Your phone really does make you feel good, study says

by Lynn La

Processors are vital to running all our computerized devices, even if we hardly ever think about them. That's why it's a big deal that they have major vulnerabilities, such as Spectre and Meltdown, that leave them open to hacking attacks.

As they run all the essential processes on your computer, these silicon chips handle extremely sensitive data. That includes passwords and encryption keys, the fundamental tools for keeping your computer secure.

The Spectre and Meltdown vulnerabilities, revealed Wednesday, could let attackers capture information they shouldn't be able to access, like those passwords and keys. As a result, an attack on a computer chip can turn into a serious security concern.

So how did this happen? And what will chip companies like Intel, Arm and AMD (and the hardware
makers that put the chips in their products) do to fix the problem? Here's what you need to know:

**What are the vulnerabilities?**

Researchers found two major weaknesses in processors that could let attackers read sensitive information that should never leave the CPU, or central processing unit. In both cases, attackers could see data that the processor temporarily makes available outside of the chip.

Here's why that happens: To make computer processes run faster, a chip will essentially guess what information the computer needs to perform its next function. That's called speculative execution. As the chip guesses, that sensitive information is momentarily easier to access.

One flaw, Spectre, would let attackers trick the processor into starting the speculative execution process. Then attackers could read the secret data the chip makes available as it tries to guess what function the computer will carry out next.

The other flaw, Meltdown, lets attackers access the secret information through a computer's operating system, such as Microsoft Windows or Apple's High Sierra.

Security experts refer to these sorts of incursions as side-channel attacks, because they access information as it's being used by a legitimate process on the computer.

**What are tech companies saying and doing about this?**

Intel CEO Brian Krzanich says the problems are well on their way to being fixed, at least in the case of Intel-powered PCs and servers. Intel said Thursday that [90 percent of chips released in the last five years will have fixes available](https://www.intel.com/content/www/us/en/security/intel-technology-security-center/fixes.html) by the end of next week and that for chips up to 10 years old, fixes will be released in the coming weeks.

Microsoft on Wednesday released [patches for the Windows operating system](https://www.microsoft.com/en-us/p/windows-security-update) and its Internet Explorer and Edge browsers, but warned that your antivirus software needs to be updated to support those patches.

Apple said that it has [released mitigations](https://support.apple.com/en-us/HT204068) for the Meltdown flaw for the operating systems on its Mac computers, Apple TVs, iPhones and iPads, and that neither Meltdown nor Spectre affects the Apple Watch. Apple also said Thursday that it will release patches "in the coming days" for the Safari browser to help defend against Spectre exploits and that it will continue to release patches in future updates of its iOS, MacOS and TVOS software.

**Which chips are affected?**

A number of chip designs from Intel, Arm and AMD are susceptible to one or more variants of the attacks. The issue is so widespread because those chips, used in devices made by Apple, Google,
Microsoft, Amazon and others, all share a similar structure.

What's more, the flaws don't just affect personal computers -- Meltdown also affects servers, the backbone of all major cloud services. So yes, Amazon Web Services and Google Cloud are susceptible to the problem, too. Google said it has secured all its affected products, and Amazon said it would finish securing all affected products on Wednesday.

**How long has this been a problem?**

Researchers at Google's Project Zero, as well as a separate team of academic researchers, discovered the problems in 2017, but the issue has existed on chips for a long time -- perhaps more than 20 years.

That's because the issue doesn't result from a badly written computer code. Instead, the problem comes down to the way the chips are intentionally designed.

Processors are supposed to make the secret information easier to access as they gear up to run the next process on a computer. As the programming quip goes, this is a feature, not a bug.

**Has anyone been hacked via these flaws?**

Researchers, chipmakers and computer companies all say there are no known examples of hackers using these weaknesses to attack a computer. However, now that the details of the design flaws and how to exploit them are publicly available, the chances of hackers using them are much higher.

The good news is that hackers would first need to install malicious software on your computer in order to take advantage of these flaws. That means they need to select their targets and hack each one of them before running a sophisticated attack to steal a computer's sensitive information.

**What can I do to protect myself?**

As chipmakers and computer companies roll out software updates, be sure to install them. Beyond that, since hackers would have to install malware on your computer, do your best to make that harder for them.

That means you should keep all your other software updated, including your web browsers and Flash (if you’re still using it). Also, run security software to make sure you don’t have any malicious software on your computer right now.

Finally, look out for phishing emails. Emails that trick you into clicking on a link and downloading malicious software are still the number one way for hackers to get a foothold on your computer.

First published Jan. 3 at 6:01 p.m. PT

**Update Jan. 4 at 4:19 p.m. PT:** Added statement from Apple.