computers, including utilities built into Windows XP Home Edition, and third-party utilities and remote backup services.

The five most important protections that should be used for Windows XP Home Edition computers connecting to the Internet are as follows:

- Using a personal firewall that is configured to restrict incoming network activity to only that which is required
- Using a limited user account for typical daily use of the computer
- Running up-to-date antivirus software and antispyware software that is configured to monitor the computer and applications often used to spread malware (e.g., e-mail, Web) and to quarantine or delete any identified malware
- Applying updates to the operating system and major applications (e.g., e-mail clients, Web browsers) regularly, preferably through automated means that check for updates frequently
- Performing regular backups so that data can be restored in case an adverse event occurs.



## 4. Installing Windows XP Home Edition

This section of the guide provides guidance and step-by-step instructions for installing Windows XP Home Edition. This guide assumes that Windows XP Home Edition is being installed or reinstalled on the computer, which means that all existing operating system settings, applications, and data on the computer are destroyed unless first backed up to removable media or otherwise preserved. The alternative to performing a full installation is doing an upgrade of the existing operating system (e.g., Windows 98, Windows Millennium Edition [ME]).<sup>54</sup> Upgrading an existing computer can result in different security configuration settings than the default Windows XP Home Edition settings; as a result, using the advice in this guide on an upgraded computer may be inappropriate and could possibly cause problems. Also, the instructions in this section should not be used on any computer that is or will be dual booting, which means that a single computer has another operating system installed in addition to Windows XP Home Edition (e.g., Linux, Unix, another version of Windows).

If the computer has been used previously, it may contain user data (e.g., e-mails, documents), application configuration settings (e.g., Web browser bookmarks), or other information that needs to be preserved before Windows XP Home Edition is installed or reinstalled onto the computer. In that case, the person performing the Windows XP Home Edition installation should follow a five-phase process:

1. **Prepare for the Installation.** This involves basic preparatory actions, such as gathering the software media and documentation that will be needed for the installation.
2. **Back Up Data and Configuration Files.** This focuses on the transfer of user data and configuration settings from the computer to external media, such as CD-ROMs or flash drives.
3. **Install Windows XP Home Edition.** This is the actual installation of Windows XP Home Edition.
4. **Secure the Computer.** This involves performing various actions to secure Windows XP Home Edition, such as applying service packs and software updates.
5. **Restore Data and Configuration Files.** This causes the user data and configuration settings that were backed up during phase 2 to be transferred back to the computer.

If there is no need to preserve data and configuration settings from the existing computer, the user should omit phase 2 (Back Up Data and Configuration Files) and phase 5 (Restore Data and Configuration Files).

---

<sup>54</sup> It is not possible to upgrade certain versions of Windows, such as Windows 95 and Windows 2000, to Windows XP Home Edition.

---

---

## 4.1 Prepare for the Installation

The first thing the user should do is perform some simple preparatory steps, as follows:

1. Determine which software applications (and versions of each) are installed on the computer. These may include Web browsers, e-mail clients, office productivity tools (e.g., word processors, spreadsheets), instant messaging software, multimedia utilities (e.g., audio and video players), graphics tools, and security software (e.g., antivirus software, personal firewall). The two primary ways of identifying the installed applications are as follows:
  - From the **Control Panel**, run the **Add or Remove Programs** utility. It shows which software applications, security updates, hardware drivers, and other types of programs are installed on the computer.
  - Review the folders and icons on the Start Menu and the Desktop, in particular the All Programs shortcut on the Start Menu, to find application shortcuts listed there.
2. Document critical settings for the OS and applications. This should include any information needed to connect to the user's Internet Service Provider (ISP), as well as usernames or server names or addresses for applications. Examples are as follows:
  - Network configuration information from an ISP, if the ISP does not provide this information automatically when the computer connects. Examples of network configuration information include a statically assigned IP address for the computer, default gateway IP address, and DNS server names or addresses.
  - E-mail server names stored in e-mail clients.
  - Usernames or nicknames used for e-mail, instant messaging programs, and other applications.
3. Gather the necessary software.<sup>55</sup> This usually includes, but is not limited to, the following:
  - Windows XP Home Edition CD and the Product Key (a series of letters and numbers in the format XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)<sup>56</sup>
  - Windows XP service packs on CD, if Internet connectivity is low-bandwidth (e.g., dial-up modem). Microsoft provides Windows XP Service Pack 2 on CD for free.<sup>57</sup>

---

<sup>55</sup> Only copies of Windows XP Home Edition that are properly licensed for the computer should be used. For more information on Windows XP Home Edition licensing, visit Microsoft's Software Piracy Protection Web site at <http://www.microsoft.com/piracy/default.mspx>.

<sup>56</sup> Some computer vendors do not provide a Windows XP Home Edition CD to their customers. One common alternative is to provide a system CD that installs Windows XP Home Edition and various third-party applications. Using such a system CD involves using the vendor's instructions in place of portions of the directions presented in Section 4.3. Some computer vendors do not provide operating system CDs with their computers; instead, the computer has software on its hard drive with which the user can create a system CD. Also, some vendors' versions of Windows XP Home Edition CDs do not include Product Keys.

- CDs, DVDs, floppy disks, and other media provided by the computer manufacturer and hardware add-on manufacturers (e.g., printers, scanners, digital cameras)
  - CDs, DVDs, floppy disks, and other media for the software applications identified in step 1
4. Gather the documentation for the computer and hardware and software added onto the computer, in case any issues arise during the installation.
  5. Acquire media, such as blank writable CDs or DVDs, an external backup disk drive, or flash drives, that can be used for backing up data and configuration files, if needed.

---



---

## 4.2 Back Up Data Files and Configuration Settings

This step involves backing up any information that needs to be preserved from a previously used computer. (If the computer is new or does not contain any needed information, skip to Section 4.3.) Choose a backup method based on the information presented in Section 3.4, then perform the following steps:

1. Find the needed files and/or configuration settings to be backed up.
2. Transfer the files to media and verify the backup using the chosen method:
  - a. Backup or Restore Wizard
    - i. By default, the backup utility is not installed with Windows XP Home Edition. Before performing a backup for the first time, the user needs to load the backup utility onto the computer. This can be done using the following steps:
      1. Insert the Windows XP Home Installation CD into the CD drive.
      2. **Open My Computer.** Right-click on the CD-ROM drive and select **Explore**. Find the file located at `\VALUEADD\MSFT\NTBACKUP\NTBACKUP.msi`. Double-click it.
      3. The backup utility installation wizard should begin.
      4. When the wizard is complete, click **Finish**.
    - ii. Go to **Start**, then **All Programs**, and choose **Accessories**. Next, select **System Tools**, and click on the **Backup** icon. This should launch the Backup or Restore Wizard.
    - iii. Click the **Advanced Mode** link. Click on the icon for **Backup Wizard (Advanced)**, then click **Next**.

---

<sup>57</sup> Ordering information is provided at [http://www.microsoft.com/windowsxp/downloads/updates/sp2/cdorder/en\\_us/default.mspx](http://www.microsoft.com/windowsxp/downloads/updates/sp2/cdorder/en_us/default.mspx).

- iv. The **What to Back Up** window appears, asking the user what should be backed up:

The **Back up everything on this computer** option can be used by a person logged in with an administrator account to create a backup of all users' data.

The **Back up selected files, drives, or network data** option requires someone to specify exactly which files and folders should be backed up. This option should only be used by someone who knows where all data is located.

The **Only back up the System State data** option backs up the Windows Registry, system boot files, and other information that should not be transferred to the new Windows XP Home Edition installation, so this backup option should not be used when rebuilding the computer.

Choose the appropriate option and click **Next**. If the **Back up selected files, drives, or network data** option was specified, then choose which data should be backed up and click **Next** when done.

- v. The **Backup Type, Destination and Name** window appears. Select a place to store the backup, such as a writable CD, and specify a name for the backup. Click the **Next** button.
  - vi. Click the **Advanced** button to specify backup options.
  - vii. Select the **Normal** backup type, and then click the **Next** button.
  - viii. Choose the **Verify data after backup** option, and then click the **Next** button.
  - ix. Choose to **Replace the existing backups** and click **Next**.
  - x. Select **Now** to perform the backup now.
  - xi. Confirm that the settings are correct and click the **Finish** button to start the backup.
  - xii. Once the backup is complete, click the **Close** button.
- b. Files and Settings Transfer Wizard<sup>58</sup>
    - i. Click on **Start**, then **All Programs**. Choose **Accessories**, then **System Tools**. Select the **Files and Settings Transfer Wizard**, then click **Next**.
    - ii. Select **Old computer** to capture the current settings.

---

<sup>58</sup> This backup method is generally not preferred because it does not provide a simple way for the user to verify the integrity of the backup.

- iii. Choose **Other** and select a location to store the files and settings to removable media, such as a CD-RW. Then click **Next**.
  - iv. Choose to back up **Both files and settings**, then click on **Next**.
  - v. The wizard backs up the files and settings. Click on **Finish** when it is done. It creates a folder with a large file (all the files and settings bundled together) and a very small status file.
- c. Third-Party Backup and Restore Utility
- i. Run the utility and perform the backup based on the utility vendor's documentation.
  - ii. Using features provided by the utility, verify the integrity of the backup.
- d. Third-Party Remote Backup Service
- i. Perform the backup using the remote backup service's software and directions.
  - ii. Verify the integrity of the backup using features provided by the remote backup service.
- e. File Copy to Media
- i. Select the files to be backed up, and drag them onto the media. Alternately, copy the files to be backed up, and paste them onto the media. Perform this as many times as needed to back up the files to be preserved.
  - ii. Verify the integrity of the backup by accessing a sample of files on the media and ensuring that they are undamaged.
3. Perform an antivirus scan on the media to ensure that it does not contain any malware. Consult the antivirus software documentation for instructions on how to do this.
4. Safeguard the media. The media should be kept in a proper physical location. The media should be protected from environmental threats such as water and excess heat. Also, if needed, the media should be protected from unauthorized physical access by locking it up.

---

---

### 4.3 Install Windows XP Home Edition

After performing any needed backups, the next step is to install Windows XP Home Edition.<sup>59</sup> This section provides recommendations and step-by-step instructions for doing so, focusing on the settings that have security implications. Because every computer is different, the exact steps for installing Windows XP Home Edition may vary from the ones listed in this section. Users should consult their Windows XP Home Edition documentation, the Microsoft Web site, or Windows XP Home Edition experts whenever in doubt as to what actions to perform.

Because the computer is unsecured and vulnerable to exploitation through networks during installation, the computer should be disconnected from all networks before the installation begins.<sup>60</sup>

- If the computer uses broadband (e.g., DSL, cable modem) or is part of a wired home network, disconnect from the computer the cable that provides its network access.
- If the computer uses a wireless network, no action is necessary because the process of installing Windows XP Home Edition will effectively cause wireless networking to be unconfigured. (By default, a new installation of Windows XP Home Edition will not automatically join any wireless networks.)
- If the computer uses dial-up (i.e., phone line and modem), no action is necessary because the installation process will not try to use the modem.

The first part of the installation process is to load and start the Windows XP Home Edition CD. This can be done using the following steps:

1. Place the Windows XP Home Edition CD into the CD-ROM drive.
2. Restart the computer. A BIOS message might appear that says to press any key to boot from the CD.<sup>61</sup> If so, press any key while the message is displayed to start the boot.
3. Windows Setup should open and load files. When the screen titled **Windows XP Home Edition Setup** appears, press **Enter** to begin the setup.
4. The Windows XP Licensing Agreement should be displayed. Review it and press the **F8** key if it is acceptable.

---

<sup>59</sup> The instructions in this section are based on the assumption that the user has a standard Windows XP Home Edition CD, and not a system CD provided by the computer's manufacturer. More information on system CDs is provided in Section 4.1.

<sup>60</sup> The computer should not be connected to any network until the installation has been completed and initial security measures have been implemented.

<sup>61</sup> If the computer does not boot from the CD, then the computer might not be configured to boot from CD-ROM before other media, such as the hard drive or floppy drive. Consult the computer's hardware documentation for instructions on how to alter its BIOS settings so that the computer will boot from the CD-ROM drive before the floppy drive or hard drive. It is also possible that the Windows XP Home Edition setup program does not recognize the CD-ROM drive. In that case, it may be necessary to create a set of boot floppy disks. Consult the vendor documentation for more information on this.

The next part of the process involves wiping out the information already on the computer's hard drive. Steps for doing this are as follows:

1. If a previous Windows XP installation is detected, it will be reported. Press the **Esc** key to install a new copy rather than updating the existing copy.
2. The next decision is which hard drive partition Windows XP Home Edition should be loaded onto. On most computers, this is the C:\ partition. Highlight the correct partition and press **Enter**. If there are multiple old partitions from a single physical drives, these can be deleted by pressing **D**, then a new partition created by pressing **C**.
3. If a warning appears that there is already another operating system on the partition, confirm that the correct partition has been selected, then press **C** to continue loading Windows XP Home Edition.
4. The next decision is which file system should be used, File Allocation Table (FAT) or NT File System (NTFS). NTFS offers security features that FAT does not, so unless there is a specific reason why FAT needs to be used, select the **Format the partition using the NTFS file system (Quick)** option and press **Enter**. If the hard drive has been in use for a while and has a lot of data on it, it might be preferable to select the **Format the partition using the NTFS file system** option (without the "Quick"). This will perform a full format, wiping all data from the drive. This could take between several minutes to an hour depending on the size of the hard drive.<sup>62</sup>
5. If asked, press **F** to initiate the formatting. (This question is only displayed if the hard drive has existing data on it.)

Once the drive has been formatted, Windows XP Home Edition will be installed onto the computer. This will typically take between several minutes and a few hours, depending on the computer's hardware. The user is next prompted to make certain basic configuration choices, as follows:

1. The **Regional and Language Options** window appears. Make any desired changes and click **Next** when done.
2. The **Personalize Your Software** window appears. A name must be entered; the organization name is optional. When done, click **Next**.
3. The **Product Key** (a series of letters and numbers in the format XXXXX-XXXXX-XXXXX-XXXXX-XXXXX) must then be entered. It is usually found on or with the packaging containing the Windows XP Home Edition CD. After entering, click **Next**. (Note that some vendor-specific versions of Windows XP Home Edition may not require a product key to be entered, and will skip this step.)

---

<sup>62</sup> For more information on NTFS and FAT, see *NTFS vs. FAT: Which Is Right for You?*, which is available at [http://www.microsoft.com/windowsxp/using/setup/expert/russel\\_october01.msp](http://www.microsoft.com/windowsxp/using/setup/expert/russel_october01.msp).

4. The **What's your computer's name?** window appears. Type in a generic name for the computer that does not use personal information or describe the physical location. Do not use the automatically generated name. Click **Next** when done.
5. The **Modem Dialing Information** window appears next if Windows XP Home Edition recognizes a modem in the computer. If so, enter the requested dialing information. Even if the modem is not going to be used, the area code still needs to be entered so that the setup process can continue. After doing so, click **Next**.
6. The **Date and Time Settings** window appears. Set the correct date, time, time zone, and daylight saving settings. Once set, click **Next**.
7. The **Networking Settings** window appears. Select **Custom settings** and click **Next**.
8. In the **Networking Components** window, unselect the check box for **QoS Packet Scheduler**. Also unselect the check box for **File and Printer Sharing for Microsoft Networks** unless this computer will be sharing its files or printers with other computers on the local network. If the computer will not be using shared folders or printers from other computers on the local network, also unselect the check box for **Client for Microsoft Networks**. When done, click on **Next**.

After the initial configuration is complete, the computer will reboot. If prompted to press a key to boot from CD, do **not** press a key. Windows XP Home Edition will be launched. Once the reboot has been completed, additional configuration settings need to be made, as follows:

1. Click on **Next** to start the configuration process.
2. If the CD included Windows XP Home Edition Service Pack 2, the next screen asks if Automatic Updates should be enabled. This setting is configured later in the instructions, so at this time choose the **Not right now** option and click **Next**.
3. Choose the option that reflects how the computer will first connect to the Internet:
  - **Telephone modem**. Settings will be entered later in the configuration process.
  - **Digital subscriber line (DSL) or cable modem**. The next screen that appears asks the user whether or not a username and password is needed to connect to the Internet. This is different from an e-mail username and password; some DSL and cable modem providers supply a separate username and password just to get Internet access. If a username and password are required, enter them.<sup>63</sup>
  - **Local area network (LAN)**. Settings will be entered during the next step.
4. If **Digital subscriber line (DSL) or cable modem** or **Local area network (LAN)** was selected in the previous step, perform the following steps to enter the network settings:

---

<sup>63</sup> For DSL access, the DSL username and password are usually cached on the DSL router. For cable modem access, the cable modem's MAC address is typically used to authenticate to the cable provider network, so no username and password are required.



- a. If the ISP or a local device (e.g., firewall appliance) issues an IP address to the computer automatically (usually through the Dynamic Host Configuration Protocol [DHCP]), check the **Obtain IP automatically** box. Otherwise, enter the static IP address assigned to the computer, along with the corresponding subnet mask and default gateway settings.
  - b. If the ISP or a local device issues DNS server addresses to the computer automatically (usually through DHCP), check the **Obtain DNS automatically** box. Otherwise, enter the IP addresses for the primary and alternate DNS servers. The primary DNS server address is required, and the alternate DNS server address is optional.
  - c. Click **Next** to continue.
5. The next screen prompts the user to register Windows XP Home Edition. Because the computer is not yet network-connected, registration cannot be performed at this time. Select the **No, remind me every few days** option and click on **Next**.
  6. The next screen that appears is the Internet access setup screen. Select **No, not at this time** and click **Next**.
  7. At least one user account must be created during the configuration process. Any accounts created at this time will have administrative privileges, so only one account should be added now. Once the computer is fully secured, other accounts can be created. Enter a username for the computer's administrative account in the **Your name** box, then click **Next**.
  8. The installation of Windows XP Home Edition is complete. Click **Finish**.

Windows XP Home Edition should open with the user account that was just created.<sup>64</sup>

---

---

## 4.4 Secure the Computer

The next step in the installation process is to secure the computer. The user should do this immediately, based on the detailed guidance presented in Section 5. The major steps in securing the computer are as follows:

1. Perform preparatory actions, such as gathering software media and documentation.
2. Apply updates to Windows XP Home Edition, and configure it to update itself automatically in the future.
3. Install and configure additional security software, such as antivirus software and a personal firewall.
4. Alter the default Windows XP Home Edition configuration to further improve security.

---

<sup>64</sup> This account will be assigned a strong password during the execution of the steps described in Section 4.4.

5. Document the installed software applications for future use in troubleshooting problems.

Once the computer has been secured, the users should configure each user account and the folders and applications to improve their security, as described in Section 7. This should result in a reasonably well-secured computer that is ready to be used.

---

---

## 4.5 Restore the Data Files and Configuration Settings

The final step in the Windows XP Home Edition installation process is to restore previously backed up data files and configuration settings, if needed.<sup>65</sup> When restoring settings from backups, users should be very careful about overwriting existing settings on the computer. For example, old application settings may be insecure; restoring them onto the computer could inadvertently affect the security of the application, which in turn could reduce the security profile of the computer. Users should also be aware of differences in directory structures; some versions of Windows have used different directories for holding files. Consequently, it may be necessary to restore file backups to different directories so that files are in the proper locations.

To restore data files or configuration settings that were backed up using the directions in Section 4.2, perform the following steps:

1. Retrieve the media that contains the backup.
2. Transfer the files and settings from the media to the Windows XP Home Edition computer using the chosen method:
  - a. Backup or Restore Wizard
    - i. Go to **Start**, then **All Programs**, and choose **Accessories**. Next, select **System Tools**, and click on the **Backup** icon. This should launch the Backup or Restore Wizard.
    - ii. Click the **Next** button. Select **Restore files and settings**, then click the **Next** button.
    - iii. The **What to Restore** window appears, asking the user which backup file to restore. Select the backup file to restore and click the **Next** button.
    - iv. Click the **Finish** button to restore the files that were backed up.
    - v. Once the restore is complete, click the **Close** button.
  - b. Files and Settings Transfer Wizard

---

<sup>65</sup> Data files should not be restored until antivirus software and antispyware software has been installed, updated fully, and configured to scan all files, in case the backup media contains any malware or spyware. These precautions should have already been performed as part of the Section 4.4 recommendations.

- i. Click on **Start**, then **All Programs**. Choose **Accessories**, then **System Tools**. Select the **Files and Settings Transfer Wizard**, then click **Next**.
  - ii. Select **New computer** to restore the previously captured files and settings, then click **Next**.
  - iii. Choose the **I don't need the Wizard Disk** option, since the backup was already performed, then click **Next**.
  - iv. When prompted for the location of the files and settings, choose **Other** and select the location of the backup. Then click **Next**.
  - v. The wizard restores the files and settings. When it is done, click **Finished**. The computer may need to be rebooted before the new settings take effect.
- c. Third-Party Backup and Restore Utility
    - i. Run the utility and perform the restore based on the utility vendor's documentation.
  - d. Third-Party Remote Backup Service
    - i. Perform the restore using the remote backup service's software and directions.
  - e. File Copy to Media
    - i. Select the files on the media to be restored, and drag them onto the appropriate folder on the Windows XP Home Edition computer. Alternately, copy the files to be restored, and paste them into the appropriate folder. Perform this as many times as needed to restore all the preserved files.

---

---

## 4.6 Summary

Instead of upgrading an older version of Windows to Windows XP Home Edition, Windows XP Home Edition should be installed or reinstalled on a computer, which means that all existing Windows XP Home Edition settings, applications, and data on the computer are destroyed unless first backed up to removable media or otherwise preserved. The installation process for Windows XP Home Edition has five phases, as follows:

1. **Prepare for the Installation.** This involves basic preparatory actions, such as gathering the software media and documentation that may be needed for the installation, documenting critical OS and application settings, and acquiring blank media for backups.
2. **Back Up Data and Configuration Files.** This is the transfer of user data files and configuration settings from the computer to external media, such as CD-ROMs or flash drives.

3. **Install Windows XP Home Edition.** This is the actual installation of Windows XP Home Edition. The computer should be disconnected from all networks before the installation begins.
4. **Secure the Computer.** This involves performing various actions to secure Windows XP Home Edition. It also involves installing and securing applications that will be run on the computer.
5. **Restore Data and Configuration Files.** This causes the user data and configuration settings that were backed up during phase 2 to be transferred back to the computer.

Once this installation process has been completed, each user account on the computer needs to be secured. Section 7 contains step-by-step directions for accomplishing this.

## 5. Securing a New Windows XP Home Edition Installation

Before anyone uses a newly installed Windows XP Home Edition computer, it should be properly secured to minimize the possibility of a security breach. This section provides guidance and step-by-step instructions for securing a new installation of Windows XP Home Edition.<sup>66</sup>

The guidance in this section assumes that the computer has not been attached to any networks since Windows XP Home Edition was installed. If the computer has been on a network, it could have already been compromised because Windows XP Home Edition has few security features enabled by default. This section also assumes that the computer has not yet been used and does not yet contain any data. For readers who do not have the time or expertise to follow all of the instructions in these sections, Appendix A contains instructions for the most essential security protections for Windows XP Home Edition computers.

---



---

### 5.1 Prepare to Secure the Computer

Users need to perform some preparatory actions before beginning to secure a computer. These actions can be grouped into three categories: gathering needed materials, setting the default view for Control Panel, and identifying the Windows XP Home Edition service pack currently in use. These categories are discussed in Sections 5.1.1 through 5.1.3.

---

#### 5.1.1 Gather Needed Materials

Before securing the computer, gather the software media and documentation that might be needed, including the following:

- Documentation and support information from the computer's manufacturer
- Windows XP Home Edition software, including the Windows XP Home Edition CD and service pack CDs (if applicable)
- Software from the computer's manufacturer
- Software for third-party user applications, such as word processors, graphics tools, e-mail clients, and Web browsers
- Software for third-party security applications, such as antivirus software, personal firewalls, and data encryption utilities
- Serial numbers for third-party applications that may be needed to register them.

If antivirus software and antispyware software is not already present, it should be acquired before starting to secure the computer. If the existing security software is significantly out of date (generally, several years old), it should be upgraded to a new version if possible, otherwise replaced with a new version. For example, outdated antivirus software typically lacks newer detection capabilities and other features that are needed to detect and stop relatively recent malware threats.

---

<sup>66</sup> This section attempts to make no assumptions about the default settings in Windows XP Home Edition, because computer vendors may customize various settings in their Windows XP Home Edition installations.

### 5.1.2 Set the Default View for Control Panel

Control Panel has two views: Classic and Category. Classic View lists each Control Panel item separately, and Category View groups similar items together. The instructions in this guide assume that Classic View is being used.

1. Open the **Control Panel**.
2. Look at the text in the upper left hand corner of the Control Panel window.
  - If it contains a link that says **Switch to Category View**, no action is needed because **Classic View** is already the default setting.
  - If it contains a link that says **Switch to Classic View**, click on that link to change the default view from Category View to Classic View.
  - If it does not contain either a **Switch to Category View** or a **Switch to Classic View** link, no action is needed because the Windows classic folders option is enabled, which allows only Classic View to be used.

---

### 5.1.3 Identify Service Pack Currently in Use

It is very important to determine which Windows XP Home Edition service pack the computer is currently running. Certain directions in this section are specific to a particular service pack version. To identify the running service pack, perform the following steps:

1. From the **Control Panel**, double-click the **System** icon. The System Properties window should appear.
2. Under the **General** tab, the information displayed for the **System** should indicate which service pack is currently loaded on the computer, such as Service Pack 1 or Service Pack 2. Figure 5-1 shows an example from a Service Pack 2 computer. If no service pack is listed, then the computer does not have a service pack installed.
3. Click on **OK**.



Figure 5-1. System Properties

---

---

## 5.2 Update Windows XP Home Edition

The next step in securing Windows XP Home Edition is to apply updates to it. Although some updates may be available on CD, such as Windows XP Home Edition Service Pack 2, most need to be downloaded from the Internet. Before the computer is connected to any network to get updates, a personal firewall needs to be set up on the computer to block malicious activity from other computers, such as worms.<sup>67</sup> Without a personal firewall enabled and configured to block unauthorized network activity, a computer connected to the Internet that has not had updates applied is typically compromised in minutes.<sup>68</sup> This section provides step-by-step instructions for identifying, acquiring, and applying the updates, as well as guidance on configuring a personal firewall to protect the computer during the updating process.

**Until the computer has been fully updated, applications such as e-mail clients, instant messaging clients, and word processors should not be used. The only application use should be that which is required to update the computer or configure the personal firewall. Web browsers should be used only for updating the computer and not for general Web surfing or other purposes.**

---

### 5.2.1 Configure a Personal Firewall

All pre-SP2 versions of Windows XP Home Edition have a built-in personal firewall called Internet Connection Firewall (ICF). ICF offers the ability to block unauthorized network activity directed at a Windows XP Home Edition computer, but by default ICF is disabled. Windows XP Home Edition SP2 replaces ICF with a new built-in personal firewall called Windows Firewall. By default, Windows Firewall enables itself if a third-party firewall is not already present. Many new computers contain trial versions of third-party personal firewalls, so new Windows XP Home Edition computers could have two or more personal firewalls installed. This guide recommends using the built-in personal firewall and disabling all others, but users could instead use a third-party personal firewall and disable all others. Follow the appropriate set of directions below to enable and configure the built-in personal firewall to block all unnecessary activity during patching.

