

Real-World Scenario 3-1: Securing the UEFI/BIOS

Scenario: Your boss asks you to secure the UEFI/BIOS on a desktop computer. Your job is to modify the boot order, disable unnecessary devices, and configure a supervisory password.

NOTE As I did in the book, to simplify, I'll refer to UEFI/BIOS as simply *BIOS*.

The BIOS boots before the operating system. It can be configured to boot from optical discs and removable media. This change is fairly simple to make as long as a person can log in to the BIOS setup program. If no password is configured, this is even easier. You can imagine the amount of havoc that can be wreaked upon a machine if a malicious individual were to gain access to the BIOS.

Try securing the BIOS program on a test computer. Before you make any changes, back up the BIOS settings. When you are finished, return all settings back to normal.

Real-World Scenario 3-1 Solution

For this example solution we use an Asus BIOS on a physical computer to make some configuration changes, thus securing the BIOS. The steps are as follows:

Step 1. Restart the computer and access the BIOS using the correct key (Delete, F2, etc.), which is usually displayed during bootup.

NOTE If your resources are limited and you want to connect to a virtual BIOS, you can use Microsoft Virtual PC, but it must run on Windows 7 or older. However, your best option is to make these configurations on real PCs and laptops.

Step 2. Back up the current BIOS settings.

Step 3. Change the Boot device priority order. Make sure that the hard drive is first on the list so that removable media cannot be booted to.

Step 4. Disable unnecessary devices, such as USB connections and possibly optical drives.

Step 5. Configure a complex administrator password. The user password (AKA power-on password) is not necessary, but you can configure that if you want.

Step 6. Disable virtualization.

Step 7. Return the BIOS settings to normal.

NOTE If you would like to keep any of the settings you just configured, be sure to back up the BIOS again. Memorize your passwords!

Video Solution: Watch the video solution "3-1: Securing the BIOS."

Simulation: Complete the simulation "3-1: Securing the BIOS."