PC Magazine Windows Vista Security Solutions
byDan DiNicolo
John Wiley & Sons 2007 (360 pages)
ISBN:9780470046562

Providing a valuable roadmap to the Golden Rules of Windows security, this guide explains the steps to take in order to remain safe in the super-charged breeding ground for security and privacy threats that is the Internet.

Table of Contents

Back Cover

When you want to defend Windows Vista, it's good to know a *PC Magazine* expert.

Unless a time machine just dropped you in the 21st century, you already know that protecting your computer is essential. Now, here's Vista-new enough that no one is sure exactly what security threats might arise to hijack your system. That's why the road map that Dan DiNicolo provides in this book is so valuable. Follow these steps, abide by the Golden Rules of Windows security, and you'll sleep better. We promise.

See at a glance what's critical for security

- Follow easy steps to implementing logon security, strong passwords, and firewall configuration
- Ensure that security holes are patched regularly
- Find out how to protect your Vista system against viruses-for free
- Recognize the difference between malware and viruses and install the right anti-spyware protection
- Implement parental controls to protect your kids online
- Explore additional layers of security, such as e-mail encryption and secure file deletion

Five Golden Rules of Windows security

1. Implement user accounts properly and protect them all with strong passwords.
2. Install a firewall.
3. Update your system regularly to be sure you have all security patches and Service Packs installed.
4. Use up-to-date anti-virus software and scan regularly for viruses.
5. Use up-to-date anti-spyware protection and scan regularly for spyware and related threats.

About the Author

Dan DiNicolo is a freelance author, trainer, and consultant based in the snowy backwoods of Canada. He is the author of *PC Magazine Windows XP Security Solutions* and has written scores of magazine articles about securing Windows systems. In his spare time Dan enjoys dreaming of a world where computers are as easy to use as toaster ovens.

PC Magazine Windows Vista Security Solutions

Dan DiNicolo
Wiley Publishing, Inc.

Published by
Wiley Publishing, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
http://www.wiley.com

Indianapolis, Indiana

Published simultaneously in Canada

978

0-470-04656-2

10 9 8 7 6 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data: Available from Publisher.

For everyone who has ever helped a friend, family member, or neighbor out of a computer-related jam.

About the Author

Dan DiNicolo is a freelance author, trainer, and consultant based in the snowy backwoods of Canada. He is the author of *PC Magazine Windows XP Security Solutions* and has written scores of magazine articles about securing Windows systems. In his spare time Dan enjoys dreaming of a world where computers are as easy to use as toaster ovens.

Credits

Acquisitions Editor Katie Mohr

Development Editor Maryann Steinhart

Technical Editor Todd Meister

Production Editor Angela Smith

Copy Editor Travis Henderson

Editorial Manager Mary Beth Wakefield

Production Manager Tim Tate

Vice President and Executive Group Publisher Richard Swadley

Vice President and Executive Publisher Joseph B. Wikert

Proofreading Word One

Composition Maureen Forys, Happenstance Type-O-Rama

Indexing Ted Laux

Anniversary Logo Design Richard Pacifico

Acknowledgments

Thanks to Katie Mohr and Maryann Steinhart at Wiley for all of their help in getting this book from idea to print. Thanks also to Todd Meister for his eagle eye and ideas throughout the tech editing process.

I'm not sure whom to thank for putting snakes on the cover of this book, but I love it.

As always, thanks to the family and friends who put up with me (and my craziness) when I take on big writing projects

Last, but certainly not least, thank you, Jessica. The excellent adventure continues!

Introduction

I've been writing about computers and the need to keep them properly secured for a long time. Back in the good old days, protecting your computer involved little more than installing anti-virus software, keeping it updated, and scanning for threats regularly. Unfortunately, the good old days are long gone.

Today, computers and the Internet form a super-charged breeding ground for a myriad of security and privacy threats. There are people and programs trying to obtain personal information in a bid to steal identities. Unscrupulous marketers use adware and spyware to track online wanderings and target advertising to your personal preferences. People attempt to install keylogging programs on PCs to capture banking-related usernames and passwords. Neighbors steal high-speed Internet access from neighbors. Scammers attempt to sell everything under the sun via the scourge known as spam. Predators are seeking out children online. As useful a resource as the Internet may be, safe it is not.

Thankfully, all is not lost. If you take the time to understand the threats that exist, then you can do something to protect against them. My goal with this book is to not only explain the risks that you'll encounter when connecting to the Internet or using Windows Vista, but also to show you the steps to take to ensure that you, your PC, and your family remain safe.

Securing a computer running Windows Vista isn't difficult, but it does take some dedication on your part. Ultimately, the actions you take will be the difference between owning a secure PC and remaining safe online, or leaving you and your system exposed on the Internet.

I sincerely hope that you make the right choice.

May the force be with you!

Part I: Getting Down to the Business of Securing Windows Vista

Chapter List

Chapter 1: A Short Introduction to Securing Windows Vista

Overview

Ioriginally planned to start this book with a long diatribe on the importance of taking the steps necessary to ensure that your Windows Vista system remains safe and secure. Thankfully, at the last minute I changed my mind. The reason is simple enough: I assume that if you're reading this, then you already have at least a basic understanding of the fact that computer security is important. So, I'm not going to lecture you. Instead, I'm going to provide you with a map.

Yes, a map, and a fairly basic map at that. Securing any computer running Windows Vista - or just about any Windows operating system for that matter - is as easy as following simple instructions. Some tasks are absolutely essential, and without them your system has little chance of remaining secure. Others are only relevant to users with a home or small office network. Some topics are just plain good to know, meaning they'll help to improve the security of your system but aren't going to be the deciding factor as to whether your system remains safe. Last but not least, there are topics geared toward those of you who truly want to take things up a notch by ensuring that not only your computer remains secure, but also that your personal files and communications remain private.

