Windows Vista Privacy Statement for Installation Features

At Microsoft, we're working hard to protect your privacy, while delivering products that bring performance, power, and convenience to your personal computing experience. This privacy statement explains the data collection and use practices of these Windows Vista installation features: Activation, Dial-up Networking, Installation Improvement Program, Dynamic Update, Microsoft Error Reporting Service, Phishing Filter, Windows Defender, and Windows Update. These features send information to and from the Internet when you're installing and setting up Windows Vista. This disclosure does not apply to other online or offline Microsoft websites, products, or services.

For a more comprehensive privacy statement for this software, see the online Windows Vista Privacy Statement at http://go.microsoft.com/fwlink/?LinkId=52526

Collection of information about your computer

Windows Vista contains several Internet-enabled features that collect standard information from your computer ("standard computer information"). Standard computer information generally includes such information as your computer's Internet Protocol (IP) address; operating system version; browser version; hardware ID, which indicates the device manufacturer, device name, and version; and your regional and language settings. Some features may collect additional information. The privacy details for each Windows feature listed in this privacy statement will disclose the additional information that is collected and, if the feature sends the information to Microsoft, how it is used.

Use of information

Information that is collected by or sent to Microsoft may be stored and processed in the United States or any other country or region in which Microsoft or its affiliates, subsidiaries, or agents maintain facilities. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union. Microsoft may disclose information about you if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft or the site; (b) protect or defend the rights or property of Microsoft and its family of websites; or (c) act in urgent circumstances to protect the personal safety of Microsoft employees, users of Microsoft software or services, or members of the public.

Microsoft occasionally hires other companies to provide limited services on its behalf, such as providing customer support, processing transactions, or performing statistical analysis of reports. Microsoft will provide these companies only the information they need to deliver the services. They are required to maintain the confidentiality of the information and are prohibited from using it for any other purpose.

Security practices

Microsoft is committed to protecting the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. For example, we store the information that you provide on computer servers that have limited access and that are located in controlled facilities.

For more information

If you have questions about this privacy statement, please contact us by submitting your questions online to Privacy Feedback at https://support.microsoft.com/common/survey.aspx?scid=sw;en;1213&showpage=1&ws=WindowsVista

Or by postal mail:

Windows Vista Privacy Statement for Installation Features
c/o Microsoft Privacy Response Center
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052

Installation Features

Activation

What this feature does

Activation helps reduce software counterfeiting, thereby helping to ensure that Microsoft customers receive the software quality they expect. Once your software is activated, a specific product key becomes associated with the computer (the hardware) on which your software is installed. This association prevents the product key from being used to activate the same copy of the software on multiple computers as counterfeit software. Some changes to your computer components or the software may require you to reactivate the software.

Information collected, processed, or transmitted

During activation, product key information is sent to Microsoft along with a hardware hash, which is a non-unique number generated from the computer's hardware configuration. The hardware hash does not represent any personal information or information about the software. The hardware hash cannot be used to determine the make or model of the computer and it cannot be backward calculated to determine any additional information about your computer. Along with standard computer information, some additional language settings are collected.

Use of information

Microsoft uses the information to confirm that you have a licensed copy of the software, and then it is aggregated for statistical analysis. Microsoft does not use the information to identify you or contact you.

Choice and control

Activation is mandatory and must be completed within a predefined grace period. If you choose not to activate the software, you cannot use it after the grace period expires. If the software is not correctly licensed, you will not be able to activate it.

Installation Improvement Program

What this feature does

If you choose to participate in the Installation Improvement Program, the feature sends a single report to Microsoft. The report contains basic information about your computer and how you installed Windows Vista. We use this information to help improve the installation experience and to create solutions to common installation problems.

Information collected, processed, or transmitted

The report generally includes information about your installation and setup experience, such as the date of installation, the time it took for each installation phase to complete, whether the installation was an upgrade or a new installation of the product, version details, operating system language, media type, computer configuration, and success or failure status, along with any error codes.

The report is sent to Microsoft when you are connected to the Internet. This report does not contain contact information such as your name, address, or phone number. A globally unique identifier (GUID) is generated and sent with the report. The GUID is a randomly generated number that uniquely identifies your computer; it does not contain personal information.