**If the computer is not yet using Service Pack 2** (it is using either Service Pack 1 or no service pack at all), perform the following steps to ensure that a personal firewall is enabled and providing adequate protection for the computer:

1. Log on to the computer using an administrative-level account.

---

<sup>67</sup> At this point, installing antivirus software is generally not necessary. It is likely that the antivirus software media is several months out of date and will not be effective at stopping most malware threats until the computer is connected to a network and updated.

<sup>68</sup> If configured properly, a firewall router can also be effective at protecting unpatched computers during the update process. However, because firewall routers are third-party hardware devices, it is outside the scope of this document to discuss their configurations. Also, computers that are protected by firewall routers should also be protected by personal firewalls as an additional layer of defense, particularly against other computers on the same local network that may become infected with malware.



2. If any third-party personal firewall programs are installed on the computer, refer to the software vendors' documentation and help files, and follow their directions to disable them.
3. In the **Control Panel**, double-click the **Network Connections** icon. The Network Connections configuration box should be displayed.
4. Right-click the connection that needs to be configured with ICF, then click **Properties**.<sup>69</sup>
5. Select the **Advanced** tab. Enable ICF by checking the box for **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
6. Click on **OK** to save the firewall configuration.

**If the computer is already using SP2**, perform the following steps to ensure that Windows Firewall is enabled and providing adequate protection for the computer:

1. Log on to the computer using an administrative-level account.
2. In the **Control Panel**, double-click on the **Security Center** icon. The Security Center should be displayed.
3. The firewall status should indicate if a third-party firewall is enabled. If so, refer to the software vendors' documentation and help files, and follow their directions to disable them.
4. Check the firewall status. If it is listed as **OFF**, perform the following sub-steps:
  - a. Click on the **Recommendations...** button.
  - b. Turn the firewall on by clicking the **Enable now** button. A notification window should appear, saying that the firewall was enabled successfully. Click on **Close**.
  - c. Click on **OK** to close the **Recommendation** window. The firewall status should now be listed as **ON**.
5. Close the **Security Center**.

---

## 5.2.2 Connect the Computer to the Network

The next step is to connect the computer to a network. Networking options include telephone modems, broadband (e.g., DSL, cable modem), or a wired or wireless Local Area Network (LAN). This section provides the steps needed to set up a Windows XP Home Edition computer to use each of these networking options. If the computer will use multiple forms of networking, such as a cable modem and wireless, follow each applicable set of directions below.

---

<sup>69</sup> If a dial-up modem is being used, it may be necessary to first implement the Section 5.2.2 directions for configuring a dial-up connection first, and then return to this step.

**If the computer uses a telephone modem for its access to other networks**, follow these steps:

1. From the **Control Panel**, double-click on the **Network Connections** icon.
2. Click on **File**, then **New Connection** to run the New Connection Wizard. When the wizard window appears, click **Next**.
3. Click on the **Connect to the Internet** option and click **Next**.
4. The user needs to choose from three options: **Choose from a list of Internet service providers (ISPs)**, **Set up my connection manually**, and **Use the CD I got from an ISP**. Select the appropriate option based on the ISP's instructions or documentation, and click **Next**.
5. Provide all requested information and follow the prompts based on the ISP's instructions or documentation.
6. After filling in the ISP-specific information, click on **Add a shortcut to this connection to my desktop**, and then click **Finish**.

**If the computer uses a wired local area network or broadband (e.g., DSL, cable modem) for its access to other networks**, simply connect the network cable to the computer to establish network connectivity. All necessary configuration settings should have already been entered during the Section 4.3 instructions for installing Windows XP Home Edition.

**If the computer uses a wireless local area network**, follow the steps listed below:

*These instructions assume that the wireless connectivity features built into Windows XP Home Edition are being used to configure and manage the wireless network card. In some cases, it may be desirable to use a separate wireless configuration utility provided by the vendor of the wireless network card, or a vendor's version of Windows XP Home Edition may use such a utility by default. If a separate utility is to be used, skip the steps below and instead follow the directions from the utility's vendor on how to configure it to establish wireless network connectivity. If you are unsure if a separate utility is being used, it should become obvious after attempting a few steps of the directions whether or not these steps are correct for your situation.*

1. From the **Control Panel**, double-click on the **Network Connections** icon.
2. Right-click the wireless connection that needs to be configured, then click **Properties**. (If a wireless network connection entry does not exist, the proper driver for the wireless network card may not be installed. Follow the wireless card manufacturer's directions for installing the driver.)
3. A list of wireless networks in range should be displayed (if not, select **View Wireless Networks** to display them). Select the correct wireless network and click on the

**Connect** button. Note that wireless networks can be “hidden” so that their names do not appear in the list. If the network is “hidden”, click the **Add** button and manually type the network’s SSID (wireless network name), then click **OK** to connect.

4. If a WEP or WPA key is required by the wireless access point, enter it when requested and click on **Connect**.<sup>70</sup>

---

### 5.2.3 Activate Windows

Before downloading updates, Windows XP Home must be activated, because Microsoft will not allow downloading of the latest Service Packs without ensuring that a legitimate copy of Windows is being used.<sup>71</sup> Activating just ensures that the version of Windows is legitimate and is not the same as registering, though registration can be accomplished at the same time.

1. Run **Activate Windows**. This can be accomplished in any of the following ways:
  - Begin activation when the **Activate Windows** window pops up automatically when logging in.
  - Click on **Start**, then **All Programs**, then **Accessories**, then **System Tools**. Select **Activate Windows**.
  - Click on the **Activate Windows** icon in the Quick Launch area. The icon looks like a set of keys.
2. Assuming there is a working Internet connection, click on **Yes, let’s activate Windows over the Internet now**. Alternatively, activation can be performed by telephoning Microsoft customer support and following their guidance.
3. Register and click **Next**. Registration data should then be entered on the next page.
4. Activation should then complete automatically. If Windows cannot connect to the Internet, a connection screen will appear to help connect to the Internet. If activation fails, call Microsoft customer support.

---

### 5.2.4 Apply Updates

The next step is to identify, download, and install necessary updates for the computer, as described in Section 3.1.1. If a service pack CD is available, it should be used first before downloading additional updates. Both Automatic Updates and Microsoft Update can be used to download some updates. However, although Automatic Updates can acquire and install all Windows XP Home Edition security-related updates, it does not include all updates, such as hardware drivers. The Microsoft Update Web site can be used to acquire and install all types of updates, both security and non-security-related. To use Microsoft Update, perform the steps below.

---

<sup>70</sup> Section 5.4.2.2 provides additional information on wireless security, including WEP and WPA keys.

<sup>71</sup> For additional information on the Windows XP Home Edition activation process, see MSKB article 307890, available at <http://support.microsoft.com/kb/307890/>.

Because the predecessor to Microsoft Update was named Windows Update, Windows XP Home Edition computers that are not fully updated may display “Windows Update” instead of “Microsoft Update” on some screens.<sup>72</sup> This should not be a cause for concern; during the update process, Windows Update will eventually be replaced with Microsoft Update.

1. Run Internet Explorer. Click on **Tools**, then **Windows Update**, to start Microsoft Update.<sup>73</sup>
2. If a prompt appears asking to install and run Windows Update, click **Yes**.
3. If a prompt appears saying that a new version of the Windows Update or Microsoft Update software is available, click on **Install Now** or **Download and Install Now** to install the new version. Multiple updates may be needed. If prompted to do so, close Internet Explorer or reboot the computer so that the new version of the update software takes effect. (If a reboot is needed, restart these instructions at step 1 after the reboot completes.)
4. Click on the **Custom** button to identify available updates.<sup>74</sup>
5. Microsoft Update checks for updates and lists the available ones. Figure 5-2 shows an example of how updates are listed. Depending on the service pack level of the Windows XP Home Edition installation CD, either Service Pack 2 or non-service pack updates should be displayed. Follow the appropriate step:
  - a. **Non-service pack updates** are grouped by high priority updates, optional software updates, and optional hardware updates.<sup>75</sup> Install them using the following steps:
    - i. Review the list of available updates, select the desired ones (or accept the default setting), then click **Review and install updates**. In some cases, one patch may need to be installed by itself; therefore, it may not be possible to install all desired patches at once.
    - ii. Confirm that the correct updates are listed, and click the **Install Updates** button to perform the installations. Review any licensing agreements that are displayed and click on the appropriate button for each.
    - iii. The download and installation process will begin. Depending on the number of updates and the network bandwidth available, it may take from a few minutes to a

---

<sup>72</sup> Windows Update was renamed Microsoft Update in mid-2005. The directions in this section reflect the titles assigned to the update Web site and local software components as of August 2005.

<sup>73</sup> Alternatively, Microsoft Update can be started by entering the URL <http://update.microsoft.com/> into the Internet Explorer address bar.

<sup>74</sup> The Custom option can install both high priority and optional updates, and allows the user to select which updates should be installed. The Express option can only install high priority updates, and does not allow the user to specify which updates should be installed. Using the Express option may cause the system to download and install service packs automatically.

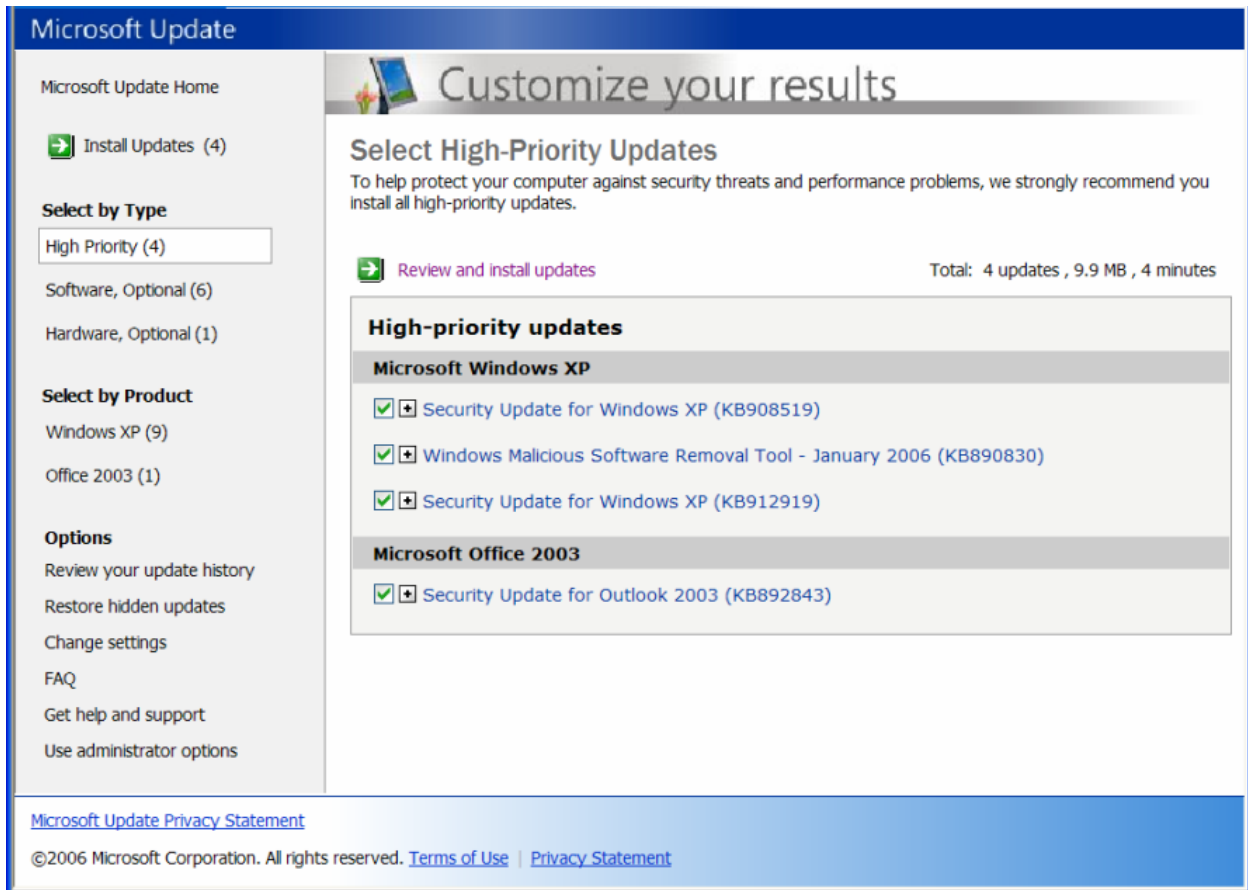
<sup>75</sup> High priority updates are defined as critical updates, hotfixes, service packs, and security rollups. Optional updates are unrelated to fixing security problems, but may contain new security features.

few hours to download and install the updates. When the installations are done, Microsoft Update should report which updates were successfully installed. It will also prompt the user to reboot the computer if any of the updates require a reboot to complete the installation. Click on **OK** to reboot immediately or **Cancel** to manually reboot the computer later.

- b. **Service Pack 2** can be installed through Microsoft Update using the following steps:<sup>76</sup>
  - i. Click on **Download and Install Now**.
  - ii. Review the license agreement and click on the appropriate button.
  - iii. Service Pack 2 should be downloaded and installed. This may take considerable time, depending primarily on the size of the service pack and the type of Internet connectivity and bandwidth available. The Windows XP Service Pack 2 Setup Wizard may prompt the user at some point; click **Next** to continue.
  - iv. Once the installation has ended, a summary should be displayed that reports the installation was successful. Click **Restart Now** to reboot the computer.
  - v. After the reboot, the **Help protect your PC** screen appears. The Automatic Updates setting is configured later in the instructions, so at this time, choose the **Not right now** option and click **Next**.
  - vi. The **Security Center** opens and displays the status of security programs. Since antivirus software and other security programs have not yet been installed on the computer, the current status is irrelevant. Close the **Security Center**.
6. Repeat all of these steps until no more updates are available. Depending on which service pack was included with the Windows XP Home Edition CD, and the number of additional updates that need to be applied, it may take several rounds of updating the computer and rebooting it to bring a new Windows XP Home Edition installation completely up-to-date.

---

<sup>76</sup> If a service pack is being installed from a CD instead of through Microsoft Update, the steps to be performed will differ.



**Figure 5-2. Microsoft Update**

During the updating process, the computer may state that additional updates cannot be downloaded until Windows XP Home Edition has been validated or activated. If so, follow the instructions provided by Windows XP Home Edition to activate the software through the Internet, dial-up, or telephone.

It is also important to update other applications on the Windows XP Home Edition computer. Follow these steps for each application:

1. Install the application.<sup>77</sup>
2. Review its documentation for guidance on how to update it and how to configure it to update itself automatically (if possible).
3. Implement the vendor's recommendations. If needed, close and restart the application, or reboot the computer, so that the changes take effect.

<sup>77</sup> It is often advantageous to install applications such as e-mail clients and Web browsers before installing security software. For example, when antivirus software is installed, it may automatically identify installed email clients and configure itself so that it monitors their activity for malware.

## 5.2.5 Configure the Computer for Automatic Updates

To keep Windows XP Home Edition fully updated at all times, it is highly recommended that the Automatic Updates service built in to Windows XP Home Edition be enabled, as described in Section 3.1.1. This should keep both Windows XP Home Edition and key Microsoft applications (e.g., Internet Explorer, Outlook Express) fully updated. To enable and configure Automatic Updates, perform the following steps:

1. From **Control Panel**, double-click **Automatic Updates**.
2. Choose the appropriate radio button, as shown in Figure 5-3.
  - If the computer has high-speed Internet access, select **Automatic (recommended)**. Then select the frequency and timeframe in which the updates should be downloaded and installed (e.g., every day at 3:00 A.M.)
  - If the computer has low-speed Internet access, select **Notify me but don't automatically download or install them**. This allows the user to control when updates are downloaded.
3. Click on **OK** to save the Automatic Updates configuration.



Figure 5-3. Automatic Updates Configuration

---

---

## 5.3 Install and Configure Additional Security Software

The next task in securing a new Windows XP Home Edition computer is installing and configuring security software. Section 5.2.1 already described how to enable and configure a personal firewall to block unauthorized network access to the computer. This section provides guidance on configuring other types of software, such as antivirus software, Web browser popup blocking, and content filtering programs, that can be effective at preventing malware infections and other types of attacks.

---

### 5.3.1 Malware Protection

After applying updates to the computer, users should next install malware protection utilities, as described in Section 3.3.1. Antivirus software is a necessity, and antispyware software is also recommended if the antivirus software does not include a robust antispyware capability. Install the antivirus software (and separate antispyware software, if needed) using the documentation provided with the software. During the software installation process, or immediately afterward, the software should be configured as follows, using directions provided within the software documentation:

- Scan critical operating system components such as startup files, memory, system BIOS, and boot records
- Perform real-time scans of each file as it is downloaded, opened, or executed
- Monitor common applications such as e-mail clients, Web browsers, file transfer and file sharing programs, and instant messaging software
- Scan all hard drives regularly (at least once a week)
- Attempt to disinfect files, and quarantine infected files that cannot be disinfected
- Automatically download and install updates daily.

After installation, the software should be fully updated. Consult the software documentation or help files for directions on how to download and install updates. Most antivirus software and antispyware software have a menu option that causes the software to check for, download, and install updates immediately. After doing so, it may be necessary to repeat the update process once or a few times, because some updates might need to be installed before other updates. Also, it may be necessary to reboot the computer after applying certain updates.

---

### 5.3.2 Content Filtering

Users may also want to use content filtering software, such as spam and Web content filtering software, as described in Section 3.3.3. Some e-mail clients and Web browsers have such capabilities built-in; they can also be performed by third-party software. Content filtering programs are helpful in stopping certain types of malware, but are not necessities. If content filtering is to be performed on the computer, install and configure the software using the documentation provided. The software should be configured to check for updates frequently and



either to download and install updates automatically, or to let the user know when updates are available so that the user can download and install them at a convenient time.

After installation, the software should be fully updated. Consult the software documentation or help files for directions on how to download and install updates. Most content filtering programs or software features have a menu option that causes the software to check for, download, and install updates immediately. After doing so, it may be necessary to repeat the update process one or a few times, because some updates might need to be installed before other updates. Also, it may be necessary to reboot the computer after applying certain updates.

---

### 5.3.3 Personal Firewall

Section 5.2.1 provides instructions for enabling the Windows Firewall. Because third-party personal firewall programs may offer additional functionality, users may choose to disable Windows Firewall and use a third-party firewall instead. Only one personal firewall should be enabled on the computer at a time. Because a Windows XP Home Edition computer should always have a personal firewall enabled when it is connected to a network, users who want to switch firewalls should first enable the second firewall and then immediately disable the first firewall.<sup>78</sup> Section 3.3.2 provides additional information on personal firewalls.

To disable Windows Firewall, perform the following steps:

1. In the **Control Panel**, double-click on **Security Center**.
2. In the **Security Center**, choose to manage security settings for **Windows Firewall**.
3. Set the **Off** option, then click **OK**.
4. Close the **Security Center**.

Users should configure the personal firewall to use the following settings whenever possible:

- Enable the personal firewall to protect every network interface on the computer, including wired and wireless networks cards, as well as dial-up access
- Only permit authorized activities; deny all others by default, or prompt the user to manually accept or reject each unknown activity<sup>79</sup>
- Restrict both incoming and outgoing activity.

---

<sup>78</sup> An alternative is to disconnect the computer from all networks, then disable the first firewall and enable the second firewall. This may be necessary if the second firewall cannot be enabled while the first firewall is still enabled.

<sup>79</sup> Prompting the user to make these decisions works best with users that have strong knowledge of software and security. Novice users are unlikely to understand the messages presented by the firewall, so they tend to allow unknown activity, which defeats the purpose of having the firewall. Accordingly, personal firewalls should be set to prompt the user only if it is reasonably certain that users will make the right decisions.

---

---

## 5.4 Alter the Windows XP Home Edition Configuration

Once computer security programs have been installed and configured, the next step is to alter the Windows XP Home Edition configuration to further improve security. This section recommends specific changes to the default Windows XP Home Edition configuration. The step-by-step instructions in this section build upon the recommendations presented in Sections 3.1 and 3.2, such as disabling unnecessary functions and services, and creating separate accounts for each user.

---

### 5.4.1 User Accounts and Sessions

To make the changes recommended in Section 3.1.2 related to user accounts and user sessions, perform the following steps:

1. From the **Control Panel**, double-click on **User Accounts**.
2. Create strong passwords and safeguard them on password reset disks or paper for all administrator accounts. To do so, perform the following steps for each computer administrative account:
  - a. Select the account.
  - b. Click **Create a password**.
  - c. Enter a new password and type it once more to confirm it. Do not enter a password hint. Click the **Create Password** button.<sup>80</sup>
  - d. By default, the administrative account's files and folders are available to other users of the computer. To make them private, click on the **Yes, Make Private** button.
  - e. If the computer has a floppy drive, perform the following steps:
    - i. In the **Related Tasks** box, click on the **Prevent a forgotten password** link.
    - ii. The Forgotten Password Wizard should start. Click on **Next**.
    - iii. As directed, place a blank, formatted floppy disk into the drive and click **Next**.
    - iv. Enter the current administrative password and click **Next**.
    - v. The wizard creates the disk. When the creation is completed, click **Next**, then click **Finish**.
    - vi. Store the password reset disk in a physically secure area, because anyone could use it to gain administrative access to the computer.

---

<sup>80</sup> Recommendations for creating strong passwords are available from the Microsoft article "Selecting Secure Passwords", located at [https://www.microsoft.com/smallbusiness/support/articles/select\\_sec\\_passwords.mspx](https://www.microsoft.com/smallbusiness/support/articles/select_sec_passwords.mspx).

- f. If the computer does not have a floppy drive, write the password for the administrative account on a piece of paper and store it securely, such as in a safe or lockbox.
3. For each person that will be using the computer, create a separate limited user account for daily use:
    - a. Click **Create a new account**.
    - b. Enter the user name; it can be up to 20 characters long and contain letters, numbers, spaces, and some other types of punctuation. When finished, click the **Next** button.
    - c. Set the account type to **Limited**, then click on the **Create Account** button.
    - d. Have the user choose a strong password and enter it after clicking **Create a password**. Ask the user not to enter a password hint.
  4. Enabling the Fast User Switching feature allows two users to be logged on simultaneously without having access to each other's sessions.<sup>81</sup> To enable the feature, perform these steps:
    - a. From the **Control Panel**, click on **User Accounts**.
    - b. Click on **Change the way users log on or off**.
    - c. Check the **Use the Welcome screen** and **Use Fast User Switching** options to enable the Welcome screen and FUS features.
    - d. Click on **Apply Options**.
  5. Close the **User Accounts** window.

It is important to ensure that the default Administrator account has a password set. Because this account can only be accessed from Safe Mode, the computer needs to be rebooted to set the password. Perform the following steps:

1. Close all programs. From the **Start** menu, click **Turn Off Computer**, then click the **Restart** icon.
2. When the computer starts to reboot, hit the **F8** key to display the Windows Advanced Option Menu. Choose **Safe Mode** and hit the **Enter** key.
3. At the next screen, select **Microsoft Windows XP Home Edition** and hit the **Enter** key. Various text messages should be displayed on the screen, and eventually the Windows XP logon screen should appear.<sup>82</sup>

---

<sup>81</sup> This is particularly useful for logging in as an administrator to perform a specific task when already logged in with a limited user account.

4. Log in as the **Administrator** user. If asked if the computer should be run in Safe Mode, choose **Yes**.
5. Perform Steps 1 and 2 from the previous list of steps. These steps will ensure that the default Administrator account has a password set and that if the password is forgotten, that access can still be gained through the physically secured copy of the password or the password reset disk.
6. Close the **User Accounts** window and the **Control Panel**.
7. From the **Start** menu, click **Turn Off Computer**, then click the **Restart** icon. The computer should reboot normally.

---

## 5.4.2 Networking

This section contains recommendations for making the following changes related to networking, as described in Section 3.1.3:

- Disabling unneeded networking features
- Disabling the use of remote access tools
- Configuring wireless networking security
- Disabling or configuring ICS.

### 5.4.2.1 Disable the use of remote access tools

Windows XP Home Edition's Remote Assistance feature, as well as all third-party remote access tools installed on a Windows XP Home Edition computer, should be disabled except when specifically needed.<sup>83</sup> To disable the use of Remote Assistance, perform the following steps:<sup>84</sup>

1. From the **Control Panel**, double-click the **System** icon. The System Properties window should appear.
2. Click the **Remote** tab.
3. Uncheck **Allow Remote Assistance invitations to be sent from this computer**.
4. Click **OK**.

---

<sup>82</sup> The graphics and font sizes are likely to be different; this is a characteristic of Safe Mode only, and the graphics and fonts will return to normal when the computer is rebooted regularly.

<sup>83</sup> Third-party tools should also be configured to require a username and password before permitting remote access. The username and password should be different from all of the Windows XP Home Edition user accounts and passwords.

<sup>84</sup> To temporarily enable Remote Assistance, perform the same steps except for checking the box instead of unchecking it.

### 5.4.2.2 Secure wireless networking

If the computer uses wireless networking, review the documentation provided with the wireless access point and the computer's wireless network card, then implement the following recommendations according to the vendor directions.<sup>85</sup> These directions assume that the Microsoft wireless management utility is being used, not a third-party utility provided by the computer's vendor or the wireless network card's vendor. If a third-party utility is being used, do **not** follow the directions in this section; instead, consult the vendor's directions for additional guidance on secure configuration.

1. Create a long and complex WEP key (also known as a WPA key or WPA passphrase). Configure the wireless access point so the WEP key is required. Enter it into the wireless access point and the Windows XP Home Edition computer. To do the latter, perform the following steps:
  - a. From **Control Panel**, double-click **Network Connections**.
  - b. Right-click on the wireless network connection configuration and select **Properties**.
  - c. Click on the **Wireless Networks** tab. Highlight the correct wireless network in the **Preferred Networks** list and click the **Properties** button. Figure 5-4 shows an example of the security configuration settings that need to be made.
  - d. Set **Data encryption** to the highest possible setting that both the wireless access point and the Windows XP Home Edition wireless network card can use. The encryption choices will vary depending on the wireless network card. Recommended choices, in order with the most highly preferred option first, are as follows:
    - i. WPA2 with AES
    - ii. WPA1 with AES
    - iii. WPA1 with TKIP
    - iv. WEP with 128-bit encryption.