The moral of the story is that you could read this book in the traditional cover-to-cover manner, but it isn't essential. I've tried to organize topics in the most linear manner as possible, but there are topics that some of you can safely skip. Pretty much every chapter in this book can stand on its own, so if you're in the mood to tackle issues around the security of your wireless network you can simply flip to that chapter to learn how it's done. Will reading the entire book front-to-back hurt you? Of course not! However, I do recognize that different people have different levels of tolerance for this computer security stuff, and I certainly don't want you to feel overwhelmed. What I do want, however, is for you to take at least the key steps necessary to ensure that your computer remains as secure as possible. If you choose to go beyond those steps, that's excellent. When all is said and done, there are six chapters I insist you read and take action on - seven if you're a parent. I'll get to all the dirty details on what's important in a moment.

Before I go there, however, you need to understand two things:

- **Security is an ongoing process.** As time goes on, new security threats will emerge that will require you to take action. I can't predict the future, but I can spot trends. If the last few years have shown anything, it's that the "bad guys" are always looking for new ways to compromise your computer. In other words, just because your computer is secure today, it doesn't mean that it will be completely safe tomorrow. To some degree, you'll need to keep an eye (or ear) on the news to ensure you're informed as new risks arise. You'll also need to be somewhat diligent about ensuring that the techniques you use to secure your computer remain intact, and updated as required.
- **Windows Vista is a new operating system.** It hasn't stood any true test of time just yet, so it's almost impossible to guess what security and privacy issues will arise, or when. Right now, the steps you need to take to ensure that your computer remains properly secured are very similar to those associated with securing any computer running Windows, be it Windows XP or even Windows 2000. Certainly Windows Vista offers some key security improvements over previous versions, and some of the steps you'll need to follow to get things done have changed. However, there's simply no telling what the future may hold. Although the security and privacy improvements in Windows Vista look very promising, I'd be very rich and living on a private island if I could accurately guess what the next big security risk is.

Fortunately, all is not lost. If you look at the key steps outlined in this book as being essential (and take the necessary actions, of course!), your Windows Vista system will be as secure as it can possibly be right now. In fact, if you take the time to get things done properly right from the get-go, you're unlikely to experience any real security breakdowns at all. However, I can only explain what you need to do to set things up correctly, and then how to maintain your setup. If you decide that security is important today and then don't ever give it another thought, your Windows Vista system may well end up being at serious risk.

Oh yeah, the map! The journey begins by ensuring you understand the five golden rules of Windows security, and then getting the directions you need. The next few sections will help you on your way.

The Five Golden Rules of Windows Security

The five golden rules of securing any Windows system are quite basic and easy to understand:

1. You must implement user accounts properly, and protect all user accounts with a strong password.
2. Your Windows Vista system must be protected by a firewall.
3. Your Windows Vista system must be updated regularly to ensure that you have all necessary security patches and Service Packs installed.
4. Your Windows Vista system must be protected by up-to-date antivirus software, and you must scan for viruses regularly.

5. Your Windows Vista system must be protected by up-to-date antispyware software, and you must scan for spyware and related threats regularly.

That's the extent of the golden rules of Windows security, honestly. Yes, there are other important concepts to consider, but these five are crucial. If you neglect to follow any of these rules, your Windows system will always be at risk.

The Security Map

There's always more than one way to get from point A to point B, and I'm not going to assume that you'll follow the exact directions that I provide. The truth is that I'm not 100 percent sure of your exact situation. For example, you may already be well aware of the importance of having a firewall in place, but it's equally possible that you don't have a clue as to what a firewall does. So, just to be on the safe side, I'm going to assume that you need a little guidance. The following sections explain the relevant importance of topics covered in this book according to a highly scientific ranking scale that I've developed:

- **No excuses!** The topics outlined in this section are important. Really important. Everyone, excluding perhaps the family pet, needs to know this stuff. Please read these chapters!
- **Got a network?** As the name suggests, these chapters are relevant to anyone who has a home or small office network. A network can be as simple as one laptop computer with a wireless network card connecting to a wireless router, or be a setup that includes multiple computers wired through a switch, hub, or router. It doesn't matter. If you have a network, you'll want to be secure, and you should read these chapters.
- **Nice to know.** None of the topics covered in these chapters are absolutely imperative from a basic system security perspective, but each is still important in its own way. Can you improve the security of your Windows Vista system by reading these chapters? Absolutely, but I'm not going to recommend that you stay up all night trying to implement every single recommendation that I offer in these chapters. Getting a good night's sleep is always important.
- **For those who want to take things up a notch.** If you're serious (or really keen) about locking down your system, then you should read these chapters. Actually, if you're really serious, you should probably read every chapter because you'll learn lots of cool stuff, but I digress. These chapters are really aimed at those of you who want to know how to do some of the more advanced security stuff, like encrypting files or e-mail messages. Not for everyone to be sure, but there are some cool techniques and concepts outlined in these chapters for those who want to take things to a higher plane of security consciousness. That's pretty deep, man.

No Excuses!

All of the chapters listed in this section directly relate to the five golden rules of Windows security. Understanding the concepts and following the techniques covered in these chapters is absolutely essential if there is to be any hope of keeping your Windows Vista secured. Chapters that fall into the No Excuses category include:

- **Chapter 2: Implementing User Accounts and Logon Security.** User accounts form the foundation upon which all other Windows Vista security features are built. If you don't implement them correctly, you'll never be the proud owner of a secure Windows Vista system.
- **Chapter 3: Implementing Password Security.** You've no doubt heard that passwords are important. The truth is that they're really important. Really, really, really important. As with user accounts, neglecting the importance of using strong passwords is a really, really, really bad idea. Really.
- **Chapter 7: Protecting Windows Vista with a Firewall.** A firewall is the component that keeps Internet users from being able to connect to your PC without your permission. If you don't have a

good firewall in place (or neglect to configure it correctly), you're effectively leaving your system open to every security threat imaginable.

