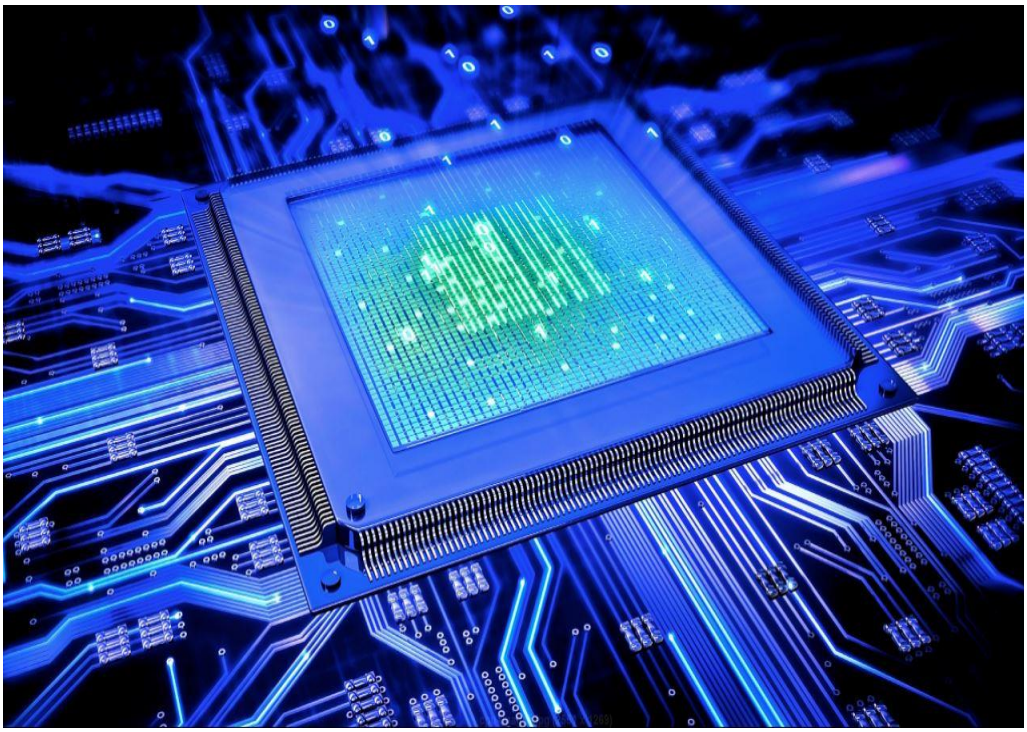

Dimensional Dispatch

7th Dimension Newsletter

7th Dimension
5005 Windplay Drive, Ste. 1
El Dorado Hills, CA 95762
(916) 221-0855

February 2018

"INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY"

IN THIS ISSUE

Meltdown and Spectre

A review of the biggest vulnerabilities so far this year

What are Meltdown and Spectre?

Two security vulnerabilities made public in January were Meltdown and Spectre. Meltdown and Spectre are flaws in the way chips have been designed for the last decade. Therefore, these vulnerabilities affect **billions of devices** powered by modern processors from Intel, AMD, and ARM by **allowing attackers to steal sensitive information** like passwords and encryption keys using locally installed applications or simple web scripts.

What You Should Do

Making sure all of your devices are patched to the latest updates is **the best way to protect** yourself. Most people know that these issues affect their computers and servers, but do not realize that their **smartphones** are just as vulnerable. Ensure that your iPhone or Android device has the latest update. If you are under a fully managed services program with 7th Dimension, you can rest assured that your servers and computers are being updated with the latest patches. 7th Dimension is following proper guidance released by all manufacturers, deploying patches and updates within our own IT infrastructure in line with best security practices.

What's Next

Many issues and caveats have become known with the new patches being released for all devices so there is likely much **more to come**. For example, Intel released patches that caused reboot problems for older processors, whereas updates for computers with newer chips caused frequent reboots. System performance has also been affected by patches, causing slowdowns up to 25 percent. For now, the best course of action is to carefully test and implement updates as they become available, and to above all, remain calm.

How to Avoid Runaway IT Projects That Empty Your Wallet

These tips will help your 2018 projects stay on track.

Page 2

Does This Password Sound Familiar?

Avoid these common passwords for added security.