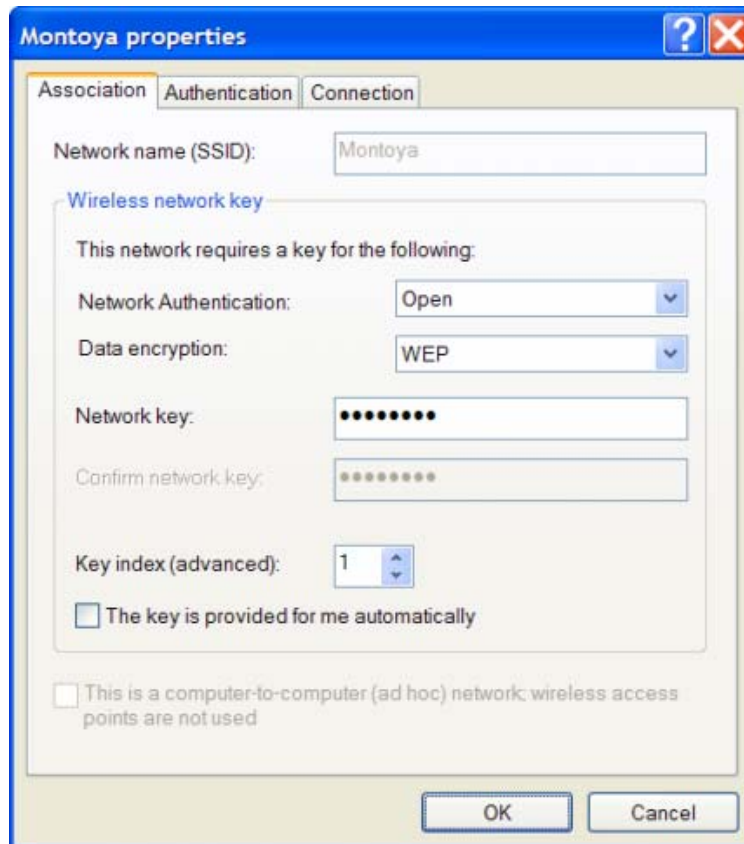
Also, configure the access point to use the selected data encryption option, if it does not already use it by default. Consult the access point manufacturer's documentation for information on how to do this.

- e. Clear the check box labeled **The key is provided for me automatically**.

---

<sup>85</sup> The guidance provided in this section is specific to wireless network hardware and software based on the IEEE 802.11b and 802.11g standards. To secure other types of wireless networks, consult the vendor's documentation and security recommendations. These recommendations also assume that an access point (infrastructure mode) is being used instead of a peer-to-peer network (ad hoc mode), because access point-based networks are more common than peer-to-peer.

- f. Set the **Network authentication** to **Open**. Enter the WEP key in the **Network key** and **Confirm network key** boxes.
- g. Click **OK** to save the changes, then click **OK** to close the wireless network connection properties window. Close the **Network Connections** window.



**Figure 5-4. Wireless Networking Security Properties**

2. On the Windows XP Home Edition computer, configure Wireless Auto Configuration so that it will not attempt to join any wireless network automatically and it will only connect to wireless access points. To do so, perform the following steps:
  - a. From **Control Panel**, double-click **Network Connections**.
  - b. Right-click on the wireless network connection configuration and select **Properties**.
  - c. Click on the **Wireless Networks** tab. Click the **Advanced** button in the lower right-hand corner.

- d. Select the option labeled **Access point (infrastructure) networks only**.<sup>86</sup>
  - e. Clear the check box labeled **Automatically connect to non-preferred networks**, then click **Close**.
  - f. Remove any networks from the Preferred Networks list that the computer should not be using.
  - g. Click **OK** to close the wireless network connection properties window. Close the **Network Connections** window.
3. Review the wireless access point's documentation. If it permits access to be restricted by the media access control (MAC) addresses of wireless network cards, enter the MAC addresses of all authorized wireless devices into the access point. To identify the MAC address for a wireless network card on a Windows XP Home Edition computer, perform the following steps:
    - a. From **Control Panel**, double-click **Network Connections**.
    - b. Double-click on the wireless network connection configuration.
    - c. Click the **Support** tab, then the **Details...** button.
    - d. The value listed for the **Physical Address** is the MAC address. It should be displayed in the format XX-XX-XX-XX-XX-XX, where each X is a digit or a letter in the range A to F. Write down the MAC address.
    - e. Click **Close**, then **Close**. Close the **Network Connections** window.

#### 5.4.2.3 Configure ICS

If the computer uses dial-up networking to access the Internet, and other computers on the same home network need to share that Internet access, then it may be necessary to enable ICS. Otherwise, ICS should be disabled. To configure ICS properly, perform the following steps:

1. From the **Control Panel**, select **Network Connections**.
2. Right-click on the network connection with Internet access and select **Properties**.
3. Click on the **Advanced** tab.
4. Perform the appropriate step based on the need for ICS:
  - **If ICS is not needed**, disable it by clearing the check box labeled **Allow other network users to connect through this computer's Internet connection**.

---

<sup>86</sup> If the computer will be participating in ad hoc wireless networks (such as a peer-to-peer network with another computer), select the **Any available network (access point preferred)** option instead of **Access point (infrastructure) networks only**.

- **If ICS is needed**, check the item labeled **Allow other network users to connect through this computer's Internet connection**. Then, uncheck the item labeled **Allow other network users to control or disable the shared Internet connection**.

5. Click on **OK**, then close the **Network Connections** window.

---

### 5.4.3 Files and Folders

This section contains recommendations for making changes related to files and folders, as described in Section 3.2.2. Specifically, it addresses configuring folder sharing.

The Shared Documents folder is available so that users of a Windows XP Home Edition computer can share files with each other. In most cases, this is sufficient; however, if there is a need to create a share that permits read-only access, perform the following steps:

1. Open **My Computer** and right-click the folder that should be shared. Click on the **Sharing and Security...** option.
2. Click on the link labeled **If you understand the security risks but want to share files without running the wizard, click here**.
3. Select the **Just enable file sharing** option and click **OK**.
4. To share the folder with users on other computers, check the **Share this folder on the network** box and enter a name (or use the default name) for the share in the **Share name** box. Uncheck the **Allow network users to change my files** box so that users can read but not modify the files.
5. Click **OK**.

If the Shared Documents folder needs to be made available to users on other computers of the local network, perform the following steps:

1. Open **My Computer** and right-click the **Shared Documents** folder. Click on the **Sharing and Security...** option.
2. Check the **Share this folder on the network** box. Enter a name (or use the default name) for the share in the **Share name** box. If network users should be able to read and modify the shared files, check the **Allow network users to change my files** box, otherwise uncheck it.
3. Click **OK**.



## 5.5 Document the Installed Software Applications

A helpful next step in securing the computer is to document the software applications installed on the computer. Examples of applications include Web browsers, e-mail clients, office productivity tools (e.g., word processors, spreadsheets), instant messaging software, multimedia utilities (e.g., audio players), graphics tools, and security software (e.g., antivirus software, personal firewall). The value of having a list of software is that if problems occur in the future, the current and previous application listings for the computer can be compared and differences identified. These differences can be investigated to determine if any of them appear to be malicious, such as malware and spyware programs that have infected a computer.

To document the installed applications, use the following methods and write down the results:

- From the **Control Panel**, run the **Add or Remove Programs** utility. As the example in Figure 5-5 illustrates, it shows which software applications are installed on the computer, as well as security updates, hardware drivers, and other types of programs.
- Review the folders and icons on the Start Menu and the Desktop to find application shortcuts listed there.

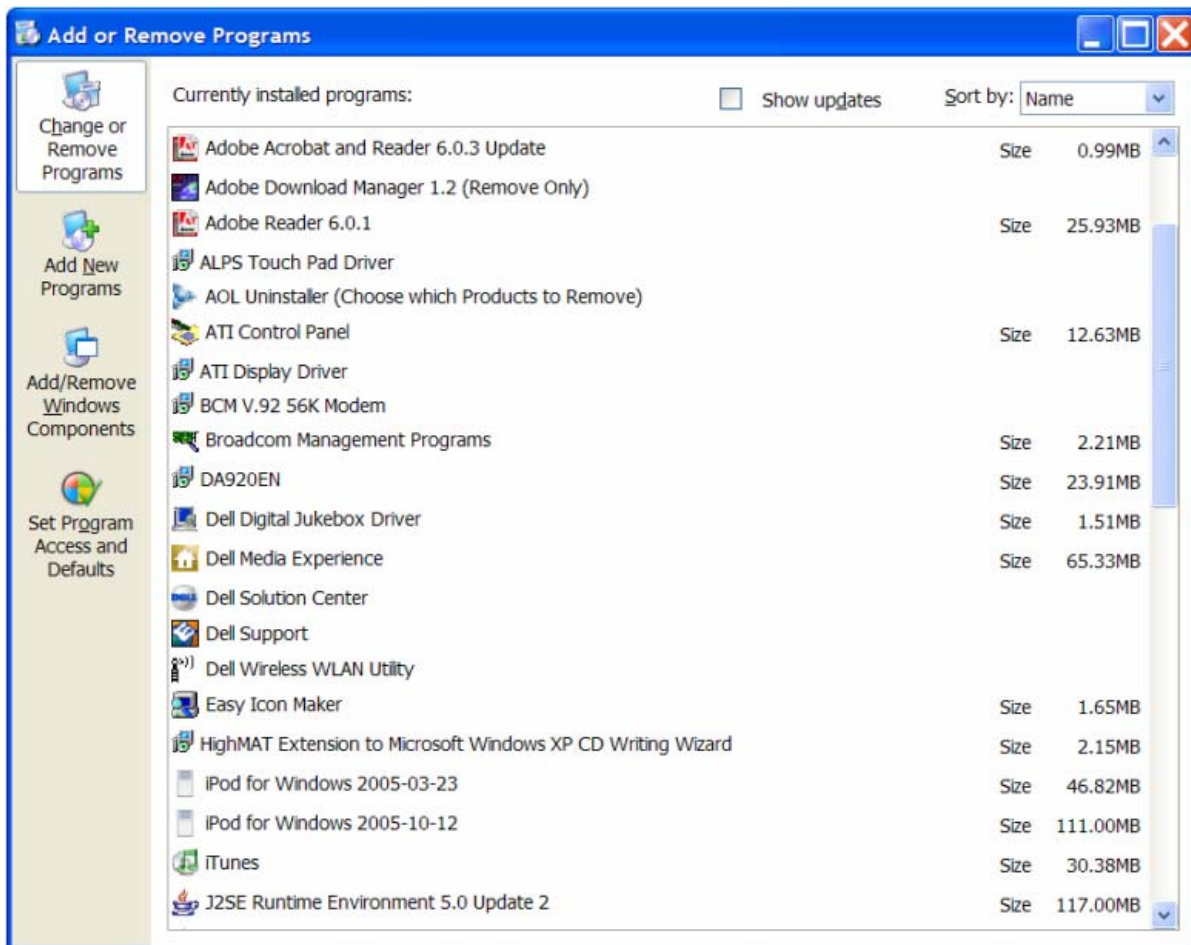


Figure 5-5. Viewing Installed Program Names

It is also very helpful to document which applications are configured to run automatically when the computer starts and which applications are currently running on the computer. Again, these lists can be very helpful in the future in identifying malware and spyware that might infect a computer. To generate and record these lists, perform the following steps:

1. From the **Start** menu, select **All Programs**, then **Accessories**, then **System Tools**, then **System Information**. System Information should open.
2. Select **System Summary**, which should be in the upper left corner of the window.
3. Click on **File**, then **Save**. This will save the system information to a file. Choose a location for the file to be saved and a name for the file. When done, click **Save**.
4. Close **System Information**.

The saved file includes information on the applications that were running at the time the information was saved and the applications loaded at startup. Within the saved file, this information is located under **Software Environment/Running Tasks** and **Software Environment/Startup Programs**, as shown in Figures 5-6 and 5-7, respectively. The saved file can be viewed by running System Information and opening the file from it.

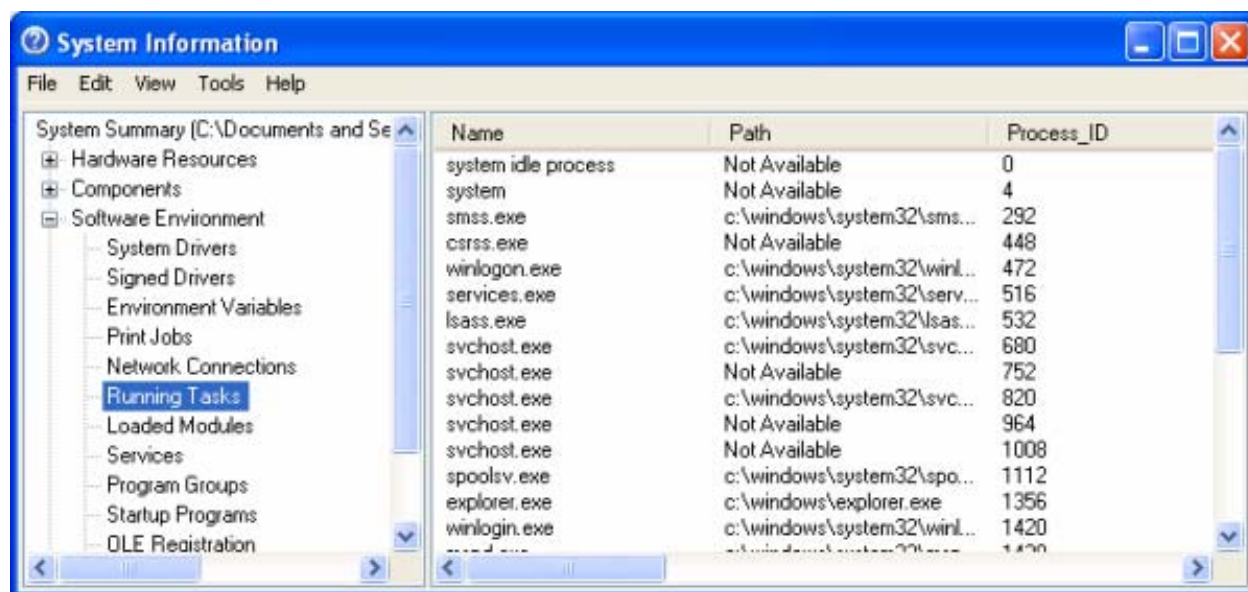


Figure 5-6. Running Tasks

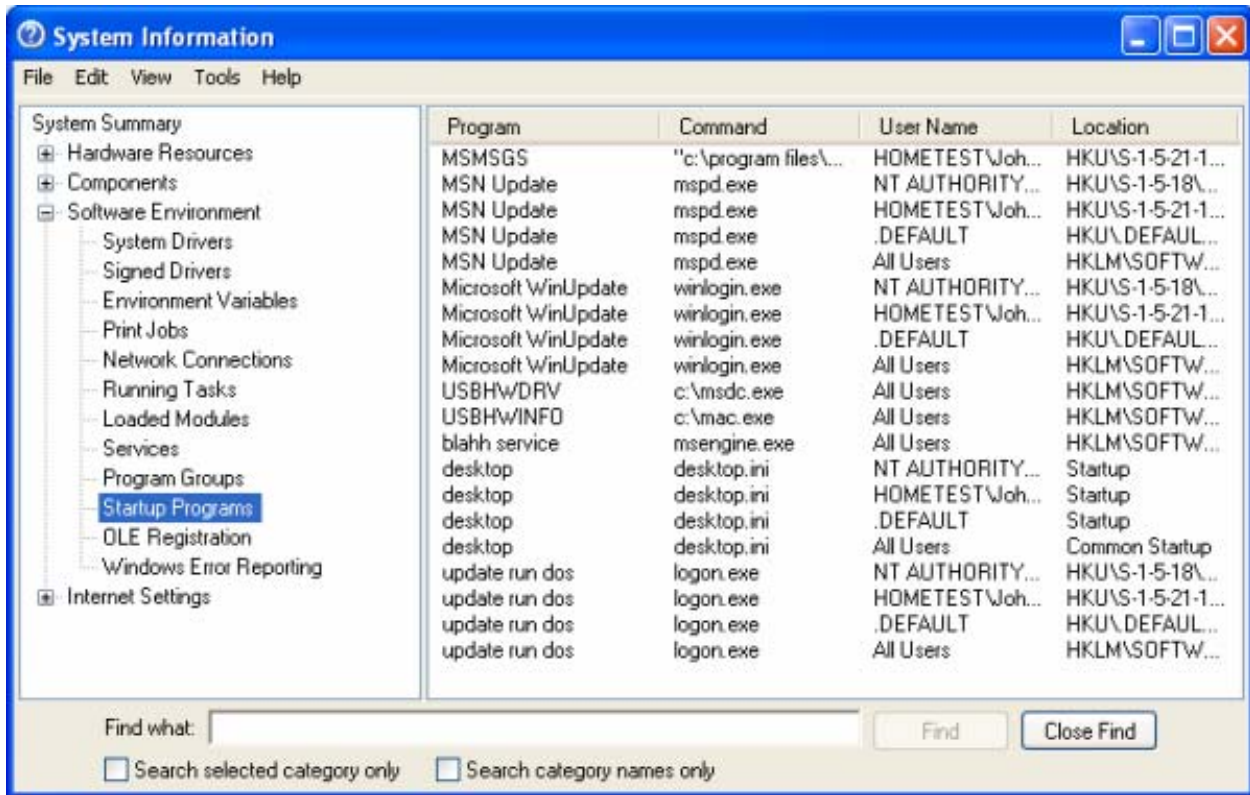


Figure 5-7. Startup Programs

If the Microsoft Windows Defender program is installed, it can be used to view and edit information on startup programs and currently running programs. To do so, run Windows Defender and use the **Software Explorer** option of the **Tools** menu, as shown in Figure 5-8.

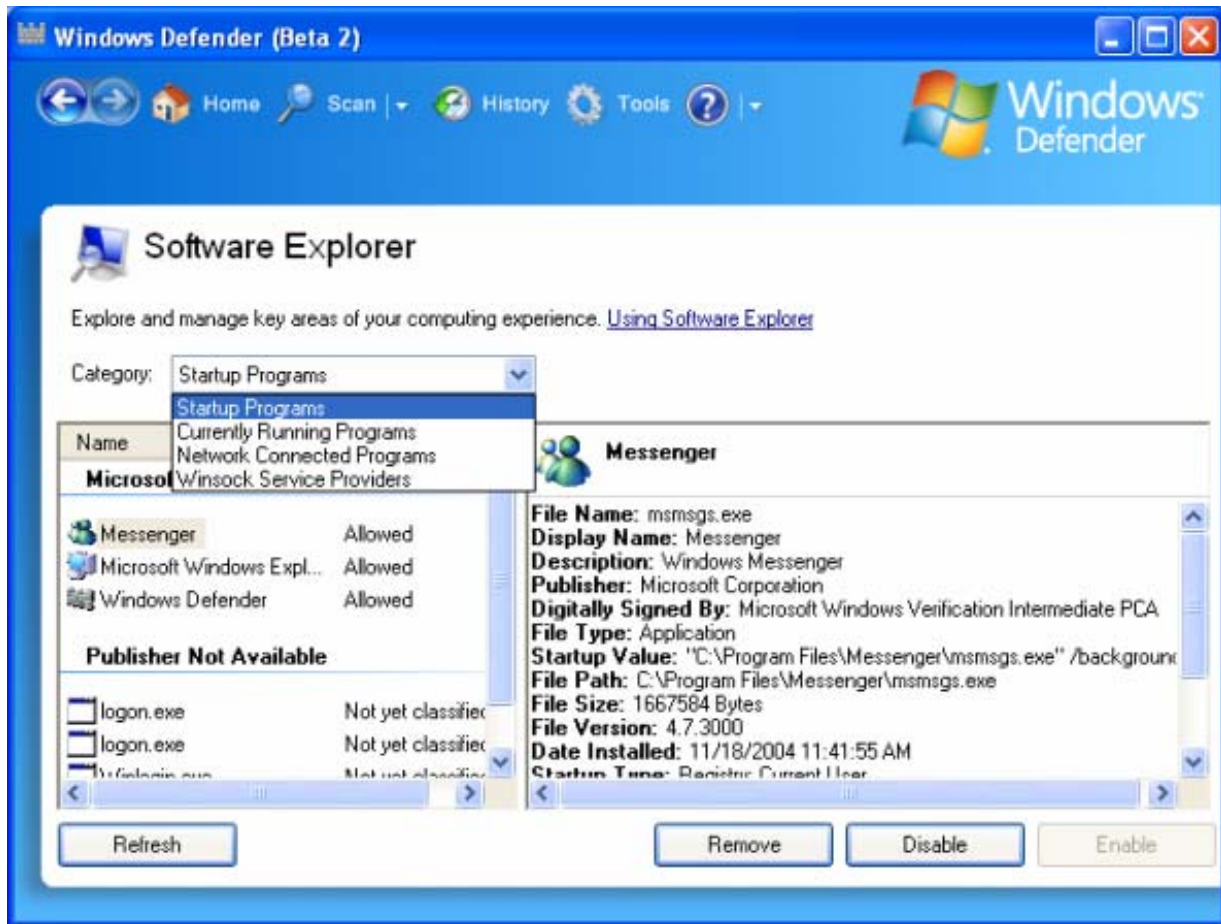


Figure 5-8. Windows Defender

---

---

## 5.6 Summary

A new Windows XP Home Edition computer should be secured properly before it is used or connected to a network to minimize the possibility of a security breach. As a first step, users should perform preparatory actions, including gathering needed materials, setting the default view for Control Panel, and identifying the Windows XP Home Edition service pack currently in use. The next step is to apply updates to the computer. Before doing this, a personal firewall needs to be set up on the computer to block malicious activity from other computers. Until the computer has been fully updated, applications such as e-mail clients should not be used; the only application use should be that which is required to update the computer or configure the personal firewall. Microsoft Update provides a convenient way to identify, download, and install updates for Windows XP Home Edition and selected Microsoft applications. Windows XP Home Edition computers should also be configured to use the built-in Automatic Updates feature, which helps to keep the computer up-to-date.

After completing the updating process, the next step in securing a Windows XP Home Edition computer is installing and configuring additional security software. Antivirus software is a necessity; antispyware software should also be installed if the antivirus software does not include a robust antispyware capability. Users may also want to use content filtering software, such as spam and Web content filtering software, and a third-party personal firewall.

Once security software has been installed and configured, the next step is to alter the Windows XP Home Edition configuration to further improve security. This includes creating separate password-protected user accounts for each person, securing networking features, protecting temporary files, and configuring folder sharing. A helpful next step is to identify the software applications installed on the computer; such a list of applications can be used in the future to find malware and spyware by comparing the original list of the applications to the current one and investigating all differences.

The instructions provided in this section are only part of the process of installing and securing Windows XP Home Edition. Section 4 describes the complete process. After the instructions in Section 4 have been completed, each user account still needs to be secured, as described in Section 7.

**This page has been left blank intentionally.**

## **6. Securing an Existing Windows XP Home Edition Installation**

Section 5 describes how to secure a computer with a new installation of Windows XP Home Edition. This section provides similar guidance for computers with previously used installations of Windows XP Home Edition. It is generally preferable to secure a new installation rather than a previously used installation. The security state of a previously used installation is often unknown, so it may take considerable time to determine if the computer has been infected with malware or attacked successfully in other ways. If the damage to the computer caused by infections or attacks is serious, it is recommended to reinstall Windows XP Home Edition and secure the new installation.

Although it is usually preferable to secure a new installation, users may decide in some cases that it is more convenient to secure an existing installation instead. For example, if a computer has been running antivirus software and other security controls, and the computer has many applications installed and large amounts of data stored on the computer's hard drive, users may consider it to be unnecessary and overly time-consuming to back up all of the data, reinstall Windows XP Home Edition and all of the applications, and restore all of the data. In such cases, users should follow the directions provided in this section to secure their computers. Users should still be prepared to reinstall Windows XP Home Edition if their computers have been affected significantly by malware or other attacks.

---

---

### **6.1 Prepare to Secure the System**

Users need to perform some preparatory actions before beginning to secure a computer. Section 5.1 describes three categories of actions: gathering needed materials, setting the default view for Control Panel, and identifying the service pack currently in use. Users should perform all the actions described in Section 5.1.

---

---

### **6.2 Assess the Computer's Security**

After the preparatory actions have been completed, the user should assess the current state of the security of the computer. Essentially, the user should attempt to determine if the computer has adequate security controls in place and if there is evidence of a successful attack, such as a worm infection or spyware installation. This section describes actions that users can perform to make such an assessment.

---

#### **6.2.1 Identify Installed Programs**

Users should determine which software applications (and versions of each) are installed on the computer. These include Web browsers, e-mail clients, office productivity tools (e.g., word processors, spreadsheets), instant messaging software, multimedia utilities (e.g., audio players), graphics tools, and security software (e.g., antivirus software, personal firewall). The two primary ways of identifying the installed applications are as follows:

- From the **Control Panel**, run the **Add or Remove Programs** utility. It shows which software applications are installed on the computer, as well as security updates, hardware drivers, and other types of programs.
- Review the folders and icons on the Start Menu and the Desktop to find application shortcuts listed there.

The primary purpose of identifying the applications on the computer is to attempt to remove all applications that are not desired. Examples include the following:

- Software installed on the computer by unauthorized parties or their automated mechanisms (e.g., malware). This software may be malicious.
- Malicious software such as spyware inadvertently installed onto the computer by authorized users.<sup>87</sup>
- Software that was installed by authorized users or the computer's vendor but is no longer needed. Although such software might not be directly harmful to the computer, current or future vulnerabilities in the software could potentially be exploited in attacks, especially if the software is not maintained regularly.

**Removing needed applications can significantly impair the functionality of the computer. If users are unsure whether particular applications should be removed, they should review the documentation for the applications, perform research using data sources on the Internet, or seek expert guidance so that they understand exactly what functionality the application provides.**

To remove applications, perform the following steps:

1. From the **Control Panel**, run the **Add or Remove Programs** utility.
2. Select the application that should be removed and click on the **Remove** or **Change/Remove** button (whichever is available).
3. Follow the prompts provided by the application's uninstall program.
4. If prompted to reboot the computer so that changes will take effect, first close all other open programs, and then reboot the computer. If several applications are being uninstalled, generally it is acceptable to perform steps 2 and 3 repeatedly, then perform a single reboot of the computer.

Another important reason to identify installed applications is to determine if the needed security software is on the computer. Antivirus software is a necessity; additionally, antispyware software should be used if the antivirus software does not have robust antispyware capabilities. The computer should also use a personal firewall (either the Windows Firewall built into Windows XP Home Edition or a third-party personal firewall). Users should acquire and install

---

<sup>87</sup> Most malware will not appear in application listings. It will need to be removed using antivirus software.



any security software that the computer is lacking. Section 6.2.3 provides additional information on this.

---

## 6.2.2 Identify Running Applications and Startup Programs

Users should determine which applications are currently running on the computer and which applications are configured to start automatically when Windows XP Home Edition is loaded. This can be done through the System Information utility. Section 5.5 contains step-by-step instructions for doing this. Creating a list of applications running on the computer and applications configured to start automatically can be helpful for troubleshooting future problems.

---

## 6.2.3 Check Security Software Configuration

After identifying installed software and removing unneeded programs, the next step is to ensure that the security software on the computer is enabled and configured correctly. Section 6.2.1 discusses the types of security software and provides guidance on identifying what security software is installed on the computer.

Periodically, users should review the status and configuration of each security application to confirm that it is still providing the expected level of protection.<sup>88</sup> To do a status and configuration review, perform the following steps for each security application, based on the documentation provided by the software vendors:

1. Ensure that the application is configured to run automatically at system restart and is enabled by default.
2. Ensure that the application is configured to update itself automatically (if such functionality is available) and that the application software, signatures, and other components are all up-to-date.
3. Ensure that the application is configured in accordance with the recommendations provided in Section 3.3.