- **Chapter 8: Keeping Windows Vista Patched and Protected.** Windows Vista is built with millions of lines of programming code, and from time to time, problems with bits of code are discovered. These security holes can leave your system exposed to a variety of security threats, so patch them immediately as fixes become available. In this chapter, you learn how easy it is to ensure that Windows Vista remains properly patched and protected, automatically.
- **Chapter 9: Protecting Against Viruses.** Viruses have been around for a long, long time, and continue to present a threat to your computer's security. To protect against threats like viruses, worms, and Trojan horses you need to have antivirus software installed, keep it updated, and then scan for viruses regularly. This chapter explains how to get the protection you need without spending a penny in the process.
- **Chapter 10: Fighting Malware: Protecting Against Spyware, Adware, and Browser Hijackers.** Most users consider any pest-related infection to be a virus, but technically spyware, adware, and browser hijackers are different beasts requiring their own dedicated preventative measures. As their names suggest, these pests are typically designed to infect your system and then spy on you and your online activities. You don't want them on your system, and the right antispyware setup helps to ensure your Windows Vista system remains properly protected. This chapter shows you how it's done.

That's it - a total of six chapters covering the five golden rules. I did mention another important chapter for parents, and that's Chapter 6, "Implementing Parental Controls." If you have kids and want to keep them safe online, you really need to read that chapter as well. Because it doesn't apply to everyone, I've outlined it in a little more detail in the "Nice to Know" section.

Got a Network?

It wasn't all that long ago that having a computer network in your home was the exception rather than the rule. With the advent of high-speed Internet connections, however, many people realized that they could easily share the connection among different computers simultaneously. Although this ended the process of queuing up to use the Internet, it brought with it a whole new set of issues with respect to network security. There are a number of references to networks and security throughout this book, but you can find the majority in the last two chapters:

- **Chapter 16: Securing Shared Folders and Printers.** Most people install a home network to share Internet access between two or more computers simultaneously, but you can also use a network to share resources like files, folders, printers, and more within that network. In this chapter you learn how you can use Windows Vista's built-in network security features to control who has access to shared folders and printers on your network.
- **Chapter 17: Securing Windows Vista on Wireless Networks.** Wireless technologies make it easier to implement a home network than ever before, but if you don't take the time to secure your wireless network connection you can end up granting access to your computers (and the Internet) to neighbors or anyone within range. If you want your wireless network to remain secure and private, then you must take the time to secure it correctly. The good news is that it's not tough to do. This chapter explains everything you need to ensure that outsiders can't freely roam your network or piggyback on your expensive high-speed Internet connection without your permission.

If you don't have a home or small-office network, you can safely skip these chapters. If you have a laptop with a built-in wireless connection (or even connect to a wired network at work), then you'll still find helpful information in both chapters.

Nice to Know

There are plenty of security threats out there, but some (like viruses and spyware) are more dangerous than others. Personally I'd consider the information supplied in the following chapters to be very useful towards

keeping your computer's security (and your personal privacy) intact, but they are by no means absolutely essential. With different users and needs in mind, I'll designate the information in the following chapters as being nice to know:

- **Chapter 4: Using Built-in Tools and Settings to Improve Windows Vista Security.** Windows Vista includes a number of built-in security tools and advanced features that you can use to better protect your PC and keep you in the loop. From reviewing the Windows Vista security log to using the Control Panel Security Center to determine the current status of security tools and settings, this chapter gives you a better idea of what's built into (and possible with) Windows Vista.
- **Chapter 5: Securing Your Web Browser.** Internet Explorer 7 is the new web browser included with Windows Vista, and its default security settings do a great job toward keeping your browsing experience safer. In past iterations, Internet Explorer has been the source of some major security concerns, but this new release shouldn't subject you to major ills like spyware and browser hijacks. Even so, this chapter explores some of the primary security settings in Internet Explorer 7, and how you can tweak them, if necessary. It also outlines alternatives to using IE as your browser such as Firefox, Netscape, and Opera.
- **Chapter 6: Implementing Parental Controls.** If you have children, this chapter should be considered essential reading. The Internet is a dangerous place, and without the right controls in place, your children can literally venture anywhere online and be exposed to all manner of content. The new Parental Controls feature in Windows Vista now makes it possible for parents to control exactly what types of content kids can access, the programs they can use, the types of games they can play, and even the times at which they can use your Windows Vista system. This chapter shows how to implement controls on a user-by-user basis.
- **Chapter 11: The Dark Side of Spam.** Junk e-mail stinks, and nobody I know likes receiving it. Beyond being an annoyance, however, spam can also be a security risk. Junk messages sometimes carry viruses, try to steal your personal information (via phishing attempts), or lead to even more spam. If you want to learn more about lowering your spam intake and making your e-mail inbox a safer place, this chapter is for you.
- **Chapter 13: Controlling Access to Your Personal Files.** Windows Vista does a good job of keeping different users' personal files separated and relatively secure if you set things up correctly. In this chapter, you learn how to keep your personal files private using security permissions, and how to share files (including to what extent) using new sharing features built into this latest version of Windows.

Honestly, you'll learn something useful in every one of these nice-to-know chapters. Although none of them provide a clear answer as to the meaning of life, they still have some wonderful nuggets of information that may help you on your journey.

For Those Who Want to Take Things Up a Notch

My experience has shown that most people want to keep their computers secure to avoid the hassles associated with pests like viruses and spyware. However, I also understand that many people are increasingly interested in protecting their personal privacy. Although the techniques outlined in the No Excuses! chapters help keep your computer safe, they won't necessarily protect your personal files and Internet communications to the level you would like. To properly secure these elements and to make them private, using encryption techniques is your only option.

