PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions
September 2016

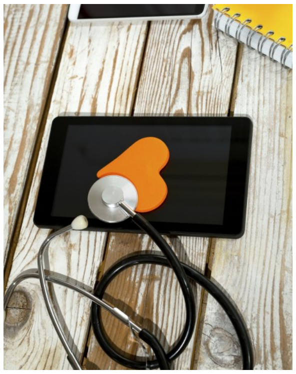
Inside this Issue:

September 2016

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.



Go Mobile - Without Killing Your Data

What if you could tap into the top talent in your industry, no matter where in the world they are? With the power of the mobile web, your all-star team is now – literally – at your fingertips.

Consider this: 83% of workers report that they prefer using cloud apps over those deployed on-premise. Millennials, who will make up almost 50% of the available workforce by 2020, are "digital natives." And don't forget how much money remote workers allow you to save on real estate and office equipment.

Yet there are risks. Spreading your network around the world on a variety of devices you don't control can expose your data in more ways than ever before. The key is to find the right balance between protection and productivity. Here, then, are five ways to effectively "mobilize" your workforce – without endangering your data:

Collaborate In The Cloud – A plethora of online collaboration tools have sprung up that make it easy for a geographically dispersed team to access and share the same files in real time. These tools not only make sharing easy and instantaneous, they help your team communicate quickly and effectively. Tools like Slack, HipChat, Asana, Podio and Trello – to mention just a few of the most popular options – are proving to make teams more productive. And that includes keeping critical data safe and secure.

Expand Elastically – In-house investments in IT hardware, software and staff can lock you into a rigid structure that can't easily adapt to changes in demand. A cloud-based mobile workforce is able to contract and expand more easily as needs arise, and with very little loss of capital. Bottom line: use a VPN (virtual private network) and cloud-based collaboration tools to remain agile, flexible and competitive.

continued on page 2

Cut Costs Dramatically – Physical work areas, equipment, software and on-site security expenses can add up. Instead of spending money on office space, equipment and infrastructure, invest it in innovation and refinement. Combine the power of the cloud with a well-designed workflow to reduce the number of people needed to get things done. That will free up your key players to focus on more important tasks – the ones that boost productivity and ROI.

> *"Doing nothing simply makes you a sitting duck for a cyber-attack."*

Deal With BYOD – Let's face it, BYOD (bring your own device) can be your greatest IT security threat. Yet, like it or not, workers will use their own devices on the job. Foisting strict controls without buy-in will just backfire. Yet doing nothing simply makes you a sitting duck for a cyber-attack. Solution? First, audit how your employees use their devices. Note the data they access and the apps they rely on. Group them by the levels of security and compliance they need to be governed by. A CEO, for example, may need to abide by financial regulations. An HR manager must deal with employment laws. Armed with information from your audit, you can roll out new policies as well as technical and process controls. Train your team in safe practices. And be sure to contact us for help in getting all this done securely and effectively.

Go Remote Without Risk – Whether you want to cut commuting time for your team, tap into the talents of experts outside your locale or simply accommodate a worker caring for family members, mobilizing your workforce can have big benefits. The trick is defending it at all points. Make sure remote workers share files and communicate with other employees only via a secured network. Make sure they use adequate virus protection. And, if they are using WiFi, either at home or on the road, make sure they do it safely. For instance, ensure that their tablet isn't set to automatically connect to the default wireless network. That's often an easy access point for hackers.

Free Mobile Risk Assessment – Limited Time Only!
To help you manage a mobile workforce without endangering your data, we're giving away a Free Mobile Risk Assessment, **normally valued at over $300**, to the first 10 companies who request it by October 7th. E-mail me at info@palmtech.net or **call us at (561)969-1616** to set yours up today. It's your best bet for keeping ahead of the competition – while keeping your company's data safe and secure.

**Offer valid to qualified prospective clients with 10 or more computers and a minimum of 1 server.*

FREE HIPAA TRAINING FOR YOUR STAFF

Take the next step toward HIPAA compliance with FREE HIPAA Training for you and your staff courtesy of PalmTech! Any Medical Office, Law Firm, or Corporation that handles medical records MUST take steps to have all of their employees trained as part of a comprehensive HIPAA compliance strategy. PalmTech has reached an agreement with our HIPAA auditing partner to provide access to their computer-based video training material free for 30 days – plenty of time to get your whole team through the program. Your staff will also be tested and given a HIPAA Certificate upon successful completion of the training course. Call our sales team at (561)969-1616 or email sales@palmtech.net to get your training portal set up today.

Shiny New Gadget Of The Month:

FitBark Keeps You And Your Dog Healthy

Do you know how well your dog slept last night? How much nutrition – or exercise – your dog really needs? Whether your pup is being well-cared for at doggy day care?

With FitBark you would know all this, and more, about your favorite canine pal.

Doggy health monitors are nothing new. But, according to hundreds of verified reviews on Amazon, Best Buy, App Store and Google Play, FitBark leads the pack.