If any significant misconfigurations are found during the review, this indicates an increased likelihood that the computer has been attacked successfully by malware or other threats. For example, many instances of malware attempt to disable antivirus software, personal firewalls, and other security tools. Even a properly secured computer can still be compromised, so users should not assume that a properly secured computer does not merit attention to its security. Rather, a poorly secured computer generally requires greater attention than a properly secured computer in performing a security review, configuring the computer's security, and addressing existing security problems, such as malware infections.

---

<sup>88</sup> As described in Section 3.3, the Security Center provides status and some configuration information for the computer's antivirus software and personal firewall software. The information provided by the Security Center might not be sufficient to do the status and configuration review described in this section. In that case, users should check the antivirus software or personal firewall configuration settings within the individual application itself, and not through the Security Center.

---

---

## 6.3 Identify and Remove Malware

The next step in securing an existing Windows XP Home Edition computer is to identify and remove any malware on the computer.<sup>89</sup> Common signs of a malware infection include the following:

- The computer's antivirus software, antispymware software, or personal firewall reports possible malware activity
- The computer's antivirus software, antispymware software, or personal firewall is disabled but the computer's users and administrators did not disable it
- The computer does not load Windows XP Home Edition, or error messages are displayed while it is loading
- Windows XP Home Edition or applications hang or crash
- Applications start slowly, run slowly, or do not run at all
- The computer's hardware is being used unexpectedly, such as a hard drive thrashing with heavy activity or a network card showing high volumes of communications
- Unknown applications are running on the computer
- The number of e-mails being sent and received suddenly increases
- Unexpected changes occur to the templates for word processing documents, spreadsheets, and other common types of files
- The Web browser's configuration is altered, such as the appearance of a different home page or a new toolbar
- User files are deleted, corrupted, or otherwise inaccessible
- Unusual items appear on the screen, such as odd messages, graphics, and overlapping or overlaid message boxes
- Unexpected dialog boxes appear, requesting permission to do something
- Personal firewall logs show that the computer has been connecting to unknown computers.

Most of these signs could be caused by something other than malware, such as a faulty application or a hardware failure. Accordingly, the occurrence of some of these signs should be a cause for further investigation, but is not a definite indication that there is a malware infection.

---

### 6.3.1 Malware Scanning Options

When securing an existing computer, users should perform a full scan of the computer using antivirus software (and antispymware software, if applicable) to identify and remove any malware

---

<sup>89</sup> This should be done before applying Windows XP Home Edition updates because certain types of malware can interfere with installing updates.

on the computer (e.g., quarantine, disinfect, or delete affected files).<sup>90</sup> This can be done using any of the following:

- **Antivirus or antispyware software installed on the computer.** In many cases it is possible to remove malware using the antivirus or antispyware software already installed on the computer. Many antivirus and antispyware vendors also make specialized utilities that can detect and eliminate one specific instance of malware, such as a new worm. If it is already known which malware has infected a computer, and a specialized removal utility for that malware is available, then the utility could be placed onto the computer and run in an attempt to remove the malware.
- **Antivirus or antispyware software on media** (e.g., CD, flash drive, external hard drive). An alternative to running antivirus or antispyware software or specialized removal utilities from a computer is to run them from separate media. The media can be protected or accessed in such a way that it cannot be infected by malware. This can be very helpful when scanning for malware because certain types of malware interfere with security software, such as modifying or reconfiguring antivirus software so that it does not report infections. In such cases, it is much more effective to perform malware scans from protected media.
- **Online malware scanning service.** Some antivirus and antispyware software vendors offer Internet-based malware scanning services. Unlike antivirus or antispyware software installed on a computer, which constantly checks the computer for malware, an online malware scanner is run only when a user manually activates it, so such services are not a substitute for antivirus and antispyware software. However, if the software on the computer has been damaged by malware, an online service could be helpful in cleaning the computer.

Users should rely primarily on the antivirus and antispyware software installed on their computers for finding and removing malware. Using separate media can be more effective, but it can require considerable expertise and effort to create and maintain the media with all the necessary up-to-date utilities. Section 6.3.2 provides instructions for using antivirus and antispyware software on a computer to eradicate malware. If these efforts are unsuccessful, users should try an online malware scanning service from a major antivirus or antispyware software vendor. If this does not work, users should ask an expert to examine their computers and attempt to clean them. Experts can provide assistance on creating, maintaining, and using separate media to scan computers in such situations.

---

### 6.3.2 Removing Malware

On an infected computer, users should try to remove the malware using the computer's antivirus and antispyware software. The steps listed below provide general guidance for attempting to remove malware.<sup>91</sup> Vendors of antivirus and antispyware software often provide detailed instructions for removing malware, such as specific steps for removing a particular virus or worm. Once the specific type of malware on a system has been identified, consider checking the antivirus and antispyware software vendors' Web sites for more suggestions on how to remove

<sup>90</sup> As described in Section 3.3.1, the Windows Malicious Software Removal Tool is a free utility provided by Microsoft that users can run to identify and eliminate certain common instances of malware.

<sup>91</sup> An additional source of general guidance for removing malware is *Recovering from a Trojan Horse or Virus* by Michael Durkota of US-CERT, available at [http://www.us-cert.gov/reading\\_room/trojan-recovery.pdf](http://www.us-cert.gov/reading_room/trojan-recovery.pdf).

it. If the antivirus or antispyware software has specific removal procedures, these should be followed instead of the general guidance below.

*Before attempting to remove malware, users should perform a backup of their critical personal data in case the malware or the malware removal process causes damage to the data. Directions on performing backups are provided in Section 4.2. Users should be cautious with the backups because they might contain malware-infected files. Once all malware has been removed from the computer and the antivirus and antispyware programs are fully updated, the backup media should be fully scanned by the antivirus and antispyware programs to determine if any of the files are infected.*

Follow these steps to attempt to remove malware:

1. Have the antivirus and antispyware software check for updates to verify that they are fully up-to-date. If any updates are available, apply them.<sup>92</sup>
2. Close all of the applications running on the computer except for security tools such as antivirus software, antispyware software, and personal firewalls. Applications that should definitely be closed include Web browsers, e-mail clients, office productivity tools, and instant messaging clients.
3. Disconnect all of the computer's network connections. This could include one or more of the following:
  - Disconnecting a call made by a telephone modem
  - Unplugging a network cable from the computer
  - Disabling a wireless network card. To do so, perform the following steps:
    - a. From the **Control Panel**, double-click on **Network Connections**.
    - b. Right-click the wireless network card and select **Disable**.
    - c. Close the **Network Connections** window.
4. Turn off the System Restore feature, because it can cause malware that is removed from the computer to be restored inadvertently.
  - a. Right-click on **My Computer**, then choose **Properties**.
  - b. Click the **System Restore** tab. Select **Turn off System Restore**.
  - c. Click on **Apply**, then **Yes**, then **OK**.

---

<sup>92</sup> If the computer is disconnected from the network, or can no longer be connected to a network, the antivirus software and antispyware software could possibly be updated by downloading the updates from an uninfected computer, placing them onto removable media (e.g., CD), and using the removable media in the infected computer to update the antivirus and antispyware software.

5. Run the antivirus software, antispyware software, or specialized malware removal tool. Follow the vendor's instructions to perform a full scan and to remove any malware from the computer (including disinfecting or quarantining all infected files).
6. Based on the results of the scan listed below, perform the appropriate actions:
  - **Malware was found and eliminated or quarantined.** Perform another full scan to confirm that there is no longer any malware on the computer. If no malware is present, go to Step 7. If malware is found, start Step 6 again.
  - **Malware was found but could not be eliminated or quarantined.** Certain types of malware can only be removed when the computer is booted in safe mode. To run the scanning software from safe mode, perform the following steps:
    - a. Reboot the computer. As soon as the initial hardware self-test is done, press the **F8** key. This should cause the Windows Advanced Options menu to be displayed.
      - i. If the menu is displayed, choose **Safe Mode**.
      - ii. If the menu is not displayed, reboot the computer again and hit the **F8** key repeatedly shortly after the computer restarts. When the menu is displayed, choose **Safe Mode**.
    - b. Perform a full scan. The malware should be eliminated or quarantined during the scan.
    - c. After the scan has completed, perform another scan to confirm that no more malware is remaining.
  - **The scan failed or could not be performed.** The malware might be interfering with the scanning. Perform steps **6a** through **6c** as listed above.
7. Once all malware is removed from the computer, re-enable System Restore:
  - a. Right-click on **My Computer**, then choose **Properties**.
  - b. Click the **System Restore** tab. Uncheck the **Turn off System Restore option**.
  - c. Click on **Apply**, then **Yes**, then **OK**.
8. Reconnect the network connections. This could include one or more of the following:
  - Making a phone call with a telephone modem
  - Plugging a network cable into the computer
  - Enabling a wireless network card. To do so, perform the following steps:
    - a. From the **Control Panel**, double-click on **Network Connections**.

- b. Right-click the wireless network card and select **Enable**.
  - c. Close the **Network Connections** window.
9. Update all antivirus and antispymware software on the computer. It may be necessary to perform multiple updates, since some updates need to be applied consecutively. Also, check the configuration of the antivirus and antispymware software to ensure that it corresponds to the guidance provided in Section 3.3.1.

*If all malware cannot be removed from the computer, seek expert assistance, as described in Section 8.5.1. If the malware cannot be removed completely from the computer by an expert, or the malware causes serious damage to the computer's operating system, it might be necessary to reinstall Windows XP Home Edition and all applications, and restore user data from backups. Continuing to operate a computer that is infected with malware could cause other computers to become infected, other files and data to become damaged or destroyed, and personal data such as passwords, credit card numbers, and PIN numbers to be provided to unauthorized parties.*

---

---

## 6.4 Secure the Computer

If the scans described in Section 6.3 indicate that the computer does not have any malware, or the scans are successful at removing all malware from the computer, the user should continue securing the computer using the directions presented in Section 5, starting with Section 5.2. The major steps presented in Section 5 for securing the computer are as follows:

1. Apply updates to Windows XP Home Edition, and configure it to update itself automatically in the future.
2. Install and configure additional security software, such as antivirus software and a personal firewall.
3. Alter the default Windows XP Home Edition configuration to further improve security.
4. Document the installed software applications for future use in troubleshooting problems.

If all malware cannot be removed from the computer, the user should seek expert assistance, as described in Section 8.5.1, or follow the directions in Section 8.5.2 for attempting to recover the system (e.g., restoring it from a backup, reinstalling Windows XP Home Edition).

---

---

## 6.5 Summary

Although it is usually preferable to secure a new installation of Windows XP Home Edition, users may decide in some cases that it is more convenient to secure an existing installation instead. Because the security state of a previously used installation is often unknown, it may take considerable time to determine if the computer has been infected with malware or attacked

successfully in other ways. If the computer has suffered serious damage, it may be necessary to reinstall Windows XP Home Edition and secure the new installation instead.

Before beginning to secure an existing installation, a user should perform preparatory actions, including gathering needed materials, setting the default view for Control Panel, and identifying the service pack currently in use. The next step is to assess the current state of the security of the computer; the main focus of this is ensuring that security software is installed and up-to-date, as well as checking its configuration. The computer should then be scanned for malware, and all identified malware removed. The security of the computer needs to be maintained on an ongoing basis, as described in Section 8.

**This page has been left blank intentionally.**



## 7. Securing User Accounts and Settings

This section provides recommendations for securing each individual user account on a Windows XP Home Edition computer. The steps in this section should be performed for every user account, including each administrative account. Section 7.1 explains necessary changes to user accounts and files. The rest of Section 7 discusses changes to application configurations that should improve security. The types of applications covered in this section are e-mail clients, Web browsers, instant messaging clients, and office productivity suites. Users should also consider disabling unneeded features and capabilities from other applications whenever possible.

---

---

### 7.1 Secure User Accounts and Files

This section contains the following recommendations for securing user accounts and files on a Windows XP Home Edition computer:

- Setting a strong password for each user account
- Configuring each user's folder to be private
- Modifying settings for file associations and extensions.

---

#### 7.1.1 Set a strong password for each account

The user should log on; no password is required. As soon as logon is complete, the user should perform the following steps to set a password:

1. From the **Control Panel**, double-click on **User Accounts**.
2. Click **Create a password**.
3. Enter a new password and type it once more to confirm it. Do not enter a password hint. Click the **Create Password** button.
4. Close the **User Accounts** window.

---

#### 7.1.2 Make the user's folder private

By default, the user's files and folders are available to other users of the computer, as described in Section 3.2.2. To change this, the user should perform the following steps:

1. From the **Start** menu, double-click on **My Computer**.
2. Locate the letter for the drive where Windows XP Home Edition is installed (typically **C:**). Open the **\Documents and Settings** folder (click **Show the contents of this folder** if necessary). Within it, find the folder that matches the username. The folder should contain the user's My Documents folder, as well as the user's desktop, cookies, favorites, start menu icons, and other user-specific information.

3. Right-click on the user's folder and click on **Properties**. Click on the **Sharing** tab. Check the box labeled **Make this folder private**.
4. Click on **OK**.

---

### 7.1.3 Modify settings for file associations and extensions

Perform the following steps to modify the settings for default file associations and the display of file extensions, which should help to prevent some successful malware attacks (as described in Section 3.1.4):

1. From the **Control Panel**, select **Folder Options**.
2. Select the **View** tab. In the **Advanced settings** area, make the following settings:
  - a. Uncheck the box for **Automatically search for network folders and printers**.
  - b. Check the box for **Display the contents of system folders**.
  - c. Uncheck the box for **Hide extensions for known file types**.
3. Click the **Close** button.

---

---

## 7.2 Configure E-mail Clients

Make the following changes (described in Section 3.3.6.2) to the configuration of each e-mail client on a Windows XP Home Edition computer:

- Change the default message reading format to plain text. This can cause pictures, hyperlinks, and other content provided through HTML to be omitted or displayed only through alternative text. The default message sending format should also be set to plain text as a courtesy to other security-conscious users that will be reading the e-mails.
- Disable the automatic download of remote graphics. With this setting in place, most e-mail clients will tell the user if an e-mail contains remote graphics and allow the user to choose to download them.
- Disable mobile code support. By default, ActiveX and Javascript mobile code support should be disabled within e-mail messages.
- Disable the automatic opening of e-mail messages.

Appendix C.4 contains step-by-step instructions for implementing these recommendations for three e-mail clients: Eudora, Microsoft Outlook Express, and Thunderbird. Users with other e-mail clients should consult the vendor's documentation for guidance on altering these settings.

---

---

### 7.3 Configure Web Browsers

Make the following changes (described in Sections 3.2.1 and 3.3) to the configuration of each Web browser for each user on a Windows XP Home Edition computer:

- Enable popup blocking and configure it to permit trusted Web sites to create popup windows
- Change cookie handling practices so that session cookies and first-party cookies are allowed, and third-party cookies are rejected
- Do not store passwords automatically
- Prevent software installation within the browser.

Appendix C.5 contains step-by-step instructions for implementing these recommendations for three Web browsers: Firefox, Microsoft Internet Explorer, and Mozilla. Users with other Web browsers should consult the vendor's documentation for guidance on altering these settings.

---

---

### 7.4 Configure Instant Messaging Clients

As described in Section 3.3.6.3, users should review the configuration settings for their instant messaging clients and identify settings that are related to security and privacy. For example, instant messaging clients typically permit users to suppress the display of their e-mail addresses; this helps to preserve users' privacy. Also, requiring each incoming file transfer to be approved by the user can prevent malicious parties from transferring malware to the computer. Appendix C.6 contains step-by-step instructions for implementing these recommendations for three instant messaging clients: AOL Instant Messenger (AIM), Windows Messenger, and Yahoo! Messenger.

---

---

### 7.5 Configure Office Productivity Suites

Users should review the configuration settings for their office productivity suite programs (e.g., word processor, spreadsheet, database) and make the following changes to each program, as described in Section 3.3.6.4, based on the vendor's documentation that support increased security and privacy:

- Prompt the user to accept or reject running each macro
- Limit the personal information (e.g., mailing address, phone number) stored in the user settings
- Use folders within My Documents or other user-specific areas as the default locations for saving documents and holding temporary files (including auto-save and backup copies of documents)
- Store custom dictionary entries in a user-specific file in one of the user's protected folders.

Appendix C.6 contains step-by-step instructions for implementing these recommendations for three instant messaging clients: AOL Instant Messenger (AIM), Windows Messenger, and Yahoo! Messenger.

---

---

## **7.6 Summary**

Each user account on a Windows XP Home Edition computer, including the administrative accounts, should be secured. This includes setting a strong password and protecting it, configuring the personal folder to be private, and modifying default settings for file associations and extensions. Each user's e-mail client and Web browser configuration settings also need to be altered to improve their security. For e-mail clients, this includes reading messages in plain text, not downloading remote graphics automatically, not opening new messages automatically, and disabling mobile code support. Web browsers should be configured to block unwanted popup windows, to not store passwords automatically, to prevent software installation, and to handle cookies in a way that balances functionality and privacy. Users should also make minor security-enhancing configuration changes to instant messaging clients and office productivity suites.

After all user accounts have been secured, the security of the computer and the user accounts needs to be maintained on an ongoing basis. Section 8 contains advice for doing so.

## 8. Maintaining and Monitoring a Computer's Security

After a Windows XP Home Edition computer has been secured using the guidance provided in Section 5 or 6, the computer's security needs to be maintained on an ongoing basis. This section provides guidance and step-by-step instructions for maintaining the security of a Windows XP Home Edition computer. This section assumes that the advice provided in Section 5 or 6 has already been applied properly to the computer. The administrators and users of a Windows XP Home Edition computer share the responsibility for maintaining the computer's security, so this section provides specific recommendations for each of them.

---

---

### 8.1 Perform Backups and Restore Data As Needed

The administrator of the computer or the individual users should perform backups of their data and settings on a regular basis. Sections 4.2 and 4.5 describe how to perform backups and restore information from backups, respectively.

---

---

### 8.2 Perform Administrative Maintenance

Administrators are primarily responsible for maintaining the security of Windows XP Home Edition computers. Their responsibilities fall into the following categories:

- Ensuring that Windows XP Home Edition and application updates are applied
- Checking the status of security software
- Creating new user accounts
- Deleting old system restores
- Creating new system restore points
- Reviewing shared folders
- Synchronizing the computer's clock
- Retiring user accounts that are no longer needed.

---

#### 8.2.1 Apply Updates

As described in Section 3.1.1, administrators should keep the Windows XP Home Edition operating system and applications up-to-date. This is particularly important for security-related OS and application patches, as well as updates for security software such as malware prevention and intrusion detection software, which need to download information on the latest attacks to be able to recognize them. See Section 5.2 for instructions on configuring Windows XP Home Edition and applications to update themselves automatically.<sup>93</sup> For applications that do not offer

---

<sup>93</sup> Even if Automatic Updates is configured to download and install updates automatically, users should also run Microsoft Update periodically because it can retrieve lower-priority updates that Automatic Updates cannot.

this feature, administrators should check for updates on a regular basis and ensure that they are installed and configured properly.

Administrators should also consider subscribing to mailing lists that announce the availability of updates for the software that they use. For example, Microsoft offers a service called Security Update Alerts, which provides information about new security concerns through e-mail, instant messaging, and other means.<sup>94</sup> Many vendors send out e-mails as soon as new versions of their software are available. Subscribing to such lists is particularly important for applications that lack automatic updating capabilities.

It may also be necessary to acquire, install, and configure completely new versions of security software occasionally (e.g., every few years), instead of upgrading existing software. This may be due to a software vendor dropping support for an older version of the software, or additional beneficial features in a newer version of the software.

---

### **8.2.2 Check the Status of Security Software**

Administrators should periodically check the status of the computer's security software to ensure that it is still enabled, configured properly, and up-to-date. If a computer becomes infected with malware, the malware may disable or uninstall some of the security software, allowing many more infections to occur. Accordingly, it is important to check the status of the security applications frequently. This includes verifying that regular scans performed by antivirus software and antispyware software (if applicable) find no infections on the computer.

Administrators should also review the alerts and log messages created by security software to ensure that automatic updates are being performed successfully on a regular basis. For example, Figure 8-1 shows an example of Security Center reporting that a computer's antivirus software is out of date. Section 6.2 contains specific recommendations and directions for checking the status of security software.

---

<sup>94</sup> More information on Microsoft Security Update Alerts is available at <http://www.microsoft.com/security/bulletins/alerts.aspx>.



**Figure 8-1. Security Center Status Reporting**

---

### 8.2.3 Create New User Accounts

Whenever another person needs to start using the computer, the administrator should create a new user account, based on the instructions in Section 5.4.1. Also, a person with a new user account should follow the directions in Section 7 to secure the account.

---

### 8.2.4 Delete Old System Restore Points

A *system restore point* is a snapshot of the configuration of a Windows XP Home Edition computer. System restore points are typically saved automatically both periodically and when new software is installed onto the computer. Administrators should delete old system restore points periodically, perhaps once every three months (more often if free hard drive space is low). The Disk Cleanup utility built into Windows XP Home Edition can be used to purge several types of files, including system restore points, from Windows XP Home Edition computers. Because this eliminates all system restores except the most recent, it should be performed only when the system is functioning normally and has not been changed significantly recently. To remove the old system restores, perform the following steps:

1. From the **Start** menu, select **All Programs**, then **Accessories**, then **System Tools**. From there, choose **Disk Cleanup**.
2. It may take a few minutes for the Disk Cleanup utility to load and perform its initial space calculations. When the utility completes loading, clear the checkboxes in the **Files to delete** box.
3. Select the **More Options** tab. Click on the **Clean up...** button in the **System Restore** window pane. When asked to confirm that the old restores should be deleted, click the **Yes** button.
4. Next, click **OK** in the **Disk Cleanup** window. Click **Yes** again to confirm the deletions.

---

### 8.2.5 Create New System Restore Points

Administrators may want to create new system restore points manually on occasion, such as before installing a new application or applying application updates. To create a restore point manually, perform the following steps:

1. From the **Start** menu, select **All Programs**, then **Accessories**, then **System Tools**. From there, choose **System Restore**.
2. From the introductory screen, choose **Create a restore point**.
3. Create a descriptive name for the restore point. When finished, click **Create**.

---

### 8.2.6 Review Shared Folders

Administrators should review the list of shared folders periodically to ensure that all folders being shared should be. To do so, perform the following steps:

1. Right-click on **My Computer** and select **Manage**.
2. Under **Shared Folders**, click on **Shares**. As Figure 8-2 illustrates, this should show the default IPC\$ share, which is standard on every Windows XP Home Edition computer, as well as all administrator or user-created shares that are intended to be accessed by others. If any other shares are shown, the administrator should talk to the user that set up the share to determine if others should be able to access it.

Shared F...	Shared Path	Type	# Client Connections
Cdrive	C:\	Windows	0
Documents	C:\Documents and ...	Windows	0
IPC\$		Windows	0
Shared Folder	C:\test	Windows	0

**Figure 8-2. Shared Folders**



---

## 8.2.7 Synchronize the Computer's Clock

Administrators should periodically check to make sure that the computer's clock is reasonably accurate. This is beneficial for general computer use, such as having the correct timestamp in e-mails that are sent, but it also has security benefits. For example, if an expert is reviewing a computer's logs to investigate a security problem, having accurate timestamps in the logs can help the expert to correlate log entries with actions performed by the computer's user.

Administrators can manually adjust the clock by performing the following steps:

1. From the **Start** menu, select **Control Panel**, then double-click on the **Date and Time** icon.
2. Adjust the date, time, and time zone settings as needed.
3. Click on **OK** when completed.

Administrators can also configure Windows XP Home Edition computers to synchronize their clocks automatically with an authoritative external time server. These time servers are extremely accurate and can be used for free. Administrators can perform the following steps to set up automated synchronization:

1. From the **Start** menu, select **Control Panel**, then double-click on the **Date and Time** icon.
2. Click on the **Internet Time** tab.
3. Check the box labeled **Automatically synchronize with an Internet time server**. Choose either **time.windows.com** or **time.nist.gov**.
4. To test the configuration, click the **Update Now** button. It might take a minute for the synchronization to occur; status messages should be displayed during the update. If it completes successfully, a success message should be displayed.
5. Click on **OK** when completed.

If automated synchronization is enabled, administrators should check its status periodically to ensure that it is working properly. To do so, perform the following steps:

1. From the **Start** menu, select **Control Panel**, then double-click on the **Date and Time** icon.
2. Click on the **Internet Time** tab.
3. Review the status message in the middle of the window. It should say that the time has been successfully synchronized within the past few weeks. If not, click the **Update Now** button to trigger another synchronization attempt.

4. Click on **OK** when completed.

---

### 8.2.8 Retire Unneeded User Accounts

When a person no longer needs to be using a computer, the administrator should retire that person's user account. If the user who no longer needs access is an administrator of the computer, then a new administrative account should be created for the person who will become the new administrator, and the previous administrator's user and administrative accounts both deleted. A new administrative account can be set up using the instructions in Section 5.4.1; the only difference is that the account should be set up as a computer administrative account instead of a limited user account.

To delete a user or administrative account that is no longer needed, perform the following steps:

1. From the **Control Panel**, double-click on **User Accounts**.
2. Select the account to be deleted.
3. Choose the **Delete the account** option. Windows XP Home Edition prompts the person performing the deletion to save the user's files. To save them, choose the **Keep Files** option, otherwise choose the **Delete Files** option.
4. Click **Delete Account** to delete the user account.
5. Close **User Accounts**.

---

---

## 8.3 Perform User Maintenance

Each user of a Windows XP Home Edition computer, including administrative account users, should perform security-related maintenance duties periodically. These responsibilities fall into the following categories:

- Changing Windows XP Home Edition passwords regularly
- Deleting unneeded files
- Clearing information from Web browsers.

Users should also monitor the Security Center on an ongoing basis. If Security Center determines that the computer's antivirus software or personal firewall is disabled or uninstalled, it should notify the user at login and display a red icon in the taskbar to alert the user of the issue. This is helpful in identifying major problems with the antivirus software or personal firewall on a daily basis. The user should then contact the computer's administrator as soon as possible so that the problem can be corrected.

### 8.3.1 Change Windows XP Home Edition Password Regularly

If passwords are being used on a Windows XP Home Edition computer, users should change their Windows XP Home Edition passwords regularly—at least once every three months—as well as changing them immediately if it is suspected or known that an unauthorized person has learned them. Section 3.1.2.2 describes recommendations for password strength. To change a Windows XP Home Edition password, perform the following steps:

1. From the **Control Panel**, double-click on **User Accounts**.
2. Choose the **Change my password** option.
3. Enter the old password, then enter a new password and type it once more to confirm it. Do not enter a password hint. When done, click the **Change Password** button.

---

### 8.3.2 Delete Unneeded Files

Users who are particularly concerned about the privacy of their information should delete unneeded files periodically. The Disk Cleanup utility built into Windows XP Home Edition can delete files stored in several places, including Web browser caches (also called Temporary Internet Files), the Recycle Bin, and temporary files. To do so, perform the following steps:

1. From the **Start** menu, select **All Programs**, then **Accessories**, then **System Tools**. From there, choose **Disk Cleanup**.
2. It may take a few minutes for the Disk Cleanup utility to load and perform its initial space calculations. When the utility completes loading, review the descriptions and recommendations for each item in the **Files to delete** box. Select the appropriate checkboxes or accept the default suggestions.
3. When done, click **OK**, then confirm with **Yes**. It may take a while to delete the files, depending on the volume of files to delete and the hardware capabilities of the computer.

