# What is TPM 2.0? How can you tell if your computer supports it?

As you know, upgrading to Windows 11 requires a TPM 2.0 chip on your computer. So what is a TPM 2.0 chip? How do you check the TPM 2.0 chip on your computer? Let's find out the answers in the article below.

After introducing Windows 11 at its online event on June 24th, Microsoft also announced the Windows 11 installation requirements, including the TPM 2.0 chip requirement. The most frequently asked questions then became, " **What is TPM?"** and " **How do I know if my computer supports TPM 2.0?"** The good news is that most computers manufactured since 2016 have TPM 2.0 chips. Below is everything you need to know about this chip.

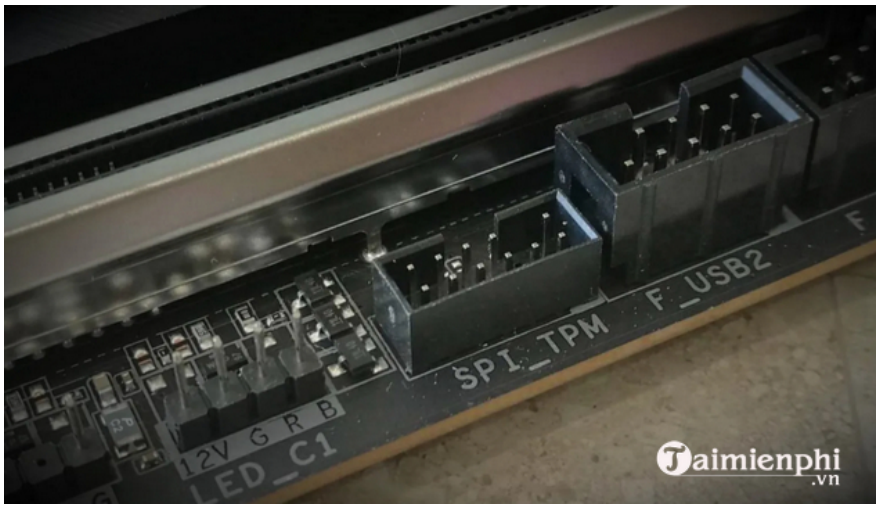

**What is TPM 2.0? How to check if your computer supports TPM 2.0?**

**Table of Contents:**


## *1. What is TPM 2.0?*

Regarding the question "What is TPM?", TipsMake would like to explain that TPM stands for Trusted Platform Module. It's a separate chip soldered onto the computer's motherboard, designed to provide hardware-based security-related functions.

A TPM chip is like the keypad electronic door lock you use to turn off your home security alarm every time you walk through the door, or it functions like the authentication app you use on your phone to log into your bank account.

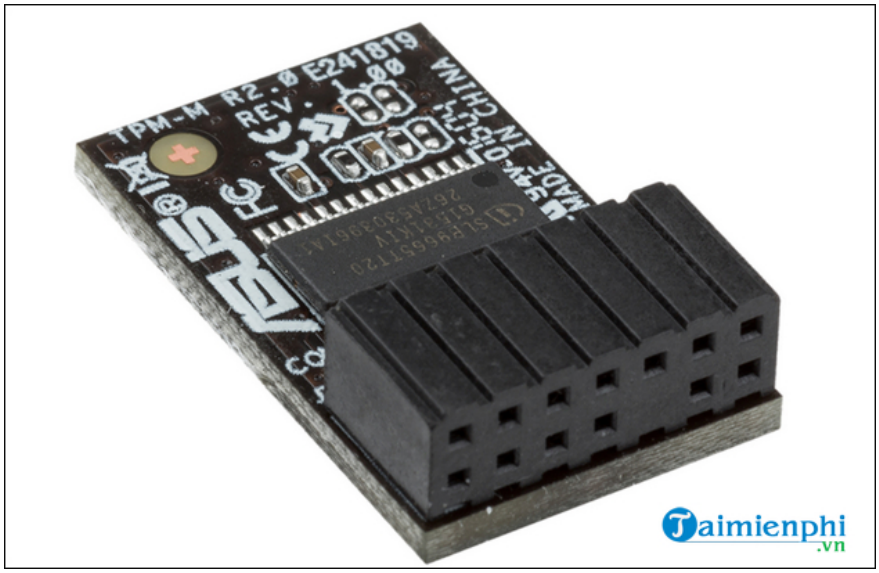



After turning on the power button on a computer with Full-Disk Encryption (FDE) and a TPM chip, this chip will provide a unique code called the cryptographic key. If everything goes normally, the drive encryption will be unlocked and your computer will start up. If there is a problem with the key, such as if a hacker steals your computer and tries to break into the encrypted hard drive inside, the computer will not boot up.

