# Meltdown & Spectre FAQ

## What are Spectre and Meltdown?

Spectre and Meltdown utilize a vulnerability left in modern electronic devices in order to gain access to personal data located in the memory of your processor.

## How are Spectre and Meldown able to access my data?

Computer researchers have recently found out that the main chip in most modern computers and smartphones—the CPU—has a hardware bug. It's really a design flaw in the hardware that has been there for years. This is a big deal because it affects almost every computer on your network, including your workstations, tablets, smartphones and all your servers.

This hardware bug allows Spectre and Meltdown to steal data that is being processed in your computer memory. Normally, applications are not able to do that because they are isolated from each other and the operating system. This hardware bug breaks that isolation.

So, if the bad guys are able to get malicious software running on your computer, they can get access to your passwords stored in a password manager or browser, your emails, instant messages and even business-critical documents. Just remember that these vulnerabilities cannot be exploited unless there is already malware on the machine, so it is important to utilize good anti-malware software in addition to being careful about what you download and what links you click.

To our knowledge there has not been a breach of this vulnerability in the wild yet.

## What can we do, now?

We will need to update and patch all the machines on your network. This is going to take some time, some of the patches are not even available from the hardware vendors yet. Your computers, tablets and smartphones will need to be up to date with OS patches. You may have to replace some mission-critical computers to fix this hardware design flaw. CoreTech uses a combination of Webroot software, WatchGuard firewall, and Proofpoint email filters to help keep every aspect of your devices free from malware.

It is especially important that your system does not contract any malware at this time to safeguard against Meltdown and Spectre. We offer end-user education from KnowBe4 that we suggest all our clients implement. At CoreTech, we utilize this program ourselves to teach our staff how to stay safe from phishing emails and unsafe sites. If you do not already utilize this training, contact us about adding it to your services.

## What can I expect, moving forward?

We are expecting firmware updates released from HP very soon.

We will continue to update you as we gather more information.

Please contact us with any questions at support@coretech.us.

Until then, know that we are taking all of the prudent steps to keep your systems secure.