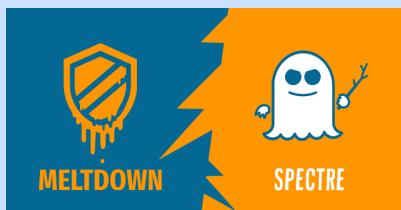## Cybersecurity Alert:
Meltdown & Spectre

Your smartphone or computer contains a chip that hackers can exploit to get access to sensitive information. Are you protected?

Visit
www.palmtech.net/meltdown/
for more information!
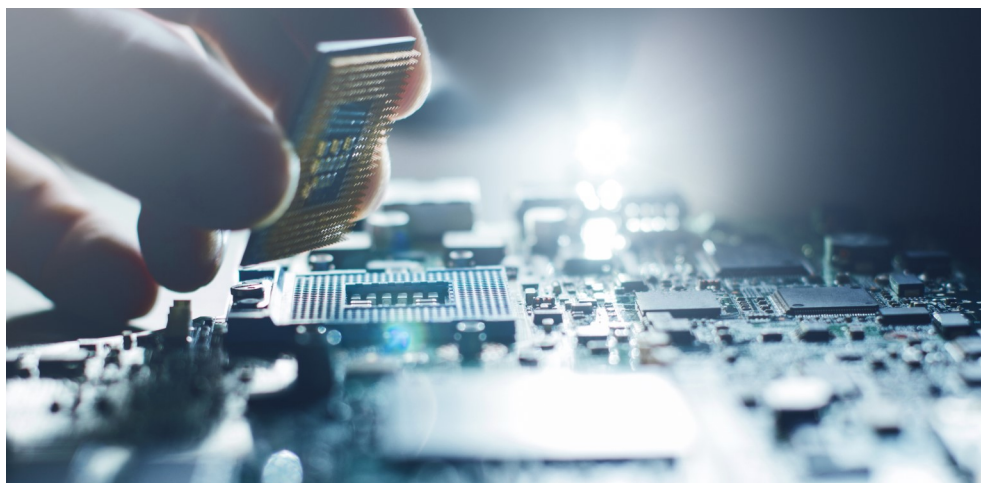

MELTDOWN   SPECTRE

January 2018

This monthly publication provided courtesy of Chuck Poole, President of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

Do You Really Want The Cheapest Computer Technician Working On Your Company's Network?

These days, small businesses are more dependent on IT systems than at any other time in history. Because of this, even the slightest technological hiccups in our cyberspace-centered workflow can have expensive, lasting consequences. Perhaps the most dramatic illustration of this occurred back in 2013, when Amazon went dark for half an hour. Sure, it was a paltry 30 minutes, no big deal, until you consider the megagiant was theoretically hemorrhaging $66,240 every 60 seconds, based on their quarterly revenue.

Of course, your company probably isn't a staple of international commerce like Jeff Bezos' beloved brainchild. Because of this, many small business owners think that a downed server or small security breach here and there won't matter too much for their bottom line. For these unlucky few, IT takes a backseat to more "pressing" issues, and they go

the cheap route with their technicians. This cost-cutting solution seems like the idea of the year, and will undoubtedly work great for the business — until it doesn't.

Maybe your long-time technicians fail to notice a piece of outdated equipment, and your server gives up the ghost during peak business hours. Virtually all work grinds to a halt, and your employees are forced to wile away the two hours shooting three-pointers into the trash bins. Add up the two hours of wasted wages for your entire team, the financial cost of missed business, and the much more intangible loss of customer goodwill as they struggle with diminished service on a workday, and you'll come up with a sum that disabuses any business owner of their illusions about "cheap" IT.

And that's not even close to the worst-case scenario. Imagine, for a minute, that your technicians assure you,

Get More Free Tips, Tools and Services At Our Web Site: www.PalmTech.net
(561) 969-1616

despite the lack of regular monitoring and maintenance, your network is secure. These words of comfort sound nice until the day a team of expert hackers actually attempt to access your systems, and find outdated, ramshackle security solutions in place — basically, a front door left wide open. At that moment, your business becomes a criminal's playground. They're free to access financial information and personal data of your customers and employees, hijack your business to send out floods of malicious software and spam, hold nearly every aspect of the company ransom for thousands of dollars, and cause chaos to their hearts' content.

The fact is, fixing problems is a lot more expensive than preventing them. When you cut corners and utilize subpar IT professionals (if any at all), you're paying for an array of shoddy, Band-Aid solutions that will be applied piecemeal, and usually too late, like a finger plugging a hole in a dam. But when you make a substantial investment in your IT support, you're

> **"These words of comfort sound nice until the day a team of expert hackers actually attempt to access your systems, and find outdated, ramshackle security solutions in place — basically, a front door left wide open."**

investing in the most basic aspects of the future of your company.

Robust network security, dependable computers and servers, consistent internet access, and other fundamental components of your company network are far from luxury items. These days, technology forms the scaffolding upon which businesses run. If any piece of the operation fails, the whole system suffers, usually accompanied by a fat financial penalty.

There is an ever-growing, endless list of potential technological pitfalls that can have permanent consequences for your business: teams of hackers zeroing in on vulnerable small businesses, rogue employees with a grudge, lost laptops, aging and unreliable hardware, fire, natural disasters, and IT "professionals" that have no idea what they're doing, to name just a few. As technology progresses, and companies depend increasingly more on it to stay competitive, it simply doesn't make sense to relegate IT to the neglected corners of your budget.