Use of information

Microsoft uses the report to improve our software installation experience. We use the GUID to correlate this data with data collected by the Customer Experience Improvement Program (CEIP), a program you can choose to participate in when you are using Windows Vista. This GUID enables us to distinguish how widespread the feedback we receive is and how to prioritize it. For example, the GUID allows Microsoft to distinguish between one customer experiencing a problem 100 times and other customers experiencing the same problem once. Microsoft will not use the information in the report to identify you or contact you.

For more information, about the Customer Experience Improvement Program, see these frequently asked questions online at http://go.microsoft.com/fwlink/?LinkID=52095

Choice and control

You can choose to participate in this program when you set up Windows Vista.

Dial-up Networking

What this feature does

Dial-up Networking allows you to access the Internet using a dial-up modem and a broadband technology, such as a cable modem and digital subscriber line (DSL). It also allows you to connect to private networks using a virtual private network (VPN) connection and Remote Access Service (RAS). RAS is a component that connects a client computer (typically your computer) to a host computer (also known as a remote access server) using industry standard protocols. VPN technologies allow users to connect to a private network, such as a corporate network, over the Internet while maintaining secured communications.

Dial-up Networking includes dialer components such as RAS Client, Connection Manager, and RAS Phone, as well as command-line dialers like Rasdial.

Information collected, processed, or transmitted

The dialer components collect information from your computer such as your user name, password, domain name, and phone number. This information is sent to the system that you are attempting to connect with. To help protect your privacy and the security of your computer, security-related information such as your user name and password are encrypted and stored on your computer.

The Connection Manager Administration Kit (CMAK) is a server component that allows administrators to collect information from users on a network. The information that is collected is determined by the administrator. For more information, contact your system or network administrator.

Use of information

Dialer information is used to help your computer connect to the Internet. For CMAK, the information that is collected is used to create connection profiles, which help administrators deploy and manage connections across a network.

Choice and control

For non-command-line dialers, you can choose to save your password. However, this option is turned off by default, so you may be prompted to provide your password to connect to the Internet or a network. For command-line dialers like Rasdial, there is no option to save your password.

Dynamic Update

What this feature does

Dynamic Update enables Windows Vista to perform a one-time check with the Microsoft Update website to get the latest updates for your computer while your operating system is being installed. If updates are found, Dynamic Update automatically downloads and installs them so your computer is up to date the first time that you log on or use it.

Information collected, processed, or transmitted

The types of updates Dynamic Update can download to your computer include:

- **Installation updates**: Important updates for installation files to help ensure a successful installation
- **In-box driver updates**: Additional hardware drivers that enable Windows Vista to successfully interact with your computer's hardware
- **Windows updates**: Important updates for the version of Windows that you are installing
- **Microsoft Windows Malicious Software Removal Tool updates**: Updates for the latest version of this tool which can help remove malicious software such as viruses and worms if it detects them on your computer

To install compatible drivers, Dynamic Update works with Windows Update (see below) to send information to Microsoft about your computer's hardware.

Use of information

Dynamic Update software reports information about your computer's hardware to find compatible drivers. For more information about how information collected by Dynamic Update is used, see Windows Update (below).

Choice and control

During Windows Vista setup, you can choose to use Dynamic Update.

Microsoft Error Reporting Service

What this feature does

Microsoft Error Reporting Service helps Microsoft and Windows partners diagnose problems in the software you use and provide solutions. Not all problems have solutions, but when solutions are available, they are offered as steps to solve a problem you've reported or as updates to install. As part of setup and installation, the Microsoft Error Reporting Service sends back information about setup or installation failures in order to attempt to diagnose the problem. To help prevent problems and make software more reliable, some solutions are also included in service packs and future versions of the software.

Many Microsoft software programs, including Windows Vista, are designed to work with the reporting service. If a problem occurs in one of these software programs, you are asked if you want to send a report so you can check for a solution. You can view the details of the report before sending it, although some files might not be in a readable format.

Windows Vista also allows you to report problems automatically instead of requesting your consent each time a problem occurs. If you use automatic reporting, you are not typically prompted to review the information in a report before it is sent. However, no information is sent unless you (or your system or network administrator) choose to report problems. You can choose to stop reporting problems at any time.

Enterprise customers can use the Microsoft Corporate Error Reporting Service to manage error reporting and data collection, and to choose the information that is sent to Microsoft.

For more information, see the Corporate Error Reporting website at http://go.microsoft.com/fwlink/?LinkId=55127

Information collected, processed, or transmitted

The reporting service can collect information about problems that interrupt you while you work, and about errors that occur behind the scenes. It is important to diagnose errors that occur behind the scenes because these problems, if left unsolved, might cause additional problems such as performance or program failures.

