Mobile Device Security & Virtualization

Securing mobile devices is incredibly difficult. They often have privileged access to sensitive data that they connect to via unprotected network connections. Virtualization vendors are finding ways to include solutions to these problems in their products and they're perfect for small businesses.

Read More at:
www.palmtech.net/secure-device/

PALMTECH
I.T. SOLUTIONS FOR BUSINESS

November 2017

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.

How The Cloud Could Have Averted Disaster For Hundreds Of Companies Affected By These Catastrophes

Two months after hurricanes Harvey and Irma wreaked havoc on coastal cities, large swaths of the United States are still reeling from their impact. In their wake, the nation has been moved as we witness numerous communities unite to rebuild, finding their bearings among the millions of dollars of flooding damage and rampant destruction. Though the wonderful people of these cities will persevere, these wounds will leave indelible scars on the affected areas.

Even with the concerted efforts of thousands of volunteers and community members alike, Russel Honore — the former Joint Task Force Katrina commander — told the FOX Business Network that an estimated "40% of small businesses don't survive" widespread natural disasters like hurricanes. Part of this is due to raw damage, lack of proper insurance or business infrastructure

simply being washed away in the flood. Other businesses can't afford to hemorrhage money as they wait for the electricity grid to come back online, and are forced to shutter operations for good.

However, what is even more commonly fatal to companies both big and small is the loss of vital data. Many businesses can handle cleaning up flood damage, and they regain their footing quickly after a natural disaster. Still, if on-site servers, computers or network infrastructure soaks up the brunt of the water, then it's going to be difficult, if not impossible, to get the company back to a pre-disaster point. If a company's main server fails, it can mean thousands of hours of hard work down the drain, the loss of most clientele and hundreds of hours of downtime spent desperately trying to recover key data, which usually

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

remains lost forever. But if, prior to catastrophe, a business has migrated their precious data to the cloud, they're going to have a much easier time getting back on their feet and going straight to work. Even if an entire business is leveled, with cloud computing, employees can easily access the data central to the company's operation and keep it afloat in the interim.

Most cloud services back up your data with several levels of redundancy, making it almost impossible to lose it all, regardless of what may come. Whether it's earthquakes, hurricanes or solar flares, you can rest easy knowing that your data is safe and sound and ready for you to access it. It's a much safer, more secure way to go than having a server lurking in your back office, where it's far more exposed than you might think.

This principle applies not only to environmental disasters, but to numerous other ways companies lose data each and every day. Whether it's a disgruntled employee damaging or stealing precious data, or a hacker snaking their way deep into your systems and holding them for ransom, it's all too easy to lose localized data. Some business owners feel

> **"The cloud sidesteps these concerns almost entirely, guarding your data behind highly secure cloud-based computing solutions and providing you with numerous backup options."**

uncomfortable holding their data off-site, citing security concerns, but it's quite the opposite: the cloud sidesteps these concerns almost entirely, guarding your data behind highly secure cloud-based computing solutions and providing you with numerous backup options. Not to mention, according to a 2012 Alert Logic report, "on-premises environment users actually suffer more incidents" than those that use the cloud, and also suffer "significantly more brute force attacks compared to their counterparts."

While it's true that not every business is right for the cloud, it's certainly something business owners should look into if they want to ensure the longevity of their company. If you're interested, sign up to get our free cloud computing report at www.palmtech.net/cloud-report/.

Shiny New Gadget Of The Month:

Security Cameras Just Got Cheaper

The average American household is packed to the gills with expensive electronic equipment and a startling amalgamation of pricey knickknacks, so investing in home security is an attractive investment. And these days, you don't have to shell out a sum equal to the stuff you're protecting to get peace of mind.

Take the Kodak 180-degree Panoramic HD WiFi Security Camera, for example, a high-end security camera you can pick up right now for just under 70 bucks (regularly priced at $149.99). Place the camera anywhere in your house, and it'll automatically record motion-triggered video clips straight to the cloud with its 180-degree lens, accessible on any Internet-enabled device. The camera uses wide dynamic range to automatically adapt to changes in lighting, ensuring that it doesn't miss a thing. Perhaps best of all, you can check in on the camera's feed at any time, streaming its HD video straight to your phone or computer.

Disrupt Yourself: Being The Game Changer

Change is a constant. Ho-hum, right? Everybody knows that. But, if you really do expect change, what are you actually going to do about it?

If you're committed to making your best even better, you won't just react to change. You'll create it.

In my book The Potential Principle, I encourage readers who want to reach their best to focus on four areas of the Potential Matrix: the performing quadrant, the learning quadrant, the thinking quadrant, and the reflecting quadrant. But there's one tool that you can use in all of these areas at once to create breakthrough improvement and move closer toward realizing your full potential. The first tool is **to disrupt yourself before someone or something else does it for you.**

If change hits you from some outside source — say, a disruptive technology, company or nation — you'll find yourself scrambling to adapt. You'll struggle to catch up rather than strive to stay ahead.

But what if you're the one bringing the change? What if you're the one driving innovation? That makes you the game changer!

Think about the habits, practices and routines in your life that need to be shaken up a bit. It's human nature to become complacent and keep doing things the way you've always done them. But people who are dedicated to self-improvement unsettle complacency, combat mediocrity and challenge the status quo, both in themselves and in those around them. They keep growing, and they keep the people in their families and companies growing as well.