When it comes to business, there's a lot to worry about these days. A total collapse of your company's technological infrastructure doesn't need to be one of them. Invest in a robust, managed IT package from tried-and-tested professionals, and leave the worrying to the experts. You can rest assured that our IT team of experts truly has you covered. Contact us at **(561)969-1616** or at info@palmtech.net for more information.
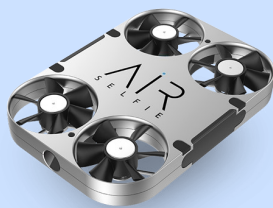
The Risks Of Auto Complete Passwords

If you're disturbed by advertisements and "helpful" suggestions that are based on your internet browsing habits, recent research has found yet another source of online tracking. It's a sneaky tactic that also comes with serious security concerns. Let's take a look at what you can do to stop it from targeting you.

Why auto-fill passwords are so dangerous

In 2015, the average internet user had 90 online accounts, a number that has undoubtedly grown since then. This has forced users to create dozens of passwords, sometimes because they want to practice healthy security habits and other times because the platforms they're using have different password requirements.

Web browsers and password manager applications addressed this account overload by allowing usernames and passwords to be automatically entered into a web form, eliminating the need for users to hunt down the right credentials before logging in.

The process of tricking a browser or password manager into giving up this saved information is incredibly simple. All it takes is an invisible form placed on a compromised webpage to collect users' login information without them knowing.

Using auto-fill to track users

Stealing passwords with this strategy has been a tug-of-war between hackers and security professionals for over a decade. However, it has recently come to light that digital marketers are also using this tactic to track users.

Two groups, AdThink and OnAudience, have been placing these invisible login forms on websites as a way to track which sites users visit. These marketers made no attempts to steal passwords, but security professionals said it wouldn't have been hard to accomplish. AdThink and OnAudience simply tracked people based on the usernames in hidden auto-fill forms and sold that information to advertisers.

One simple security tip for today

Turn off auto-fill in your web browser. It's quick, easy, and will go to great lengths to improve your account security.

If you use Chrome - Open the Settings window, click Advanced, and select the appropriate settings under Manage Passwords

If you use Firefox - Open the Options window, click Privacy, and under the History heading select "Firefox will: Use custom settings for history." In the new window, disable "Remember search and form history."

If you use Safari - Open the Preferences window, select the Auto-fill tab, and turn off all the features related to usernames and passwords.

This is just one small thing you can do to keep your accounts and the information they contain safe. For managed, 24x7 cybersecurity assistance that goes far beyond protecting your privacy, call us today at (561)969-1616.
www.Techadvisory.org

The No. 1 Most Important Word In Business, Which You Rarely Hear

Recently, a video podcaster named Nina asked me a simple question with complicated implications: "What's the most important mindset for success in business?"

At first, I doubted that I'd be able to identify a single mindset that was key to success. Ordinarily, my team and I emphasize the importance of context. Usually, it depends on a leader fitting a given situation, which has many variables that are difficult to reduce to a single answer.

That said, I realized there was one common mindset that I had observed in the many successful clients I've advised over the years — one severely lacking in those that continuously struggled. And not just casually, either. My firm has formally conducted over 17,000 in-depth interviews of leaders from all over the world, so we get to see which behaviors work in a variety of situations and which don't.

I realized the single most important word in business, a word that you rarely ever hear, is generosity.

No, not honesty, kindness, respect, learning, empathy or even abundance. None of those things actually force you to be a proactive agent of change. Leaders who succeed are generous, and they treat people — whether they're customers, employees, shareholders or members of the community — with a fundamental mindset centered around that generosity. Those that lack the spirit of generosity never succeed in the long term.

Once when I was speaking with the CEO of a mortgage company, I almost immediately got a bad feeling about his character. He implied that his business succeeded by "tricking" low-income homeowners into signing up for mortgages that had hidden terms unfavorable to them. Well, of course, that mindset backfired. When the housing crisis hit in '08, his company and career were snuffed out under a pile of lawsuits.

In contrast, I remember being impressed early in my career by the mindset of a self-made billionaire named Ted Waitt — the owner of Gateway, that old computer company. When asked about his success, Ted talked about making computers, which were scary for most people at the time, more friendly and fun. Ted loved making technology less stressful for customers, giving good people good value for their dollar, an enjoyable buying experience and just generally being eager to make lives better through his products.

There are dozens of such examples, both of selfish business owners getting their comeuppance, and generous ones being rewarded with abundant success and positivity. If you can spread a spirit of generosity throughout your team, you'll see the benefits immediately.

Geoff Smart is Chairman and Founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book Who: The A Method for Hiring and the author of the #1 Wall Street Journal best-seller Leadocracy: Hiring More Great Leaders (Like You) into Government. Geoff co-created the Topgrading brand of talent management. Geoff is the Founder of two 501c3 not-for-profit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in Economics with Honors from Northwestern University, an MA, and a PhD. in Psychology from Claremont Graduate University.

© MARK ANDERSON   WWW.ANDERTOONS.COM

"Say what you want, that's good drama."