Meltdown and Spectre

Computer vulnerabilities that affect your privacy.

Your passwords and sensitive data may be at risk.

Recent studies have shown that most computers, tablets, and smartphones have a common defect that allow hackers to access your private information. Researchers have named the two methods of attack "Meltdown" and "Spectre."

How do the security vulnerabilities work?

Both Meltdown and Spectre exploit similar defects in computer processors — the silicon chips that power your devices. Malicious apps can use these defects to gain access to all files, passwords, and other private information on your device without your permission.

Exploiting how your device predicts your behavior

The computer processor in each of your electronic devices are incredibly fast, making thousands of calculations per second. Some of these calculations are based on what your device predicts you're going to do next, such as opening the Facebook app, taking a selfie, or checking your email. Meltdown and Spectre attacks exploit defects in your processor to secretly access these predictions. Access to your processor's predictions could allow a simple flashlight app to secretly read an account number in a your bank app. Even with an anti-virus, it can be difficult to detect when an app is making use of Meltdown or Spectre.

Protecting against Meltdown

Most electronic devices have similar computer processors with the same defect that makes Meltdown attacks possible. The Meltdown attack allows a malicious app to access the memory of other programs, putting all information on your device at risk.

Technology companies such as Microsoft, Apple, and Intel are working together to create a software updates that protect customers from malicious apps that use the Meltdown attack. Your computer, tablet, or smartphone may notify you if there are software updates available.

Older devices may not receive software updates if the manufacture has discontinued support. A full replacement to a recent model is recommended to avoid Meltdown attacks.

Protecting against Spectre

Spectre attacks use a similar technique to break the isolation between programs. While similar software updates are available, the nature of this attack is still being researched. It's likely that older devices may need replacement to be completely safe from Spectre attacks.

How can I keep my personal information safe?

Computer manufacturers frequently discover vulnerabilities and release software updates to patch them. However, not all devices are updated before hackers can gain access to your data. You can reduce your chances of being a victim with a few extra precautions.

Ensure all your electronic devices are using the latest software and apps

Older devices may no longer receive updates, putting them at risk for unpatched vulnerabilities. If a complete replacement isn't possible, consider limiting how much personal information is left on the device.

Protect your email account

Almost all online services use your email address to verify your identity. Keeping your email account safe with a strong password can decrease the chances of an attacker accessing your account. Many online services can also send a special code to your phone to verify that your password isn't being use without your permission. This extra verification is recommended for other services such as your bank, Facebook, Instagram, and Dropbox.

Learn more about handling Meltdown and Spectre

An detailed explanation of the vulnerabilities and available updates — Graz University of Technology

How to set up two-factor authentication on all your online accounts — The Verge