---

### 8.3.3 Clear Web Browser Information

Users may also wish to clear the Web browser history and delete cookies periodically as additional measures in protecting their privacy. To do so for Internet Explorer 6.0, perform the following steps:

1. Run **Internet Explorer**.
2. From the **Tools** menu, select **Internet Options**.
3. To clear the history, click on the **Clear History** button and then choose **Yes** to confirm the deletion.
4. To delete cookies, click on the **Delete Cookies** button and then choose **OK** to confirm the deletion.

5. Close **Internet Explorer**.

---

---

## 8.4 Identify Security Issues

Administrators should use security assessment tools periodically to identify security issues on Windows XP Home Edition computers. Many utilities are available to identify security issues on a local computer. The Microsoft Baseline Security Analyzer (MBSA) is a free security assessment utility that is particularly helpful for Windows XP Home Edition security. For Windows XP Home Edition and some common Microsoft applications (e.g., Internet Explorer, Office), MBSA can identify which updates are missing and certain other security issues, such as insecure configurations and settings. MBSA identifies the problems and also provides recommendations for fixing each problem. For example, a user can click on a Download icon to retrieve an update. MBSA must be run from an administrative account.

*Administrators may need considerable expertise in computer security and Windows XP Home Edition to understand all of the security issues and recommendations in MBSA reports. Administrators without this expertise should use MBSA in conjunction with an expert that can provide guidance on the MBSA reports.*

To acquire MBSA, perform the following steps:

1. From **Internet Explorer**, go to the MBSA Web site, which is located at <http://www.microsoft.com/technet/security/tools/mbsahome.mspx>.
2. Click on the hyperlink for the newest version of MBSA.
3. Scroll down the page and choose to download the English version of MBSA. If Windows validation is required, follow the prompts to allow validation to occur.
4. Scroll down the download page to the **Files in This Download** section. Choose the English version of the file, **MBSASetup-EN.msi**.
5. When prompted to open or save the file, choose **Save**, specify a location for the file, and click on **Save**.
6. Close **Internet Explorer**.

To install MBSA, perform the following steps:

1. Double-click on the **MBSASetup-EN.msi** file. The MBSA Setup window should open.
2. Close all other open programs on the computer, such as Web browsers and e-mail clients.
3. Click the **Next** button. Review the license agreement, change the license agreement setting as needed, and click on the **Next** button.

4. Choose a location for the MBSA installation or accept the default setting, and click on the **Next** button.
5. Click on the **Install** button to initiate the actual MBSA installation. The installation should take a matter of seconds. When it is done, a successful completion notice should be displayed. Click **OK** to close it.

To use MBSA, perform the following steps:<sup>95</sup>

1. From the **Start** menu, select **All Programs**, then **Microsoft Baseline Security Analyzer 2.0**.
2. Choose to **Scan a computer**.
3. By default, the computer's name should be listed as the computer to scan. The other default options should also be acceptable. To begin the scan, click on **Start scan**.
4. The scan typically takes a few minutes to run. When it is finished, MBSA displays a report that includes scores for various aspects of Windows XP Home Edition security. Figure 8-3 shows part of an example report. Red X's indicate serious security issues, and yellow X's indicate minor security issues.
5. After reviewing each item on the report, close **MBSA**.

---

<sup>95</sup> These directions are based on MBSA version 2.0. These directions may vary significantly for other versions of MBSA.



Figure 8-3. Microsoft Baseline Security Analyzer Report

## 8.5 Investigate Unusual Behavior

If a computer begins to display unusual behavior, users and administrators should act quickly to investigate it. Generally, the best first step is to reboot the computer. Many functional errors are cleared through a reboot, and some forms of malware that are memory-resident are flushed from the computer by a reboot. If a problem persists, the next recommended step is to update the computer's antivirus software and antispyware software (if applicable) and perform a full scan of the computer. If no malware is detected, then additional troubleshooting steps need to be performed. Examples include the following:

- Checking antivirus vendor Web sites for instances of malware that cause the unusual behavior being seen
- Reinstalling an application that is not functioning properly
- Searching the Microsoft knowledge base Web site for information on similar problems
- Using utilities that can provide insights as to what is happening on the system.

If the problem still cannot be resolved, seek expert assistance. Section 8.5.1 contains additional information on this. Section 8.5.2 provides additional information on attempting to recover from a failure or security compromise.

One of the most common security problems that users and administrators face is false alarms. Hoaxes involving the security of home computers, such as descriptions of powerful new viruses, often spread via e-mail throughout the Internet. Some of these hoaxes are malicious in nature, and implementing their directions could cause a computer to be damaged or have its security reduced, not improved. Recipients of e-mails warning of new security threats should confirm their authenticity with an authoritative source, such as antivirus vendors, the vendor of the software that is supposed to be vulnerable, or reputable security Web sites.<sup>96</sup>

Besides hoax e-mails, users often receive e-mail messages that appear to have been originally sent from the users' e-mail accounts and rejected by a remote e-mail server. These e-mails appear to have contained malware which was removed or rejected by the remote server. In most cases, these e-mails are deceptive; the sender e-mail was chosen at random or taken from someone else's address book, and does not reliably indicate who really sent the e-mail. Users who are concerned about the legitimacy of these e-mails should perform an antivirus scan of their computers and assume that if the scan does not identify any malware, that the e-mails are probably forged and that their computers are not infected.

---

### 8.5.1 Seek Expert Assistance

In some cases, a Windows XP Home Edition computer may have a technical problem that is difficult to solve. For example, malware can damage Windows XP Home Edition and applications such as Web browsers, causing a currently or previously infected computer to operate strangely. Hardware problems are another common source of challenging technical problems. Sometimes the configuration for a part of Windows XP Home Edition or an application is incorrect, and it may not be easy for a user to determine what is wrong or how it can be fixed.

When difficult problems occur, users should seek the assistance of people with strong expertise in Windows XP Home Edition or Windows XP in general. Section 8.5.1.1 describes how to use the Remote Assistance feature built into Windows XP Home Edition. Users can also assist experts with troubleshooting by collecting and documenting information regarding the problems.

---

<sup>96</sup> Resources that can be helpful for determining the legitimacy of virus alerts include the Computer Incident Advisory Capability (CIAC) (<http://ciac.llnl.gov/ciac/>) and the Computer Virus Myths site (<http://www.vmyths.com/>).

The rest of this section provides examples of information that may be helpful to capture and recommendations on how to capture it.

### 8.5.1.1 Remote Assistance

The Remote Assistance feature built into Windows XP Home Edition can be very helpful in troubleshooting problems. However, it is not always available for use. If a computer cannot get network access, then it cannot be contacted by a remote computer. Also, if the computer is separated from the Internet by a device such as a firewall router that performs network address translation, it is probably not possible for an external expert to initiate a Remote Assistance session to the computer.

To use Remote Assistance, perform the following steps:

1. Ensure that the Remote Assistance feature is enabled. Section 5.4.2.1 explains how to do this.
2. Initiate a request for remote assistance. (This can be performed through instant messaging or e-mail; these instructions assume that e-mail is being used.)
  - a. From the **Start menu**, click on **Help and Support**.
  - b. Choose to **Invite a friend to connect to your computer with Remote Assistance**.
  - c. Choose the **Invite someone to help you** option. Enter the e-mail address of the person whose assistance is desired, and click **Continue**.
  - d. Fill in the requested invitation information, such as name and a description of the problem. When done, click **Continue**.
  - e. Set a timeframe for the invitation. Check the **Set a password** option, and specify a hard-to-guess password. This password should not be an existing password for the Windows XP Home Edition computer or the user (e.g., an e-mail account or Web site password). Click **Send Invitation** to send the invitation e-mail to the expert.
  - f. Contact the expert, preferably by phone, to provide the password corresponding to the invitation.
3. Wait for the expert to take control of the computer remotely. When the expert attempts to connect, a message box is displayed on the computer, asking if the expert should be allowed to connect. Click **Yes** to permit the connection.
4. During the session, the expert and user can communicate through a chat feature built in to the Remote Assistance software. This can be helpful in troubleshooting the problem and gathering additional information.
5. When the expert has completed the session, Remote Assistance displays a message to the user, stating that the expert has disconnected from the computer.



### 8.5.1.2 Error Messages

If an error message is displayed, it should be preserved. The following are the most common ways of doing so:

- **Write down the error message verbatim on paper.** This is the simplest method for capturing the information, and is most effective for simple error messages.
- **Copy and paste the error message.** In some cases, a user can copy the text. It can then be pasted into an e-mail and sent to an expert, or pasted into a text file and saved for future use.
- **Perform a screen capture.** For a complex error message, particularly one that cannot have its text copied or that includes helpful graphics, it may be best to perform a screen capture. To do so, perform the following steps:
  1. Arrange the windows on the computer so that the error message is displayed completely.
  2. Hold the **Shift** key down. Press and release the **Print Screen** or **PrtSc** key. Release the **Shift** key.
  3. From the **Start** menu, select **All Programs**, then **Accessories**, then **Paint**. Microsoft Paint should open.
  4. Click on **Edit**, then **Paste**. A copy of the screen should appear in the Paint window.
  5. Click on **File**, then **Save**. Choose a location for the picture of the screen to be saved, and give the picture file a name. In the **Save as type** box, select **JPEG**. When done, click on **Save**.
  6. Close **Paint**.

### 8.5.1.3 System Configuration

Windows XP Home Edition provides a utility known as System Information.<sup>97</sup> This utility collects a wealth of helpful information, including the following:

- Hardware information (e.g., memory, processor, drives, external peripherals)
- Network configuration for all network interfaces
- Software configuration, including hardware drivers, print jobs, network connections, running processes, service configurations, and programs loaded at startup
- Microsoft Internet Explorer and Office applications configuration

To use System Information, perform the following steps:

1. From the **Start** menu, select **All Programs**, then **Accessories**, then **System Tools**, then **System Information**. System Information should open.

---

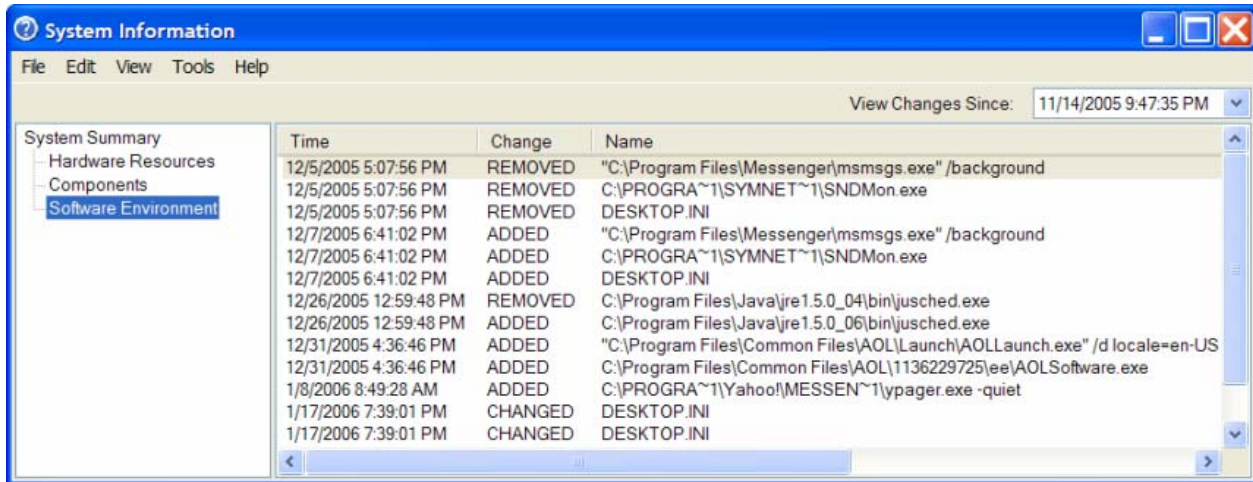
<sup>97</sup> For more information on System Information, see MSKB article 308549, which is available at <http://support.microsoft.com/kb/308549/>.

2. Select **System Summary**, which should be in the upper left corner of the window.
3. Click on **File**, then **Save**. This will save the system information to a file. Choose a location for the file to be saved and a name for the file. When done, click **Save**.
4. Provide the saved file to an expert for review. For example, the file could be e-mailed to someone; placed onto a CD, flash drive, or other removable media; or reviewed at the computer by an expert at a later time. The expert can review the file by running System Information and opening the file from it.
5. Close **System Information**.

#### 8.5.1.4 System History

In addition to recording information on a computer's current configuration, the System Information utility described in Section 8.5.1.3 can also provide information on the computer's history. Figure 8-4 shows an example of recent software changes made to a computer. To capture system history information for someone else to review, perform the following steps:

1. From the **Start** menu, select **All Programs**, then **Accessories**, then **System Tools**, then **System Information**. System Information should open.
2. From the **View** menu, select **System History**.
3. Highlight the **System Summary** text in the upper left corner.
4. In the **View Changes Since** dropdown box, select a date that is earlier than when the problem is believed to have started. If unsure, select a date at least a few months in the past (if available).
5. Click on **File**, then **Save**. This will save the system information to a file. Choose a location for the file to be saved and a name for the file. When done, click **Save**.
6. Provide the saved file to an expert for review. For example, the file could be e-mailed to someone; placed onto a CD, flash drive, or other removable media; or reviewed at the computer by an expert at a later time. The expert can review the file by running System Information and opening the file from it.
7. Close **System Information**.



**Figure 8-4. History from System Information Utility**

### 8.5.1.5 Event Logs

The event logs on a Windows XP Home Edition computer contain records related to various successful and failed actions, such as logging into the computer and restarting a computer. This information may be helpful in determining when a malicious event happened. Figure 8-5 shows an example of event log data. To capture event logs for someone else to review, perform the following steps:

1. Right-click on **My Computer**, then select **Manage**.
2. Under **System Tools**, highlight the **Event Viewer** item.
3. For each of the three log types (Application, Security, and System), perform the following steps:
  - a. Right-click on the log type and select **Save Log File As**.
  - b. Choose a location for storing the log file.
  - c. Enter a unique filename and click on **Save**.
4. Provide the saved log files to an expert for review. For example, the files could be e-mailed to someone; placed onto a CD, flash drive, or other removable media; or reviewed at the computer by an expert at a later time. The expert can review the files by running Event Viewer and opening each log file from it.
5. Close **Event Viewer**.

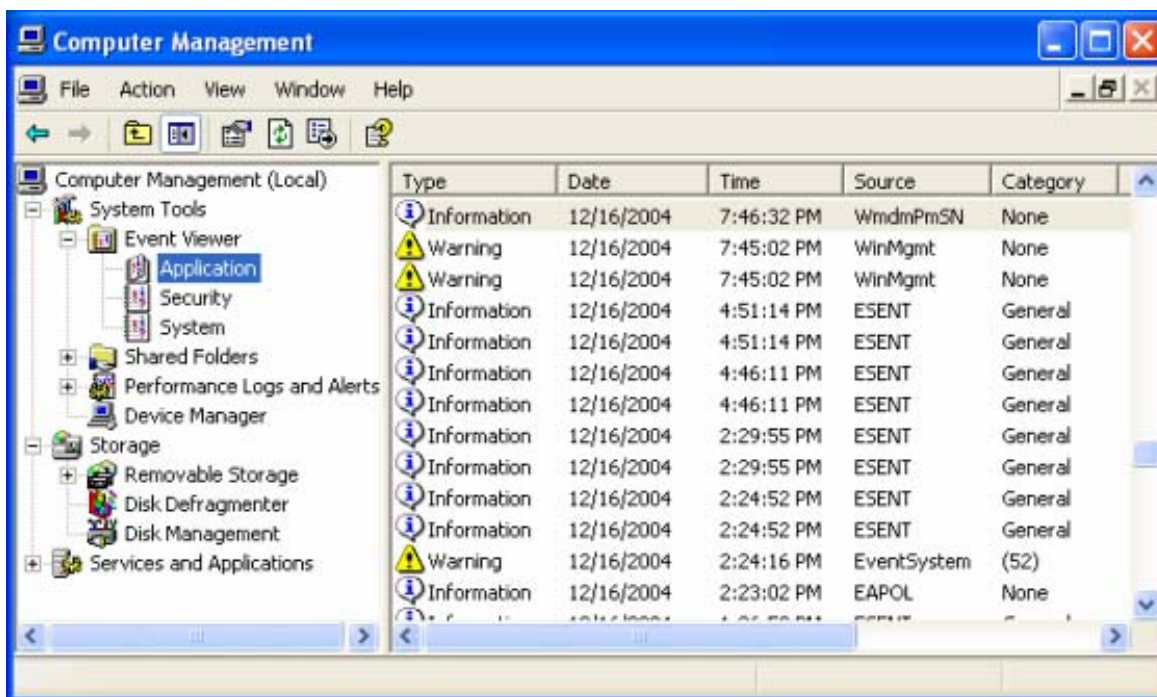


Figure 8-5. Event Viewer

### 8.5.1.6 File Signature Verification Utility

The System Information utility described in Section 8.5.1.3 includes several diagnostic tools, including the File Signature Verification Utility. This utility checks Windows XP Home Edition operating system files to ensure that they have been digitally signed by Microsoft. Files that fail this match could have been added by a benign third party, such as a hardware vendor, or by malware or other attacks. To check the Windows XP Home Edition files, perform the following steps:

1. From the **Start** menu, select **All Programs**, then **Accessories**, then **System Tools**, then **System Information**. System Information should open.
2. Under **Tools**, run the **File Signature Verification Utility**.
3. Click **Start** to begin the file scan. It typically takes at least a few minutes for the scan to run. When the scan has completed, click **Close**.
4. Click the **Advanced** button, then the **Logging** tab.
5. Click the **View Log** to display the log for the scan. The items with a status of **Not Signed** are the files of most interest.
6. To save the file for an expert to review, click **File**, then **Save As**. Specify a location and name for the file, then click **Save**.
7. Click **OK**, then **Close**.

8. Close **System Information**.
9. Provide the saved log file to an expert for review. For example, the file could be e-mailed to someone; placed onto a CD, flash drive, or other removable media; or reviewed at the computer by an expert at a later time. The expert can review the file by opening it in Notepad or another text editor.

### 8.5.1.7 Blue Screen Information

If a serious error occurs on a Windows XP Home Edition computer, the result may be a blue screen that contains rather cryptic diagnostic information. When this blue screen occurs, a user can best capture the error message by writing it down. Generally, it is sufficient to copy only the first few lines. If the computer reboots itself before the entire message can be documented, it may be necessary to reconfigure Windows XP Home Edition so that it does not reboot automatically after failure. To do so, perform the following steps:

1. From the **Control Panel**, select **System**.
2. Select the **Advanced** tab, then click on the **Settings** button within the **Startup and Recovery** window pane.
3. In the **System Failure** window pane, clear the option to **Automatically restart** the computer upon failure.
4. Click **OK**, then **OK**.

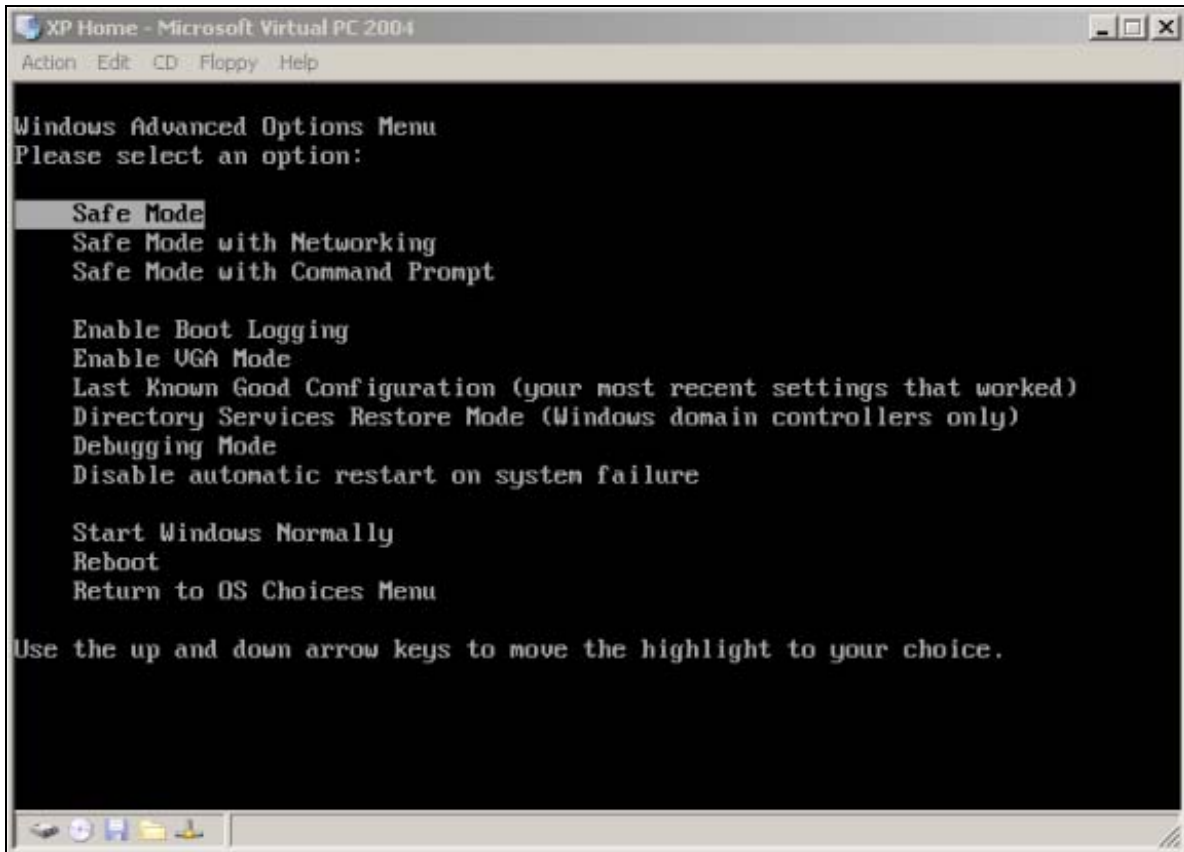
---

## 8.5.2 Recover from a Failure or Compromise

Recovering the proper functionality of a Windows XP Home Edition computer from a failure, such as a crash, or a security compromise can be challenging. For example, it may be nearly impossible to remove certain types of malware (particularly spyware) from a computer without causing major damage to the computer. This section describes options for attempting to recover a Windows XP Home Edition computer. Users who are unfamiliar with these tools should consult with a Windows XP Home Edition expert before using these tools to modify their computers.

### 8.5.2.1 Boot Options

When problems have occurred, it is often helpful to boot Windows XP Home Edition using a mode other than the default. As Windows XP Home Edition first begins to boot, it briefly displays a message about hitting the F8 key. If the user does so, the Advanced Options menu is displayed, which lists several boot options; this is shown in Figure 8-6. One option is to boot in Safe Mode, which causes Windows XP Home Edition to be loaded with the necessary components only. In Safe Mode, networking is disabled, as are many other functions. Safe Mode is most helpful for troubleshooting hardware and hardware driver problems, but it can also be used to confirm that the core Windows XP Home Edition installation is functioning properly and that a failure is being caused by an application, service, or other software component such as malware above the core Windows XP Home Edition files.



**Figure 8-6. Windows Advanced Options Menu**

Another boot option that is helpful for recovery is called Last Known Good Configuration. This causes the Windows Registry, which stores configuration information for Windows XP Home Edition, applications, and users, to be restored to the copy used at the beginning of the previous boot. If the event that is causing problems occurred since the last reboot, then using the Last Known Good Configuration option could cause some of the damage inflicted by the event to be undone. However, it will also cause other configuration changes made to the computer since the last reboot to be undone.

### **8.5.2.2 System Restore**

Windows XP Home Edition computers save their state periodically in a format known as a *restore point*. Administrators can also save restore points manually as desired. The System Restore utility built into Windows XP Home Edition can be used to restore the state of the computer to the state captured in a restore point. The goal is to select a restore point from a date that is before the problem began, but as late as possible so that previous application changes, computer updates, and other changes to the system are not lost.

To restore the computer to an earlier state, perform the following steps:

1. From the **Start** menu, choose **All Programs**, then **Accessories**, then **System Tools**. From there, choose **System Restore**.
2. Click on **Restore my computer to an earlier time**, and then click **Next**.
3. Select a restore point date. After choosing a date, click **Next**.
4. Verify that the desired restore point has been chosen. Click **Next** to proceed.
5. The changes to the computer since the restore point will be reversed. When completed, the computer will shut down and restart.

### 8.5.2.3 Recovery Console

The Recovery Console is considered a last-resort option when other recovery methods have failed. It also requires expert-level knowledge of Windows XP Home Edition. To use the Recovery Console, perform the following steps:

1. Insert the Windows XP Home Installation CD into the CD drive, and reboot the computer.
2. When the setup screen appears, choose **R** to start the Recovery Console and the repair process.
3. Enter the administrative password.
4. Type in the necessary commands at the prompt. To display a list of available commands, type **help**.
5. When finished, type **exit** to close the Recovery Console. Remove the CD from the computer and reboot.

### 8.5.2.4 Windows XP Home Edition Reinstallation

When all else fails, Windows XP Home Edition may need to be reinstalled, and all data restored from backups. Section 4 describes how to do this.

---

---

## 8.6 Prepare a Computer for Retirement

When a Windows XP Home Edition computer is not going to be used any more, it should be prepared for retirement. The computer's hard drive most likely contains information that users might not want others to see. For example, the computer might have files from tax return software. Even if the user deletes all of the tax return-related files and software from the computer, curious people who get access to the computer might be able to recover the tax information using free or inexpensive software utilities specifically designed to recover deleted files. Accordingly, users should ensure that all data on the computer's hard drive is wiped out before donating, selling, or discarding a computer. Methods of doing this include the following:

- **Use a third-party disk scrubbing utility.** There are several commercial software products available that are specially designed to remove traces of data from computers. Follow the vendor directions on removing data from the hard drive.
- **Retain the hard drive.** Following the instructions in the computer vendor's documentation, a user can remove the hard drive from the computer. If other people want to use the computer in the future, they can purchase a new hard drive and install Windows XP Home Edition or another operating system onto the computer. This is the best option if the computer is no longer functioning properly, preventing the use of disk scrubbing utilities.
- **Destroy the hard drive.** Hard drives can be degaussed, which involves applying a magnetic field to the drive that makes it unusable. Hard drives can also be shredded or otherwise physically destroyed through specialized equipment and services.

---

---

## 8.7 Summary

After a Windows XP Home Edition computer has been secured using the guidance provided in previous sections, the computer's security needs to be maintained on an ongoing basis. This includes the following:

- The administrator or individual users should perform backups of their data and settings on a regular basis.
- The administrator should perform regular security maintenance. This includes ensuring that Windows XP Home Edition and application updates are applied, checking the status of security software, creating new user accounts, and retiring accounts that are no longer needed.
- Each user, including administrative account users, should perform regular security maintenance for their own accounts and data. This includes changing their passwords regularly, deleting unneeded files, and clearing information from Web browsers. Users should also monitor the Security Center on an ongoing basis.
- Administrators should use security assessment tools periodically to identify security issues on Windows XP Home Edition computers.

