How to protect your PC from the major Meltdown and Spectre CPU flaws

Stay safe(r) with this guide. **BY BRAD CHACOS**

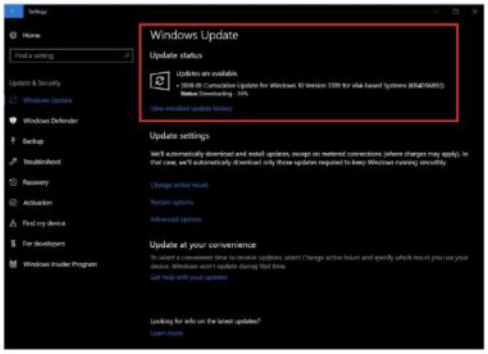
A pair of nasty CPU flaws recently exposed have serious ramifications for home computer users. Meltdown and Spectre let attackers access protected information in your PC's kernel memory, potentially revealing sensitive details like passwords, cryptographic keys, personal photos and email, or anything else you've used on your computer. These are serious flaws. Fortunately, CPU and operating system vendors pushed out patches fast, and you can

IMAGE: THINKSTOCK

protect your PC from Meltdown and Spectre to some degree.

It's not a quick one-and-done deal, though. They're two very different CPU flaws that touch every part of your operating system, from hardware to software to the operating system itself. Check out *PCWorld*'s Meltdown and Spectre FAQ on page 7 for everything you need to know about the vulnerabilities themselves. We've cut through the technical jargon to explain what you need to know in clear, easy-to-read language. We've also created an overview of how the Spectre CPU bug affects phones and tablets (go.pcworld.com/phta).

The guide you're reading now focuses solely on protecting your computer against the Meltdown and Spectre CPU flaws.



Where to update Windows 10.

HOW TO PROTECT YOUR PC AGAINST MELTDOWN AND SPECTRE CPU FLAWS

Here's a quick step-by-step checklist, followed by the full process.

- Update your operating system
- Check for firmware updates
- Update your browser
- Update other software
- Keep your antivirus active

First, and most important: Update your operating system *right* now. The more severe flaw, Meltdown, affects "effectively every [Intel] processor since 1995," according to the Google security researchers that discovered it. It's an issue with the hardware itself, but the major operating system makers have rolled out updates that protect against the Meltdown CPU flaw.

Microsoft pushed out an emergency Windows patch late in the day on January 3. If it didn't automatically update your PC, head to *Start* > *Settings* > *Update & Security* > *Windows Update*, then click the *Check now* button under "Update status." (Alternatively, you can just search for "Windows Update," which also works

for Windows 7 and 8.) Your system should detect the available update and begin downloading it. Install the update immediately.

You might not see the update, though. Some antivirus products aren't playing nice (go.pcworld.com/nice) with the emergency patch, causing Blue Screens of Death and boot-up errors. Likewise, the Meltdown patch rendered some AMD computers unbootable (go.pcworld.com/unb0), which forced Microsoft to temporarily halt its roll-out of the fix to potentially impacted systems. It's fixed now, but because of the barrage of severely system-breaking errors, we **do not recommend** manually installing the Windows Meltdown patches if Microsoft hasn't pushed them to your PC via Windows Update. We aren't even going to link to the download page for the Meltdown updates. Don't do it.

Apple quietly worked Meltdown protections into macOS High Sierra 10.13.2, which released in December. If your Mac doesn't automatically apply updates, force it by going into the App Store's *Update* tab. Chromebooks should have already updated to Chrome OS 63 in December. It contains mitigations against the CPU flaws. Linux developers are working on kernel patches. Patches are also available for the Linux kernel.

You also need to install CPU microcode/firmware fixes to protect against one of the Spectre variants, which can't be combated by operating system patches alone.

CHECK FOR A CPU FIRMWARE UPDATE

You also need to install CPU microcode/firmware fixes to protect against one of the Spectre variants, which can't be combated by operating system patches alone. Intel released firmware updates for most of its processors released in the past five years—but the "fix" can cause system instability and reboot errors (go.pcworld.com/1nst). Intel has identified the root cause but advises that users do not install currently available CPU firmware patches, reversing its earlier guidance. Instead, the company counsels users to wait until new, more stable microcode updates arrive, which are currently being tested by Intel's hardware partners. We'll update this article when the new fixes are available.

Now for more bad news. The operating system and CPU firmware patch combo will slow down your PC (go.pcworld.com/sl0w), though the extent varies wildly depending on your CPU and the workloads you're running.