Reports contain information that is most useful for diagnosing and solving the problem that has occurred, such as:

- Where the problem happened in the software or hardware; occasionally, empty files might be included as an initial indication of a problem
- The type or severity of the problem, if known
- Files that help describe the problem (typically, system or report-generated files about software behavior before or after the problem occurred)
- Basic software and hardware information (such as operating system version and language, device models and manufacturers, or memory and hard disk size)

Reports might unintentionally contain personal information, but Microsoft does not use the information to identify you or contact you. For example, a report that contains a snapshot of computer memory might include your name, part of a document you were working on, or data that you recently submitted to a website. If you are concerned that a report might contain personal or confidential information, you should not send the report. If a report is likely to contain this type of information, Windows will ask if you want to send it, even if you have turned on automatic reporting. This gives you the opportunity to review the report before sending it to Microsoft. Reports that you have not yet sent to Microsoft, including files and data attached to those reports, may be stored on your computer until you have an opportunity to review and send them. Reports that you have already sent, including files and data attached to those reports, may also be stored on your computer.

After you report a problem, you might be asked to complete a survey about the error experience. If you choose to provide a phone number or e-mail address in response to the survey, your error report will no longer be anonymous. Microsoft may contact you to request additional information to help solve the problem you reported.

Use of information

Microsoft uses information about errors and problems to improve Windows and the software and hardware designed for use with Windows operating systems. Microsoft employees, contractors, vendors, and partners may be provided access to information collected by the reporting service. However, they may use the information only to repair or improve the products that they publish or manufacture.

For example, if an error report indicates that a third-party product is involved, Microsoft may send that information to the vendor of the product. The vendor may provide the information to sub-vendors and partners; however, all parties must abide by the terms of this privacy statement.

To improve the products that run on Microsoft software, Microsoft may share aggregate information about errors and problems. Microsoft uses aggregate information for statistical

analysis. Aggregate information does not contain specific information from individual reports, nor does it include any personal or confidential information that may have been collected from a report.

Choice and control

To view your problem history, check for new solutions, or delete problem reports and solutions, go to Problem Reports and Solutions in Control Panel or see Windows Help and Support for more information.

Phishing Filter

What is phishing?

Online phishing is a technique used to trick computer users into revealing personal or financial information through an e-mail message or website. A common online phishing scam starts with an e-mail message that appears to come from a trusted source but actually directs you to provide information to a fraudulent website. Phishing Filter is designed to warn you if you're visiting websites that display phishing characteristics or that have been reported to Microsoft as fraudulent.

What this feature does

Phishing Filter is designed to warn you if the website you are visiting might be impersonating a trusted website. Phishing Filter does this by first checking the address of the website you are visiting against a list of website addresses stored on your computer that have been reported to Microsoft as legitimate ("legitimate list").

The first time you attempt to visit a website that is not on the legitimate list, you will be asked whether you would like to have Phishing Filter automatically check all websites you visit. If you opt in, addresses that are not on the legitimate list will be sent to Microsoft and checked against a frequently updated list of websites that have been reported to Microsoft as phishing, suspicious, or legitimate websites. You may also choose to use Phishing Filter manually to verify individual sites as you visit them.

Information collected, processed, or transmitted

When you use Phishing Filter to check websites automatically or manually, the addresses of the websites that you visit are sent to Microsoft, together with some standard information from your computer such as Internet Protocol (IP) address, browser type, and Phishing Filter version number. To help protect your privacy, the address information sent to Microsoft is encrypted using Secure Sockets Layer (SSL) and is limited to the domain and path of the website. Other information that may be associated with the address, such as search terms, data you entered in forms, or cookies, is not sent.

For example, if you visit the MSN Search website at http://search.msn.com and enter "weather" as the search term, instead of sending the full address "http://search.msn.com/results.aspx?q=weather&FORM=QBHP," Phishing Filter removes the search term and sends only "http://search.msn.com/results.aspx." Address strings might unintentionally contain personal information, but Microsoft does not use the information to identify you or contact you. If you are concerned that an address string might contain personal or confidential information, you should not report the site.

Anonymous statistics about your usage of Phishing Filter, such as the duration and total number of websites browsed since an address was sent to Microsoft for analysis, are also sent to Microsoft.

