

SECURITY SETTINGS FOR WINDOWS VISTA USERS

Contents

Introduction	3
What Is Windows Vista?	3
Why Do I Need This Book?	3
Windows Vista Information	4
Overview of Windows Vista	4
Purchasing Windows Vista	4
Minimum System Requirements	5

Introduction

What Is Windows Vista?

On January 30th, 2007, Microsoft released Windows Vista worldwide. This brand new operating system serves personal computers, including desktops, laptops, Tablet PCs, and media centers. So what makes Windows Vista distinct from other Microsoft operating systems like Windows XP and Windows 2000? Windows Vista was released more than five years after the release of Windows XP, its immediate predecessor and it ultimately contains hundreds of new features in addition to various reworked features from the older operating systems. Above all, Windows Vista focuses on providing a more dramatic experience with enhanced graphic features and multimedia tools that allow the user to more easily create audio, visual, and print products.

Why Do I Need This Book?

The purpose of this book is to discuss the complexities of Windows Vista security features, noted for their dramatic improvement on the features and settings of previous Windows operating systems, including Windows XP. This book should help you understand why Windows Vista, the latest operating system from Microsoft, is particularly advantageous from a security point of view. Reviewing the key features, we've compiled information about the most commonly reported problems for this book and just in case we miss anything, you can check out the list of further resources pointing you in the direction of books and websites that provide further information about common problems with the platform program.

Windows Vista Information

Overview of Windows Vista

What do you really need to know about Windows Vista? The main idea behind Windows Vista, it seems, was to provide Windows users with a more convenient system that integrated a heck of a lot of multimedia elements. After all, in the last five years, the Internet has come a long way and now most regular computer users, during their online stints, like to make some use of media, whether it's by creating a video for YouTube or just tuning in to their favorite radio station streaming online. Of course, there's also digital photography. Who hasn't got a digital camera? Windows Vista makes it easy for the average computer user to make use of these various types of media with relatively little hassle. It also provides a range of other program upgrades for standard features like word processing and database management, reducing the extent to which the lack of Microsoft Office, no longer preinstalled on the Windows systems, is felt.

Purchasing Windows Vista

Believe it or not, one of the most frequently asked general questions about Windows Vista is "What do I have to buy?" It seems many people are confused about how they get their hands on Windows Vista and what precisely it means to have this operating system installed on a computer. Other common questions we're going to answer in this section, "purchasing Windows Vista", include questions about editions of Windows Vista, comparing features, and what disks you need (or don't need, as the case may be) to prepare yourself in case of a system failure. Computers that come with Windows Vista operating systems preinstalled will generally have what is called the Windows Vista Home Basic edition. Many people wonder about upgrades and yes, like most systems, it is possible to upgrade your edition of Windows Vista. If you have Home Basic, you can upgrade to either the Windows Vista Home Premier Edition or the Windows Vista Ultimate. With Windows Vista Business, and you generally have to select this operating system over the Home Basic when you buy your computer system, then you can also upgrade to the Windows Vista Ultimate edition if you prefer.

Your best bet, if you're considering an upgrade is to head on over to the Windows Vista website where you can compare the features of the various editions and make a determination as to whether an upgrade is going to be worth your while. The website address is https://na.windowsanytimeupgradestore.com/WAU_DIRECT/Home.aspx and you simply follow the link to compare editions; pricing information for the upgrades is provided there as well.

Since Windows Vista does not always come along with a set of recovery discs, another common question with regard to purchasing is whether or not you need to pay for or

otherwise secure a Windows Vista disc. If you decide to secure an upgrade for your Vista system then you are likely to receive a disc in the mail as part of your order. In this case, you are paying for the disc as part of your upgrade. Otherwise, you may have to make your own recovery discs using blank rewritable CDs. Generally you will receive a prompt about this close to the time that you start up your computer for the first time (if it's a new computer) or periodically when you are going about using your computer.

Minimum System Requirements

The minimum system requirements for Vista capability are as follows: Processor speed of 800MHz, memory of 512MB RAM, DirectX 9 capable graphics card, 20GB hard drive and at least 15GB of free space plus a CD-ROM drive.. The minimum system requirements for the Vista Premier are stated as follows: Processor speed of 1.0GHz, 1GB RAM, DirectX 9 capable GPU with Hardware Pixel Shader v.2.0, 128MB RAM, 40GB of hard drive, at least 15 GB, and a DVD-ROM drive.