Unfortunately, using encryption (and using it correctly) can be a challenge. I'd love to tell you that using encryption to keep files and e-mail messages secure is as easy as clicking a button, but if I did that, I'd be lying. Encryption is a more advanced concept than many others in the computer security world, and one for which you need to take a little time to learn the process. Do it right, and you'll benefit from some industrial-strength privacy; get it wrong, and you may find yourself permanently locked out of your own stuff.

The following chapters are suitable for those of you who want to take things up a notch on the security and privacy front:

- **Chapter 12: Securing E-mail Messages Using Encryption and Digital Signatures.** Ever wondered why e-mail programs include buttons marked Encrypt and Digitally Sign? You can make your e-mail communications with other users completely secure and private, but there's a little work involved. If you don't want to run the risk that others can potentially read (or change) the e-mail messages you send, then this chapter is for you.
- **Chapter 14: Improving File Security Using Encryption.** Certain editions of Windows Vista include a built-in feature that enables you to secure your personal files using strong encryption. Even if you don't have the right edition, however, you can find other programs that can help you to ensure that your files remain for your eyes only. This chapter explains how to use the Windows Vista native file encryption facilities and third-party tools to encrypt files securely to levels at (or beyond) government standards.
- **Chapter 15: Erasing Files and Hard Drives Securely.** This topic technically isn't about encryption, but the manner in which it works is similar. Normally when you delete a file, it remains potentially recoverable using various tools designed to undelete or restore files. When you erase files the right way, however, you cannot recover them. Whether you need a way to ensure that files you delete are gone for good, or want to wipe your hard drive clean prior to donating or selling an old PC, this chapter explains how to do the job properly and permanently.

It's true - I did consider naming this section "security stuff for the completely paranoid." However, I quickly realized that I would then be calling myself paranoid. My neighbors, friends, and relatives already use the term to describe me, so I changed the title. I don't like to think of myself as paranoid; I'd rather say that I like to take things up a notch.

Summary

Securing your Windows Vista system is essential. Some of the things you need to do are very important, others not quite as important, relatively speaking. The Golden Rules have been outlined, and you have a map that outlines the relative importance of topics covered in this book. The ball is now in your court. Read on to secure Windows Vista systems!

Chapter 2: Implementing User Accounts and Logon Security

Securing your computer is in many ways like securing your home - you shouldn't rely on any one method to keep the outside world from getting in. Instead, you take a number of different measures that may include locking doors, installing an alarm system, and hopefully not alerting would-be attackers that there's lots of cool stuff inside.

When it comes to securing Windows Vista, you're given the choice of leaving the front door open, or putting a lock in place. This door lock is known as a *user account*, specifically a user account that includes a password. If ever there was a first line of defense in the quest to secure Windows Vista and ensure user privacy, user accounts are very much where the story begins.

This isn't to say that user accounts are strictly a security-related feature of Windows Vista; they certainly have other reasons for being. However, user accounts are a key component in changing your computer from being an open book to a secure fortress.

This chapter focuses on what user accounts are, the different types that exist, and how to create and configure them to ensure a better level of system security. Along the way, you'll learn about a new feature - User Access Control - that can help improve the security of your Windows Vista system.

Exploring User Accounts

When it comes to Windows Vista, user accounts represent the foundation upon which all other security concepts and techniques rely. Quite simply, you can install any piece of security software - from firewalls and antivirus programs to antispyware tools and encryption utilities - and it's effectively all for naught if user accounts are not implemented correctly or properly protected. It could easily be argued that most Windows Vista users consider the user account logon process an annoyance rather than a security feature. Unfortunately, neglecting or ignoring this essential security feature is the very reason why the majority of user desktop systems are insecure and vulnerable to an Internet's worth of security and personal privacy threats.

At the most basic level, a user account is nothing more than an object on a Windows Vista system that represents a particular user. Made up of a username, and hopefully a password, user accounts represent the credentials that users need to supply to gain access to a Windows Vista system. Beyond simply identifying a user, a user's account dictates what tasks he can perform on a computer, what files he has access to, and more. In a nutshell, user accounts are not an optional part of securing a Windows Vista system - quite to the contrary, they're absolutely essential.

In a departure from previous versions of Windows aimed at home and small office users, Windows Vista offers true user account security facilities in a way that cannot be easily ignored or dismissed. Although pressing the Esc key might have gotten a user past the logon dialog box on a Windows 98 system, Windows Vista offers much more robust and comprehensive logon security. As a matter of fact, the logon security capabilities of Windows Vista are fundamentally similar to those used to secure servers running Windows 2000 Server or Windows Server 2003. In other words, Windows Vista user account security offers a high level of protection for your system. If you're serious about your system's security and privacy, you'll want to take advantage of it.

The good news is that Windows Vista makes it easy to create and manage user accounts via tools like the User Accounts applet in Control Panel (see Figure 2-1). Before you jump into creating any accounts, however, it's essential that you to understand the benefits user accounts provide, and important details about the different types of accounts that exist.

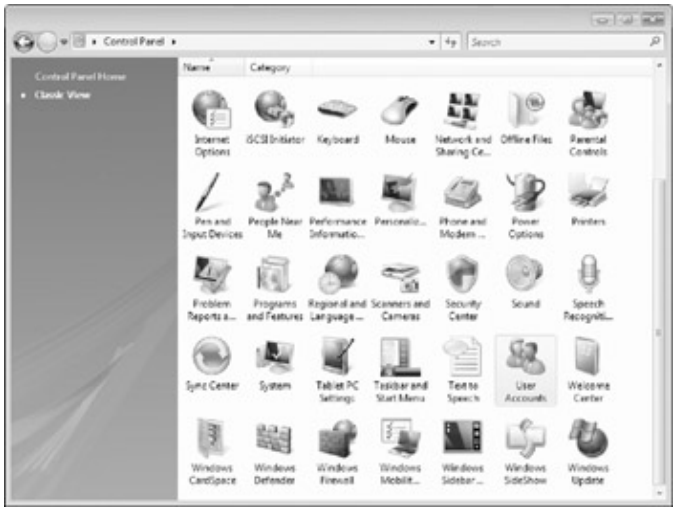

Figure 2-1: Click the User Accounts item in Control Panel to create and manage user accounts.