FitBark attaches to your dog's collar and shares data with FitBark Explore, a dog health data bank that collaborates with over 20 leading universities and research institutions in North America and Europe to gain a better understanding of dog health.

You benefit from all this data by tapping into what FitBark calls truly unprecedented insights into canine health and data. All toward keeping Fido – and you – on the path to health and happiness.

$59.95 at Fitbark.com.

How To Stop Ransomware Before It Strikes

Ransomware is a type of malware (like a virus) that blocks access to a computer system or even an entire network unless you pay a sum of money to the malware's author. Here are PalmTech's top tips for foiling these extortionists before they strike:

- Reassess Your Current Antivirus Protection and Next-Generation Security Layers for Maximum Protection.
  - √ Having endpoint security that prevents malware infections in the first place is vital.
  - √ Look for security that protects web browsing, controls outbound traffic, guards system settings, proactively stops phishing attacks, and continuously monitors individual endpoints.
- Implement and Regularly Audit Backup and Business Continuity Recovery.
  - √ If there is a crypto-ransomware infection, then the only recourse is to recover data and minimize business downtime.
  - √ Use redundant on premise and cloud-based backup and continuity solutions, and regularly confirm that these systems are functioning.
  - √ Business continuity also means minimal downtime so business can quickly return to normal without disrupting client services.
- Control Plugins and Create Strong Windows Policies
  - √ Generally speaking, if certain plugins are not used, it's better not to have them installed. If they are being used, make sure they are up to date (for example, do not disable automatic Java updates).
  - √ Windows Policies can block certain paths and file extensions from running. Policies can be set up in groups, which is useful if varying levels of access are required.
- Educate Users
  - √ As always with security, users are often the weakest link.
  - √ Malware will continue to thrive and be a viable business as long as staff is unaware and uneducated on the risks of the Internet.
  - √ It is critical to stay abreast of the current and future threat landscape. If you're not staying current, you've already lost the battle.
  - √ Continuous user education is required to avoid being easy prey. Ensure your staff is trained on how to handle and kept updated on the constantly evolving and shifting cyber-attacks and scams.

Don't wait until after disaster strikes! Schedule your ***FREE Security Assessment today** by calling us at **(561)969-1616** or email us at info@palmtech.net!

**Offer valid to qualified prospective clients with 10 or more computers and a minimum of 1 server.*

Business Email Compromise: The Threat of Sophisticated Attacks

Hacking into "secure", corporate email systems has recently become a lucrative business. To date, business email systems that have been compromised have caused companies worldwide to lose over 2 billion dollars. Due to the success of these scams, that number only continues to rise.

This type of email breach is more sophisticated than the scam emails users click on that implant a virus. The scheme is designed to have employees wire money to bogus accounts. Many of these emails are created by impersonating key personnel and doing it well. They are socially adept, making them difficult for the regular person to detect. In one example, a CEO was fired after cyber attackers imitated him in an email that lost the company $47 million.

How is it possible for an email scam to cause so much damage? For a cyber attack of this magnitude to be successful, the culprit has to spend quite a bit of time learning about the business they're targeting and its executives. They are able to gain access to email accounts and spend time studying how the targeted person communicates and the business' financial policies. When they have mastered the language and nuances necessary to avoid detection, the fake email is sent.

Three different types of emails used in these particular schemes have been identified. The first is a false invoice email. With this email, the scammers request a payment location change to a fraudulent account. The next type of scam is CEO fraud. In this fraud scheme, an email is crafted as being from the CEO, president, managing director, etc., requesting that an urgent transfer be made to a fake account. The third type of email scam is an account compromise where an employee's email account is used to request payments from vendors found in the contacts list. With each of these scams, detection is made difficult because of the time spent learning the language used by each victim.

If business email compromises are so successful, how can you protect yourself from them? The best way is to look at the processes involved in monetary actions. Does an employee need more verification than just an email to transfer money to different accounts? If not, then a second validation of payments needs to be made mandatory to keep employees from receiving what they perceive as a valid request, and losing the business thousands of dollars. Employee education will raise awareness of business email compromise. Ensure your staff reports all successful hacks and any suspicious activity. These simple steps could be what saves you from becoming a victim.

Business email compromise is a sophisticated email scam plaguing businesses worldwide. Billions have been lost already but your company does not have to join those who have already lost. Mindfulness and education could be the route to preservation for your business.

Allow PalmTech to assist in not only ensuring that your network is secure, but that your staff is kept abreast of the latest cyberthreats as well as the processes that should take place when faced with a scam. Contact us at info@palmtech.net about obtaining a CyberSecurity Consultation & Assessment by September 30th FOR FREE!

Win Free Coffee and an iPad!

Don't Keep Us a Secret!
Recommend PalmTech to Your Professional Contacts.

Details here:
Www.PalmTech.net/referral-program/

© MARK ANDERSON, WWW.ANDERTOONS.COM

"So our project has been greenlit. But since we're dogs I don't know what that means."