Are you doing things that used to succeed but no longer work as well, if at all? Are you spending valuable time on unproductive activities when that time could be better invested elsewhere?

What is the ratio between your "daydreaming" and your "daily doing?" You can plan and prepare too much if it prevents you from taking action. And sometimes, it's good to recognize that a daydream is really just a fantasy, and you'd be better off focusing your energy on more important goals.

Maybe you're spinning your wheels in unhealthy relationships. This can be the hardest area of your life to disrupt. But if someone is influencing you negatively, you might need to change, limit or end your relationship with them.

Disrupting yourself will make you stronger. The path to progress and success isn't a leisurely walk through the countryside. It's a rocky, steep path of resistance — and resistance develops muscle. Breaking up patterns and unsettling stable but humdrum practices can result in new enthusiasm, energy and opportunities.

If you want to be the best you can be, don't let someone or something else change your game. Be proactive and disrupt the things that need to change in your life yourself.

Mark Sanborn, CSP, CPAE, is the president of Sanborn & Associates, Inc., an "idea studio" that seeks to motivate and develop leaders in and outside of business. He's the bestselling author of books like Fred Factor and The Potential Principle and a noted expert on leadership, team building, customer service and company change. He holds the Certified Speaking Professional designation from the National Speakers Association and is a member of the Speaker Hall of Fame. Check out any of his excellent books, his video series, "Team Building: How to Motivate and Manage People" or his website, marksanborn.com, to learn more.

Secure Your Passwords Now
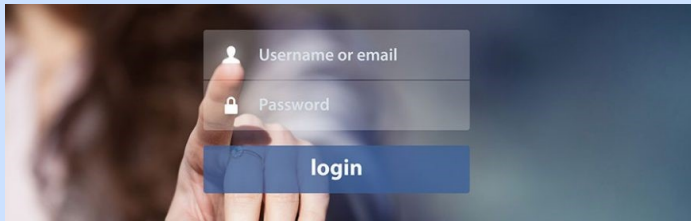
For years, we've been told that strong passwords include three things: upper and lower-case letters, numbers, and symbols. And why wouldn't we when the National Institute of Standards and Technology (NIST) told us they were the minimum for robust passwords? Here's why and how it involves you.

The problem

The issue isn't necessarily that NIST advised people to create passwords that are easy to crack, but it did steer people into creating lazy passwords, using capitalization, special characters, and numbers that are easy to predict, like "P@ssW0rd1."

This may seem secure, but in reality, these strings of characters and numbers could easily be compromised by hackers using common algorithms.

To make matters worse, NIST also recommended that people change their passwords regularly, but did not define what it actually means to "change" them. Since people thought their passwords were already secure with special characters, most only added one number or symbol.

NIST essentially forced everyone, including you and your colleagues, to use passwords that are hard for humans to remember but easy for computers to guess.

The solution

One cartoonist pointed out just how ridiculous NIST's best practices were when he revealed that a password like "Tr0ub4dor&3" could be cracked in only three days while a password like "correcthorsebatterystaple" would take about 550 years.
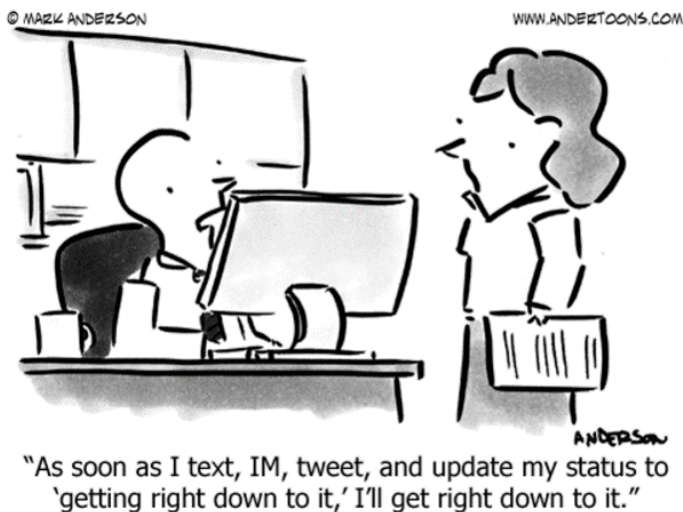
Simply put, passwords should be longer and include nonsensical phrases and English words that make it almost impossible for an automated system to make sense of.

Even better, you should enforce the following security solutions within your company:

♦ Multi-factor Authentication - which only grants access after you have successfully presented several pieces of evidence

♦ Single Sign-On - which allows users to securely access multiple accounts with one set of credentials

♦ Account Monitoring Tools - which recognize suspicious activity and lock out hackers

When it comes to security, ignorance is the biggest threat. If you'd like to learn about what else you can do to fortify security, just give us a call at (561)969-1616.

--TechAdvisory.org

"As soon as I text, IM, tweet, and update my status to 'getting right down to it,' I'll get right down to it."

"We must find the time to stop and thank the people who make a difference in our lives." -- John F. Kennedy

Our team at PalmTech Computer Solutions would like to express how grateful we are to our clients, associates, and friends. We wish you a peaceful Thanksgiving holiday.