Benefits of User Accounts

Some user accounts are configured for general day-to-day use, including tasks such as surfing the Web, working with e-mail, and playing games. Others are designed with system administration and configuration tasks in mind, including installing software and making changes to firewall settings.

Ultimately, each person who uses a Windows Vista system should be assigned his or her own personal user account, which provides the following benefits:

- A dedicated and customizable desktop environment.
- A dedicated user profile where personal files, e-mail messages, and settings are stored.
- The capability to control access to the desktop environment by adding a user account password.
- The capability to secure personal files and folders, making them inaccessible by other users.

Creating a dedicated user account for every person who uses a Windows Vista system is not unlike setting up a number of Windows Vista systems, where each user has her own personal desktop environment. This model eliminates the hassles associated with older systems like Windows 3.1, where users shared a common desktop and all related settings. In the world of Windows Vista, having your own user account means being able to log on, set your desktop wallpaper image to something crazy or fun, and not having to deal with friends or family members who want to change it. Your desktop can be neatly organized (recommended), or a complete mess (recommended only if you thrive in chaotic environments). Most importantly, having your own user account enables you to control which users can access your files, and to what extent.

User Account Types

Although the idea of each user having her own dedicated account is a great one, all user accounts are not created equal. There's a definite hierarchy in this part of the computing world, and Windows Vista offers no exception. Some user accounts allow unrestricted access to every last bit of a Windows Vista system, including files belonging to other users. Others limit what users can do while logged on, stopping them from carrying out common tasks such as installing software. When it comes to the security of your Windows Vista system, creating user accounts is important. However, assigning users an appropriate user account type is even more critical.

Windows Vista includes three main types of user accounts:

- Administrator
- Standard
- Guest

Each of these user account types is examined in more detail in the following sections.

Note In the world of Windows Vista, a *user* is the person actually using the computer - your spouse, Mom, Dad, son, daughter, or a friend. A *user account* is the object assigned to a user for the purpose of logging on. Some users will have only one user account, while others may have more than one user account - one for day-today use and another for system administration tasks.

ADMINISTRATOR ACCOUNTS

In the parallel universe that is Windows Vista, one type of user account stands head and shoulders above the rest: the all-seeing, all-knowing Administrator account. User accounts of this type have complete control over every element of a Windows Vista system; users with this privilege level can literally do anything, up to and including actions that could irreparably damage a Windows Vista installation.

A user configured as Administrator can:

- Install and uninstall programs, hardware, and drivers.
- Make system-wide configuration changes.
- Create, delete, and manage all user and group accounts.
- Read or open any file, including those belonging to other users.
- Grant rights to or implementing restrictions on other users.

One limitation is that the Administrator cannot delete his account or change its type to Standard if it is the last Administrator account on the Windows Vista system.

Windows Vista creates one Administrator account by default (named Administrator) during its installation process. You may not even be aware that this account exists because it isn't displayed on the Welcome logon screen by default. This account is always present, however, and cannot be deleted.

The Administrator user account type is supposed to work for the forces of good, not evil. However, this account type was never designed with normal, everyday, use in mind. As the list of its broad capabilities shows, Administrators yield complete control over not only the Windows Vista system itself, but also other users' accounts.

For that reason, regular users should never be granted Administrator privileges. In fact, for security purposes alone, even the Administrator should never log on to Windows Vista with an Administrator account unless he needs to perform configuration tasks that require this level of power. Unfortunately, Windows Vista systems can run into security-related problems (such as infections by viruses and spyware programs) due to unnecessary or careless everyday use of the massive firepower the Administrator account.

Caution Deciding which users should be granted Administrator rights is ultimately up to you, but always keep system security in mind. Generally, any user with access to the Administrator account should have an appropriate level of Windows Vista knowledge. More importantly, she should be someone who can be trusted not to abuse or misuse the account's power. On some systems, every user may be responsible enough to be granted access to an Administrator account to perform tasks like installing programs. On others, the situation might dictate that only the owner of the PC has access to an Administrator account. The bottom line is that on your computer, you get to choose who has access to Administrator accounts, so choose wisely.

STANDARD USER ACCOUNTS

Unlike Administrator accounts, Standard user accounts are designed for everyday personal use. Many people argue that these accounts are excessively restrictive in that they stop users from carrying out common tasks such as installing hardware and software, changing security settings, and making system configuration changes. That's true, but they're also very much to the point - Standard user accounts are designed to keep users from making potentially harmful and dangerous changes to a system and, by extension, help to ensure a better-performing and more secure Windows Vista system overall.

A user with a Standard account can:

- Add, change, or remove his user account password.
- Create a password reset disk for use in cases where his password is lost or forgotten.
- Make changes to his user desktop environment.
- Make his personal files private (except from the Administrator account).
- Use software programs installed for all users.

But the user cannot:

- Make changes to system configuration settings or delete key files.
- Install hardware or software programs.

Although Standard user accounts typically cannot install hardware and software, there are exceptions. On the hardware front, Windows Vista systems do allow Standard users to plug in and use a variety of USB devices, including pen drives, MP3 players, and the like. Most other hardware changes are restricted. As for software, Standard users can often install single-user programs that do not make any changes to system configuration settings, as is the case with many older programs designed for previous Windows versions. However, Standard users cannot install multiuser programs, or those that install new system services. Words like *often, typically, many*, and *most* are the name of the game here. The best way to see whether a program will install for a Standard user is to attempt the installation. In some cases it may work, and in others it will fail. Although the conveniences associated with having an Administrator account have appeal, everyday user accounts should always be of the Standard type if you're serious about securing your system. Unfortunately, going that route can lead to frustration (and even conflict) in cases where one user wants to do something on a computer, but is unable to because of restrictions imposed as a result of her Standard status.

