HOW TO ENABLE WINDOWS DEFENDER'S SECRET "CRAPWARE" BLOCKER

Windows Defender does a good job overall, but it lets crapware through. A hidden setting intended for organizations will boost the application's security, making it block adware, potentially unwanted programs, PUPs, or whatever you want to call this junk.

Why You Should Block This Junk

Crapware is often bundled with free software downloads. It's not technically malware, but it often shows advertisements, tracks your browsing, slows down your PC, and is just the kind of thing you don't want on your computer.

This type of software includes browser toolbars, weather programs, and assistants like Bonzi Buddy. PC optimization tools that claim your PC is slow or vulnerable and want money to fix the problem are also common.

Malwarebytes and many other antimalware programs also have a setting that blocks these "potentially unwanted programs," which have been called "malware with a legal team." Windows Defender can block this garbage, too. But it doesn't block this software by default.

How to Enable the Crapware Blocker

You can enable this setting from a Windows PowerShell prompt with administrator permissions.

To access the PowerShell, type *power shell* in the Search box. Right-click on the power shell item at the top of the column and select *Run as Administrator*. Then open the resulting User Account Control.

Copy and paste (or type) the following command at the prompt, and then press Enter:

```
Set-MpPreference -PUAProtection 1
```

The crapware blocker is now enabled. If you want to disable it in the future, just run the above command again, replacing the “1” with a “0”.

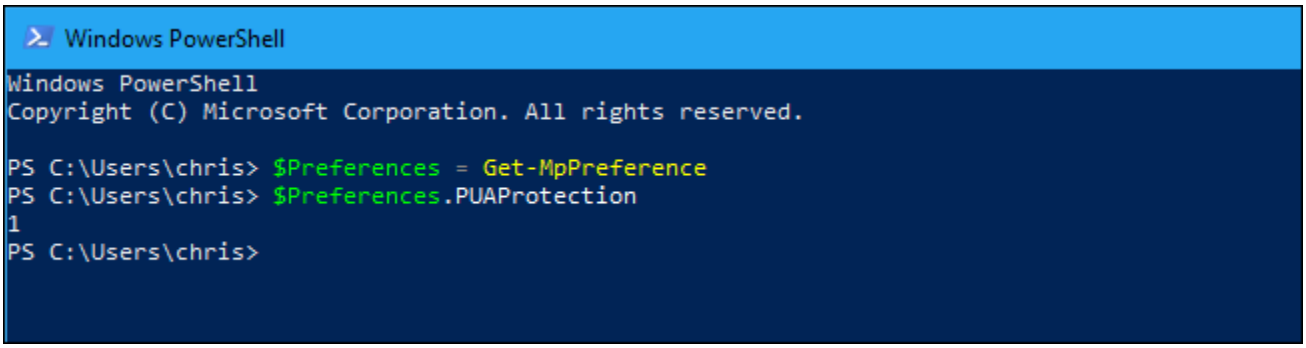
How to Check if the Crapware Blocker is Enabled

You can check if the crapware blocker is enabled on a PC by running the following two commands at a PowerShell prompt. Copy and paste (or type) the commands separately and press Enter after each:

```
$Preferences = Get-MpPreference

$Preferences.PUAProtection
```

If you see a “1,” the blocker is enabled. If you see a “0,” it’s disabled.

