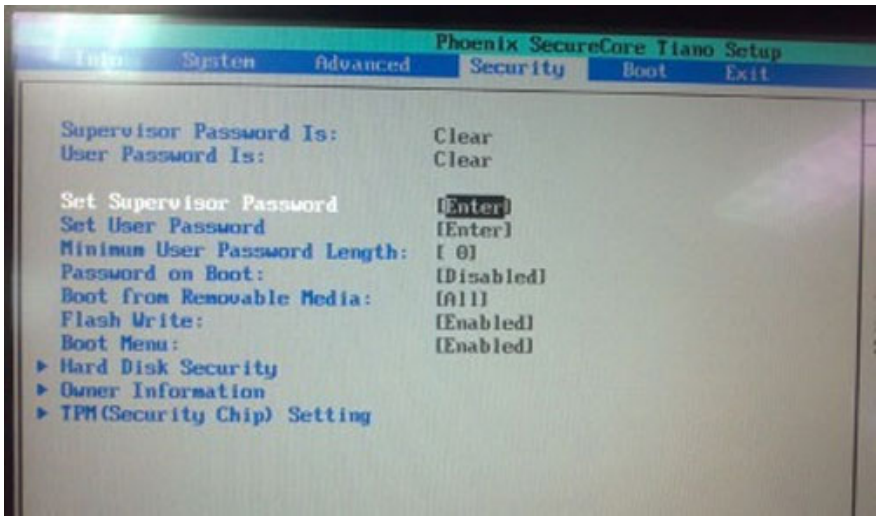
Prevent malware from breaking into the BIOS

Malware (malware) can sneak into the BIOS in your computer and then activate itself before any anti-malware has a chance to detect it. Therefore, you should set the password for the BIOS.

Malware (malware) can sneak into the BIOS in your computer and then activate itself before any anti-malware has a chance to detect it. Therefore, you should set the password for the BIOS.

You can rarely pay attention to *'interacting'* with the basic BIOS import / export system on the computer (BIOS - Basic Input / Output Operating System), but actually the BIOS occupies a unique and unique position. in computer architecture.



The BIOS is considered the first program to run when the computer boots - and before you enter user information the malware (malware) can sneak into the BIOS and then activate itself before any anti-malware software. Any chance to find out. A sophisticated low-level malicious program can also control your computer without leaving a trace.

Fortunately, there are very few confirmed cases of malware infection at the BIOS level. The most famous case is the Chernobyl virus in 1998, and these vulnerabilities are currently not available on new computers. Needless to say, the integrated firmware interface (Unified Extensible Firmware Interface - UEFI) and the security boot mechanism in Windows 8 are being considered as BIOS *'successors'* .

Anyway, with the current BIOS, users need to have a precautionary way rather than a bad situation. The first step in the plan is that you should protect the BIOS thanks to the admin password. This is the password you need to enter before you want to affect the BIOS.

Step 1:

Start or restart your computer. While booting, press the **'DEL', 'F1'** key or some special key (specified by the computer) to enter the BIOS. Information about these special keys is usually displayed right on the screen during the boot process, although it may not be displayed immediately.

For example, the following text, which appears verbatim, is located at the bottom of the screen in a snap after the user starts the computer.

~~: BIOS Setup: XpressRecovery: Boot Menu: Qflash~~

Step 2:

When your BIOS setup menu (menu) appears, look at the items that allow you to set a password. Can create more than one password. For example, in the BIOS, there is a password setting for both administrators and users. Normally, you must log in with an administrator password to make changes in the BIOS. The user password only allows you to see the current settings in the BIOS.

Step 3:

Select the item to create and enter the password (usually 2 times, to authenticate what you type for the first time). If you are afraid that you might forget your password later because you have recently accessed the BIOS, it is better to save the password in a password management utility, like **LastPass** . After that, save the changes in the BIOS and restart the computer. From now on, if you want to change any value in the BIOS, you need to enter the password, and this also ensures that the malware will be very difficult to break into your computer.

You finished reading the article "**Prevent malware from breaking into the BIOS**" 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.