Start 2017 Right With…

FREE HIPAA TRAINING FOR YOU AND YOUR STAFF IF YOU ACT NOW!

Visit www.palmtech.net/Free-HIPAA/ for details!

2017

January 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.

3 "Must-Do" IT Resolutions For 2017

"Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today." That's what *The Evolution of Ransomware*, a study by Mountain View, California-based cybersecurity firm Symantec, reported recently.

If you have any illusions that your company is safe from cyber-attack in 2017, consider just a few findings stated in a recent report by the Herjavec Group, a global information security firm:

- Every second, 12 people online become a victim of cybercrime, totalling more than 1 million victims around the world every day.
- Nearly half of all cyber-attacks globally last year were committed against small businesses.
- Ransomware attacks rose more than an astonishing 300% in 2016.
- The world's cyber-attack surface will grow an order of magnitude larger between now and 2021.
- The US has declared a national emergency to deal with the cyberthreat.
- There is no effective law enforcement for financial cybercrime today.

Clearly, your company's information and financial well-being are at greater risk than ever in 2017. And you cannot count on the federal or state government or local police to protect your interests. That's why I STRONGLY SUGGEST that you implement the following resolutions starting **TODAY.**

Resolution #1: Tune up your backup and recovery system. The #1 antidote to a ransomware attack is an up-to-date backup copy of all your data and software. Yet managing backups takes more than just storing a daily copy of your data. For one thing, if your business is at all typical, the amount of data you store grows by 35% or more PER YEAR. If your data

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

management budget doesn't expand likewise, expect trouble.

Resolution #2: Harness the power of the cloud—but watch your back.
Huge productivity gains and reduced costs can be achieved by making full use of the cloud. Yet it's a double-edged sword. Any oversight in security practices can lead to a breach. Here are two things you can do to harness the cloud safely:

> *"Not all cloud vendors are the same."*

- *Determine which data matters.* Some data sets are more crucial to your business than others. Prioritize what must be protected. Trying to protect everything can take focus and resources away from protecting data such as bank account information, customer data and information that must be handled with compliance and regulatory requirements in mind.

- *Select cloud providers carefully.* Cloud vendors know that data security is vital to your business

and promote that fact. Yet not all cloud vendors are the same. You can't control what happens to your data once it's in the cloud, but you can control who's managing it for you.

Resolution #3: Set and enforce a strict Mobile Device Policy. As BYOD becomes the norm, mobile devices open gaping holes in your network's defenses. Don't miss any of these three crucial steps:

- *Require that users agree with acceptable-use terms before connecting to your network.* Be sure to include terms like required use of hard-to-crack passwords, conditions under which company data may be "wiped" and auto-locking after periods of inactivity.

- *Install a Mobile Device Management System on all connected devices.* A good system creates a virtual wall between personal and company data. It lets you impose security measures, and it protects user privacy by limiting company access to work data only.

- *Establish a strong protocol for when a connected device is lost or stolen.* Make sure features that allow device owners to locate, lock or wipe (destroy) all data on the phone are preset in advance. That way, the user can be instructed to follow your protocol when their phone is lost or stolen.

Free Network And Security Audit Resolves Your Biggest Data Security Problems and Makes Your Systems Run Like A Fancy Swiss Watch

Ever asked yourself why some business owners and CEOs seem so blithely unconcerned about data protection? Don't let their ignorance lull you into a false sense of security. If you've read this far, you are smart enough to be concerned.

Call us right now at (561)969-1616 and we'll send one of our top network security experts over for a FREE Network and Security Audit. It's your best first step to a safe and prosperous 2017.

*Offer valid to qualified prospects with 15 or more computers and a minimum of 1 server.

PalmTech's Tidbits

Here's an easy way to start 2017 with a clean e-mail in-box.
Ever wonder how in the world you ended up on so many e-mail lists? They just pile up until you can't even keep up with unsubscribing from the new ones. Unroll.me lets you manage your subscriptions by unsubscribing and bundling the ones you want to keep into a single daily "rollup." It makes unsubscribing easy and painless. It simply lists all your subscriptions for you. You just click an X next to

the ones you want to unsubscribe from and Unroll.me takes care of the rest. It's a great way to organize your in-box while keeping all the subscriptions you love.
–Lifewire.com

Imagine your team, smarter and faster in 2017.
Unlike project collaboration platforms, Asana is an app that specializes in workflow management. While it doesn't give

you Gantt charts and billing information, it's one of the best tools you'll find to keep track of the daily to-do's of your business, while giving employees a more productive workspace than e-mails to track job progress. It's web-based and sports a free mobile app for iPhone and Android. And it also lets you work offline. Asana works best when one person envisions how it will work and then sets it up that way. This can be a powerful work tool.

Shiny New Gadget Of The Month:

New Nintendo Classic Rules Them All!

For anyone in their late 20s to early 40s, chances are nothing shaped your life more than Nintendo. If it was your first "gadget," if may even have been love at first sight.

And now, for Nintendo lovers, the Nintendo Entertainment System is back and better than ever with the NES Classic Edition. It's tiny, but designed to look just like the original NES. Setup is a snap. Just plug it into your TV's USB port. Hit the power button and you're greeted with a screen where you can browse games and options. You can even select a CRT filter that replicates the lines and look of an old TV.