If a computer begins to display unusual behavior, users and administrators should act quickly to investigate it. Generally, the best first step is to reboot the computer, which can clear many functional errors as well as some forms of malware that are memory-resident. If a problem persists, the next recommended step is to update the computer's security tools and scan the computer for malware. If no malware is detected, then additional troubleshooting steps need to be performed, such as reinstalling malfunctioning applications, checking antivirus vendor Web sites for information on malware that might be causing the problems, and checking the Microsoft Web site for information on similar problems.

If malware cannot be removed from a computer or other technical problems occur that cannot be resolved, users may need to seek expert assistance. Users should use the Remote Assistance feature built into Windows XP Home Edition or third-party remote access utilities when needed to allow a trusted friend, family member, or coworker to assist in troubleshooting such problems.



Users should also collect information as needed to help others in performing troubleshooting. Users can also use recovery tools under the guidance of an expert to attempt to recover from major failures or compromises. If all else fails, the user may need to reinstall Windows XP Home Edition and restore all data from previous backups.

**This page has been left blank intentionally.**

## Appendix A—Essential Security Settings

Appendix A contains step-by-step instructions for implementing the most essential recommendations for securing Windows XP Home Edition computers. Implementing the instructions in Sections 5 through 8 provides stronger security than implementing just the instructions in this section. However, there are instances where all of the Section 5 through 8 instructions cannot be followed because of a lack of time or expertise. In these cases, using only the instructions in this section should provide the most essential security protection for a Windows XP Home Edition computer.

Figure A-1 displays a flowchart of the high-level steps for implementing the most essential security recommendations.

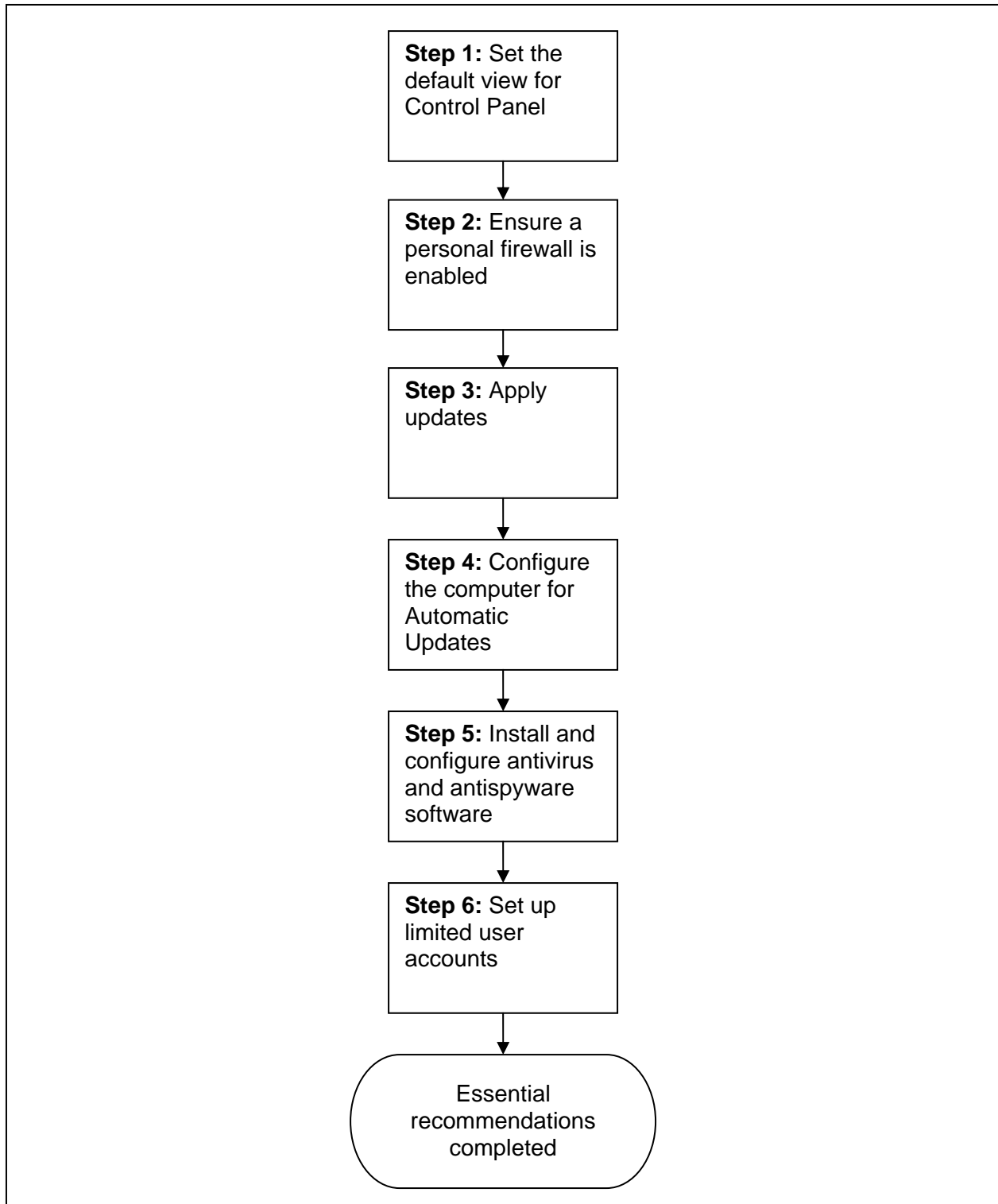


Figure A-1. Flowchart for Applying Essential Recommendations

---

---

## Step 1: Set the Default View for Control Panel

Control Panel has two views: Classic and Category. Classic View lists each Control Panel item separately, and Category View groups similar items together. The instructions in this section assume that Classic View is being used.

1. Log on to the computer using an administrative-level account.
2. Open the **Control Panel**.
3. Look at the text in the upper left hand corner of the Control Panel window.
  - If it contains a link that says **Switch to Category View**, no action is needed because **Classic View** is already the default setting.
  - If it contains a link that says **Switch to Classic View**, click on that link to change the default view from Category View to Classic View.
  - If it does not contain either a **Switch to Category View** or a **Switch to Classic View** link, no action is needed because the Windows classic folders option is enabled, which allows only Classic View to be used.

---

---

## Step 2: Ensure a Personal Firewall Is Enabled

Every Windows XP Home Edition computer should have a personal firewall enabled. Windows XP Home Edition has a built-in firewall; it is called the Internet Connection Firewall (ICF) before SP2, and the Windows Firewall on SP2 computers. Because third-party personal firewall programs may offer functionality that the built-in firewall does not, users may choose to use a third-party firewall instead. Only one personal firewall should be enabled on the computer at a time.

Perform the following steps to ensure that a personal firewall is enabled and providing adequate protection for the computer:

1. In the **Control Panel**, look for a **Security Center** icon.
  - a. If the icon is present, follow the **SP2** instructions below.
  - b. If the icon is not present, follow the **Pre-SP2** instructions below.

For SP2 computers (ones with a Security Center icon), perform the following steps:

1. Double-click the **Security Center** icon. The Security Center should be displayed.
2. The firewall status should indicate if a third-party firewall is enabled. If it is, refer to the software vendor's documentation and help files to ensure that the third-party firewall is configured properly. Close the **Security Center** and skip the rest of these firewall instructions.

3. If the firewall status is listed as **ON**, the built-in firewall is already enabled. Close the **Security Center** and skip the rest of these firewall instructions.
4. If the firewall status is listed as **OFF**, perform the following steps:
  - a. Click on the **Recommendations...** button.
  - b. Turn the firewall on by clicking the **Enable now** button.
  - c. A notification window should appear, saying that the firewall was enabled successfully. Click on **Close**.
  - d. Click on **OK** to close the **Recommendation** window. The firewall status should now be listed as **ON**.
  - e. Close the **Security Center**.

For pre-SP2 computers (ones without a Security Center icon), perform the following steps:

1. In the Control Panel, double-click the **Network Connections** icon. The Network Connections configuration box should be displayed.
2. Right-click the network connection that is used to get Internet access, then click **Properties**.
3. Select the **Advanced** tab. Enable ICF by checking the box for **Protect my computer and network by limiting or preventing access to this computer from the Internet**.
4. Click on **OK** to save the firewall configuration.

---

---

### Step 3: Apply Updates

The next step is to identify, download, and install necessary updates for the computer.

1. Run Internet Explorer. Click on **Tools**, then **Windows Update**, to start Microsoft Update.<sup>98</sup>
2. If a prompt appears asking to install and run Windows Update, click **Yes**.
3. If a prompt appears saying that a new version of the Windows Update or Microsoft Update software is available, click on **Install Now** or **Download and Install Now** to install the new version. Multiple updates may be needed. If prompted to do so, close Internet Explorer or reboot the computer so that the new version of the update software takes effect. (If a reboot is needed, restart these instructions at step 1 after the reboot completes.)
4. Click on the **Custom** button to identify available updates.<sup>99</sup>
5. Microsoft Update checks for updates and lists the available ones. Figure A-2 shows an example of how updates are listed. Depending on the service pack level of the Windows XP Home Edition installation CD, either Service Pack 2 or non-service pack updates should be displayed. Follow the appropriate step:
  - a. **Non-service pack updates** are grouped by high priority updates, optional software updates, and optional hardware updates.<sup>100</sup> Install them using the following steps:
    - i. Review the list of available updates, select the desired ones (or accept the default setting), then click **Review and install updates**. In some cases, one patch may need to be installed by itself; therefore, it may not be possible to install all desired patches at once.
    - ii. Confirm that the correct updates are listed, and click the **Install Updates** button to perform the installations. Review any licensing agreements that are displayed and click on the appropriate button for each.
    - iii. The download and installation process will begin. Depending on the number of updates and the network bandwidth available, it may take from a few minutes to a few hours to download and install the updates. When the installations are

---

<sup>98</sup> Because the predecessor to Microsoft Update was named Windows Update, Windows XP Home Edition computers that are not fully updated may display “Windows Update” instead of “Microsoft Update” on some screens. This should not be a cause for concern; during the update process, Windows Update will eventually be replaced with Microsoft Update.

<sup>99</sup> The Custom option can install both high priority and optional updates, and allows the user to select which updates should be installed. The Express option can only install high priority updates, and does not allow the user to specify which updates should be installed. Using the Express option may cause the system to download and install service packs automatically.

<sup>100</sup> High priority updates are defined as critical updates, hotfixes, service packs, and security rollups. Optional updates are unrelated to fixing security problems, but may contain new security features.

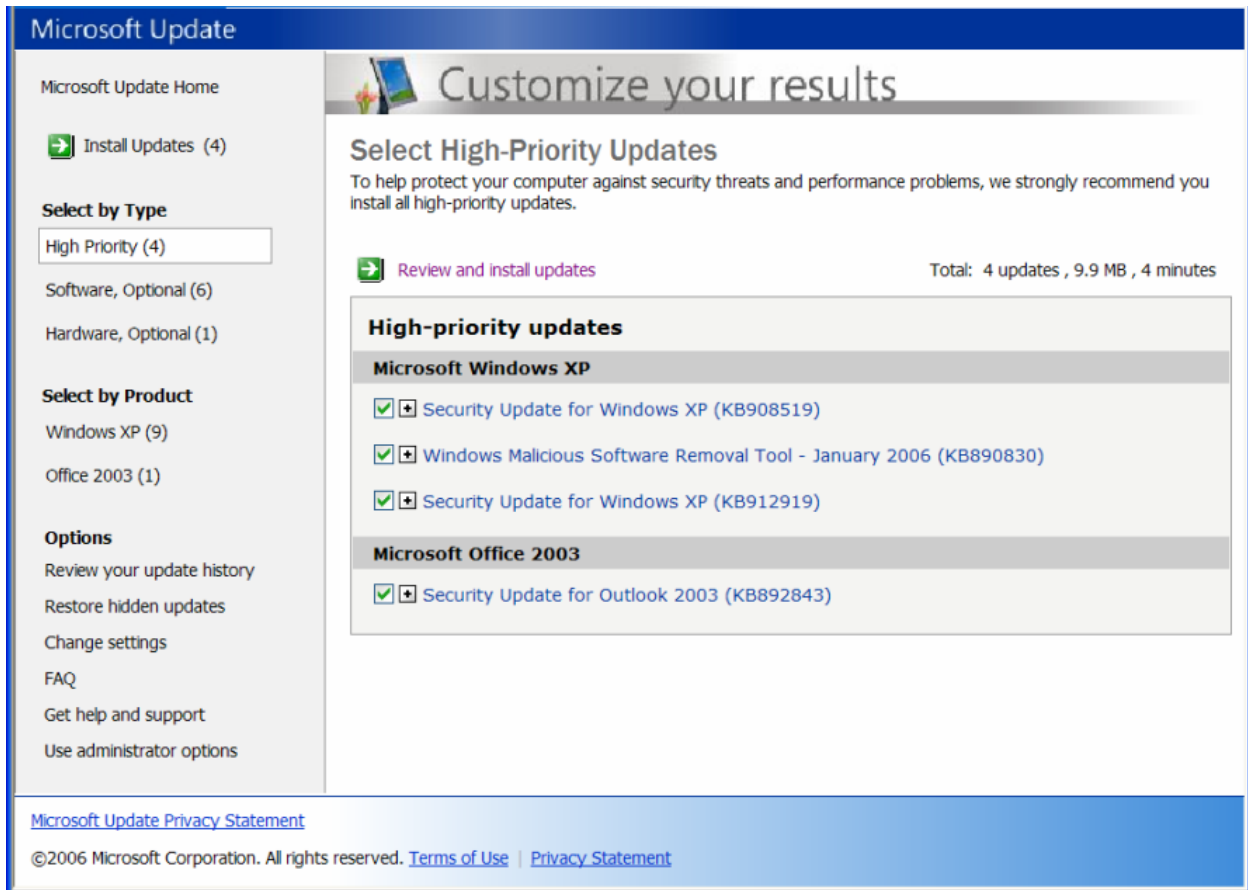
done, Microsoft Update should report which updates were successfully installed. It will also prompt the user to reboot the computer if any of the updates require a reboot to complete the installation. Click on **OK** to reboot immediately or **Cancel** to manually reboot the computer later.

- b. **Service Pack 2** can be installed through Microsoft Update using the following steps:<sup>101</sup>
  - i. Click on **Download and Install Now**.
  - ii. Review the license agreement and click on the appropriate button.
  - iii. Service Pack 2 should be downloaded and installed. This may take considerable time, depending primarily on the size of the service pack and the type of Internet connectivity and bandwidth available. The Windows XP Service Pack 2 Setup Wizard may prompt the user at some point; click **Next** to continue.
  - iv. Once the installation has ended, a summary should be displayed that reports the installation was successful. Click **Restart Now** to reboot the computer.
  - v. After the reboot, the **Help protect your PC** screen appears. The Automatic Updates setting is configured later in the instructions, so at this time, choose the **Not right now** option and click **Next**.
  - vi. The **Security Center** opens and displays the status of security programs. Since antivirus software and other security programs have not yet been installed on the computer, the current status is irrelevant. Close the **Security Center**.
6. Repeat all of these steps until no more updates are available. Depending on which service pack was included with the Windows XP Home Edition CD, and the number of additional updates that need to be applied, it may take several rounds of updating the computer and rebooting it to bring a new Windows XP Home Edition installation completely up-to-date.

---

<sup>101</sup> If a service pack is being installed from a CD instead of through Microsoft Update, the steps to be performed will differ.





**Figure A-2. Microsoft Update**

During the updating process, the computer may state that additional updates cannot be downloaded until Windows XP Home Edition has been validated or activated. If so, follow the instructions provided by Windows XP Home Edition to activate the software through the Internet, dial-up, or telephone.

It is also important to update other applications on the Windows XP Home Edition computer. Follow these steps for each application:

1. Install the application.<sup>102</sup>
2. Review its documentation for guidance on how to update it and how to configure it to update itself automatically (if possible).
3. Implement the vendor's recommendations. If needed, either close and restart the application or reboot the computer so that the changes take effect.

<sup>102</sup> It is often advantageous to install applications such as e-mail clients and Web browsers before installing security software. For example, when antivirus software is installed, it may automatically identify installed email clients and configure itself so that it monitors their activity for malware.

---

---

## Step 4: Configure the Computer for Automatic Updates

To keep Windows XP Home Edition fully updated at all times, the Automatic Updates service should be enabled.

1. From **Control Panel**, double-click **Automatic Updates**.
2. Choose the appropriate radio button, as shown in Figure A-3.
  - If the computer has high-speed Internet access, select **Automatic (recommended)**. Then select the frequency and timeframe in which the updates should be downloaded and installed (e.g., every day at 3:00 A.M.)
  - If the computer has low-speed Internet access, select **Notify me but don't automatically download or install them**. This allows the user to control when updates are downloaded.
3. Click on **OK** to save the Automatic Updates configuration.

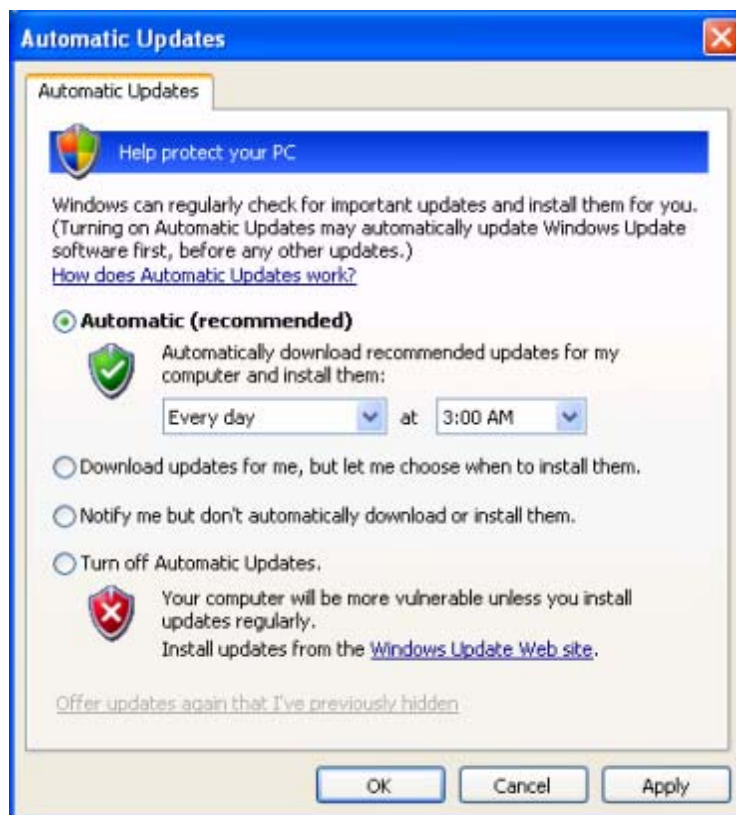


Figure A-3. Automatic Updates Configuration

---

---

## Step 5: Install and Configure Antivirus/Antispyware Software

Users should next install malware protection utilities. Antivirus software is a necessity, and antispyware software is also recommended if the antivirus software does not include a robust antispyware capability itself. Install the antivirus software (and separate antispyware software, if needed) using the documentation provided with the software. During the software installation process or immediately afterward, the software should be configured as follows using directions provided within the software documentation:

- Scan critical operating system components such as startup files, memory, system BIOS, and boot records
- Perform real-time scans of each file as it is downloaded, opened, or executed
- Monitor common applications such as e-mail clients, Web browsers, file transfer and file sharing programs, and instant messaging software
- Scan all hard drives regularly (at least once a week)
- Attempt to disinfect files, and quarantine infected files that cannot be disinfectd
- Automatically download and install updates daily.

After installation, the software should be fully updated. Consult the software documentation or help files for directions on how to download and install updates. Most antivirus software and antispyware software have a menu option that causes the software to check for, download, and install updates immediately. After doing so, it may be necessary to repeat the update process once or a few times, because some updates might need to be installed before other updates. Also, it may be necessary to reboot the computer after applying certain updates.

---

---

## Step 6: Set Up Limited User Accounts

A separate limited user account needs to be set up for each person that will be using the computer.

1. From the **Control Panel**, double-click on **User Accounts**.
2. For each person that will be using the computer, create an account:
  - a. Click **Create a new account**.
  - b. Enter the user name; it can be up to 20 characters long and contain letters, numbers, spaces, and some other types of punctuation. When finished, click the **Next** button.
  - c. Set the account type to **Limited**, then click on the **Create Account** button.
  - d. Have the user choose a strong password and enter it after clicking **Create a password**. Ask the user not to enter a password hint.

3. Close the **User Accounts** window.

## Appendix B—Advanced Security Settings

Appendix B contains step-by-step instructions for implementing additional security recommendations on Windows XP Home Edition computers running Service Pack 2.

**The steps throughout this appendix should be performed only by advanced users with strong knowledge of Windows XP Home Edition security features. The actions performed in this section may be difficult to perform, or they may be difficult to undo if problems occur. Implementing the recommendations in this appendix will further improve the security of Windows XP Home Edition computers, but adequate security can be achieved without them by implementing the other recommendations presented throughout this document.**

---

---

### B.1 Configure Data Execution Prevention

Advanced users should consider enabling the Data Execution Prevention (DEP) feature for all programs and services, as described in Section 3.3.7. By default, the feature only works for essential Windows programs and services; enabling it for all programs and services provides more robust protection. However, the DEP feature might cause certain applications to malfunction, so users that fully enable DEP should monitor their applications' behavior closely after configuring it and reconfigure DEP if problems occur.<sup>103</sup> To fully enable DEP, perform the following steps:

1. From the **Control Panel**, double-click on **System**. The **System Properties** window should be displayed.
2. Click on the **Advanced** tab. Within the **Performance** pane, click the **Settings** button.
3. From the **Performance Options** window, click the **Data Execution Prevention** tab.
4. Choose the **Turn on DEP for all programs and services except those I select** option.
5. Click on **OK**.

---

---

### B.2 Disable Default User Accounts

Windows XP Home Edition includes several default user accounts that are not shown in the User Accounts listing in Control Panel.<sup>104</sup> These accounts are enabled by default, so it is possible that attackers could attempt to use them to gain unauthorized access to the computer. To disable these accounts, advanced users should perform the following steps:

---

<sup>103</sup> If problems occur, perform the numbered steps and change step 4 so that the **Turn on DEP for essential Windows programs and services only** option is chosen.

<sup>104</sup> Although the Guest account appears in the User Accounts listing, it can only be partially disabled from there. The directions in this section can be used to disable the Guest account fully.

1. Click the **Start** menu, choose **All Programs**, select **Accessories**, and click on **Command Prompt**.

2. Within the Command Prompt window, type in the command

**net user Support\_388945a0 /active:no**

and hit the **Enter** key to run it.<sup>105</sup> The response should be **The command completed successfully**. If not, confirm that the command was typed correctly and enter it again if needed. Figure B-1 shows the command and expected response.

3. If the computer does not need to share any folders or printers with other computers, then type in the following command within the Command Prompt window:

**net user guest /active:no**

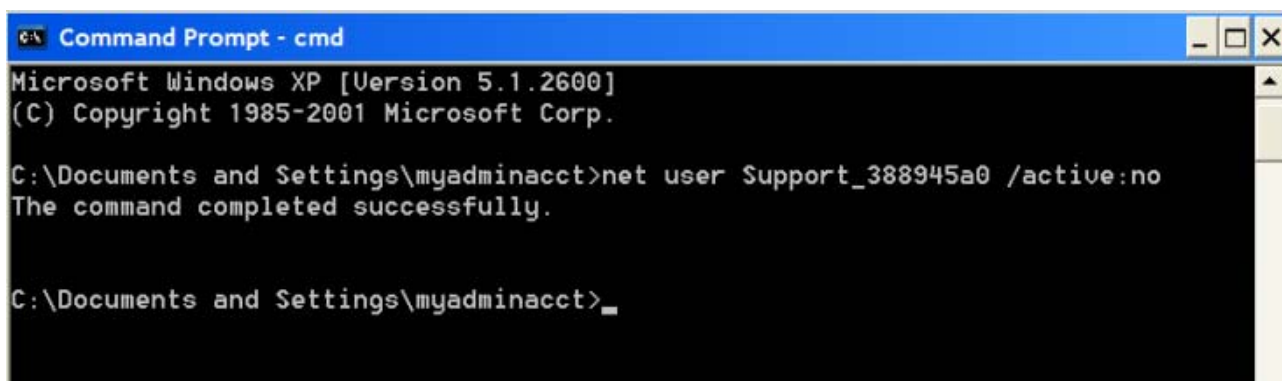
and hit the **Enter** key to run it. The response should be **The command completed successfully**. If not, confirm that the command was typed correctly and enter it again if needed.<sup>106</sup>

4. If the computer will not be using the Remote Assistance feature, then type in the following command within the Command Prompt window:

**net user HelpAssistant /active:no**

and hit the **Enter** key to run it. The response should be **The command completed successfully**. If not, confirm that the command was typed correctly and enter it again if needed.<sup>107</sup>

5. Close the **Command Prompt**.

A screenshot of a Windows XP Command Prompt window. The title bar reads "Command Prompt - cmd". The window content shows the following text: "Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. C:\Documents and Settings\myadminacct>net user Support\_388945a0 /active:no The command completed successfully. C:\Documents and Settings\myadminacct>".

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\myadminacct>net user Support_388945a0 /active:no
The command completed successfully.

