Declassified: the dangerous security flaws that affect almost everyone

There’s a doozy of a security flaw out there that affects all types of devices and all types of operating systems. So whether you’ve got a Windows, Mac, or Linux computer, you’ll want to listen up.

In fact, the flaw is so bad that, at first, it wasn’t publicly released in order to give Microsoft, Apple, and Linux time to come up with some kind of security patch to stop it.

The rush of new security patches changed the way that systems handle virtual memory. Those who keep an eye on such things knew something was up, but they didn’t know what because everyone was being tight-lipped about it.

Before I go into what exactly the issue is, I want you to make sure that your computer, whether it be Windows, Mac, or Linux has all of the latest updates available. Go do it now. You can read this later. If you never come back to this article to find out why the updates were so important, it doesn’t matter. It matters that your device is up-to-date.

Everything up-to-date? Cool. Let’s get to the flaws. They are called Meltdown and Spectre. These would make great names for super-villains, and it’s not too far off. These buggers can do a lot of damage. These issues affect the chips, which are basically the brains, of computers. And by computer, I mean your laptop, desktop, smartphone, tablet, and smart home devices.

Right now the focus is on Intel chips, but it’s likely that all chips are affected. It’s a design flaw in the chips that can allow someone to gain access to the cache of the chips and thereby access potentially sensitive information. The folks at Google’s bug-hunting Project Zero have a much more detailed explanation posted. If you’ve got the technical chops to understand it, you can click here to read.

There’s no evidence that anyone has actually taken advantage of these flaws yet, but researchers have been able to demonstrate how it would work. And, of course, now that the information is out there, the hackers are sure to try to exploit it.
Aside from the patches for computers, there’s not any other way for the home user to protect themselves. Right now, you’ll just want to make sure your system is up to date and keep an eye out for updates to mobile operating systems.

More importantly, always stay vigilant when it comes to bank accounts, credit and debit cards, and other sensitive information. In this case, it’s more likely hackers will go after companies and their sensitive data, which is also your sensitive data. Staying alert is probably your best defense.