WINDOWS DEFENDER FIREWALL: BUILT-IN ANTI-VIRUS

Windows Defender is included with Windows 10 and helps keep malware from infecting your PC in two ways:

- ✓ Providing real-time protection. Windows Defender notifies you when malware tries to install itself or run on your PC. It also notifies you when apps try to change important settings.
- ✓ Providing anytime scanning options. Windows Defender automatically scans your PC for installed malware on a regular basis, but you can also start a scan whenever you want. Windows Defender automatically removes (or temporarily quarantines) anything that's detected during a scan. A Quick scan is usually adequate. However, if you suspect trouble that's causing your computer to hiccup, do a manual Full scan. Just remember that a Full scan can take a couple hours to complete.

To access Windows Defender, type *defender* in the search box to the right of the Start menu, then click on the *Windows Defender Firewall* that appears at the top of the list.

As an excellent complement to Windows Defender, many gurus advise that you download and install **MALWAREBYTES' ANTI-MALWARE**. The third-party application is a perpetual favorite among security experts. It's not uncommon to find another company's tech support agents calling on Malwarebytes to clean up a stubborn infestation. It's a tiny download, it installs quickly, and it gets right to business. What it won't do is protect your system from attack. The product's paid edition offers the added feature of malware blocking. Unless you purchase the commercial edition, you will need to run it manually. Neither the free version nor the commercial version will conflict with Windows Defender.

Many experts have concluded that having Windows Defender turned on with Malwarebytes running in the background is one of the best AV combinations available.