FLASH. MUST. DIE.

ADOBE FLASH—THAT INSECURE, ubiquitous resource hog everyone hates to need—is under siege, again, and hopefully for the last time. The latest calls for its retirement come from some of the Internet's most powerful players, but if the combined clattering of Facebook, Firefox, and a legion of unsatisfied users isn't enough finally to put it in the ground, scroll down to see how to axe it from your devices yourself.

Why would you want to?

Because Flash is a closed, proprietary system on a web that deserves open standards. It's a popular punching bag for hackers, which puts users at risk over and over again. And it's a resource-heavy battery suck that at this point mostly finds its purchase in pop-up ads you didn't want to see anyway.

This week, in the wake of newly discovered vulnerabilities in Flash, Facebook security boss Alex Stamos called for a termination date for Flash, and late Monday night Mozilla disabled all current versions of the plug-in by default in its Firefox browser. Even Google is limiting Flash's impact; last month, it announced that future versions of Chrome will "intelligently pause" Flash-based content that isn't part of a website's core experience (e.g. video ads).

That doesn't mean this is the end … yet. Facebook still uses Flash to play video on some browsers, and Firefox reintroduced Flash support on Tuesday when a secure update arrived. The point is clear, though: Flash is officially more trouble than it's worth. And it has been for some time.

There's always been a moderate anti-Flash undercurrent rumbling through the web; there's even an "Occupy Flash" movement whose stated goal is strongly (but blandly) stated as "To get the world to uninstall the Flash Player plugin from their desktop browsers." In fact, killing of Flash has been on-trend since being software non-grata on the original iPhone. Steve Jobs penned a famous open letter in April, 2010, explaining why he wouldn't let Flash

anywhere near Apple's mobile products, highlighting concerns over openness, security, and its impact on battery life.

More than five years later, the case against Flash remains largely unchanged—and the security problem is the most immediate and important. After all, the newly discovered critical vulnerability that led Mozilla to quarantine Firefox from Flash was the third problem of its kind discovered this week thanks to a data breach of controversial digital surveillance firm Hacking Team.

When we reached out to Adobe to ask about those security holes and the mounting calls for Flash to disappear altogether, a representative directed us to a statement that says the company fixed the issues and has pushed an update. It also had this to say about its security issues generally:

"Flash Player is one of the most ubiquitous and widely distributed pieces of software in the world, and as such, is a target of malicious hackers. We are actively working to improve Flash Player security, and as we did in this case, will work to quickly address issues when they are discovered."

However actively Adobe has been working on Flash Player security, it doesn't seem to be enough. This week's mistrials are but the latest in a string of security lapses that have plagued Flash for years. Exploit kits—packets of code that take advantage of these sorts of vulnerabilities in your browser to push malware or ransomware—have used Flash to futz with countless sites. So-called zero-day vulnerabilities (a security hole that hackers find before the software company does) are found on Flash with such regularity they almost feel like a feature.

"The Flash Player is a very interesting target for attackers because it really is ubiquitous and runs in all major browsers," says Jérôme Segura, senior security researcher at Malwarebytes. "On top of zero-days, many end users are still running older versions which explains why the number one piece of software exploit kit writers go after is Flash."

That last point is critical; Adobe releasing a secure new version of Flash doesn't guarantee its users will download it.

As quickly as Adobe can beat back trouble, more pops up. It's a never-ending game of Whac-a-Mole.

As quickly as Adobe can beat back trouble, more pops up. It's a never-ending game of Whac-a-Mole, with the fun twist that you always end up losing.

Segura's torn on whether Flash should die altogether. "At the moment it is the most responsible thing to do," he says, "But I also think it may be short sighted. After all, malicious actors can easily move on to a new target."

The good news is, you don't have to wait for Adobe to pull the plug. You can do it yourself.

How to Ditch Flash

First things first: You can do this! Truly. In fact, you almost certainly already have, on your phone. As we said, iOS gave Flash the boot years ago, and Android followed suit in 2012. (Adobe AIR does allow developers to use Flash content in iOS and Android apps; we're talking instead about the more prevalent Flash Player plug-in that got axed on both platforms).

In the early days of the iPhone, no Flash was a moderate annoyance. Certain sites wouldn't load, certain videos wouldn't play. Today, though, you're more likely to meet a talking dog than a mobile site that won't load because of a missing Adobe product.

That's increasingly true on desktops as well, thanks in large part to the steady advance of HTML5, an open standard that's been widely embraced for video (as of January, YouTube uses it by default; Netflix made the leap from Microsoft's Silverlight even earlier). Gaming has made a small retreat as well; the Unity game engine severed ties with Flash in 2013.

There are, of course, still plenty of Flash Player holdouts; lots of casual games, Amazon Instant Video (on Chrome, at least; it uses Silverlight on Firefox, Safari, and Internet Explorer), lots and lots of pop-up video ads. They're the sort of internet items, though, that you can go for days if not weeks without

encountering, or caring that you've missed. The bottom line: While Flash used to be ubiquitous on the desktop, it's not anymore. You likely won't even notice that it's gone.

Okay then! Ready? Here we go, broken down by browser.

Chrome: Go to chrome://plugins in your search bar. Scroll down to Adobe Flash Player. Click Disable.

Safari: Go to Safari > Preferences. Click Security. ClickManage Website Settings. Click Adobe Flash Player. Go to the When visiting other websites dropdown and click Block.

Firefox: Go to the hamburger icon in the upper righthand corner. Click Add-ons. Go to the lefthand column and clickPlugins. Go to the dropdown next to Shockwave Flash and select Never Activate.

Internet Explorer: Go to the gear icon in the upper righthand corner. Click Internet options. Click Programs. Click Manage add-ons. Click Shockwave Flash Client. In the lower righthand corner, click Disable.

And you're done! You can also uninstall Flash altogether on Mac and Windows by following those links, but you'll save yourself a lot of potential time and trouble—and reap the same benefits—by making strategic, browser-specific surgical strikes.

Feeling good? You should! Just remember that Segura's right; Flash isn't the only vulnerable software out there, and if it does disappear altogether you'll need renewed vigilance elsewhere (looking at you, Java).

In the meantime, in the unlikely event you find yourself missing Flash too terribly, you can always go back. At least, until Occupy Flash—and its friends at Facebook and elsewhere—finally have their way.

Source: http://www.wired.com/2015/07/adobe-flash-player-die/