Use of information

The information described above is used to analyze the performance and improve the quality of the Phishing Filter service. Microsoft does not use the information it receives to personally identify you.

Some URLS that are sent might be saved to be included in the legitimate list and then provided as client updates. When URLs are saved, additional information such as Phishing Filter and operating system version information, as well as your browser language, is saved.

Choice and control

If you choose the recommended settings during Windows Vista setup, you turn on automatic website checking with Phishing Filter. You can also turn Phishing Filter on or off in Internet Explorer.

To turn Phishing Filter off

1. In Internet Explorer, click the **Tools** button, click **Phishing Filter**, and then click **Phishing Filter Settings**.

2. In the list of options, scroll to the **Phishing Filter** section under **Security**, click **Disable Phishing Filter**, and then click **OK**.

Phishing Filter will no longer check for or warn you about phishing sites that you might visit.

Windows Defender

What this feature does

Windows Defender is an antispyware program included with Windows. It offers two ways to help keep spyware and other potentially unwanted software from infecting your computer:

- **Real-time protection**. Windows Defender alerts you when spyware or potentially unwanted software attempts to install itself or run on your computer. It also alerts you when programs attempt to change important Windows settings.
- **Scanning options**. You can use Windows Defender to scan for spyware and other potentially unwanted software that might be installed on your computer, to schedule scans on a regular basis, and to automatically remove any malicious software that is detected during a scan.

If you choose the recommended settings during Windows Vista setup, Windows Defender real-time protection will be enabled and automatic scanning will occur at 2:00 A.M. each day. Windows Defender will automatically install updated definitions before scanning, and then remove software with severe alert levels that it detects during the scan. If your copy of Windows is genuine, Windows Defender will also remove software with high alert levels that it detects during a scheduled scan.

For more information about the Windows Genuine Advantage, go to http://go.microsoft.com/fwlink/?LinkID=51371

Information collected, processed, and transmitted

If you choose the recommended settings during Windows Vista setup, you will also join Microsoft SpyNet with a basic membership. The online Microsoft SpyNet community helps you see how other people respond to software that has not yet been classified for risks. If you choose to be notified about this software, seeing if other members of the community permit or deny the software or changes made by the software can help you decide what to do. In turn, if you participate, your choices are added to the community ratings to help other people decide what to do. You can choose to be notified about software that has not yet been classified for risks by using the options provided in Windows Defender or by joining Microsoft SpyNet with an advanced membership (see below).

Use of information

If you join Microsoft SpyNet, Windows Defender will automatically send information to Microsoft to help Microsoft determine which software to investigate for potential threats and to help improve how Windows Defender works. The information that is sent in reports is determined by your Microsoft SpyNet membership (see below).

Choice and control

You can change the recommended settings at any time by using the options provided in Windows Defender.

Windows Defender – Microsoft SpyNet Feature

What this feature does

The Microsoft SpyNet antispyware community is a voluntary, worldwide community of Windows Defender users. Through Microsoft SpyNet, users can report spyware and other forms of potentially unwanted software to Microsoft. When you set up Windows Vista, you can choose to join Microsoft SpyNet. If you choose to join, reports about spyware and potentially unwanted software are sent to Microsoft. The type of information that is sent in reports depends on your level of Microsoft SpyNet membership.

Information collected, processed, or transmitted

Microsoft SpyNet reports include information about the files or programs in question, such as file names, cryptographic hash, vendor, size, and date stamps. In addition, full URLs can be collected to indicate the origin of the file, and might occasionally contain personal information such as search terms or data entered in forms. Reports can also include the actions that you applied when Windows Defender notified you that software was detected (deny or permit). If your copy of Windows is not genuine, some software cannot be removed by Windows Defender and an error will be reported to Microsoft. An error code indicating that software was not removed because your copy of Windows is not genuine will be included in the report. Microsoft SpyNet reports include this information to help Microsoft gauge the effectiveness of Windows Defender’s ability to detect and remove malicious and potentially unwanted software. Microsoft uses the information contained in SpyNet reports to help improve Windows Defender for all users.

Reports also contain standard computer information, and are automatically sent to Microsoft when:

- Windows Defender detects software or changes to your computer by software that has not yet been analyzed for risks
- You apply actions to software that Windows Defender has detected
- Windows Defender completes a scheduled scan and automatically applies actions to software that it detects, according to your settings

Reports might unintentionally contain personal information. To the extent that any personal information is included in a report, Microsoft does not use the information to identify you or contact you.

