RMS ASSOCIATES, INC.

Your RMSCare Package

July 2015
Issue 2607

What's Inside

RMS
Smart IT For Smart Business

Randy and Claudia

As some of you know, Claudia and I spent two weeks in France in June. We had a great, much needed vacation and one I have been promising Claudia for years. We did a lot of sightseeing, rode our bike through Provence, ate some incredible food and made some lifetime memories! My staff did a great job in our absence; not only did they work hard but actually worked under terrible conditions as the weather hit the high 90s and TWO AC units in our office failed! Fortunately the AC units were replaced and everyone is much cooler now.

We also welcomed Randy Voige back to the office a couple of weeks ago. He had surgery on both knees and has been working remotely from home the past six weeks.

Because it is vacation time, I included an article concerning using your devices while on trips and how to keep your devices and information safe. And just in case you have a beach trip planned, see the information on the back about keeping safe from the shark attacks that we keep reading about in the news!

Randy

The 5 Most Dangerous Pieces Of Information To Give In An E-mail

In the book *Spam Nation*, investigative journalist and cybersecurity expert Brian Krebs revealed the single most effective (and relied upon) way cybercrime rings gain access to your bank account, credit cards and identity. Ready for it? E-mail.

Whether it's opening an attachment infected by a virus, or a phishing scam where you unknowingly give up your login to a critical web site, e-mail still remains the most popular and reliable way digital thieves can rob you blind, steal your identity and wreak havoc on your network. Worst of all? You're INVITING them in! While there are a number of things you need to do to protect yourself, here are five pieces of information you (and your team) should NEVER put in an e-mail.

1. **Your social security number.** Think of this as your "bank account" number with the government. You should never e-mail this to anyone because it can be used to open credit cards and steal your identity.

2. **Banking information.** Your bank account numbers, routing number and online banking login credentials should never be e-mailed. Further, avoid sending a voided, blank check as an attachment to an e-mail.

3. **Your credit and/or debit card information.** NEVER update a credit card via an e-mail! If you need to update a card with a vendor, there are two safe ways to do this. The first is to log in to your vendor's secured site by going to the URL and logging in. Do NOT click on a link in an e-mail to go to any web site to update your account password or credit card! Hackers are masters at creating VERY legit-looking e-mails designed to fool you into logging in to their spoof site, which LOOKS very similar to a trusted web site, to enter your username, password and other financial details, thereby gaining

Cont. on Page 3

Vacation Alert!

The ONE Thing You And Your Employees Should NEVER Do When On Vacation

’Tis the season when you and your team will be taking a little time off to head to the beach or your favorite vacation spot, and while we know we *should* completely disconnect from work, most of us will still check e-mail and do a little work while away — and that could end up causing some issues if you’re not careful while working remotely.

So before you head off to have a little fun with your laptop tucked under your arm, keep this in mind: never automatically connect to “any available network.” Not all Internet connections are secure, so if you’re going to log in to the company’s network, e-mail or other critical cloud apps that are hosting sensitive information, ONLY do so on a trusted, secured WiFi and NEVER a public one. We recommend investing in a personal MiFi (mobile WiFi) device that acts as a mobile WiFi hotspot if you’re going to be traveling a lot and accessing company info.

Second, turn off the ability to automatically connect for all of your mobile devices and laptops. You will still be able to connect manually, but it will prevent your laptop or device from connecting to a questionable network without your consent or knowledge.

Finally, disable all printer and file-sharing options on your mobile devices. This is another way hackers can gain access to your network. In an ideal world, you and your employees would take a true break from work, but if they aren’t able to completely detach themselves, then at least require them to stay safe using the above tips.

Still on Microsoft Server 2003?

Here’s Your Warning!

On July 14, 2015, Microsoft officially retired Windows Server 2003 and no longer offers support, updates or security patches. That means any Windows 2003 server is **completely exposed to serious hacker attacks** aimed at taking control of your network, stealing data, crashing your system and inflicting a host of other business-crippling problems you do NOT want to have to deal with.

This is a threat that should not be ignored; if you don’t want cybercriminals running rampant in your company’s server, you MUST upgrade ASAP. To assist our clients and friends in this transition, we’re offering a **Free Risk Assessment And Migration Plan**. At no cost, we’ll come to your office and conduct our proprietary Risk Assessment — a process that’s taken us years to perfect — to not only determine what specific computers and servers will be affected by this announcement, but also to assess other security, backup and efficiency factors that could be costing you in productivity and hard dollars.

With this Assessment, I’m confident that we will not only be able to expose a number of security risks and issues that you weren’t aware of, but also find ways to make your business FAR more efficient and productive. To request this free Assessment, call us or send an e-mail to rrowe@rmsatl.com. Due to staff and time limitations, we’ll only be able to offer this until the end of August or to the first 10 people who contact us. *(Sorry, no exceptions.)*

Shiny New Gadget Of The Month:

Navdy

Many of us realize how dangerous it is to check e-mail or text messages while we're driving, but we don't feel like we can afford to ignore our phone. Brand-new product Navdy to the rescue!