That's why the Administrator account type exists, and there's nothing wrong with granting a responsible and trusted user the capability to use an Administrator account if and when necessary. Later in this chapter you'll learn how you can allow trusted Standard users to perform administrative tasks, without leaving the safe confines of their everyday user account.

As a best practice, try to follow what is known as the *principle of least privilege* when configuring security settings for any PC. This principle dictates that you give users only the minimum level of privilege that they require, and nothing more. Although the level of control that a particular user needs is open to debate (especially in his eyes), sticking to the least privilege maxim helps to ensure a more secure computer. In the case of user accounts, this means assigning all users Standard accounts for normal everyday use. Many viruses and spyware programs rely on the current user having Administrator-level access to thoroughly infect systems and do their damage; sticking with Standard accounts helps mitigate potential risks. Suffice it to say that when it comes to Windows Vista, user accounts, and security, less can actually be more.

GUEST USER ACCOUNT

Along with an Administrator account, Windows Vista also automatically creates a user account named Guest. As its name suggests, this account is meant for users without their own dedicated user accounts. Disabled by default (see Figure 2-2), the Guest account does not have a password assigned, and has little in the way of powers beyond running installed programs.

Figure 2-2: The Windows Vista built-in Guest account is disabled by default.

The fact that the Guest account is disabled by default (and cannot be assigned a password) is a good indication that it represents a potential security risk. As a best practice, always leave the Guest account disabled and create Standard accounts for users who require occasional access to your Windows Vista system. As you'll see later in this chapter, you can create a user account in less than a minute - well worth the effort from a security perspective.

Creating User Accounts

Now that you're familiar with user accounts and the different types that exist, it's time to get down to the business of actually creating them, which really couldn't be easier.

The primary tool used to create user accounts on a Windows Vista system is the User Accounts applet in Control Panel.

Creating User Accounts in Control Panel

Administrators can use the User Accounts applet in Control Panel to create new accounts, as well as manage existing ones. Standard users can use the tool to manage settings related to their own account only.

Follow these steps to create new user accounts in Control Panel:

1. Select Start Control Panel. Click the Classic View link in the upper left of the screen and then double-click the User Accounts icon.
2. At the Make Changes To Your User Account screen, click Manage Another Account.
3. When the User Account Control window appears, click Continue.
4. Click Create A New Account.
5. Enter a username for the new account, leave the account type as a Standard user (as shown in Figure 2-3), and click the Create Account button.
6. Close the Manage Accounts window.

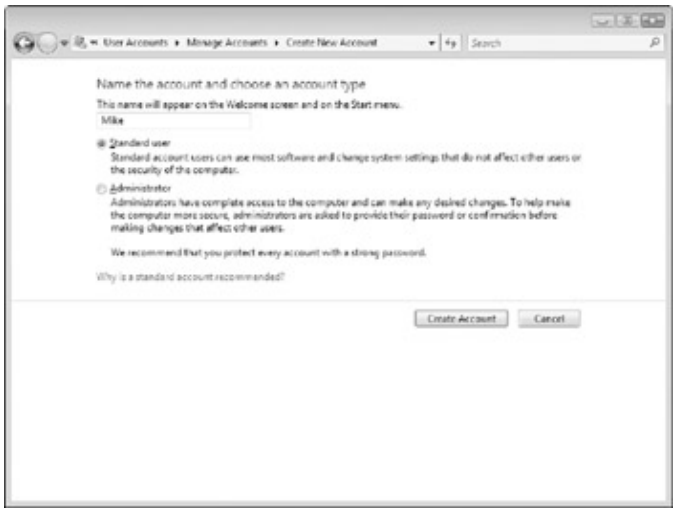

Figure 2-3: Select the new user account's type.

Managing User Accounts

Creating user accounts is only part of the job of an Administrator. After accounts have been created, they will occasionally need to be managed. Examples of security-related tasks associated with managing user accounts include:

- Changing account types
- Renaming accounts
- Adding, changing, and resetting passwords

- Deleting accounts

Each of these tasks is explained in more detail in the following sections.

Changing User Account Types

As you're now aware, using an Administrator account as your everyday user account is not recommended. Thankfully, the User Accounts tool in Windows Vista makes it easy to change an account from one type to another, such as switching an Administrator account to a Standard user, or vice versa.

Follow these steps to change a user account's type:

1. Select Start Control Panel User Accounts.
2. At the Make Changes To Your User Account screen, click Manage Another Account.
3. When the User Account Control dialog box appears, click Continue.
4. Select the name of the user account whose type you want to change.
5. Click Change The Account Type.
6. Select the type to which the account should be changed, as shown in Figure 2-4.
7. Click Change Account Type and close the Change An Account window.

Note Only an Administrator can change a user account's type. If the user whose account type is being changed is also logged onto the Windows Vista system when the change is made, the new account type takes effect the next time the user logs on.

Figure 2-4: Changing an existing user account's type.

Renaming User Accounts

Changing the name associated with an existing user account is significantly different than creating a new account. When you rename an account, only the name is changed - the actual user account fundamentally remains the same. Accounts are often renamed in corporate environments to make the transition between a departing user and his replacement easier. If the account is renamed, the new user has the same rights and permissions as the old user, along with access to the old user's files and desktop environment. This is often preferable to creating an entirely new account and then configuring required rights and permissions manually. On a home PC, user accounts are typically renamed only when a user wants to change her on-screen display name.