C:\Documents and Settings\myadminacct>
```

**Figure B-1. Disabling User Account at the Command Prompt**

<sup>105</sup> If the account needs to be enabled at some time, perform the same command, changing the **no** to **yes**.

<sup>106</sup> If there is a need in the future to share folders or printers, perform the step again, substituting **yes** for **no**.

<sup>107</sup> If there is a need in the future to use the Remote Assistance feature, perform the step again, substituting **yes** for **no**.

---

---

### B.3 Disable Unneeded Networking Features

To disable unneeded networking services, advanced users should perform the following steps for each network connection:

1. From the **Control Panel**, select **Network Connections**. Right-click on the network connection and select **Properties**. A window similar to the one shown in Figure B-2 should be displayed.
2. Uncheck the box for **QoS Packet Scheduler**.
3. If the computer will not be sharing its files or printers with other computers on the user's home network, uncheck the box for **File and Printer Sharing for Microsoft Networks**.
4. If the computer will not be accessing any shared folders or printers on other computers on the user's home network, uncheck the box for **Client for Microsoft Networks**.
5. Click **OK** to proceed.
6. Close the **Network Connections** window.

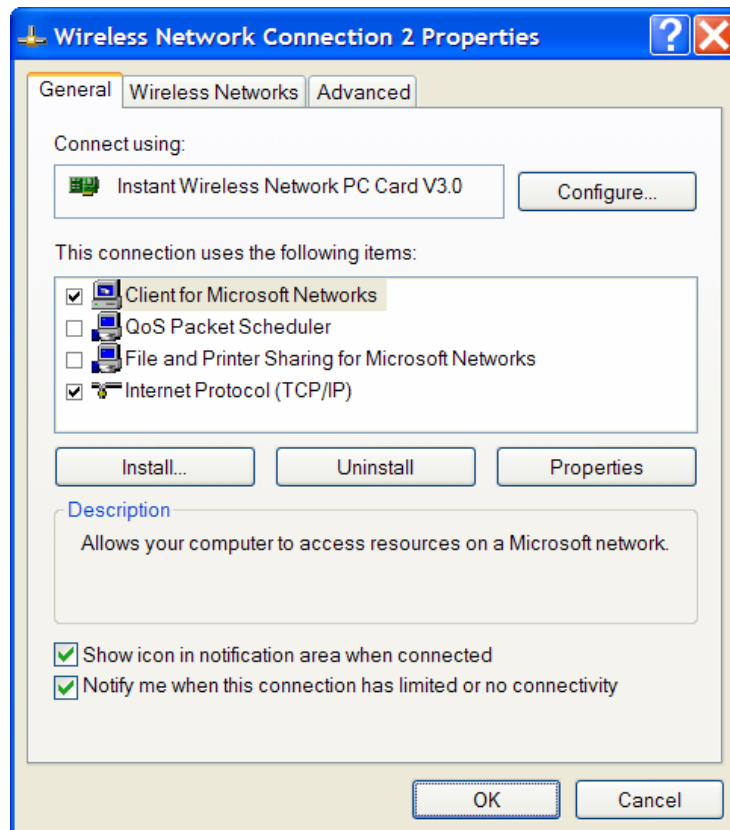


Figure B-2. Disabling Unneeded Networking Features

---

---

## B.4 Protect Temporary Files

To ensure that each user has a separate directory for temporary files, advanced users should perform the following steps:

1. From the **Control Panel**, select **System**, then click on the **Advanced** tab. Click on the **Environment Variables** button.
2. In the **System variables** pane, look for the values assigned to **TEMP** and **TMP**:
  - a. Double-click on the entry for **TEMP**. The **Variable value** should contain a value that includes **%USERPROFILE%**, such as **%USERPROFILE%\Local Settings\Temp**. If not, modify it so that it is **%USERPROFILE%\Local Settings\Temp**. Click on **OK** to close the window.
  - b. Double-click on the entry for **TMP**. The **Variable value** should contain a value that includes **%USERPROFILE%**, such as **%USERPROFILE%\Local Settings\Temp**. If not, modify it so that it is **%USERPROFILE%\Local Settings\Temp**. Click on **OK** to close the window.
3. Click **OK**, then **OK**.

If one or more users want to have additional protection for their personal files, then acquire, install, and configure a third-party encryption product according to the vendor's documentation.<sup>108</sup>

---

---

## B.5 Disable Unneeded Services

Advanced users should disable unneeded services on the computer, as described in Section 3.1.5. The services that are the most likely candidates to be disabled are as follows:

- **ClipBook**. This service permits users to share copied text and graphics with other users. It should be disabled unless there is a specific desire to share data through the Clipboard instead of other means, such as e-mail or Shared Folders.
- **Infrared Monitor**. This should be disabled if there is no need to use a computer's infrared sensor.
- **NetMeeting Remote Desktop Sharing**. This service, which is used for online conferencing with other people, should be disabled unless it is needed.
- **Routing and Remote Access**. This service should be disabled unless the Internet Connection Sharing feature is needed.

---

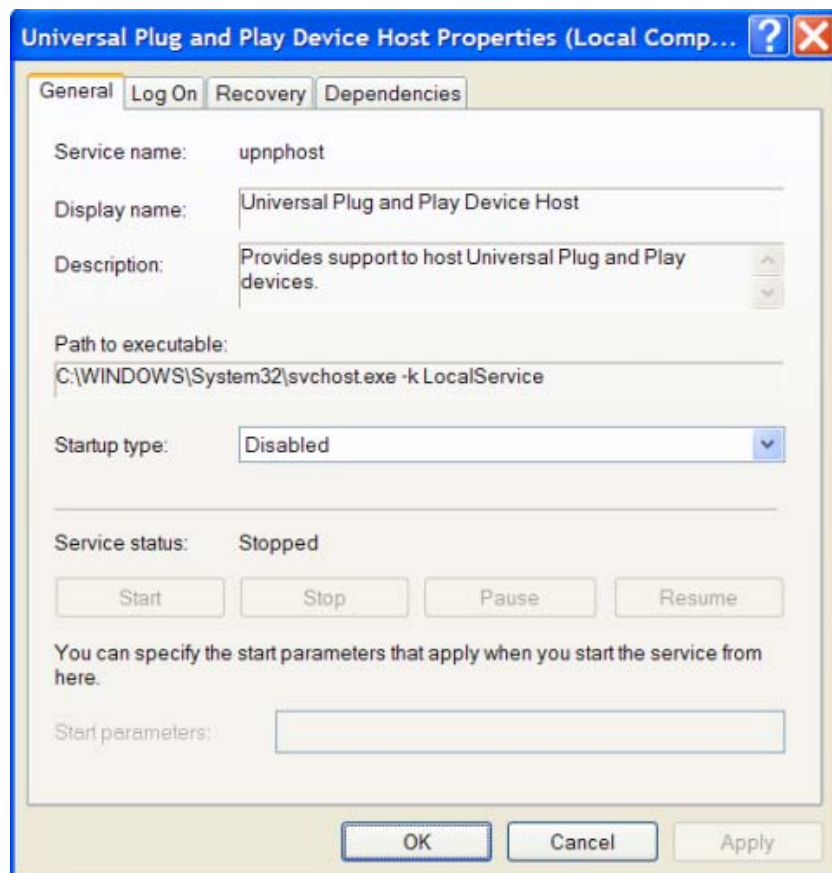
<sup>108</sup> An alternative is to use Windows XP Professional instead of Windows XP Home Edition. Windows XP Professional has the Encrypting File System (EFS), which is a built-in file encryption feature. Windows XP Professional offers other file and folder protection features that Windows XP Home Edition does not, such as specifying which types of actions can be performed on each file by each user (e.g., reading, writing, deleting).



- **Universal Plug and Play (UPnP) Device Host** and **SSDP Discovery Service**. These services should be disabled unless the computer will be interacting with UPnP-enabled consumer electronics devices connected to the same local network.
- **Wireless Zero Configuration**. This service should be disabled on any computer that is not using wireless networking.

To disable unneeded services, advanced users should perform the following steps:

1. From the **Control Panel**, select **Administrative Tools**, then double-click on **Services**.
2. For each service to be disabled:
  - a. Double-click on the name of the service. Figure B-3 shows an example of the window that should appear.
  - b. Set the **Startup type** to **Disabled**.
  - c. Click on **OK**.
3. Close the **Services** window and the **Administrative Tools** window.



**Figure B-3. Disabling Unneeded Services**

## **B.6 Modify File Associations**

Advanced users should modify the settings for default file associations, as described in Section 3.1.4. These settings need to be changed separately for every user account on the computer. To change them, perform the following steps:

1. From the **Control Panel**, select **Folder Options**.
2. Select the **File Types** tab.
3. Perform these steps to change the mappings for the following extensions: **JS, JSE, OTF, REG, SCT, SHB, SHS, VBE, VBS, WSC, WSF, and WSH**.
  - a. Scroll down the **Registered file types** window to the desired extension. Select it and click the **Change** button.
  - b. Select the **Notepad** program and click **OK**.
4. Click the **Close** button.

If a file association that was altered needs to be restored to its original setting, perform the following steps:

1. From **Control Panel**, select **Folder Options**.
2. Select the **File Types** tab. Scroll down the **Registered file types** window and select the desired extension.
3. Click the **Restore** button, then click **Close**.

## Appendix C—Directions for Securing Applications

Appendix C provides step-by-step directions for securing certain applications, primarily open source applications, in the following categories:<sup>109</sup>

- Antivirus software
- Antispyware software
- Personal firewalls
- E-mail clients
- Web browsers
- Instant messaging clients
- Office productivity suites.

These directions may also be helpful in securing the same applications run on operating systems other than Windows XP Home Edition; however, the directions have not been tested on any other operating systems to confirm their validity.

---



---

### C.1 Antivirus Software

As described in Section 5.3.1, antivirus programs should be configured to improve their security. Step-by-step directions are provided here for configuring three free antivirus programs: AVG Free Edition for Windows 7.1, Avira AntiVir PersonalEdition Classic Version 7, and avast! 4 Home Edition.

---

#### C.1.1 AVG Free Edition for Windows 7.1

To help ensure that AVG Free Edition for Windows 7.1<sup>110</sup> is configured properly, perform the following steps:

1. Run AVG Free Edition for Windows.
2. From the **Service** menu, choose **Schedule Daily Update**.
  - a. Check the boxes for **Periodically check for Internet updates** and **If Internet connection is not available, check when it goes on-line**.

---

<sup>109</sup> The applications in this section are by no means a complete list of applications to install on Windows XP Home Edition systems, nor does this guide imply any endorsement of certain products. The information in this appendix is based on the latest version of each application available at the time that testing was performed. Many of these applications are updated frequently, which may include changes to functionality, settings, and menu or option wording. Accordingly, the steps presented in this appendix may not be completely accurate for other versions of the applications.

<sup>110</sup> AVG Free Edition is available for free download from <http://free.grisoft.com/doc/2/lng/us/tp1/v5>.

- b. Set the daily check time to a time range that would be convenient.
    - c. Click on **OK**.
  3. Click the **Control Center** button.
  4. Click on the **AVG Resident Shield** panel.
    - a. Click the **Properties** button in the lower right-hand corner of the window.
    - b. Ensure that the **Turn on AVG Resident Shield protection** option is checked.
    - c. The **Use Heuristic Analysis** and **Scan floppy drives** options should also be checked.
    - d. Click on **OK** when done.
  5. Click on the **E-mail Scanner** panel.
    - a. Click the **Properties** button.
    - b. Click on **Configure** and ensure that the options to **Check incoming mail** and **Check outgoing mail** are selected.
    - c. The **Use heuristic Analysis** and **Scan inside archives** options should also be enabled.
    - d. Click on **OK**, then **OK** when done.
  6. Click on the **Scheduler** panel.
    - a. Click the **Scheduled Tasks** button.
    - b. Highlight the **Test** item and choose **Edit Schedule**. Ensure that **Periodically start scheduled antivirus test** is selected. Choose a time that would generally be convenient (e.g., a time when the computer is on but not being used).
    - c. Click on **OK** when done, then **Close**.
  7. Scroll down and click on the **Shell Extension** panel.
    - a. Click the **Settings** button.
    - b. Ensure that the following settings are selected: **Scan System Areas before the test starts**, **Use Heuristic Analysis**, **Scan inside archives**, and **Scan all files**.
    - c. Click on **OK** when done.

---

### C.1.2 Avira AntiVir PersonalEdition Classic Version 7

To help ensure that Avira AntiVir PersonalEdition Classic Version 7<sup>111</sup> is configured properly, perform the following steps:

1. Run Avira AntiVir PersonalEdition Classic.
2. From the **Extras** menu, choose **Configuration**.
  - a. Click the **Scanner** item in the left panel. Ensure that the **Boot Sector of selected drives** and **Begin scan with memory** options are checked. Also, select the **All files** option.
  - b. Click the **Guard** item in the left panel. Ensure that the **Scan when reading and writing** and **Use file extension list** options are select. Also, check the **Local drives** option.
  - c. Click **OK**.
3. Click the **Scheduler** tab. Confirm that a **Complete System Scan** is enabled to occur at least weekly, and a **Daily Update** is enabled.

---

### C.1.3 avast! 4 Home Edition, Version 4.6

To help ensure that avast! 4 Home Edition, Version 4.6<sup>112</sup> is configured properly, perform the following steps:

1. Run avast! Home Edition.
2. Click on the “eject” button in the upper left hand corner to open the menu. Select **Settings**.
3. Ensure that the **Test memory during application start-up** option is checked.
4. Click **Update (Basic)** from the left pane. Set both the **Virus database** and the **Program** options to **Automatic**.
5. Click on the disk icon (a thin box) in the right pane.
  - a. Make sure that **Scan local drives** is set to **On**; if it is not, click on the disk icon again to set it to **On**.
  - b. Ensure that **Scan removable media** is set to **On**; if it is not, click on the round icon in the right pane to set it to **On**.
6. Click **OK**.

---

<sup>111</sup> Avira AntiVir PersonalEdition is available for free download from <http://www.free-av.com/>.

<sup>112</sup> avast! 4 Home Edition is available for free download at [http://www.avast.com/eng/free\\_software.html](http://www.avast.com/eng/free_software.html).

---

---

## C.2 Antispyware Software

As described in Section 5.3.1, antispyware programs should be configured to improve their security. Step-by-step directions are provided here for configuring three free antispyware programs: Ad-Aware 1.06, Microsoft Windows Defender (Beta), and Spybot - Search & Destroy 1.4.

---

### C.2.1 Ad-Aware SE Personal 1.06

To help ensure that Ad-Aware SE Personal<sup>113</sup> is configured properly, perform the steps listed below. Administrators and users should be aware that the free Personal edition does not perform regular scans, so the scans should be initiated manually on a regular basis, preferably daily.

1. Run Ad-Aware SE Personal.
2. Select the **Configuration Window** (the gear icon).
  - a. Click the **General** button.
    - i. Ensure that the **Prompt to update outdated definitions** option is enabled.
    - ii. Set the number of days to **1**.
  - b. Click the **Scanning** button.
    - i. Check the **Scan within archives** option.
    - ii. Ensure that all of the options under **Memory & Registry** are selected.
3. Click **Proceed** to save the settings.

---

### C.2.2 Microsoft Windows Defender (Beta)

To help ensure that Microsoft Windows Defender (Beta)<sup>114</sup> is configured properly, perform the following steps:

1. Run Microsoft Windows Defender.
2. Click the **Tools** icon, then select **Options**.
3. Under **Automatic scanning**, ensure that **Automatically scan my computer**, **Check for updated definitions before scanning**, and **Apply default actions to items detected during a scan** are checked. Set the **Scan frequency** to an appropriate day of the week or to **Daily** to perform scans more often.

---

<sup>113</sup> Ad-Aware SE Personal is available for free download at <http://www.lavasoft.de/software/adaware/>.

<sup>114</sup> Microsoft Windows Defender (Beta) is available for free download at <http://www.microsoft.com/athome/security/spyware/software/default.mspx>.

4. Under **Default actions**, confirm that all three items are set to **Definition recommended action**.
5. Under **Real-time protection options**, confirm that **Use real-time protection** is enabled, and enable all of the security agents.
6. Under **Advanced options**, confirm that the **Scan the contents of archived files and folders for potential threats** and the **Use heuristics to detect potentially harmful or unwanted behavior by software that hasn't been analyzed for risks** options are both checked.
7. Under **Administrator options**, confirm that the **Use Windows Defender** and the **Allow users to use Windows Defender** options are enabled.
8. Click **Save** to save the settings.

---

### C.2.3 Spybot - Search & Destroy 1.4

To help ensure that Spybot - Search & Destroy 1.4<sup>115</sup> is configured properly, perform the following steps:

1. Run Spybot – Search & Destroy.
2. From the **Mode** menu, select **Advanced mode**. When asked to confirm the mode, click **Yes**.
3. In the left pane, click **Settings**, then click on the **Settings** entry under it. Scroll through the settings in the right pane to find and confirm the following:
  - a. Under **Main settings**, ensure that the three **Create backups** options and the two **Create system restore point** options are checked.
  - b. Under **Automation/Program start**, ensure that **Run check on program start**, **Fix all problems on program start**, **Rerun checks after fixing problems**, **Immunize on program start if program has been updated**, and **Don't ask for fixing confirmation** are enabled.
  - c. Under **Automation/System start**, ensure that **Automatically run program at system startup** is selected. Also, the **Run check on program start** and **Fix all problems on program start** options should be enabled.
  - d. Under **Automation/Web update**, ensure that **Search the web for new versions at each program start** and **Download updated include files if available online** options are enabled.
4. From the **Mode** menu, select **Default mode**.

---

<sup>115</sup> Spybot – Search & Destroy is available for free download from <http://www.spybot.info/en/index.html>.

5. Click the **Immunize** button in the left pane.
  - a. In the **Permanently running bad download blocker for Internet Explorer** box, ensure that **Enable permanent blocking of bad addresses in Internet Explorer** is enabled.
  - b. In the dialog box below it, ensure that the box is set to **Ask for blocking confirmation**.

---

### C.3 Personal Firewalls

As described in Section 5.5.3, personal firewalls should be configured to improve their security. Step-by-step directions are provided here for configuring two free personal firewalls: Windows Firewall and ZoneAlarm.

---

#### C.3.1 Windows Firewall

To configure Windows Firewall, perform the following steps:<sup>116</sup>

1. Click the **Start** menu and choose **Control Panel**. Double-click **Windows Firewall**.
2. Ensure that the firewall is set to **On**.
3. Do not check **Don't allow exceptions** unless the computer will be used on insecure networks, such as wireless hotspots or hotel networks.
4. Click the **Advanced** tab. Verify that the check boxes are selected for each network interface.
5. Click the **Settings** button for **Security Logging**. Check the **Log dropped packets** and **Log successful connections** boxes. Click **OK**.
6. Click the **Settings** button for **ICMP**. Verify that none of the check boxes are selected, then click on **OK**.
7. Click on **OK** to save all the settings.

---

#### C.3.2 ZoneAlarm 6.1

To configure ZoneAlarm,<sup>117</sup> perform the following steps:

1. Run ZoneAlarm.
2. Click on the **Preferences** tab in the upper right corner.

---

<sup>116</sup> Additional guidance on configuring Windows Firewall is available from the Microsoft Web site. It contains several helpful articles and papers; pointers to these resources are listed at <http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.msp>.

<sup>117</sup> A free version of ZoneAlarm can be downloaded from <http://www.zonelabs.com/store/content/home.jsp>.



- a. Ensure that **Check for product updates** is set to **Automatically**.
- b. In the **General** section, both the **Load ZoneAlarm at startup** and the **Protect the ZoneAlarm client** options should be enabled.
3. Click on the **Firewall** item at the left side of the window. **Internet Zone Security** should be set to **High**, and **Trusted Zone Security** should be set to at least **Medium**.
4. Click on the **Program Control** item at the left side of the window.
  - a. The **Program Control** should be set to **Medium**.
  - b. Set the **Automatic Lock** to **On**. This blocks network activity after a period of inactivity.
5. Click on the **Anti-virus Monitoring** item at the left side of the window. Ensure that **Monitoring** is set to **On**.
6. Click on the **E-mail Protection** item at the left side of the window. Ensure that **Basic MailSafe Settings** are set to **On**.

---

## C.4 E-mail Clients

As described in Section 7.2, e-mail clients should be configured to improve their security. Step-by-step directions are provided here for configuring three free e-mail clients: Eudora, Microsoft Outlook Express, and Thunderbird.

---

### C.4.1 Eudora 7

The following are suggested configuration changes to further enhance Eudora 7's security.<sup>118</sup> Unlike some other e-mail clients, Eudora does not enable most active scripting capabilities directly in the mail client. As a result, there are fewer settings that need to be adjusted to secure it.

1. Open Eudora.
2. Select **Tools**, then **Options**.
3. Select **Display**. Uncheck the option named **Automatically download HTML graphics**.
4. Select **Viewing Mail**. Uncheck the options named **Use Microsoft's viewer**, **Automatically open next message**, and **Allow executables in HTML content**.
5. Select **Styled Text**. Select the option for **Send plain text only**.
6. Click on **OK**.

---

<sup>118</sup> Eudora is available from the Eudora Web site, which is located at <http://www.eudora.com/>.

### C.4.2 Microsoft Outlook Express 6

Microsoft Outlook Express 6 is a reduced-feature version of Microsoft Outlook intended for home users.<sup>119</sup> Outlook Express offers some of the same security features as Outlook, but menu names and options often differ slightly. The default Outlook Express settings can be adjusted to make it more secure, as described in the following items:

1. Start Outlook Express.
2. Select **Tools**, then **Options**.
3. Click on the **Send** tab. Change the **Mail Sending Format** from **HTML** to **Plain Text**.
4. Click on the **Read** tab.
  - a. Check the box for **Read all messages in plain text**.
  - b. Uncheck **Automatically download message when viewing in Preview Pane**.
5. Click on the **Security** tab.
  - a. Under **Virus Protection**, set the security zone to **Restricted sites zone**.
  - b. Under **Download Images**, check the box for **Block images and other external content in HTML e-mail**.
6. Click on **OK**.

---

### C.4.3 Mozilla 1.7.12

Mozilla 1.7.12 is an open source package that includes a Web browser, an e-mail client, and an Internet Relay Chat (IRC) client.<sup>120</sup> The following changes should be made from the default Mozilla 1.7.12 configuration to improve its e-mail client's security and privacy:

1. Open Mozilla.
2. Select **Edit**, then select **Preferences**.
3. Expand the **Mail & Newsgroups** option.
4. Under the **Privacy & Security** option, select **Images**. Check the box for **Do not load remote images in Mail & Newsgroup messages**.
5. Expand the **Advanced** option.

---

<sup>119</sup> More information on Outlook Express is available from the Internet Explorer Home Page, located at <http://www.microsoft.com/windows/ie/default.mspx>.

<sup>120</sup> The Mozilla Web site is located at <http://www.mozilla.org/>.

6. Select the **Scripts & Plug-ins** option. Uncheck the box for enabling JavaScript for **Mail & Newsgroup**.
  7. Select **Software Installation**.
    - a. Check the option for **Enable software installation**.
    - b. Under **Update Notifications**, check the option for **Check for updates**, and select the radio button for **weekly**. This should cause the software to check for updates on a weekly basis.
  8. Click on **OK**.
- 

#### C.4.4 Thunderbird 1.5

Thunderbird is an e-mail client created as a branch of the Mozilla project.<sup>121</sup> Its interface and options are different from Mozilla's e-mail client. The following changes should be made from the default Thunderbird configuration:

1. Open Thunderbird.
2. Select **Tools**, then **Options**.
3. Select the **Composition** icon.
4. Click on the **Send Options** button.
  - a. For the Text Format, select **Convert the message to plain text**.
  - b. Click on **OK** to return to the Options screen.
5. Select the **Privacy** icon.
  - c. Check the option to **Block loading of remote images in mail messages**.
  - d. Check the option to **Block JavaScript in mail messages**.
6. Select the **Advanced** icon. Check the options to **Automatically check for updates to: both Thunderbird and Installed Extensions and Themes**.
7. Click on **OK** to close the Options window.

---

<sup>121</sup> More information on Thunderbird is available at <http://www.mozilla.org/products/thunderbird/>.

---

---

## C.5 Web Browsers

As described in Section 7.3, Web browsers should be configured to improve their security. Step-by-step directions are provided here for configuring three free Web browsers: Firefox, Microsoft Internet Explorer, and Mozilla.

---

### C.5.1 Firefox 1.5

Firefox is related to the Mozilla Web browser, but Firefox has a different interface and configuration options.<sup>122</sup> The following changes should be made from the default Firefox 1.5 configuration to improve security and privacy:

1. Open Firefox.
2. Select **Tools**, then **Options**.
3. Select the **Content** icon. Check the following boxes:
  - a. **Block Popup Windows**. (If any trusted sites need to be added, click the **Allowed Sites** button. Type in a URL and click the **Allow** button. Repeat as needed. When done, click **Close**.)
  - b. **Warn me when web sites try to install extensions or themes**
4. Select the **Privacy** icon.
  - a. Click on the **Cookies** tab. Check the box next to **for the originating site only**.
  - b. Click on the **Passwords** tab. Uncheck the box next to **Remember Passwords**.
5. Select the **Advanced** icon.
  - a. Click on the **Update** tab. For the **Automatically check for updates to:** section, check all the boxes.
6. Click on **OK** to close the Options window.

---

### C.5.2 Microsoft Internet Explorer 6

Microsoft Internet Explorer is installed as a default component of Windows XP Home Edition.<sup>123</sup> The following changes should be made from the default Microsoft Internet Explorer 6 configuration to improve security and privacy:

1. Open Internet Explorer.

---

<sup>122</sup> The Firefox home page is located at <http://www.mozilla.org/products/firefox/>.

<sup>123</sup> The Internet Explorer home page is located at <http://www.microsoft.com/windows/ie/default.msp>.

2. From the **Tools** menu, select **Pop-up Blocker**. If the option **Turn Off Pop-up Blocker** is displayed, popup blocking is already enabled. If the option **Turn On Pop-up Blocker** is displayed, select it to enable popup blocking.
3. From the **Tools** menu, select **Pop-up Blocker**, then **Pop-up Blocker Settings**.
  - a. Set the **Filter Level** to **Medium: Block most automatic pop-ups**.
  - b. To allow a trusted Web site to create popup windows, type the address of the desired Web site (e.g., <http://www.nist.gov/>) in the **Address of Web site to allow** text box and click the **Add** button. Repeat this process for each trusted Web site.
  - c. Click the **Close** button to apply the popup blocking settings.
4. From the **Tools** menu, select **Internet Options**.
5. Click on the **Privacy** tab, then the **Advanced...** button.
  - a. Check the option to **Override automatic cookie handling** settings.
  - b. Set the First-party Cookies to **Accept** and the Third-party Cookies to **Block**.
  - c. Check the option to **Always allow session cookies**.
  - d. Click **OK**.
6. Select the **Content** tab, then click the **AutoComplete** button.
  - a. Clear the check box for **User names and passwords on forms**.
  - b. Click **OK**.
7. Click on the **Advanced** tab.
  - a. Look at the settings in the **Browsing** section. Ensure that the **Enable Install On Demand (Internet Explorer)** and **Enable Install On Demand (Other)** options are unchecked.
8. Click **OK**.

---

### C.5.3 Mozilla 1.7.12

Mozilla is an open source package that includes a Web browser, an e-mail client, and an Internet Relay Chat (IRC) client.<sup>124</sup> The following changes should be made from the default Mozilla 1.7.12 configuration to improve its Web browser's security and privacy:

1. Open Mozilla.

---

<sup>124</sup> The Mozilla Web site is located at <http://www.mozilla.org/>.

2. Select **Edit**, then select **Preferences**.
3. Expand the **Privacy & Security** option.
4. Under the **Privacy & Security** option, select **Cookies**. Select the radio button for **Allow cookies for the originating web site only**.
5. Under the **Privacy & Security** option, select **Popup Windows**. Check the box next to **Block unrequested popup windows**.
6. Under the **Privacy & Security** option, select **Passwords**.
  - a. Uncheck the box for **Remember passwords**.
  - b. Check the box next to **Use encryption when storing sensitive data**. This feature requires the user to set a master password.
7. Under the **Privacy & Security** option, select **Master Password**. Click **Change Password** to generate a master password that will be used when Mozilla encrypts sensitive data stored locally (e.g., digital certificates, private keys).
8. Expand the **Advanced** option.
9. Select **Software Installation**.
