Free Executive Breakfast Seminar

What Do Hackers Already Know About Your Firm?

"9 Critical IT Security Protections EVERY Business Must Have In Place NOW To Avoid Cyber-Attacks, Data Breach Lawsuits, Bank Fraud and Compliance Penalties"

See Page 3 For Details!

February 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.

That Fake App Just Stole Your ID

Ryan loved tweaking photos on his Android phone.

He'd heard rave reviews from his friends with iPhones about Prisma, a new iOS app for image editing. So when he heard Prisma would soon be released for Android, he logged in to the Google Play Store to see if it was there yet.

To his surprise, he found one that looked just like what his friends were describing. Delighted, he downloaded and started using it. Meanwhile, the app—a fake—was busy installing a Trojan horse on his phone.

When he got to work the next day, he logged his phone into the company network as usual. The malware jumped from his phone to the network. Yet no one knew. Not yet, but that was about to change… Now, this isn't necessarily a true story (at least, not one we've heard of—yet…), but it absolutely *could* have been. And similar situations are unfolding as you read this. Yes,

possibly even at *your* company…

Fake apps exploded onto iTunes and Google Play last November, just in time for holiday shopping. Apple "cleaned up" iTunes in an effort to quell users' concerns, but hackers still find workarounds.

Unfortunately, these fake apps pose a real threat to the security of your network. Especially if your company has anything but the strictest BYOD (bring your own device) policies in place. And the more your network's users socialize and shop on *their* smartphones, the greater the risk of a damaging breach on *your* network.

Fake apps look just like real apps. They masquerade as apps from legitimate merchants of all stripes, from retail chains like Dollar Tree and Footlocker, to luxury purveyors such as Jimmy Choo and Christian Dior. Some of the more malicious apps give criminals access to confidential information on the victim's device. Worse yet, they may install a Trojan horse on that device

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

that can infect your company's network next time the user logs in.

So what can you do?
First, keep *yourself* from being fooled. Anyone can easily be tricked unless you know what to look for. Take the following advice to heart and share it with your team:

Beware of Fake Apps!

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:

> *"Fake apps can infect your phone or tablet and steal confidential information."*

1. When in doubt, check it out. Ask other users *before* downloading it. Visit the store's main website to see if it's mentioned there. Find out from customer support if it's the real McCoy.
2. If you *do* decide to download an app, first check reviews. Apps with few reviews or bad reviews are throwing down a red flag.
3. Never, EVER click a link in an e-mail to download an app. Get it from the retailer's website, or from iTunes or Google Play.
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.

The Most "Bullet-Proof" Way To Keep Your Network Safe:
Let's not let *your* company become yet another statistic, hemorrhaging cash as a result of a destructive cyber-attack. Call me TODAY at **(561)969-1616**, or e-mail me at info@palmtech.net, and let's make sure your systems are safe. I'll provide you with a Cyber Security Risk Assessment to check for and safeguard against any points of entry for an attack. This service is *FREE, but DO NOT RISK WAITING: contact me NOW *before* the next scam puts *your* network at risk.

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

Help Us Out And We'll Give You A Brand-New Kindle Fire For Your Trouble

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the month of February.

Simply refer any company with 10 or more computers to our office to receive a FREE Computer Network Assessment (a $497 value). Once we've completed our initial appointment with your referral, we'll rush YOU a free Kindle Fire of your choice as a thank-you (or donate $100 to your favorite charity … your choice!). Simply call us at **(561)969-1616** or e-mail us at info@palmtech.net with your referral's name and contact information today!

Shiny New Gadget Of The Month:

Mevo Puts You In The Director's Chair

A single static video camera can make for some pretty boring storytelling…but who's got multiple cameras, a crew to run them and a team of editors?

Well, now your videos can look like you have an entire crew behind the scenes, with Mevo. Mevo is a new type of video camera and app that lets you shoot and edit multiple video shots on the fly, all while recording and/or livestreaming.

Let's say you're shooting a band concert. You get to mix in shots of the guitarist, the drummer and bass player together, and a wide-angle view of the whole band. Plus Mevo follows their faces as they move around so you don't have to. You just sit back, and cut and zoom on the fly.