Overview of Windows Vista Security Settings

Windows Vista stands as the most secure Windows operating system to date. Considerable effort was made to improve the security of the system in comparison to Windows XP. In particular, Internet Explorer 7 offers greater personal information protection, less overall vulnerability, and less susceptibility to infections and the so-called defense-in-depth features like User Account Control and Internet Explorer Protection Mode help to reduce the risk and severity of potential security breaches.

Cutting costs for businesses, the security settings of Windows Vista also help individual users and organizations using the system to reduce the time they need to spend installing updates and reviewing the security settings of their systems and operating protocol.

The Windows Vista operating system was the result of more than four years of steady work during which time several billion dollars were invested into the development of this Microsoft Windows operating system with various new security technologies being employed by Microsoft to justify the frenzy of development and extensive research.

When Windows Vista was launched, Microsoft offered up a number of new security technologies integrated into the system. Specifically, they looked to address several issues that had affected previous Windows operating systems. In many respects, the improved security of the Windows system was a primary goal for the designers of the Vista system.

Among the most notable developments were the Trustworthy Computing initiatives, the User Account Control, and the anti-spyware program, Windows Defender.

Windows Vista Security Improvements

Numerous security improvements were noted upon the release of Windows Vista. The most significant of these are discussed in this chapter to provide some insight into the advantages of the Windows Vista system for individuals and business.

Microsoft's Trustworthy Computing Initiative

As mentioned, improved security was one of the primary design goals for Windows Vista according to Microsoft representatives. Chief among the improved elements was the establishment of the Microsoft Trustworthy Computing initiative. The design concept for this feature was the improvement of public trust in Microsoft products.

The Trustworthy Computing Initiative was not so much a feature of Windows Vista as a concept that developers used to establish several other key improvements in the actual application of the Windows Vista operating system.

In 2002 Microsoft CTO and senior vice president Craig Mundie authorized a white paper defining the framework of the company's Trustworthy Computing program. The paper identified several areas as key initiatives and subsequently outlined the organized efforts to align Microsoft's design goals. Key activities were identified as security, privacy, reliability, and business integrity.

Security was identified as a key component, establishing the need to create a secure and trustworthy computing environment for computing while also empowering a whole variety of groups such as law enforcement agencies and academia with the tools to provide responsible leadership in this capacity.

Privacy was another element referred to in the white paper and identified as critical to a positive computing experience. Since computing involves connecting people and transmitting information across networks, it is critical that there be a viable method for protecting the information and maintaining its privacy. Privacy is identified as the second pillar of Microsoft's Trustworthy Computing program.

Reliability was identified as the third pillar of the Trustworthy Computing program. The definition of this term is fairly broad in the context of Microsoft's usage. It covers everything from the technical aspects of computer reliability to the more conceptual issues relating to availability and performance of computers.

User Account Control

When the Windows Vista program was first released, the inclusion of the User Account Control feature was identified as one of the most significant and notable of the changes to Windows security. Perhaps the most significant changes established by the User

Account Control were the limitations established on user accounts as a default. With security technology allowing fewer privileges, the Windows Vista administrators have the power to customize limitations on non-administrator user accounts. In the past, with versions such as Windows XP, limiting user accounts effectively was often difficult. The default limited account setting was too restrictive and incompatible with much of the application software used for even basic operations.

With Windows Vista any action that requires administrative privileges first prompts the user to supply an administrator name and password. For additional security, even on administrator accounts, the user must still provide confirmation for the privileged action to be undertaken.

User Account Control asks for user name and password to stop programs from interfering with the authorization window. Specifically, the additional security step is designed to prevent spoofing, the unauthorized use of another user account information or identity.

The reason that the limited account settings proved problematic with earlier versions of Windows has also been addressed with the new User Account Control settings. Windows Vista acknowledges that many of the applications used by your average computer user are written with the assumption of being run with administrator privileges. This, of course, led to problems with earlier versions of Windows when such applications were being run from limited user accounts. The Windows security settings tended to block attempts to use such application because they attempted to access and make changes to Program Files and other such machine-wide or system directories. In some cases, changes were made to registry keys, which the User Account Settings would also attempt to prevent.

In Windows Vista, the User Account Controls limit what is known as the File and Registry Virtualization. The new settings instead redirect writes and reads of specific settings to a per-user location within the user's profile. If a program you install tries a command to write a file called without user permissions to write to that directory, the write will no longer be stopped but will be redirected to apply only to the user-specific settings.

