10 things to know about Windows Defender

Windows Vista has a built-in anti-spyware program called Windows Defender to prevent malware from entering and stealing user information.

Windows Vista has a built-in anti-spyware program called Windows Defender to prevent malware from entering and stealing user information.

Here are 10 things to know to use Windows Defender better, increase the level of security for Windows Vista.

Windows Defender was released in October 2006 as an additional antispyware program for Windows XP or Windows Server 2003, allowing users to download for free. In the latest version of Windows Vista, Windows Defender becomes a built-in security utility that enhances computer protection.

1. Windows Defender is part of a multi-layer security strategy

Defender is designed to detect, remove or isolate programs that are identified or suspected as malicious software (spyware, malware) installed on the computer but without permission from the user. Windows Defender should be used in combination with other security mechanisms such as firewalls, antivirus programs and data encryption.

2. The default Defender has been activated in Windows Vista

Users can turn on / off Windows Defender or configure its operation via Windows Defender Control Panel or access it from the Security Center in Windows Vista. The Windows Defender interface is simple, with a single click that can scan for spyware or set a schedule to scan by date.

3. Windows Defender can perform 3 types of scanning

The Quick Scan section saves time searching for spyware. The Full Scan section takes care of each search drive and directory of the system. The scan time will depend on the drive size and the number of files. The Custom Scan allows you to select which drive or folder to scan. If Defender detects spyware when using a Custom Scan, it will perform Quick Scan to remove or isolate them.

4. You can determine how Windows Defender performs detection

Windows Defender interface.

Users can determine how Windows Defender identifies a software suspected to be spyware based on templates or behavior, or based on identifying files that are supposed to be spyware. You can also create a restore point before removing detected files so that when necessary, the system error can be fixed. Finally, Defender can ignore the directories or files that the user specifies.

5. Real-time protection function

By default enabled, real-time protection can be set up to observe which security factors on the system such as Windows startup programs, configuration settings security, additional Internet Explorer components, IE settings, downloading files, programs, services or drivers, Windows utilities and any programs that are started.

6. Administrators can control how Defender works on user machines

Administrators can allow users to use Windows Defender to scan the system, select actions for Defender when they find spyware. Administrators have the ability to limit the use of the user's Defender administrative permissions because by default, everyone is allowed to use Windows Defender.

7. You can view the activities performed in the History page

On the History page, users will see information about Defender's activities performed. Descriptions of this activity, the location and information of the file, the software found when scanning, and even the registry keys associated with them. Security warnings, time when warnings are issued, security status. People can see the parts they have set to prevent execution.

8. Windows Defender has four warning levels

- *Severe* : This program is malicious code, can damage your computer.

- *High* : The program can select your personal information or change settings.

- *Medium* : The program may select personal information but is part of a reliable program.

- *Low* : The program can select information, change the settings but be installed according to the approval and permission from the user.

The software, programs marked as Severe and High, you should remove them from the system. Medium and Low depend on whether users want to remove them or not.

9. Users should update Defender regularly

For effective use, anti-spyware software needs to be updated with the new database regularly. Ideally, users should update spyware databases before scanning. You can check for new update databases manually or through the Windows Update update function.

10. Microsoft Defender user feedback from the SpyNet community

It is not required to be a member of SpyNet. However, if you are a SpyNet member and use Defender, Defender will send information to Microsoft about the spyware found and the activities you perform on spyware. You can join SpyNet by going to Tools - Settings and then selecting membership levels from basic to advanced. With the advanced membership type, you will receive a warning when Defender finds the software that has not been analyzed and more detailed information sent to Microsoft about the found software.

Thanh Truc