How to Enable Secure Boot in Windows

Secure Boot is a security standard developed to ensure that a device boots using only software that is trusted by the Original Equipment Manufacturer (OEM). When the PC starts, the firmware checks the signature of each piece of boot software, including UEFI firmware drivers (also known as Option ROMs), EFI applications, and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system.

Enabling Secure Boot in Windows is crucial for protecting your system against rootkits and other malware that can take control of your system before the operating system loads. This article will guide you through the steps to enable Secure Boot on a Windows system.

Examples:

1. **Check Secure Boot Status:** To check whether Secure Boot is enabled on your system, you can use the System Information tool.
    - Press Windows + R to open the Run dialog box.
    - Type msinfo32 and press Enter.
    - In the System Information window, look for the "Secure Boot State" under System Summary. It will show whether Secure Boot is on, off, or unsupported.

2. **Enable Secure Boot:** To enable Secure Boot, you will need to access your system's UEFI firmware settings. This process may vary slightly depending on the manufacturer of your motherboard or system.
    - Restart your computer and enter the UEFI/BIOS setup by pressing a specific key (usually F2, F10, F12, or DEL) during the boot process.
    - Once in the UEFI/BIOS setup, look for a tab or menu related to Boot or Security.
    - Find the Secure Boot option and set it to Enabled.
    - Save the changes and exit the UEFI/BIOS setup.

3. **Verify Secure Boot is Enabled:** After enabling Secure Boot, you can verify its status again using the System Information tool as described in the first example.