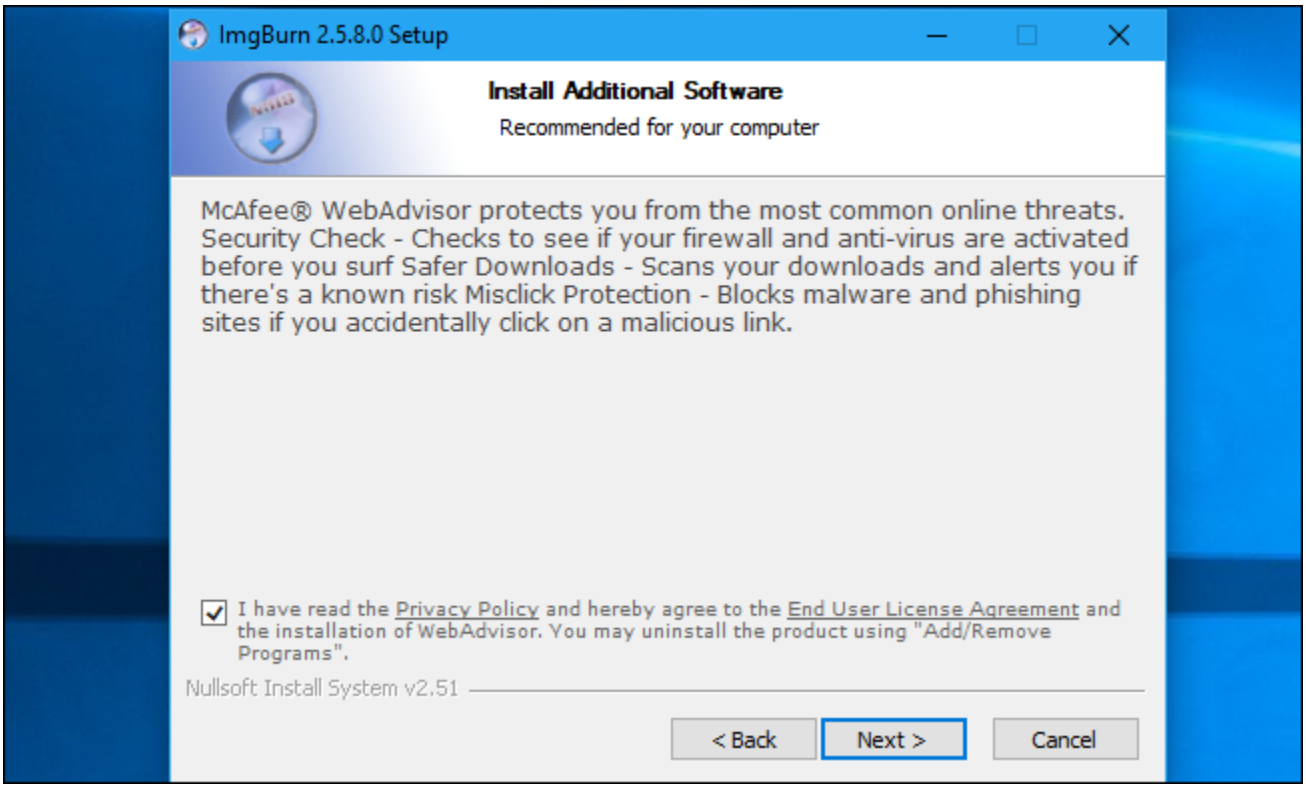


Crapware Blocking in Action

Without the crapware blocker enabled—the tester downloaded the ImgBurn installer and ran it. ImgBurn’s installer contains “InstallCore,” a bundled software system that will try to sneak additional software onto your PC as you click through the installer.

In addition, when the tester ran the installer, ImgBurn tried to install McAfee WebAdvisor. This sounds safe enough—although you don’t need browser extensions like this to protect you and such extensions often spy on you—but you never know exactly what offers are going to appear.

You're safe if you don't choose to install this software, but this is just one of the many screens you click through while installing this program. Worse yet, the confirmation box is checked by default. The software developer is counting on you just blindly clicking the "Next" button. In some cases, the developer is even sneakier and you may have to hunt down a little "Skip" link instead of clicking "Next."



With the crapware blocker enabled, Windows Defender quarantined the downloaded installer and classified it as "potentially unwanted software." Specifically, Windows Defender calls it a PUA, or a potentially unwanted application.

You can see the history of blocked threats on your computer at Settings > Update & Security > Windows Security > Open Windows Defender Security Center > Virus & Threat Protection > Threat History. Click "See Full History" under Quarantined Threats.

Windows Defender did not block every PUP the testers hoped it would. For example, Windows Defender did not challenge PC Optimizer Pro, a PUP that Malwarebytes Premium blocked from running. This setting makes Windows

Defender more aggressive, but Microsoft is still being more cautious about blocking crapware than Malwarebytes is.

In other words, Malwarebytes is still a better solution that will stop more crapware than Windows Defender will.

It’s still worth flipping this switch to ON and making Windows Defender more aggressive.