On the downside, Mevo's battery lasts only an hour, and image quality is limited to mobile viewing. Still, with all the cool possibilities you get with Mevo, you may start getting ideas about becoming the next Spielberg.

GetMevo.com

FREE Executive Breakfast Seminar:

"9 Critical IT Security Protections EVERY Business Must Have In Place NOW To Avoid Cyber-Attacks, Data Breach Lawsuits, Bank Fraud and Compliance Penalties"

Event Details:

When: March 2nd, 2017
Session Time: 8:30AM
Where: West Palm Beach Marriott
1001 Okeechobee Blvd.
West Palm Beach, FL
Limited Seating. Registration Required.

During This Must-Attend Seminar You'll Discover:

♦ **The scary risks of mobile and cloud computing – and 9 critical IT policies, procedures and protections EVERY business must have in place NOW to protect themselves**; overlook even one and you're exposing yourself to security breaches, damaging and expensive litigation, employment lawsuits and having confidential company information exposed to competitors, hackers and cybercriminals.

♦ The **#1 security threat to your business** that antivirus, firewalls and other security protocols are defenseless against.

♦ A **SHOCKING truth about bank fraud** that most businesses don't know about that could (literally) wipe out your bank account.

♦ **Why firewalls and antivirus software give you a false sense of security** – and what it REALLY takes to protect your organization against new threats and today's sophisticated cybercrime rings.

Who Should Attend?

C-Level executives and managers who are concerned about: lost or stolen devices, privacy of confidential information, employment litigation introduced when employees use personal devices to access company data, and State and Federal laws that carry heavy fines for lost or stolen data. This is of particular importance for those organizations that handle ANY sensitive data such as credit card and financial information, medical records (or serve clients who have medical records) or that simply want to avoid having their bank account wiped out due to a cyber-attack.

Register Here:
www.PalmTech.net/security-seminar/

Smart Closing Technique, Step 2

Let's say you're closing a deal and you've already taken the first step: you've *summarized the client's underlying need*…

Now you're ready for Step 2: *Say what you plan to do.*

Describe exactly what you'll do to help the client successfully satisfy their underlying need. Even smart people worry about putting themselves out there by offering a plan. They worry that someone may disagree with them. They worry about proposing a plan that doesn't work. That's why many advisors stay "safely vague" rather than offering a specific plan.

But being vague doesn't help leaders solve some of their biggest problems. You have to have the courage to propose a plan. For example: "I have some ideas about how you can achieve your goals. Want to hear them?"

"Yes!" (the client says, while taking out a notebook and a pen).

"There are five parts to what I think you need to do, in this order. They are designed to increase your power score, starting with priorities, who is on your team and relationships. First, there is no way you are going to be able to take the company in a whole new strategic direction without the board's support."

"That's true."

"So first we have to articulate your vision and your priorities on paper, with goals and strategy and budget implications, and then get the board's support."

"Right, it's going to change our budget, so rather than let the board nix it this fall, I should get out in front of this and get their support from the beginning."

"Second, you seem to have questions about the capabilities of many of the key leaders in the US, Europe and in your Asia region. It would be helpful to assess your team, to have a clear view of who is going to fit in the new organization, and who is not a fit."

"Yes, that would be helpful—to have an X-ray of the org chart and figure out who needs to go where to align with the new strategy."

"Third, fourth and fifth will be all about culture change. Change the incentives. Change the meeting cadences of what metrics are tracked and discussed—who meets when to discuss what. And what some of our most successful clients have done in situations like this is design workshops—like a roadshow—for you and key leaders to educate and train the next two levels on what you expect from them, and why, in the new world order. This gets the troops aligned behind your new vision."

"Wow! Yes, yes and yes."

"And even if you do all of that, I only give it a 70% chance you will fully actualize your goal within three years—in the market and culturally. Still, that's a lot better than the 5% chance you give yourself today."

"I'd take 70% over 5%."

Now that you've stated your plan, you are in a much better position to close the deal. *-- Dr. Geoff Smart*

About The Author: Chairman & Founder of ghSMART, Dr. Geoff Smart 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.

"What about Instagram?"