Intel expects the impact to be fairly small for most consumer applications like games or web browsing. Initial testing supports that, and reveals storage speeds can take a significant dip. Microsoft says Windows 10 PCs with Skylake (Core 6xxx series) chips or newer shouldn't see much performance

impact; Windows 10 PCs with 2015-era or older Intel processors "show more significant slowdowns;" and on Windows 7 and 8 systems with older Intel CPUs, Microsoft "expects most users to notice a decrease in system performance."

AMD will release CPU firmware updates (go.pcworld.com/firm) too, starting with Ryzen, Threadripper, and Epyc processors before moving on to older chips. They're classified as optional, however, because "differences in AMD architecture mean there is a near zero risk of exploitation" of the Spectre variant that requires firmware updates. Given Microsoft's warning of post-patch performance slow-downs, Intel's firmware stability woes, and the optional nature of AMD's fix, you may want to wait until AMD's microcode update is tested and benchmark before deciding whether or not to apply it to your system.

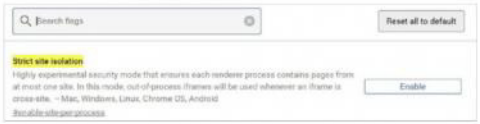
Actually *getting* those firmware updates is tricky, because firmware updates aren't issued directly from Intel and AMD. Instead, you need to snag them from the company that made your laptop, PC, or motherboard—think HP, Dell, Gigabyte, et cetera. Because of that, patches for individual systems will likely take longer than Intel and AMD's stated timelines to trickle down to home users. Most prebuilt computers and laptops have a sticker with model details somewhere on their exterior. Find that, then search for the support page for your PC or motherboard's model number.

Gibson Research's easy-to-use InSpectre scanning tool (go.pcworld.com/1nsp) can let you know if you've installed all the necessary OS and CPU patches on your system.

UPDATE YOUR BROWSER

You also need to protect against Spectre, which tricks software into accessing your protected kernel memory. Intel, AMD, and ARM chips are vulnerable to Spectre to some degree. Software applications need to be updated to protect against Spectre. The major PC web browsers (go.pcworld.com/pcwb) have all issued updates as a first line of defense against nefarious websites seeking to exploit the CPU flaw with JavaScript.

Microsoft updated Edge and Internet Explorer alongside Windows 10. Firefox 57 also wraps in some Spectre safeguards. Chrome 63 made "Site Isolation" (go.pcworld.com/sis0) an optional experimental feature. Activate it by entering **chrome://flags/#enable-site-per-process** into your URL bar, then clicking Enable next to "Strict site isolation." Chrome 64 will have more



Enabling Site Isolation in Chrome 63.

protections in place when it launches on January 23.

On January 8, Apple pushed out updates to iOS 11 (go.pcworld.com/i012) and macOS (go.pcworld.com/mc05) with "security improvements to Safari and WebKit to mitigate the effects of Spectre."

It's important that you keep your antivirus software up to date.

UPDATE OTHER SOFTWARE

Your browser is the easiest avenue for hackers to attack the Spectre CPU flaw, but other software can potentially fall prey to it as well—especially if the software sinks deep hooks into your operating system's kernel. Case in point: The GPU display driver for graphics cards. Nvidia released new drivers containing Spectre mitigations for GeForce (go.pcworld.com/gf0r), Quadro, NVS, and some Tesla hardware shortly after the CPU exploits were revealed, with fixes coming to the remaining Tesla cards and GRID GPUs later in January. Grab the newest Nvidia drivers here (go.pcworld.com/driv), and grab them now if you're an Nvidia user.

Apply all newly available software updates in the coming weeks, especially if it's somehow tied to hardware. If your printer, SSD, or system monitoring software pushes out an update, install it.

KEEP YOUR ANTIVIRUS ACTIVE

Finally, this ordeal underlines how important it is to keep your PC protected. The Google researchers who discovered the CPU flaws say that traditional antivirus wouldn't be able to detect a Meltdown or Spectre attack. But attackers need to be able to inject and run malicious code on your PC to take advantage of the exploits. Keeping security software installed and vigilant helps keep hackers and malware off your computer. Plus, "your antivirus may detect malware which uses the attacks by comparing binaries after they become known," Google says.

PCWorld's guide to the best antivirus for Windows PCs (go.pcworld.com/w1pc) can help you find the best option for your setup.