Windows 10 features help increase computer security

Windows 10 PCs are a treasure trove of hidden features that you can manually activate for even more security. In this article, we will introduce the best security features you should try out on Windows 10.

Microsoft has made security the primary focus of the Windows 10 operating system. This is demonstrated by a number of features designed to protect you from malware, exploit, and cyber attacks.

Windows 10 PCs are a treasure trove of hidden features that you can manually activate for even more security.

In this article, **TipsMake.com** will showcase the best security features that you should try out Windows 10.

PUA protection

Picture 1 of Windows 10 features help increase computer security

Starting with the Windows 10 May 2020 Update, also known as the 2004 version update, Microsoft is making it easier for users to spot potentially unwanted apps using Microsoft Defender (formerly known as Windows Defender.).

Potentially unwanted applications (PUAs) are a category of programs that can cause your computer to slow down or display unwanted ads. PUAs are not considered viruses or malware, but they may modify web browsers, default applications, install extensions, and perform other actions that may adversely affect device performance. .

To know how to enable this feature, please refer to the article: Enable PUA protection in Windows 10 to block potentially unwanted software for detailed instructions.

Memory Integrity

Picture 2 of Windows 10 features help increase computer security

Windows 10 version 1803 or higher comes with a feature called Core isolation that provides additional protection against malware and other attacks. Core isolation isolates computer processes from Windows 10 and

devices, and it adds an extra layer of security against sophisticated attacks.

Memory Integrity is part of Core isolation, and it ensures that the code that runs in the Windows kernel is designed to be secure and reliable. It uses hardware virtualization and Hyper-V to prevent attempts to put and run malware in Windows processes in kernel mode.

Memory Integrity is a powerful security feature but it is disabled by default. To use Memory Integrity of Core isolation, follow these steps:

Step 1. Open Settings.

Step 2. Navigate to **Update & Security> Windows Security** .

Step 3. Click **Device security.**

Step 4. In **Core isolation** and **Memory integrity,** turn on the switch **Memory integrity.**

Step 5. Restart Windows to apply the changes.

Windows Hello

Picture 3 of Windows 10 features help increase computer security

Windows 10 comes with a great feature called Windows Hello, which allows biometric security to work on a PC, with facial or fingerprint credentials, but requires special hardware or devices. special.

You'll be able to set up Windows Hello to log into your computer using a fingerprint sensor or a special camera that can recognize your face.

Once configured, you can log in to your computer without entering a password.

To use Windows Hello on Windows 10, follow the steps in the article: How to set up Windows Hello with facial recognition on Windows 10.

Network scan

By default, Defender can scan local files and provide real-time protection against viruses, malware, ransomware and PUA.

Luckily, Microsoft also lets you scan your network files, but this option needs to be enabled manually with PowerShell.

To turn on network scanning, follow these steps:

Step 1. Open Windows Search.

Step 2. Search for **PowerShell** and click the option **Run as administrator** to open PowerShell with admin rights.

Step 3. Enter the following command:

```
Set-MpPreference -DisableScanningNetworkFiles 0
```

Step 4. Press **Enter** to enable scanning for network files.

By following the steps above, you can use Defender to scan for network files. If you want to disable this feature, enter the following command in PowerShell:

```
Set-MpPreference -DisableScanningNetworkFiles 1
```

Controlled Folder Access

Picture 4 of Windows 10 features help increase computer security

Windows 10 also comes with a Controlled Folder Access feature that allows you to prevent unauthorized access to certain folders. In other words, you can control who can access certain folders on Windows 10.

This feature can also prevent ransomware when it tries to access and encrypt documents, photos, or other files stored in those folders. To configure Controlled Folder Access, follow the steps in the article: Enable Anti-ransomware Controlled Folder Access in Windows 10.

DNS over HTTPS (DoH)

Windows 10 preview build comes with initial support for DNS over HTTPS (DoH), and it allows DNS resolution over encrypted HTTPS connections.

With support for DoH on Windows 10, Microsoft hopes to increase privacy on the Internet by encrypting DNS queries.

In build 20185 or later, you can configure DoH directly in the Settings app.

To configure DoH for Ethernet connections, follow the steps in the article: How to enable DNS over HTTPS for all apps in Windows 10.

You finished reading the article "**Windows 10 features help increase computer security**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.