  - a. Check the option for **Enable software installation**.
  - b. Under **Update Notifications**, check the option for **Check for updates**, and select the radio button for **weekly**. This should cause the software to check for updates on a weekly basis.
10. Click on **OK**.

---

---

## C.6 Instant Messaging Clients

As described in Section 7.4, instant messaging clients should be configured to improve their security. Step-by-step directions are provided here for configuring three free instant messaging clients: AOL Instant Messenger (AIM) 1.0.3, Windows Messenger 4.7, and Yahoo! Messenger 7.

---

### C.6.1 AOL Instant Messenger (AIM) 1.0.3

To help ensure that AOL Instant Messenger (AIM) 1.0.3<sup>125</sup> is configured properly, perform the following steps:

1. Open AIM.
2. From the **Edit** menu, click on **Settings**.
3. From the Settings window, choose the **Enhanced IM** icon. Uncheck all three of the **Auto-accept** options. Click the **Save** button.
4. From the **Edit** menu, click on **Edit My Contact Info**.
5. Adjust the address cards and privacy options so that sensitive information such as phone numbers and e-mail addresses is not displayed to all users. When done, click the **Save** button.

---

### C.6.2 Windows Messenger 4.7

To help ensure that Windows Messenger 4.7<sup>126</sup> is configured properly, perform the following steps. Administrators and users should be aware that Windows Messenger does not have configuration options for file transfers; instead, file transfer security is built into the software. If someone on a user's contact list tries to transfer the user a file, the user is only warned if the file has an unsafe extension, which could indicate malicious content. If someone not on a user's contact list tries to transfer a file to the user, the user can only receive the transfer if it is of a file type generally considered safe, such as a text file or graphic file.

1. Open Windows Messenger.
2. From the **Tools** menu, click on **Options**.
3. In the **My .NET Messenger Service Display Name** box, set a display name other than an e-mail address.
4. Click on **OK**.

---

<sup>125</sup> AIM is available for free download from <http://www.aim.com/>.

<sup>126</sup> Windows Messenger is available for free download from <http://www.microsoft.com/windowsxp/using/windowsmessenger/default.mspix>.

---

### C.6.3 Yahoo! Messenger 7

To help ensure that Yahoo! Messenger 7<sup>127</sup> is configured properly, perform the following steps. Administrators and users should be aware that Yahoo! Messenger does not have configuration options for file transfers.

1. Open Yahoo! Messenger.
2. From the **Messenger** menu, click on **My Contact Details**.
3. Adjust the contact details so that sensitive information such as phone numbers and e-mail addresses are not displayed to all users. When done, click the **Save & Close** button.

---

## C.7 Office Productivity Suites

As described in Section 7.5, office productivity suites should be configured to improve their security. Step-by-step directions are provided here for configuring two suites: Microsoft Office 2003 and OpenOffice.

---

### C.7.1 Microsoft Office 2003

Macros in Microsoft Office have been used for malware propagation. As such, it is important to take measures to increase the security of Office products regarding macro vulnerabilities. The following steps should be taken:

1. Open Microsoft Word.
2. Select **Tools**, then **Macro**, then **Security**.
  - a. Set the Security Level to **Medium**.
  - b. Click **OK**.
3. Select **Tools**, then **Options**.
  - a. Click on the **User Information** tab.
  - b. Delete any personal information that should not be shared with parties receiving files created or edited with Microsoft Word.
  - c. Click on the **File Locations** tab.
  - d. For **Documents**, **User templates**, and **AutoRecover files**, set the directory to be a folder within a user-specific area, such as My Documents.
  - e. Click on the **Security** tab.

---

<sup>127</sup> Yahoo! Messenger is available for free download from <http://messenger.yahoo.com/>.



- f. Check the option to **Remove personal information from file properties on save**.
    - g. Click **OK**.
  4. Close Microsoft Word.
  5. Open Microsoft Excel.
  6. Select **Tools**, then **Macro**, then **Security**.
    - a. Set the Security Level to **Medium**.
    - b. Click **OK**.
  7. Select **Tools**, then **Options**.
    - a. Click on the **User Information** tab.
    - b. Set the **Default file location** to be a directory within a user-specific area, such as My Documents.
    - c. Click on the **Security** tab.
    - d. Check the option to **Remove personal information from file properties on save**.
    - e. Click **OK**.
  8. Close Microsoft Excel.
  9. Open Microsoft Powerpoint.
  10. Select **Tools**, then **Macro**, then **Security**.
    - a. Set the Security Level to **Medium**.
    - b. Click **OK**.
  11. Select **Tools**, then **Options**.
    - a. Click on the **Save** tab.
    - b. Set the **Default file location** to be a directory within a user-specific area, such as My Documents.
    - c. Click on the **Security** tab.
    - d. Check the option to **Remove personal information from file properties on save**.
    - e. Click **OK**.

12. Close Microsoft Powerpoint.

---

### C.7.2 OpenOffice 2.0

The following options should be configured to ensure better security in OpenOffice 2.0:

1. Start OpenOffice Writer.
2. Select **Tools**, then **Options**.
  - a. Expand the **OpenOffice.org** item; below it, select **User Data**.
  - b. Delete any personal information that should not be shared with parties receiving files created or edited with OpenOffice Writer.
  - c. From the left pane, select **Path**.
  - d. Ensure that the **Backups, My Documents, User Configuration, and User-Defined Dictionaries** options are set to folders within a user-specific area, such as My Documents.
  - e. From the left pane, select **Security**.
  - f. Ensure that the **Remove personal information on saving** option is checked.
  - g. Click the **Macro Security** button. Set the security level to **Medium** and click **OK**.
  - h. Click **OK**.
3. Close OpenOffice Writer. The settings that were made will apply to other OpenOffice components.

## Appendix D—Tools

Appendix D summarizes various tools mentioned in this document that can be used to configure, manage, and monitor Windows XP Home Edition security settings.

**Table D-1. Windows XP Home Edition Tools**

Tool Name	Relevance	Location
Automatic Updates	Checks Microsoft update server for new updates; downloads and installs them	Control Panel, Automatic Updates
Backup or Restore Wizard	Performs backups and restores, ranging from backing up the current user's files and settings to backing up the whole computer	Install from the Windows XP Home Edition installation CD (\\VALUEADD\MSFT\NTBACKUP\NTBACKUP.msi) Once installed, run from Start, All Programs, Accessories, System Tools, Backup
Disk Cleanup	Removes temporary files, deleted files, and other unneeded content from a computer	Start, All Programs, Accessories, System Tools, Disk Cleanup
Event Viewer	Displays application, security, and system log entries	Right-click on My Computer, Manage, Event Viewer
File Signature Verification Utility	Checks Windows XP Home Edition operating system files to ensure they have been digitally signed by Microsoft	Start, All Programs, Accessories, System Tools, System Information From System Information, go to the Tools menu and select File Signature Verification Utility
Files and Settings Transfer Wizard	Performs backups and restores for a single user's files and settings	Start, All Programs, Accessories, System Tools, Files and Settings Transfer Wizard
Internet Connection Firewall (ICF)	Personal firewall; replaced in SP2 by Windows Firewall	N/A (use Windows Firewall instead)
Microsoft Baseline Security Analyzer (MBSA)	Scans computer to identify security issues	Download and install from <a href="http://www.microsoft.com/technet/security/tools/mbsahome.msp">http://www.microsoft.com/technet/security/tools/mbsahome.msp</a> Once installed, run from Start, All Programs, Microsoft Baseline Security Analyzer
Microsoft Update	Checks for available updates, transfers them to system, and installs them	<a href="http://update.microsoft.com/">http://update.microsoft.com/</a>
Microsoft Windows Defender (beta)	Scans computer to identify certain types of spyware and remove them	<a href="http://www.microsoft.com/athome/security/spyware/software/default.msp">http://www.microsoft.com/athome/security/spyware/software/default.msp</a>
Recovery Console	Attempts to recover Windows XP Home Edition from serious damage; considered a last-resort option when other recovery options have failed	Windows XP Home Edition installation CD

Tool Name	Relevance	Location
Remote Assistance	Allows a user to get remote technical support assistance for a Windows XP Home Edition computer from someone else	Start, Help and Support, Invite a friend to connect to your computer with Remote Assistance
Remove Hidden Data	Allows Microsoft Office users to remove hidden data, comments, and tracked changes from Microsoft Office files	<a href="http://www.microsoft.com/downloads/details.aspx?familyid=144E54ED-D43E-42CA-BC7B-5446D34E5360&amp;displaylang=en">http://www.microsoft.com/downloads/details.aspx?familyid=144E54ED-D43E-42CA-BC7B-5446D34E5360&amp;displaylang=en</a>
Security Center	Indicates the status of Automatic Updates, antivirus software, and personal firewalls	Control Panel, Security Center
System Information	Collects a wealth of helpful information on hardware, network configuration, software configuration, and the configuration of certain Microsoft applications	Start, All Programs, Accessories, System Tools, System Information
System Restore	Creates new system restore points as requested by administrators	Start, All Programs, Accessories, System Tools, System Restore
Windows Firewall	Personal firewall; added to Windows XP Home Edition in SP2	Control Panel, Windows Firewall
Windows Malicious Software Removal Tool	Checks for and attempts to remove certain common malware threats	Installed automatically through Automatic Updates and Microsoft Update Can be downloaded or run directly from <a href="http://www.microsoft.com/security/malwareremove/default.mspx">http://www.microsoft.com/security/malwareremove/default.mspx</a>
Windows Update	Checks for available updates, transfers them to system, and installs them. Replaced by Microsoft Update.	<a href="http://windowsupdate.microsoft.com/">http://windowsupdate.microsoft.com/</a>

## Appendix E—Glossary

Selected terms used in *Guidance for Securing Microsoft Windows XP Home Edition* are defined below.

**Administrative Account:** A user account with full privileges on a computer.

**Antispyware Software:** A program that specializes in detecting both malware and non-malware forms of spyware.

**Antivirus Software:** A program specifically designed to detect many forms of malware and prevent them from infecting computers, as well as cleaning computers that have already been infected.

**Backup:** Duplicating data onto another medium.

**Cookie:** A small file that stores information for a Web site.

**Disinfect:** Remove malware from within a file.

**File Association:** The mapping between a file extension and the software that attempts to run files with that extension.

**File Extension:** A period and one or more letters at the end of a filename intended to indicate the file's type.

**History File:** A file that records all the Web sites and pages that were visited recently.

**Hotfix:** Updated code from Microsoft that addresses a specific security problem.

**Limited User Account:** A user account with limited privileges on a computer.

**Malicious Code:** See "Malware".

**Malware:** A computer program that is covertly placed onto a computer with the intent to compromise the privacy, accuracy, or reliability of the computer's data, applications, or operating system.

**On-Access Scanning:** Performing real-time scans on a computer of each file as it is downloaded, opened, or executed.

**On-Demand Scanning:** Launching scans of a computer manually as needed.

**Open Files:** Files that are currently in use.

**Persistent Cookie:** A cookie that stays on a computer, which allows a Web site to identify the Web site's user.

**Personal Firewall:** A utility on a computer that monitors network activity and blocks communications that are unauthorized.

**Phishing:** Using fraudulent e-mails and Web sites that look very similar to the legitimate sources with the intent of committing financial fraud.

**Popup Window:** A standalone Web browser pane that opens automatically when a Web page is loaded or a user performs an action designed to trigger a popup window.

**Quarantine:** Store files containing malware in isolation for future disinfection or examination.

**Restore:** Transfer data from a backup medium to a computer.

**Security Control:** A protective measure against threats.

**Security Rollup:** A collection of several hotfixes.

**Service Pack (SP):** A major upgrade to a Microsoft operating system that resolves dozens of functional and security problems and often introduces new features or makes significant configuration changes.

**Session Cookie:** A cookie that is valid for a single Web site session.

**Spam Filtering Software:** A program that analyzes e-mails to look for characteristics of spam, and typically places messages that appear to be spam in a separate e-mail folder.

**Spyware:** Malware specifically intended to violate a user's privacy.

**Vulnerability:** A security weakness of a computer.

**Web Content Filtering Software:** A program that prevents access to undesirable Web sites, typically by comparing a requested Web site address to a list of known bad Web sites.

## Appendix F—Acronyms

Selected acronyms used in the guide are defined below.

<b>AES</b>	Advanced Encryption Standard
<b>AP</b>	Access Point
<b>BIOS</b>	Basic Input/Output System
<b>CD</b>	Compact Disk
<b>DEP</b>	Data Execution Prevention
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DNS</b>	Domain Name System
<b>DSL</b>	Digital Subscriber Line
<b>EFS</b>	Encrypting File System
<b>e-mail</b>	Electronic mail
<b>FAT</b>	File Allocation Table
<b>FISMA</b>	Federal Information Security Management Act
<b>FUS</b>	Fast User Switching
<b>GB</b>	Gigabyte
<b>GUI</b>	Graphical User Interface
<b>HTML</b>	Hypertext Markup Language
<b>ICF</b>	Internet Connection Firewall
<b>ICS</b>	Internet Connection Sharing
<b>IP</b>	Internet Protocol
<b>ISP</b>	Internet Service Provider
<b>IT</b>	Information Technology
<b>ITL</b>	Information Technology Laboratory
<b>LAN</b>	Local Area Network
<b>LUA</b>	Limited User Account
<b>MAC</b>	Media Access Control
<b>MBSA</b>	Microsoft Baseline Security Analyzer
<b>ME</b>	Millennium Edition
<b>MSKB</b>	Microsoft Knowledge Base
<b>NAT</b>	Network Address Translation
<b>NIST</b>	National Institute of Standards and Technology
<b>NTFS</b>	NT File System

**OMB** Office of Management and Budget  
**OS** Operating System

**QoS** Quality of Service

**RA** Remote Assistance

**SOHO** Small Office Home Office

**SP** Service Pack

**SP** Special Publication

**UPS** Uninterruptible Power Supply

**URL** Uniform Resource Locator

**VPN** Virtual Private Network

**WEP** Wired Equivalent Privacy

**Wi-Fi** Wireless Fidelity

**WPA** Wi-Fi Protected Access



## Appendix G—Resources

This appendix lists print and online resources that could be helpful to people who want to learn more about Windows XP Home Edition and how to secure it.

### G.1 Print Resources

Bott, Ed, et al., *Microsoft Windows XP Inside Out, Second Edition*, Microsoft Press, 2004.

Bott, Ed and Siechert, Carl, *Microsoft Windows Security Inside Out for Windows XP and Windows 2000*, Microsoft Press, 2002.

Cowart, Robert and Knittel, Brian, *Special Edition Using Microsoft Windows XP Home, Third Edition*, Que, 2004.

Moulton, Pete, *SOHO Networking: A Guide to Installing a Small-Office/Home-Office Network*, Prentice Hall PTR, 2002.

Pogue, David, *Windows XP Home Edition: The Missing Manual, Second Edition*, O'Reilly, 2004.

Simmons, Curt and Causey, James, *Microsoft Windows XP Networking Inside Out*, Microsoft Press, 2002.

Thurrott, Paul, *Windows XP Home Networking, Second Edition*, John Wiley and Sons, 2004.

### G.2 NIST Documents and Resources

- Computer Security Resource Center Special Publications

- <http://csrc.nist.gov/publications/nistpubs/index.html>

- SP 800-46, *Security for Telecommuting and Broadband Communications*  
Provides recommendations for securing telecommuting computers and home networks
  - SP 800-83, *Guide to Malware Incident Prevention and Handling*  
Provides more technical information on the major types of malware

- Security Checklists for IT Products project

- <http://csrc.nist.gov/checklists/>

- Acts as a repository for checklists and guides for securing various operating systems, applications, and devices

### G.3 Microsoft Web-Based Resources

Microsoft's Web site contains a wealth of information regarding Windows XP Home Edition and Windows security. This section lists some of these resources, divided into two categories: general (e.g., setting up home networking) and security-related.

### G.3.1 Windows XP Home Edition Resources

- Features and Functionality in Windows XP Service Pack 2  
<http://www.microsoft.com/technet/prodtechnol/winxppro/plan/xpsp2ff.mspx>  
Links to various articles and papers on the features that Service Pack 2 provides, including new security features and changes to existing security features
- Home and Small Office Networking with Windows XP  
<http://www.microsoft.com/windowsxp/using/networking/default.mspx>  
Links to articles on setting up and troubleshooting wired and wireless home networks
- Microsoft Technet  
<http://technet.microsoft.com/default.aspx>  
Information on Windows XP Home Edition security for highly advanced users
- *Step-by-Step Guide to Migrating Files and Settings*  
<http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/mgrtfset.mspx>  
Information on transferring user files and settings from one computer to another
- *Troubleshooting Microsoft Windows XP-based Wireless Networks in the Small Office or Home Office*  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=35c7e5ad-59e7-477b-9d27-6a7030e67002&displaylang=en>  
Information on resolving problems with wireless networking
- Windows XP Home Page  
<http://www.microsoft.com/windowsxp/default.mspx>  
Main Web site for all editions of Windows XP, including Home Edition
- Windows XP Service Pack 2  
<http://www.microsoft.com/windowsxp/sp2/default.mspx>  
Main Web site for Windows XP Service Pack 2, with links to many Web sites and articles addressing specific Service Pack 2-related topics

### G.3.2 Windows XP Home Edition Security Resources

- *Configuring Windows XP IEEE 802.11 Wireless Networks for the Home and Small Business*  
<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx>  
Detailed technical article on securing wireless networking
- *How to Obtain the Latest Windows XP Service Pack*  
<http://support.microsoft.com/?id=322389>  
Explains how to acquire the current service pack for Windows XP
- Microsoft Download Center  
<http://www.microsoft.com/downloads/search.aspx?displaylang=en>  
Main Web site for Microsoft downloads, including security updates and security tools (e.g. Windows Malicious Software Removal Tool)

- Microsoft Security At Home  
<http://www.microsoft.com/athome/security/default.aspx>  
Main Web site for securing Microsoft products used on home computers
- Microsoft Security Home Page  
<http://www.microsoft.com/security/>  
Main Web site for securing Microsoft products; has articles on various security-related topics
- Microsoft Security Update Alerts  
<http://www.microsoft.com/security/bulletins/alerts.aspx>  
Allows users to sign up for e-mail alerts that describe major new security threats and explain how to protect computers from them
- Microsoft TechNet Security Resource Center  
<http://www.microsoft.com/TechNet/security/default.aspx>  
Information for highly advanced users on securing Microsoft products
- Microsoft Update Web site  
<http://update.microsoft.com/>  
Main Web site for identifying, downloading, and installing needed security updates
- Microsoft Windows Defender (Beta)  
<http://www.microsoft.com/athome/security/spyware/software/default.aspx>  
Information on the Microsoft Windows Defender beta utility, as well as more general information on spyware
- *Types of User Accounts*  
[http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ua\\_c\\_account\\_types.aspx](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ua_c_account_types.aspx)  
Explains the difference between limited user accounts and administrative accounts
- *Understanding Windows Firewall*  
[http://www.microsoft.com/windowsxp/using/security/internet/sp2\\_wfintro.aspx](http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.aspx)  
Information on the capabilities of Windows Firewall

#### **G.4 Other Web-Based Windows XP Home Edition Resources**

The items below are other Web-based resources that might be helpful for understanding the security and management of Windows XP Home Edition computers.

- Mark Salloway's Windows XP Resource Center  
<http://www.mvps.org/marksxp/main.php>
- Sysinternals  
<http://www.sysinternals.com/>
- Windows XP Resource Center  
<http://labmice.techtarget.com/windowsxp/default.htm>
- WXPnews  
<http://www.wxpnews.com/index.cfm>

**This page has been left blank intentionally.**

## Appendix H—Index

### A

Activate Windows, 5-7  
 Ad-Aware SE Personal, C-4  
 Add or Remove Programs, 4-2, 5-21, 6-2  
 Antispyware software, 3-22, 5-1, 5-12, 6-2, 6-4, 8-2, A-9, C-4  
 Antivirus software, 3-20, 5-1, 5-12, 6-2, 6-4, 8-2, A-9, C-1  
 AOL Instant Messenger (AIM), C-13  
 Application configuration, 3-26  
 Automated System Recovery Wizard, 3-29  
 Automatic Updates, 3-1, 3-19, 5-7, 5-11, A-8, D-1  
 avast! 4 Home Edition, C-3  
 AVG Free Edition for Windows, C-1  
 Avira AntiVir PersonalEdition Classic, C-3

### B

Backup or Restore Wizard, 3-29, 4-3, 4-10, D-1  
 Backup Utility, 3-29  
 Backups, 3-28, 4-3, 6-6, 8-1  
   Restoring, 4-10  
 Blue screen, 8-17  
 Boot options, 8-17  
 Bot, 2-3

### C

Client for Microsoft Networks service, 3-10, 4-8, B-3  
 ClipBook service, 3-13, B-4  
 Clock synchronization, 8-5  
 Computer Name, 3-15  
 Content filtering, 3-24  
 Content filtering software, 5-12  
 Control Panel  
   Default view, 5-2, A-3  
 Cookies, 3-15, 7-3

### D

Data Execution Prevention (DEP), 3-28, B-1  
 Disk Cleanup, 8-3, 8-7, D-1  
 Disk scrubbing, 8-20

### E

E-mail clients, 3-26, 7-2, C-7  
 Encrypting File System (EFS), 3-17  
 Environment. *See* Threat environment  
 Error messages, 8-13  
 Eudora, C-7  
 Event logs, 8-15  
 Event Viewer, 8-15, D-1

### F

Fast User Switching (FUS), 3-5, 3-8, 5-15  
 File Allocation Table (FAT), 4-7  
 File and Printer Sharing for Microsoft Networks service, 3-9, 4-8, B-3  
 File associations, 3-12, 7-2, B-6  
 File encryption, 3-17, B-4  
 File extensions, 3-12, 7-2  
 File Signature Verification Utility, 8-16, D-1  
 Files, 3-17, 5-20, 7-1, 8-7  
 Files and Settings Transfer Wizard, 3-29, 4-4, 4-10, D-1  
 Firefox, C-10  
 Folder Options, 3-12, 7-2  
 Folders, 5-20, 7-1  
 Forgotten Password Wizard, 5-14

### H

Hard drives, 8-20  
 History file, 3-15  
 Hotfix, 3-1

### I

Infrared Monitor service, 3-13, B-4  
 Installation, 4-1  
   Preparation, 4-2  
 Instant messaging clients, 3-27, 7-3, C-13  
 Internet Connection Firewall (ICF), 3-23, 5-4, A-3, D-1  
 Internet Connection Sharing (ICS), 3-11, 3-14, 5-19

### K

*Keystroke logger*, 2-3

### L

Last Known Good Configuration, 8-18  
 Limited user account (LUA), 3-8, 3-14, 5-15, A-9  
 Locking a session, 3-8  
 Logs. *See* Event logs

### M

Maintenance, 8-1  
 Malicious code. *See* Malware  
 Malicious mobile code, 2-2  
 Malware, 2-2, 3-20, 5-12, 6-3, 6-4, 8-2  
 Microsoft Baseline Security Analyzer (MBSA), 8-8, D-1  
 Microsoft Internet Explorer (IE), C-10  
 Microsoft Office, C-14  
 Microsoft Outlook Express, C-8  
 Microsoft Security Update Alerts, 8-2  
 Microsoft Update, 3-2, 5-7, A-5, D-1

Microsoft Windows Defender, 3-22, 5-23, C-4, D-1  
 Mobile code, 3-26, 7-2  
 Mozilla, C-8, C-11  
 My Documents, 3-17

## N

NetMeeting Remote Desktop Sharing service, 3-14, B-4  
 Network address translation (NAT), 3-12  
 Networking, 3-9, 4-8, 5-5, 5-16, B-3  
     Wireless. *See* Wireless networking  
 NT File System (NTFS), 4-7

## O

Office productivity suites, 3-27, 7-3, C-14  
 OpenOffice, C-16

## P

Password reset disk, 3-9, 5-14  
 Passwords, 3-5, 5-14, 7-1, 7-3, 8-7  
     Quality, 3-6  
 Personal firewall, 3-11, 3-22, 5-4, 5-13, 6-2, 6-4, A-3, C-6  
 Personal information. *See* Sensitive information  
 Personalized Login, 3-5  
 Pharming, 2-3  
 Phishing, 2-3  
 Physical access, 3-8  
 Physical security, 2-5  
 Popup blocking, 3-25  
 Privacy, 3-14

## Q

Quality of Service (QoS) Packet Scheduler, 3-9, 4-8, B-3

## R

Recovery Console, 8-19, D-1  
 Recovery from failure, 8-17  
 Recycle Bin, 3-14  
 Remote access, 3-10  
 Remote Assistance (RA), 3-10, 5-16, 8-12, D-2  
 Remove Hidden Data, D-2  
 Rootkit, 2-2  
 Routing and Remote Access service, 3-14, B-4  
 Run As, 3-8  
 Running Tasks, 5-22

## S

Safe Mode, 8-17  
 Security Center, 3-19, 5-13, 8-2, 8-6, A-3, D-2  
 Security control. *See* Security protections  
 Security protections, 2-4, 3-1  
     Management, 2-4  
     Operational, 2-4  
     Technical, 2-4  
 Security rollup, 3-1  
 Security software, 6-3

Security software suites, 3-25  
 Sensitive information, 2-2, 2-5, 3-5, 3-14, 3-17, 7-1, 8-7, B-4  
     Destruction, 8-19  
 Service pack (SP), 3-1  
     Identification, 5-2  
*Services*, 3-13  
 Shared Documents, 5-20  
 Shared Folders, 3-18, 8-4  
 Simple File Sharing, 3-18  
 Software applications, 5-21  
     Identification, 6-1  
 Software updates, 3-1, 5-4, 5-7, 8-1, A-5  
 Spam filtering software, 3-24, 5-12  
 Spybot - Search & Destroy, C-5  
 Spyware, 2-3  
 SSDP Discovery Service, 3-14, B-5  
 Startup Programs, 5-22  
 Stored User Names and Passwords, 3-16  
 System history information, 8-14  
 System Information, 5-22, 6-3, 8-13, D-2  
 System Restore, 6-6, 8-18, D-2  
 System restore points, 8-3

## T

Temporary files, B-4  
 The Security Center, 5-5  
 Threat environment, 2-5  
 Threats, 2-1, 2-5  
 Thunderbird, C-9  
 Trojan horse, 2-2

## U

Uninterruptible power supply (UPS), 3-28  
 Universal Plug and Play (UPnP) Device Host service, 3-14, B-5  
 User accounts, 3-5, 4-9, 5-14, 7-1, 8-3  
     Administrator, 3-7  
     Default, 3-7, B-1  
     Guest, 3-7, B-2  
     HelpAssistant, 3-7, B-2  
     Removal, 8-6  
     Support\_388945a0, 3-8, B-2

## V

Virus, 2-2  
 Vulnerability, 2-4

## W

Web browsers, 3-15, 3-26, 5-4, 7-3, 8-7, C-10  
     Cache files, 3-15  
 Web content filtering software, 3-24, 5-12  
 Wi-Fi Protected Access (WPA), 3-10  
 Windows Firewall, 3-23, 5-4, 5-13, A-3, C-6, D-2  
 Windows Malicious Software Removal Tool, 3-21, 6-5, D-2  
 Windows Messenger, C-13

Windows Update, 5-8, D-2, *See* Microsoft Update  
Windows XP versions, 2-1  
Wired Equivalent Privacy (WEP), 3-11  
Wireless Auto Configuration, 3-11, 5-18  
Wireless networking, 3-10, 5-6, 5-17  
    Wi-Fi Protected Access (WPA), 3-10  
Wireless Zero Configuration, 3-14, B-5  
Worm, 2-2

**Y**

Yahoo! Messenger, C-14

**Z**

ZoneAlarm, C-6