TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's New

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 1st Quarter.

Simply refer any company with 10 or more users to our office. We will call and schedule an appointment. When we get the appointment we will send you a $10 gift card to Scheels. If the referral you submitted becomes a client, you will receive $500 off of your next monthly service! For more information, please go to: **http://www.imsnetworking.com/about-us/referral-program/**

February 2017

This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

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

Continued page 2

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

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

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 malicious code on your device that can spread, *including to your company network*.

Take a moment and reflect on these five tips before downloading any app:

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

EDUCATION! Are you interested in learning how to educate your employees so your business doesn't fall to hackers? For a small monthly fee you can train your staff on the latest attacks and protect your network.

Let's not let *your* company become yet another statistic, hemorrhaging cash as a result of a destructive cyber-attack. Call me TODAY at 701-364-2718 or e-mail me at info@imsnetworking.com, and let's make sure your employees are well educated so this doesn't happen to your network.

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

Stolen iPads Susceptible To Security Flaw

There's nothing worse than hardware vulnerabilities that put even the most cautious of users at risk. We could lecture you about how even unimportant tablets with little to no personal information are still a security liability, but until Apple releases a patch to the iPad's newest vulnerability, everyone who owns one is at risk of losing control of his or her data. Let's take a closer look at what you need to know.

iPad owners who find themselves in the unfortunate situation of having their device stolen have the option to activate Apple's *Find My iPhone* feature from icloud.com. If an iPad has this setting turned on, its GPS can be activated from any web browser to inform the owner where it is located.

Furthermore, if a user is concerned that the tablet may have been stolen, he or she can remotely lock the device. From the moment it is locked, the device can only be accessed by logging into the corresponding icloud.com account.

It's a wonderfully intuitive feature, and tens of thousands of iPad owners have prevented data theft since it was first introduced by Apple in 2010. Unfortunately, security researchers recently announced a critical flaw that allows common thieves to totally bypass the remote lock feature simply by flooding login data fields with too many characters.

Apple is aware of the issue and has taken steps to address it with an operating system update. The latest version of iOS has fixed the issue for iPhones, but not for iPads.

Although we anticipate a patch to fix this flaw in the near future, the best way to avoid this predicament is to keep valuable data backed up separately from your iPad. One of the *Find My iPhone* options is to remotely wipe the device, which means as long as you aren't permanently losing valuable data, the worst case scenario is losing nothing more than the tablet itself.

The more mobile our technology becomes, the more susceptible it is to physical security threats. It's important to secure your devices not only from networked threats, but also from everyday ones, like someone nabbing your iPad while you step away from the table to order a coffee. For across-the-board security solutions and consulting, get in touch with us today 701-364-2718 or email info@imsnetworking.com.

Bits & Bytes

Your phone may be spying on you, warns Edward Snowden.

While TV is a medium you watch, the Internet is a medium that watches you, as you watch… For example, intelligence agencies—or anyone else, for that matter—can run a nifty little piece of malware called "Nosey Smurf" on your phone to listen in on everything going on all around you. And it's not just phones. Internet-enabled devices—from Amazon's Echo to your new toaster—can have "ears," waiting for your command…or be used for more nefarious purposes. Snowden's warnings presaged last year's DDoS attack on DNS host Dyn that used connected devices like DVRs and even baby monitors to take down major sites like Twitter, Spotify and Amazon.
-*Forbes*

This simple, 30-second breathing exercise wakes you up like a cup of coffee.

Whether you skip caffeine to get a better night's rest, or just wake up slowly, here's a quick way to activate your brain and give yourself an energy boost. It can help you beat that mid-afternoon slump, or to just get going in the morning. If you're doing it in the office, find a quiet place, like an unused corner or stairwell. Stand up straight, arms gently at your sides. Leaving your elbows pointing down, raise your hands up to shoulder level. Now, inhale deeply and raise your hands and arms straight up over your head. Quickly exhale and lower your arms. Repeat for 30 seconds, or until you're re-energized.
-*Lifehacker*

No bigger than a water bottle when folded, this "personal drone" is packed with features.

DJI's new "pro-sumer" drone, the Mavic Pro, crams lots of excitement into its compact size. Unlike other, more confusing foldable drones, it's a snap to fold or unfold. Yet, at $999, including a light yet rugged remote, it's not just a toy. The Mavic Pro can climb at 16.4 feet per second up to 1,640 feet, and can fly as far as eight miles away at speeds up to 40 mph, though you'll start in newbie mode, at a top speed of 27 mph and max height of 400 feet. Its camera features obstacle detection and gesture recognition, and shoots 4K video, stored or streamed.
-*Mashable*

Uh-oh…these AI machines just created their own secret language. And they're probably talking about us right now…

Well, sort of. And the last part is certainly not true. As far as we know… Google's AI team recently ran across something curious. Back in September, Google announced its Neural Machine Translation system had gone live. Using deep learning, it improves translation from one language to another. But the AI guys decided to take it a step further. Until then, they had to teach the machine how to translate. But having learned the process, could the machines then translate unfamiliar languages on their own? Turns out they can. So can they now talk among themselves? We don't know… Don't panic (yet), but do stay tuned.
-TechCrunch.com