Page 3

How to Avoid Runaway IT Projects That Empty Your Wallet

In 2002, McDonald's implemented a system to track, measure and monitor everything from profitability to cooking-oil quality in their 30,000 stores. "Innovate" was a massive five-year project with a billion-dollar budget.

Two years in, McDonald's abandoned the project and wrote off the $170 million invested to reduce capital expenditures. Even though YOUR business isn't McDonald's with a billion-dollar IT budget, chances are you've had at least one failed IT project that derailed and emptied your wallet. Here are four key strategies to keep you on track:

1. Begin with the end in mind. The clearer you are on what "success" is the more likely you are to achieve it. Sit down with your executive team and decide exactly what the new system LOOKS like, how it performs, what it does and how it works.

2. IT projects need to be driven by an executive who understands the business need and outcome, NOT the IT department. If you and your executive team aren't going to be heavily involved with the process, decisions and management of the project, don't start it.

3. Think in smaller, "bite-sized" projects. One of the problems with the McDonald's project was that it was so complex, affected multiple business systems and had such an enormous scope, it was almost guaranteed to fail. If you have a major system to build or overhaul, break it into smaller, manageable chunks so that problems are contained and costs controlled.

4. Manage the project hours. Scope creep is the biggest challenge to keeping your project on time and on budget. If your project starts to take on a life of its own and goes over your budgeted time frame and your budget by more than 10%, it's time to start re-evaluating what's going on. Excessive overtime is a red flag that the project was not thought through properly, that you have the wrong team working on it or that it's being grossly mismanaged. Don't ignore it.

HAVE A PROJECT IN MIND?
CALL US AT (916) 221-0855
FOR A FREE CONSULTATION

That Fake App Just Stole Your ID

In case you weren't aware, one of the latest and most dangerous Internet scams is fake apps. Scammers create apps that look and behave like a real app from a legitimate store. These fake apps can infect your phone or tablet and steal confidential information, including bank account and credit card details. They may also secretly install on your device malicious code that can spread, including to your company network.

Take a moment and reflect on these five tips before downloading any app:

1. *When in doubt, check it out.* Ask other users before downloading. Visit the store's main website to see if it's mentioned. Find out from customer support if it's the real McCoy.
2. If you do decide to download an app, first *check reviews*.
3. *Never click an e-mail link* to download an app. Get it from the retailer's website or iTunes.
4. Offer as little of your *information* as possible if you decide to use an app.
5. *Think twice* before linking your credit card to any app.

Most importantly, get professional help to keep your network safe. It really is a jungle out there. New cyberscams, malware and other types of network security threats are cropping up every day. You have more important things to do than to try and keep up with them all.

Keep Your Network Safe

Don't let your company become another statistic. Call us (916) 221-0855.

Does This Password Sound Familiar?

You know the difference between a good password and a bad one. Many of us do like the convenience of a simple, easy-to-remember password that requires no effort to recall and type when we connect to our WiFi network, buy from our favorite e-tailer or use for online bill pay. But many of us also appreciate an added layer of security so we don't use an effortless password when sensitive data is on the line.

In a recent study conducted by SplashData, they looked at a sampling of over 3 million passwords (all of which were leaked during a data breach last year). They compiled a list of the most common passwords—and the results weren't all that surprising. 123456 was the No. 1 password used last year, followed by the classic "password".

While these passwords may have the IT and security crowds shaking their heads in dismay, it's not all bad news. These popular passwords may offer next to no practical security, but according to the study, the 25 most common passwords only represent about 2% of the overall total.

This means most people don't use these passwords—or qwerty, or 111111, or iloveyou. The study found more variation among the most popular passwords versus the 2013 study. Is it a possible trend? Are people turning to more imaginative or secure passwords? Maybe, but only time will tell. Even if the study suggests most of us don't rely on overly simple passwords, SplashData's list serves as a reminder to use more secure passwords and to change them regularly.

Unsure if your passwords and password lockout policies are up to date? Is your password information for sale on the Dark Web? Call us at (916) 221-0855 to schedule a Dimensional Dark Web Scan and Password Security Audit.

7TH DIMENSION

IT without limits

5005 Windplay Drive, Suite 1, El Dorado Hills, CA 95762
(916) 221-0855
support@7thdi.com

We love having you as a customer, and quite honestly, we wish we had more like you!

Simply refer any company and earn up to $100 when your referral becomes our client.