

# Part I

## Getting Down to the Business of Securing Windows Vista

### Chapter 1

A Short Introduction to Securing Windows Vista

### Chapter 2

Implementing User Accounts and Logon Security

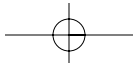
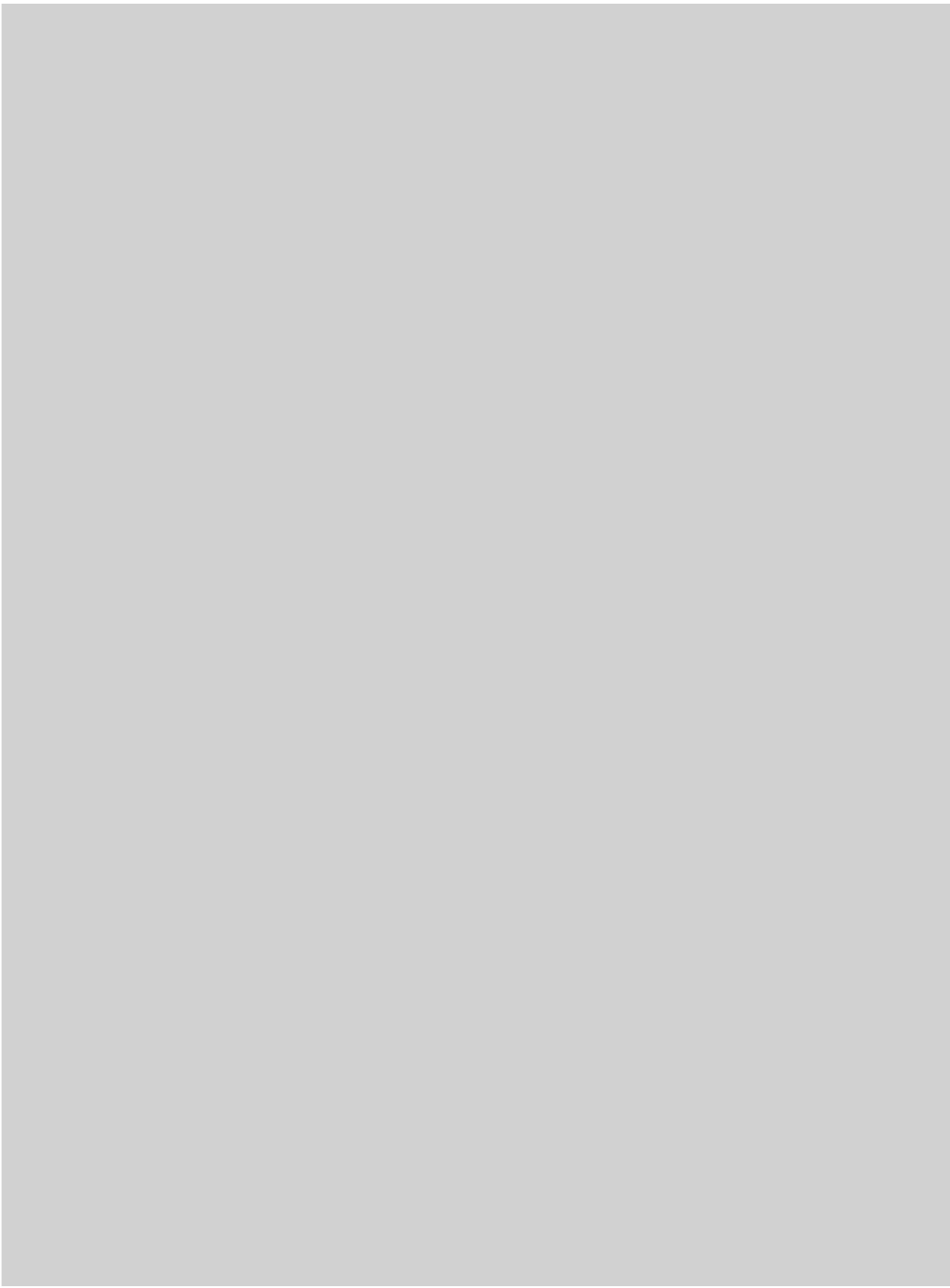
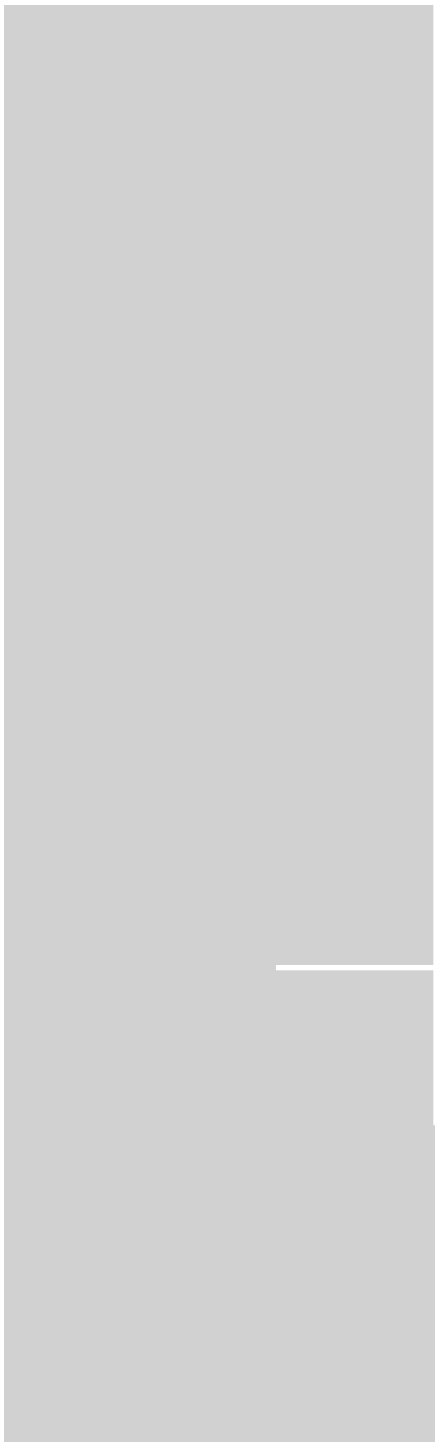
### Chapter 3

Implementing Password Security

### Chapter 4

Using Built-in Tools and Settings to Improve  
Windows Vista Security

COPYRIGHTED MATERIAL





## Chapter 1

# A Short Introduction to Securing Windows Vista



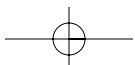
I originally planned to start this book with a long diatribe on the importance of taking the steps necessary to ensure that your Windows Vista system remains safe and secure. Thankfully, at the last minute I changed my mind. The reason is simple enough: I assume that if you're reading this, then you 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.

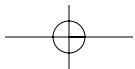
Fortunately, all is not lost. If you look at the key steps outlined in this book as being essential (and take the necessary actions, of course!), your Windows Vista system will be as secure as it can possibly be right now. In fact, if you take the time to get things done properly right from the get-go, 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:



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

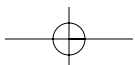


- **Chapter 2: Implementing User Accounts and Logon Security.** User accounts form the foundation upon which all other Windows Vista security features are built. If you don't implement them correctly, you'll never be the proud owner of a secure Windows Vista system.
- **Chapter 3: Implementing Password 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 antispymware 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.



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



- **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.

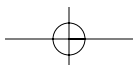
### For Those Who Want to Take Things Up a Notch

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!