You can join Microsoft SpyNet with a basic or an advanced membership. If you choose the recommended settings during Windows setup, you automatically join with a basic membership. Basic member reports contain the information described above. Advanced member reports are more comprehensive and might occasionally contain personal information from, for example, file paths and partial memory dumps. To the extent that any personal information is included in a report, Microsoft does not use the information to identify you or contact you. These reports, along with reports from other Windows Defender users who are participating in Microsoft SpyNet, enable Microsoft researchers to discover new threats more rapidly. Spyware definitions are then created for programs that meet the analysis criteria, and the updated definitions are made available to all users through Windows Update.

If you join Microsoft SpyNet with a basic or an advanced membership, Microsoft might request a Sample Submission report. This report contains specific files from your computer that Microsoft suspects might be potentially unwanted software. The report is used for further analysis. You will be asked each time if you want to send this Sample Submission report to Microsoft.

To help protect your privacy, reports that are sent to Microsoft are encrypted using Secure Sockets Layer (SSL).

Use of information

Microsoft SpyNet reports are used to improve Microsoft software and services. The reports may also be used for statistical or other testing or analytical purposes, trending, and definition generation. Only Microsoft employees, contractors, and vendors who have a business need to use the reports are provided access to them.

Choice and control

You can join or leave Microsoft SpyNet at any time. If you join Microsoft SpyNet with an advanced membership, you will be asked if you want to permit or deny changes made by software that has not yet been classified for risks. Basic members will not be asked to review changes by this software and the changes will be permitted. To change your Microsoft SpyNet membership, use the options provided in Windows Defender.

You can turn automatic scanning on or off and change the frequency and type of scans. You can also choose which actions are automatically applied to software that Windows Defender detects during a scheduled scan.

Windows Defender – History Feature

What this feature does

This feature provides a list of all software on your computer that Windows Defender detects and the actions that were taken when the programs were detected, including errors that might occur when actions are applied to that software.

In addition, you can view a list of Allowed items, which are programs that Windows Defender does not monitor while they are running on your computer. You can also view Quarantined items, which are programs that Windows Defender prevents from running until you choose to remove them or allow them to run again.

Information collected, processed, or transmitted

The list of software that Windows Defender detects, the actions that you and other users take, and the actions that Windows Defender takes automatically are stored on your computer. All users of the computer can view the history in Windows Defender to see spyware and other potentially unwanted software that has attempted to install itself or run on the computer, or that has been allowed to run by another user. For example, if you hear about a new spyware threat, you can check the history to see if Windows Defender has prevented it from infecting your computer.

Choice and control

History lists may be deleted by an administrator.

Windows Update

What this feature does

Windows Update is a service from Microsoft that provides updates for Windows operating system software and Windows-based hardware.

Information collected, processed, or transmitted

Windows Update collects basic information about your computer to identify which updates your computer needs and to improve the updating service. This information includes:

- Computer make and model
- Version information for the operating system, browser, and any other Microsoft software for which updates might be available
- Plug and Play ID numbers of hardware devices
- Region and language setting
- Globally unique identifier (GUID)
- Product ID and product key
- BIOS name, revision number, and revision date

Your IP address is also collected because you are connecting to an online service (web service) to get updates. However, your IP address is only used to generate aggregate statistics.

You might be invited to participate in a survey about the way you use Windows Update. Each survey includes a privacy statement that details the terms and use of any information submitted with that survey.

Use of information

The product ID and product key are used to confirm you are getting updates for a validly licensed copy of Windows. This information is not stored or retained after you finish using Windows Update, unless the product ID is not valid.

The information collected by Windows Update can also be used to generate aggregate statistics about which computer systems need support. Aggregate statistics help improve Windows and the updating service. To generate accurate statistics, Windows Update assigns a globally unique identifier (GUID) and stores it on your computer. The GUID provides a way to uniquely identify your computer without collecting information that can be used to identify you. The GUID is also used to record:

- The number of individual computers that use the updating service
- Whether updates were needed and which updates were applied
- Whether the download and installation of each update succeeded or failed

- Microsoft does not use the information collected by Windows Update to identify you or contact you.

Choice and control

- You can turn automatic updating on or off, change the frequency and time at which updates are installed, and choose which updates to install automatically by going to Windows Update in Control Panel.