Navdy is a transparent Head-Up Display (HUD) that projects information as if it's floating six feet in front of you. It's very similar to what commercial airline pilots use. Navdy works with any car, and with all iPhones and Androids.

Using the apps you already have on your phone, and with no service plans required, Navdy allows you to focus on the road and not on your phone.

As a phone call comes in, Navdy's built-in camera allows you to simply swipe in midair to answer calls (or dismiss them), so you no longer have to fumble with buttons or touch screens. Plus, Navdy's voice recognition uses the voice commands you're already familiar with, whether you use Google Now or Siri.

Any notification on your phone (such as text messages or social media) can be played, read aloud or disabled, based on your preferences. Navdy even allows you to keep your teenagers safe by giving you parental controls.

The product will retail for $499, but is available now for pre-order for $299. See them at: www.navdy.com

Does This Password Sound Familiar?

You know the difference between a good password and a bad one. Many of us do like the convenience of a simple, easy-to-remember password that requires no effort to recall and type when we buy online, use online bill pay or log into Facebook or Instagram. But many of us also appreciate an added layer of security so we **don't** use an effortless password when sensitive data is on the line.

In a recent study by SplashData, they looked at a sampling of over 3 million passwords (all of which were leaked during a data breach last year). They compiled a list of the most common passwords—and the results weren't all that surprising. **123456** was the No. 1 password used last year, followed by the classic **password**.

While these passwords may have the IT and security crowds shaking their heads in dismay, it's not all bad news. These popular passwords may offer no practical security, but according to the study, the 25 most common passwords only represent about 2% of the overall total.

This means most people don't use these passwords—or **qwerty**, or **111111**, or **iloveyou**. The study found more variation among the most popular passwords versus the 2013 study. Is it a possible trend? Are people turning to more imaginative or secure passwords? Maybe, but only time will tell. Even if the study suggests most of us don't rely on overly simple passwords, SplashData's list serves as a reminder to use more secure passwords and to change them regularly.

Everyone should have strong, unique passwords for each online service they use: banking, online bill payment, e-mail, social networks, shopping, etc. You know it's easy to lose track of them all—unless you are committing one of the greatest online security offenses by using one password for everything. One of the best-and most secure ways to handle your passwords is with a password manager. Consider LastPass, KeePass, and 1Password which are compatible with a number of platforms and are great ways to help keep you safe!

Dangerous *Cont. from Page 1*

access. Another way to update your account is to simply CALL the vendor direct.

4. **Login credentials and passwords.** You should never share your passwords or answers to security questions with anyone for any site, period.

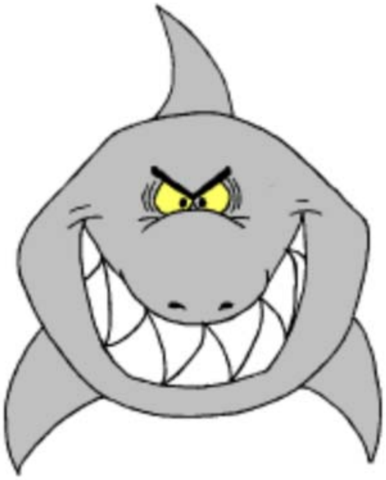
5. **Financial documents.** An ATTACHMENT that includes any of the above is just as dangerous to e-mail as typing it in. Never e-mail any type of financial documents (or scans of documents) to your CPA, financial advisor, bank, etc.

Remember: *Banks, credit card companies and the government will never ask you to click a link to provide them with any of the five items above. If you get an e-mail requesting you to update any of the above information, there's a good chance it's a phishing e-mail from a hacker. Don't be fooled!*

RMS Associates, Inc.

1850 Lake Park Drive
Suite 200
Smyrna, GA 30080
www.rmsatl.com
Phone: 770.988.9640
Fax: 770.988.9695

RMS
Smart IT For Smart Business



"Like" RMS Associates, Inc. on FaceBook to get the latest IT news, tips, and even an occasional laugh at facebook.com/RMSAssociates

Like Us On facebook

Blog

Check out our blog at mysupportguys.com/blog

Subscribe to our RSS feed at mysupportguys.com/feed.

Services We Offer

- Cloud Solutions
- Technology as a Service
- Total Business Continuity Protection
- Proactive Network Maintenance/Monitoring
- Network Design & Implementation
- Network Security
- SPAM & Virus Remediation & Prevention
- 3CX VOIP Phone System

SHARKS!!!

Due to the recent shark attacks in the SE and because it is vacation time, it is good to know how to decrease your chances of getting attacked.

1. Swim in groups as sharks typically attack lone swimmers in the water.
2. Do not enter water if bleeding as sharks can smell and taste blood.
3. Do not wear jewelry in the water as sharks like shiny things.
4. Do not swim in the dark or twilight hours.

We Would Love To Hear From YOU!

If you have noticed an RMS associate going above and beyond the ordinary for you either on-site or over the phone, please let us know so we may reward them! Please e-mail me at rrowe@rmsatl.com. Thanks!

This newsletter is printed by Imagers, a long time client and friend. If you need quality specialized printing, please call them at 404-351-5800 or see them on the web at www.imagers.com.

IMAGERS
Since 1947