Windows Defender Program

Next to the User Account Controls, the Windows Defender Program offers notable security enhancements in Windows Vista. The internet browser program, Internet Explorer 7, includes a variety of new security and safety features to prevent common internet and network problems such as phishing, spoofing, and the inappropriate use of

the internet by minors via the installation of parental controls. ActiveX controls are disabled by default, to enhance the security of the program and Internet Explorer is also capable of operating in a "protected mode". Because of the specific control security settings, the Internet Explorer 7 program, operating with lower permissions than the user, is not able to access or modify any computer files or directories aside from the Temporary Internet Files directory.

Windows Defender is Microsoft's answer to the problem of spyware. The product has not only been incorporated into Windows Vista operating systems by default, protects the operating system and user information against threats such as malware. Most changes to system configuration settings are blocked and therefore cannot be undertaken without specific user consent.

These and other new Windows Vista security features help to enhance the overall user experience by providing optimum level protection against identifiable threats while at the same time ensuring a hassle-free user experience.

New Security Features from Windows Vista

In addition to a range of enhanced and improved programs, Microsoft's commitment to security produced a number of new security features for release as part of the Windows Vista operating system package. Some of the most useful of these features are discussed in this section and include the IPv6 connection filtering system and Windows Parental Control Settings as standard.

IPv6 connection filtering

The IPv6 connection filtering system is one of several ways in which Windows Vista looks to protect user data as it is transmitted across networks. The security of outbound packets is enhanced by the filtering, which allows the user to specify both source and destination IP addresses and apply rules about port ranges through which the data is to be transmitted. By controlling this information – at the risk of becoming too technical – the user is able to enhance the effectiveness of their overall security by encrypting data and applying stringent limits to the methods used to send the data, reducing the risk of interception by third-parties.

The IPv6 offers IPsec as a fully integrated feature. It allows the acceptance or denial of connections based on security certificates and other elements such as Kerberos authentication protocol.

The system also establishes that various types of encryption may be required for different connections and establishes the basis for providing system users with an effective means of securing the necessary information using a wizard to handle complex configuration. Windows Firewall, for example, can be configured to allow traffic based on whether it is secured by IPsec.

Windows Firewall with Advanced Security provides access to many advanced options, including IPsec configuration, and enables remote administration. The ability to have separate firewall profiles for computers that share domains or are connected to

Windows Parental Controls

The Windows Parental Controls allow Vista users to include a range of controls for non-domain user accounts. User account controls implement reduced rights account identities needed for offline restrictions. An administrator can apply parental control restrictions to other users on the computer. Web browsing can be limited to children's websites. Particular sites, like pornography sites or drug-related sites can be blocked. File downloads can also be disabled as web content is filtered by a Winsock LSP filter.

The parental control settings are also particularly useful for monitoring and limiting the amount of time their children spend on the computer. User accounts can have set time limitations and can enter into a locked state via Fast User Switching when time limitations are expired. To prevent unsaved data from being lost, the user is not logged out when the time limit expires, they are simply suspended.

Parents can also place restrictions on what kind of games are played on the system. An administrator can establish restrictions based on one of five different game rating services: the ESRB ratings used in the United States and Canada, PEGI that is used in Europe, USK that is used in Germany, OFLC that is used in Australia and New Zealand, and CERO that is used in Japan. Similar to the web content features, paternal controls can be used to block games that feature certain categories regardless of game ratings.

The key to these and other new security features of the Windows Vista system is that they are all designed to promote high-level security for Vista users without undermining the functionality of the operating system.

Windows Vista Digital Rights Management

With Windows Vista, Digital Rights Management became a hot topic as part and parcel of the security features for the operating system. Microsoft introduced a number of Digital Rights Management and content-protection features to help digital content providers and corporations protect their data from being copied.

The purpose of PUMA, Protected User Mode Audio, is to maintain an environment for audio playback that restricts the copying of copyrighted audio. The feature also restricts the enabled audio outputs to forms allowed by the publisher. The purpose of the Protected Video Path – Output Protection Management (PVP-OPM) is also similar; this feature protects digital video streaming from copyrighting and other forms of unauthorized usage.

Establishing the reasoning behind the digital management focus, Microsoft established that the restrictions placed upon the use of content on PCs using their operating system would probably prevent many instance of copyright infringement. Encryption used by HD DVD, Blu-Ray Disk, and other copy-protected systems will prevent the playing of copyrighted content because the system will not issue the relevant license keys.

Authentication and logon

The security of the individual user account established by Windows Vista is a primary concern. Authentication and logon processes are essentially much more rigorous on the Windows Vista operating system than they have been on previous Windows systems.