The color is sharp, the timing dead on and each pixel is a perfect square so you see the games exactly as designed. At 60 bucks, it's a great gift for your favorite millennial (maybe even YOU!).
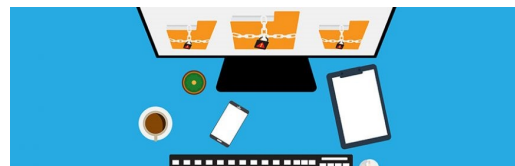
New Ransomware Demand Sacrifice

It's scary to think you can be simply browsing the Internet when WHAM! a screen pops up out of nowhere claiming that you have been hijacked and will need to pay a bitcoin to free your computer. Unfortunately, ransomware like this is not uncommon. But now there's a new, more devastating virus that asks victims to pick other victims to replace them in order to get their computer information back safely. Read on to find out how Popcorn Time is turning the ransom game on its head -- and how you can protect yourself from it.

Ransomware is nothing new. Cybersecurity miscreants have been taking advantage of online users for years by requiring payment to "unlock" a victim's computer. What Popcorn Time does differently is give users the option to spread the virus to two other victims in the hopes that they will pay the ransom -- a tactic that promises to double their money at the expense of your sense of morality (and at the expense of your friendships as well).

The Cost of Popcorn

When you inadvertently download this ransomware, you will be met with a screen that explains that your files have been hijacked/encrypted, and that to get them back you will need to pay one Bitcoin for a decryption key that they keep stored remotely. The Bitcoin fee is usually more than $700, a hefty price to pay during any season but particularly difficult for those infected following the holiday season.

Spread the "Holiday Cheer" and Hope they Bite

What makes Popcorn Time unique is the option victims have to take their cost away by allowing the ransomware to affect two of their friends for a chance to get a free decryption code. Of course, it works only if both friends pay the ransom, which leaves you looking (and feeling) like the Grinch.

Avoiding Popcorn Time this Season

The easiest way to avoid downloading ransomware is to stay off of sites that might contain questionable files. However, this is nearly impossible for modern users, and many hackers are getting good at making their files look legitimate. Limit your exposure to potential ransomware by keeping your software up-to-date and your computer protected with a security program from a reputable company (for example Norton or Symantec). If you need to learn more about how to avoid running into ransomware while you're online, give our professional cybersecurity consultants a call at (561)969-1616. We'll keep you away from the popcorn this season.

Techadvisory.org

© MARK ANDERSON, WWW.ANDERTOONS.COM

"I just got an app that shows me all the invisible fences in the neighborhood. Wanna go have some fun?"

Smart Closing Technique, Step 1

It's one thing to help a client identify a problem. It's another thing to help them solve it. Yet a key part of client service is winning the privilege to help a client solve his or her biggest problems that are standing in the way of achieving their vision.

I counsel my teammates on three simple closing techniques for smart people. I want to share them with you because I've seen what a dramatic positive difference they can make for your customers as well as your colleagues. In this issue we'll explore the first one.

Summarize the underlying need.
I was in the office of a greatly admired billionaire CEO. He had asked my colleague and me to come strategize for 90 minutes with him on how to identify and solve his top leadership challenges. His story was very animated, very passionate, and the details swirled around like a hurricane. I appreciated the candor and the urgency of the issues on the mind of the CEO. He talked about scary changes in the industry, deficiencies in his senior leadership team, tactics for changing the culture and a range of other topics, from broad strategic thoughts to tactical concerns.

Then he just stopped talking. He took a sip of water. I thought this was a perfect time for my colleague to summarize the underlying need the client has (that he is fearful that his company's spectacular stock performance won't continue and he will feel like a failure, unless he makes some big changes to his strategic priorities, shakes up his leadership team and resets the cadence of communication and accountability).

Instead, my colleague asked the client, "What do you think next steps should be?" The client was like, "Well, I don't know, I was hoping you might tell me." The closing conversation should have looked like this:

"So that's what's on my mind." (The CEO says, panting to catch his breath after giving us a lot of content for 60 minutes.)

"Thank you so much for sharing your story with us. Okay, it sounds like your biggest need is this—you have a big, bold vision that you seem to us to be very excited about."

"Yes."

"But you fear you don't have the organization to make it happen."

"Definitely."

"And if you don't make some big changes to your strategic priorities, your team and your overall culture, you worry your stock price will take a round trip, and you'll look like a failure."

"Exactly."

See how good that is for the client?

Clients want to know that you understand what their underlying need is. In this case, his underlying need was to not look like a failure. It's so real, so visceral. Once you "touch" the emotion behind all of the formality, your client will trust you to propose a plan. You are ready to move to Step 2. Watch for Step 2 in the next issue of this newsletter.

Chairman & Founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times bestselling book Who: The A Method for Hiring and the author of the #1 Wall Street Journal bestseller 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 B.A. in Economics with Honors from North-western University, an M.A., and a Ph.D. in Psychology from Claremont Graduate University.