Follow these steps to rename an existing user's account name in Control Panel:

1. Select Start Control Panel User Accounts.
2. At the Make Changes To Your User Account screen, click Manage Another Account. When the User Account Control dialog box appears, click Continue.

3. Select the name of the user account whose name you want to change.
4. Click Change The Account Name.
5. Type a new name for the account as shown in Figure 2-5 and then click the Change Name button. The account will take on the new name, but all of the old user's files and settings remain intact in the account.
6. Close the Change An Account window.

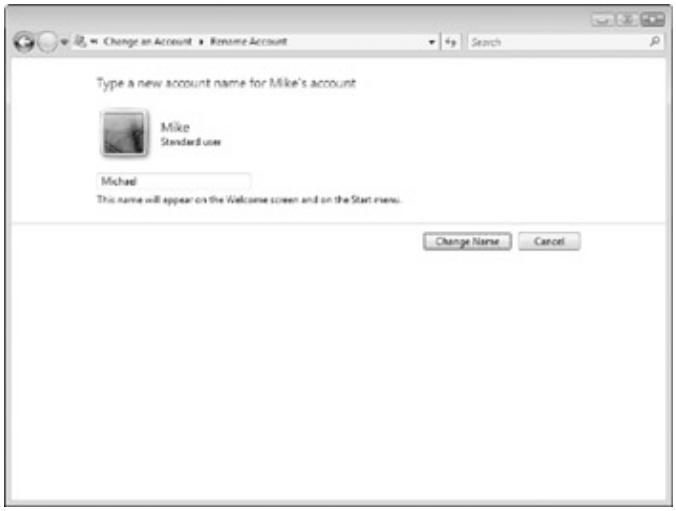

Figure 2-5: Changing a user account's name.

Tip The built-in Administrator user account may be hidden from the Windows Vista logon screen by default, but rest assured that hackers and others attempting to gain access to your computer know that it exists. Although you cannot delete this account, you can (and should) rename it to something less obvious. Choose a username for it that you'll remember, and then assign it a sufficiently complex password. This isn't to say that changing the name of the account will keep a determined hacker out of your system, but it will foil less experienced users and make life a little more difficult for those in the know. To change the password associated with this account, press F8 when your PC starts, select the option to boot into Safe Mode, log on, and use User Accounts in Control Panel to change the password associated with the Administrator account.

Managing User Account Passwords

Creating individual user accounts for every person that uses your Windows Vista system is a great start, but it's only part of the story as far as security is concerned. For user accounts to do anything more than act as a facility for separating user desktops and working environments, they must be assigned passwords. Every user should assign a password to his or her user account, and as a security/ privacy precaution, be the only person who knows the password.

Follow these steps to add a password to an existing user account in Control Panel:

1. Select Start Control Panel User Accounts.
2. At the Make Changes To Your User Account screen, click Manage Another Account.
3. When the User Account Control dialog box appears, click Continue.
4. Select the name of the user account whose name you want to change.
5. Click Create A Password.
6. At the Create A Password For *Username's* Account screen (see Figure 2-6), enter the new password, confirm it, and then type a password hint that will be seen by the user (to help him remember it) if he forgets his password or enters it incorrectly.
7. Click Create Password, and then close the Change An Account window.

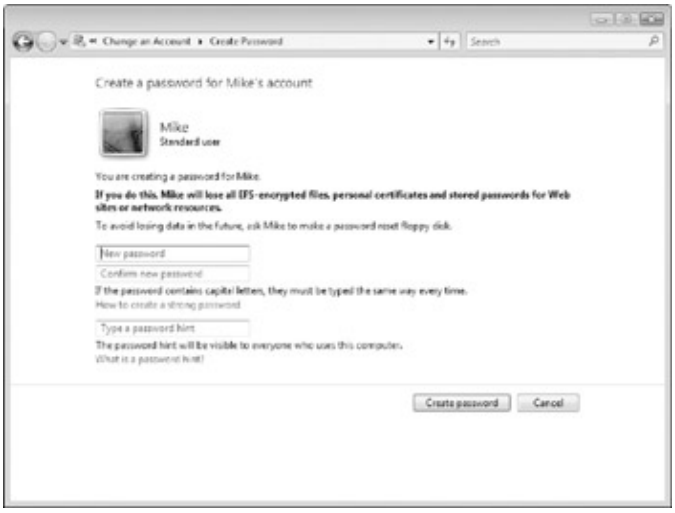

Figure 2-6: Adding a password to another user's account.

Caution Password hints exist to help you remember your password, but are visible to all users from the Windows Vista logon screen. If your hint is too obvious, other users may be able to guess your password. As a best practice, choose a password hint that makes sense to you, but won't give your password away to others.

Adding a password to your user account is an important step forward, but if you're serious about security, make a point of changing your password at least once every month or so. The User Accounts applet in Control Panel makes it easy to change (or even remove) the password associated with your user account.

Follow these steps to change the password associated with a user account in Control Panel:

1. Select Start Control Panel User Accounts.
2. At the Make Changes To Your User Account screen, click Manage Another Account.
3. Select the name of the user account whose name you want to change.
4. Click Change The Password, enter (and confirm) your new password, enter a password hint, and then click the Change Password button.
5. Close the Change An Account window.

Tip Assigning a password to all user accounts is important, even if you're the only person using a computer. Any accounts left unprotected make it easier for hackers, viruses, and spyware, and that's a risk not worth taking. Additionally, if your computer is ever lost or stolen, not having a password assigned gives others easy access to any personal data or files stored on your system.

Occasionally you may run into an issue where someone has forgotten the password associated with his or her user account, and cannot log on. Should this happen, an Administrator can reset the password by changing it using the User Accounts tool.