Credential Providers have replaced Graphical identification and authentication (GINA), used for secure authentication and interactive logon. Combined with supporting hardware, Credential Providers can be used to create additional logon security features. Users can be required to log using biometric devices such as fingerprint, retinal, or voice recognition processes. Additional passwords, PINs, and smart card certificates can also be required. Logon requirements can be customized as well and established to require specific authentication through various logon steps.

Credential Providers are specifically designed to support application-specific credential gathering. Authentication networks can be used to establish authentication of network resources and adjoining machines. Fast User Switching can operate on computers joined by a domain. While this was previously limited to workgroup computers on Windows XP, Windows Vista operates with no such restriction.

Network Access Protection

The Network Access Protection (NAP) included in the Windows Vista operating system provides security to computers connected over a network or communicating across a network. The user is required to conform to a level of system health established by the administrator of the network.

The administrator of a specific computer can establish a policy, establishing requirements that will send warnings, grant access, or otherwise limit access to network resources.

NAP can also provide software updates to computers that do not meet specific requirements. Computers can be prompted to upgrade to the required level. A Remediation Server can be used to access the network conforming client is given a Health Certificate, which it then uses to access protected resources on the network.

The objective of network access protection is to provide users with a high level of protect regarding their interests and information. Network instability was one of the main issues with Windows XP and thus a fundamental consideration for the development of Windows Vista.

Summary

Windows XP users often complained about security issues with the operating system. The system was relatively easy to compromise; networks were difficult to configure and even more difficult to maintain. They could be compromised by spyware and spam and it was relatively difficult to restore complete integrity.

Since it emerged on the market, Windows Vista has essentially become the leading solution for security. Vista's development of the User Account Control has helped to limit Internet Explorer privileges and other aspects of Web accounts.

Windows Vista dramatically improves the User Account Control and provides much greater protection for Internet users. Internet explorer cannot be completely overrun by malicious software thanks to the way that the UAC interacts with the Explorer program. The user can easily determine whether there is a security risk thanks to the new security status bar and to the phishing filter that helps users browse safely.

Windows Vista is intended to help individuals and businesses save on their expenses; because of the enhanced security settings that are part of the Vista operating system, there is no need to spend on additional security features such as spyware and spam.

The security features of Windows Vista are quite impressive overall and one of the most impressive aspects of the operating system, particularly in comparison to Windows XP. The operating system protects computers against viruses, spyware, worms, and other unwanted software. Windows Vista enhances the online experience of every user, including minors. The security feature also provides users with information to better understand security threats and what steps can be taken to enhance the efficiency of established settings.

Further Resources

Below is a list of Recommended Windows Vista Books, useful for anyone who wants to get their head around the Vista system. All of these books are available on Amazon.com.

The web sites listed below also provide further information on the security features of system and how to make the most of them.

Books

Windows Vista For Dummies by Andy Rathbone

Windows Vista(TM) Resource Kit by Mitch Tulloch

Windows Vista: The Missing Manual by David Pogue

Windows Vista All-in-One Desk Reference by Woody Leonhard

Windows Vista Inside Out by Ed Bott

Microsoft Office 2007: Introductory Concept and Techniques by Gary B. Shelly

MCTS Self-Paced Training Kit (Exam 70-620) by I. McLean

Windows Vista Annoyances: Tips, Secrets, and Hacks by David A. Karp

Windows Vista(TM) Plain & Simple by Jerry Joyce

Switching to the Mac: The Missing Manual by David Pogue

Microsoft Windows Vista Step by Step by Joan Preppernau

Teach Yourself VISUALLY Windows Vista by Paul McFedries

Windows Vista For Dummies, Special DVD Bund... by Andy Rathbone

Windows Vista(TM) Administrator's
Pocket Consultant by William R. Stanek

Windows Vista Secrets by Brian
Livingston

Windows Vista: Top 100 Simplified Tips
& Tricks by Paul McFedries

Websites

Microsoft SecurityFind

<http://www.microsoft.com/security/default.aspx>

How to Maintain Windows Security

<http://www.microsoft.com/windows/security/default.aspx>

Security Guide for Windows

<http://www.pctools.com/guides/security/>

The Security Administrator Technical Newsletter

<http://www.windowstpro.com/WindowsSecurity/>

Windows Vista Security Blog

<http://blogs.msdn.com/windowsvistasecurity/>

A Home User's Security Checklist for Windows

<http://www.securityfocus.com/columnists/220>