(Approx. 657 words)

Knowledge is Your Best Defense

Windows Defender and Firewall

By David Kretchmar, Computer Technician

Sun City Summerlin Computer Club

https://www.scscc.club

dkretch (at) gmail.com

There is a lot of confusion regarding Windows computer security. Some reviews of anti-virus software will state that **Windows Defender** is very poor, while others will say that it is very good. I would personally call it entirely adequate while lacking some features.

Microsoft Windows Defender originally was considered pretty weak. However, over the past 5 years, beginning with Windows 8 and continued in Windows 10, Microsoft has upped its game. Windows Defender, through several upgrades to Windows 10 and weekly updates, has become a real challenge to malware developers.

Windows Defender was originally known as Microsoft Security Essentials back in the days of Windows 7, when it was offered as a separate download. Now it’s built into Windows 10 and is enabled by default.

I've been using only Windows Defender and Windows Firewall from the day I moved to Windows 10 in 2015, and I have not found a virus infestation in any of my four computers.

## Different protections

There are different types of malware protection available which many people wrongly think are the same and label it under antivirus. Within antivirus software there are multiple parts; the two major ones are “Scan time Detection” and “Run time Detection”.

**Scan time detection** detects malware based on analyzing an application’s software executable and is only as good as its latest virus definition updates. Scan time protection depends on recognizing known malware signatures and types and uses that information to determine an executable’s validity (or bogusness).

Virus definitions need to be periodically updated so its definitions include the latest discovered malware.

**Run time detection** detects malware based on the way it runs, system functions it calls and system files it accesses. The run time A/V software then analyses this information to determine whether the application is malicious or has similarities to known malicious software. This is also known as heuristic analysis. Heuristic analysis is incorporated into more advanced security software to detect new threats before they cause harm, without the need for a specific signature. New viruses are called “zero-day”. The best protection against these is a real-time scanner which analyzes how software behaves on your PC. Recently this is one area where Windows defender has excelled.

## The firewall

These days the firewall is a major part of the security system, preventing unauthorized connections to your system by malicious software. The **Windows firewall** does the exact same job of blocking incoming connections as any third-party firewall. Third-party firewalls like the one included with Norton may generate pop ups more often, informing you that they’re working and maybe asking for your input. The Windows firewall just quietly does its thankless job in the background.

Windows firewall is enabled by default and should still be working unless you’ve disabled it manually or installed a third-party firewall. You can find its interface under Settings, Updates and Security, Firewall & network protection.

## You are the best defense

Some experts feel that if you know how to use a personal computer, what to browse on the web, where to click, where not to click, which software to install and which link to click then you don't need an anti-virus software. But you need to always be aware. Think before you click on anything, and never download third party software onto your system unless you understand exactly what it will do (generally, you don’t).

## Free alternatives to Windows Defender

If you don’t feel Windows Defender is adequate, and you don’t want to pay for protection, I suggest you look at the Avast or AVG free antivirus editions. Both can do a good job of protecting your computer. These third-party products offer some features that Windows Defender lacks, such as on-line monitoring for potential exploits. They are available from:

Avast: <https://www.avast.com/en-us/index#pc>

AVG: <https://www.avg.com/en-us/free-antivirus-download>

I have used both and they are very good.