Follow these steps to reset a forgotten password using User Accounts:

1. Select Start Control Panel User Accounts.
2. At the Make Changes To Your User Account Screen, click Manage Another Account.
3. When the User Account Control dialog box appears, click Continue.
4. Select the name of the user account whose name you want to change.
5. Click Change The Password. Enter (and confirm) the user's new password, enter a password hint, and then click the Change Password button.
6. Close the Change An Account window.

Caution As a general rule, do not add, change, or reset passwords for other user accounts except during the original account creation process. If you add, change, or reset a password on their behalf (even with the best intentions), those users will lose access to their encrypted files, stored Internet certificates, and stored web site passwords. Instead, have the users log on and add a password to their accounts

using the User Accounts applet in Control Panel.

Understanding that users may forget their password, Windows Vista allows all users to create a password reset floppy disk. This disk enables a user to log on and change his password without the need to worry about losing access to encrypted files and other stored settings. You'll learn more about creating a password reset disk in Chapter 3.

Deleting User Accounts

Creating individual user accounts is essential, but it's also important to delete user accounts that are no longer needed. If you believe that an account will be used again at some point in the future, disable it. If there's no chance that it will be again, deleting it is the more secure option.

Follow these steps to delete an existing user account in Control Panel:

1. Select Start Control Panel User Accounts.
2. At the Make Changes To Your User Account screen, click Manage Another Account.
3. When the User Account Control dialog box appears, click Continue.
4. Select the name of the user account whose name you want to change.
5. Click Delete The Account.
6. At the screen asking whether you want to keep the user's files (see Figure 2-7), click Keep Files to save the contents of the user's Documents folder to your desktop, or click Delete Files to remove them.
7. When asked to confirm that the account should be deleted, click Delete Account and then close the Manage Accounts window.

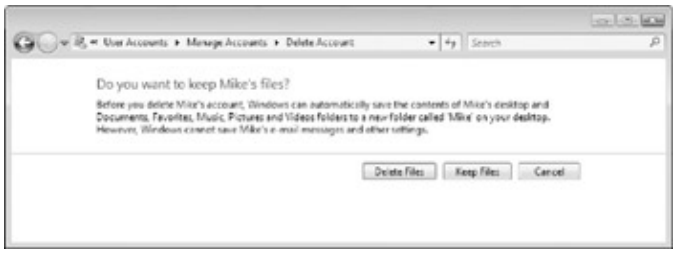

Figure 2-7: Options associated with deleting a user account.

What's in a Name?

After deleting a user account, would a new user account of the same name not smell as sweet? When it comes to how Windows Vista deals with user account names, the answer is no.

Imagine that your system includes a user account named Mike. When this user is created on a Windows Vista system, it is assigned an identifier value known as a Security ID (SID). An SID is a series of numbers that uniquely identifies a given security principal (user or group) on your system. Windows Vista identifies different users and groups using their SIDs, whereas names like Mike, Administrator, and Guest exist simply to help the mere humans keep things straight.

The reason this is important is that Mike isn't always necessarily Mike. For example, if you create a user account named Mike, delete it, and then create another user account named Mike, the two accounts are not the same. They may have the same name, and even belong to the same person. As far as Windows Vista is concerned, however, you've created one unique account (with a unique SID), deleted it, and then created another unique account (with its own unique SID). In other words, if the old Mike account had been granted any rights or permissions, the new Mike account is not automatically granted the same levels of privilege. Similarly, the new Mike may not be able to access the old Mike's files.

What it comes down to is this: deleting an account and then creating another with the same name does not the same user make.

User Account Control and the Run As Command

One of the key new security features of Windows Vista is known as User Account Control. Enabled by default, User Account Control is designed to ensure that users are prompted any time that administrative privileges are required to complete a task. If you're logged on with an Administrator account, the User Account Control dialog box appears when you try to perform an action limited to Administrators; however, you only need to click Continue to perform the requested action, as shown in Figure 2-8.

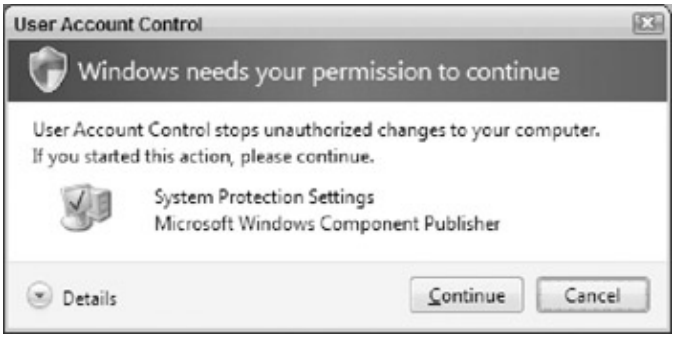

Figure 2-8: The User Account Control dialog box as it appears when you're already logged on as an Administrator.

If you're logged on as a Standard user and attempt to perform an administrative action - such as installing software or changing the system time, for example - the User Account Control dialog box prompts you to supply the credentials associated with an Administrator account, as shown in Figure 2-9.

Figure 2-9: The User Account Control dialog box as it appears when you're logged on as a Standard user.

The basic idea behind User Account Control is that you'll be alerted every time an action requires the powers associated with an Administrator account. User Account Control makes it easy for everyone to work within the confines of a Standard user account, allowing them to complete tasks as an Administrator (if or when necessary) without the need to log off and back on with an Administrator account. Of course, if a user doesn't have the password associated with an Administrator account, the action that they are trying to take will be denied.

Beyond simply helping to control which actions Standard users can take on a Windows Vista system, User Account Control also helps protect your system against threats like worms, viruses, and spyware infections. Most of these pests require Administrator-level privileges to lodge themselves onto your system, so User Account Control helps by alerting you when such actions are attempted. If you notice that the User Account Control dialog box appears at strange times, it could indicate the presence of a pest or an attempt by an