DEPARTMENT OF TECHNOLOGY & INFORMATION
DELIVERING TECHNOLOGY THAT INNOVATES

eSecurity Newsletter — SPECIAL ALERT

Earlier this month, the New York Times reported that security researchers have uncovered two major security issues, known as Meltdown and Spectre, that have the potential to improperly gather sensitive data from many kinds of computing devices. It is critical that you follow manufacturer recommendations to perform updates to secure your applications and every device you use.

Meltdown and Spectre

Meltdown and **Spectre** are names given to exploitation techniques related to access to kernel memory. They could allow hackers to steal entire memory contents of computing devices—smart phones, tablets, personal computers and servers running on cloud-based computer networks (such as Google, iCloud, and others). Spectre affects nearly all computer processors on the market, going back many years. Meltdown affects all Intel microprocessors. Essential chip design flaw means that there is no single easy fix.

Nearly every computing device is affected so it's not realistic to replace every flawed device processor. All manufactures and application developers are releasing operating system updates and patches to lessen the risk of an exploit.

What Should YOU do?

You should check often and quickly install any and all recommended updates for EACH of your devices as soon as they become available. A single update or patch is unlikely to entirely correct for these threats, so please check back frequently and make any changes your manufacturer or your application developer recommends. Don't forget kids' laptops, computers, tablets and smartphones: they need updates, too.

- Intel has a reference page with links to computer manufacturers to help locate updates and patches needed for devices using Intel chips.
- Google has its own page describing the status of mitigations for its products and devices.
- Apple has released security updates for its iOS devices and browsers, as well.

Strengthen Account Protection

Use the strongest authentication available such as biometrics, security keys or a unique one-time code through an app on your mobile device. Choose and use a password manager that creates complex, unique passwords for your accounts. Take advantage of dual authentication because usernames and passwords are not enough to protect e-mail and banking accounts.

Questions, comments or topic suggestions?
Email us at eSecurity@state.de.us.

Visit the DTI eSecurity website for previous issues.
eSecurity Newsletters

DigiKnow CYBER SECURITY DEPENDS ON YOU

Delaware Department of Technology and Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or want to print a PDF copy, go to https://digiknow.dti.delaware.gov.