360IT PARTNERS

"Partnering With Us Makes Your Business Run Faster, Easier And Increases Profitability"

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 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.

"A customer is the most important visitor on our premises, he is not dependent on us. We are dependent on him. He is not an interruption in our work. He is the purpose of it. He is not an outsider in our business. He is part of it. We are not doing him a favor by serving him. He is doing us a favor by giving us an opportunity to do so."
--Mahatma Gandhi

Kimberly Kelly
Customer Service Coordinator

July 2015
Virginia Beach, VA

Inside This Issue…

The 5 Most Dangerous Pieces of Information to Give In E-mail…….***Page 1***

Urgent Security Warning For Microsoft Server 2003 Users……***Page 2***

Trivia Question……***Page 2***

Navdy……***Page 3***

Vacation Alert!……***Page 3***

Client Spotlight……***Page 3***

Cutting the Telephone Cord of the PSTN System……***Page 4***

An Urgent Security Warning for Businesses Running Microsoft Server 2003

(And A Limited Free Assessment Offer)

On July 14, 2015, Microsoft is officially retiring Windows Server 2003 and will no longer be offering support, updates or security patches. That means any server with this operating system installed will be 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 before that deadline. To assist our clients and friends in this transition, we're offering a **Free Microsoft Risk Assessment And Migration Plan**. At no cost, we'll come to your office and conduct our proprietary 27-Point Risk Assessment — a process that's taken us over 7 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.

After performing this Assessment for hundreds of companies like yours, 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 direct or send us an e-mail today (luke@360itpartners.com). Due to staff and time limitations, we'll only be able to offer this until the end of July or to the first 10 people who contact us.** *(Sorry, no exceptions.)*

Want To Win A $25 Gift Card?

The winner of last month's Trivia Challenge was Dayspring International. Visit www.dayspringinternational.org for more information on their incredible efforts to educate and transform villages across India.

Ready to Play? Here is this month's question:

Which kind of animal did Florence Nightingale often carry around in her pocket?

a) Kitten b) Puppy c) Owl d) Snake

E-mail Kirsten Conti (kirsten@360itpartners.com) Right Now With Your Answer!
She will put all the correct answers in a hat and draw the winner at the end of each month.

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 is rumored to retail at $499, but is available now for pre-order for $299. Just visit their web site at: www.navdy.com

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 remote.

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 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.

PAYDAY PAYROLL SERVICES

Payday Payroll provides outsourced payroll and human resource services to its clients. Solutions include cloud based timekeeping, online payroll, HR support center, general ledger integration, retirement plan uploading, workers compensation administration, background checks, labor law posters, financial fitness programs for employees, merchant services, employee pay cards and much more! Payday is the local's choice for those looking for a comprehensive, boutique customer service experience. Since opening its doors in 1985, Payday has been owned and operated by the Kline family. They have proven to be an integral part of the Hampton Roads Community for the past 30 years. Payday takes great pride in offering industry leading customer service and support, providing an excellent work environment for its team and giving back to the community which it serves. If you're currently outsourcing your payroll/HR or would like more information on doing so, please call Danny Kline at 757-523-0605 or visit their website www.paydaypayroll.com for more information.

Payday is a member of the American Payroll Association (APA), Independent Payroll Providers Association (IPPA) and The Payroll Group (TPG).

Cutting the Telephone Cord of the PSTN System

Since Alexander Graham Bell made the first phone call to his assistant Watson, the phone has come a long way. But now, the standard phone system (PSTN) as we know it is nearing its final days. Thanks to Internet technology, the ability to make phone calls over the Internet using VoIP technology is proving to be the cheaper and more efficient alternative.

The upside is that most business class VoIP systems will offer you the same features you're used to with your current phone system. Typically, this includes call forwarding, call waiting, conferencing, and voice mail. Additionally, most VoIP systems include data and application sharing and the ability to transmit video with your voice.

Like any new technology, VoIP has its pros and cons- depending on your specific business, budget, and needs. Allow us to take a look at your current phone system and give you a customized pro and con analysis of making the upgrade to VoIP. Call us today to set up an appointment at **757-499-6761** or email Luke Barton at **luke@360itpartners.com**.

Discover More Information About Our Dynamic Services and Team: www.360itpartners.com

5269 Cleveland St. Suite 201
Virginia Beach, VA 23462