Currently, TPM chips come in two versions: 1.2 and 2.0. TPM 2.0 is a new security standard, released in October 2014, which includes all the functions of TPM 1.2 and adds more reliable algorithms.

## *2. What is TPM 2.0 used for?*

Some of the data we send and receive throughout the day is transmitted unencrypted. TPM chips use a combination of hardware and software to protect important passwords or encryption keys when they are sent in this unencrypted form.




If the TPM chip detects that the system's integrity has been compromised by a virus or malware, it can boot into isolation mode to help resolve the issue. Some Google Chromebooks include a TPM, and during boot, the chip scans the BIOS for unauthorized changes.

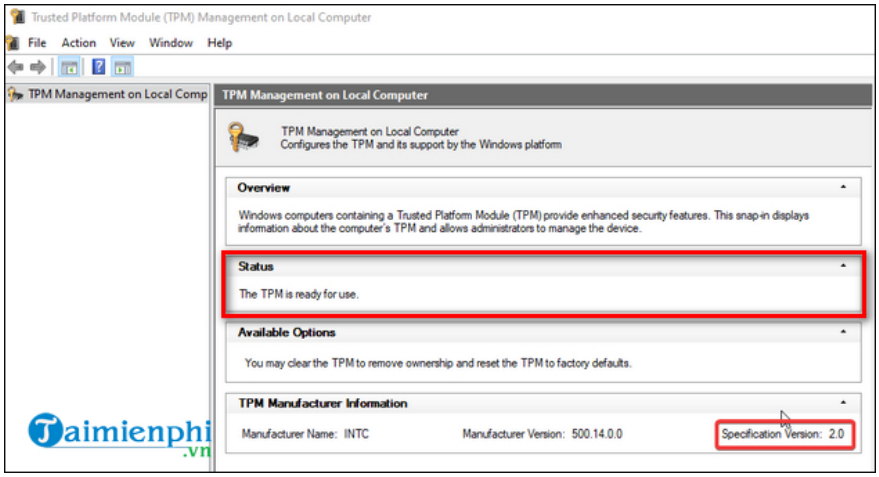
The TPM chip also provides secure storage for encryption keys, certificates, and passwords used to log into online services, a safer and more secure method than storing that data internally on a hard drive. In fact, many PC applications and features use the TPM after the system has booted up. Email applications like Thunderbird and Outlook use the TPM to process encrypted messages. Web browsers like Firefox and Chrome also use the TPM for some advanced functions, such as maintaining SSL certificates for websites.

Although TPM chips were initially developed for large businesses or companies wanting to secure their data, they are now becoming a requirement for all PCs and laptops to ensure security for all users.


Microsoft states that the TPM 2.0 chip, a mandatory requirement for installing Windows 11, is intended to help protect the system from common and sophisticated attacks such as ransomware, as well as other complex attacks. This requirement is not an issue for users who purchased computers shipped from around 2016.

### *3. How can I tell if my computer supports TPM 2.0?*

You can check if your computer has a TPM 2.0 chip by pressing the **Windows + R** key combination to open the **Run** dialog box and typing **tpm.msc** . After clicking **OK , the Trusted Platform Module (TPM) Management** window will appear. Here, if you see the status **"The TPM is ready for use"** in the **Status** section , it means your computer has a TPM chip, and you can check the TPM version in the **TPM Manufacturer Information section.**




However, if you receive the message " **Compatible TPM cannot be found** ," this means your computer does not have a TPM chip or the chip has not been enabled in the BIOS.

A TPM 2.0 chip is one of the requirements for a computer to install the Windows 11 operating system. However, there are some computer models that can still install Windows 11 without a TPM chip; you can find more information here:

You finished reading the article "**What is TPM 2.0? How can you tell if your computer supports it?**" 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.