VOLUME VI, ISSUE 7
JULY 2015
OTTAWA, ONTARIO

NEOLORE NETWORKS INC.

TECHLORE

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

INSIDE THIS ISSUE:

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

-Jim Stackhouse
NeoLore Networks Inc.

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. Don't be fooled!

FREE REPORT DOWNLOAD

Free Report Download: If You Are Considering Cloud Computing For Your Company—Don't, Until You Read This…

If you are considering cloud computing or Office 365 to save money and simplify IT, it is extremely important that you get and read this special report, "4 Critical Facts Every Business Owner Must Know Before Moving Their Network To The Cloud."

Even if you aren't ready to move to the cloud yet, this report will give you the right information and questions to ask when the time comes.

Download your FREE copy today at http://www.neolore.com/free-stuff/reports/

An Urgent Security Warning For Businesses Running Microsoft Server 2003

(And A Limited Free Assessment Offer)

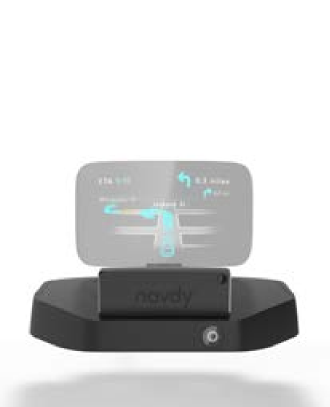
On July 14, 2015, Microsoft is officially retiring Windows Server 2003 and will no longer be offering support, updates or security patches. That means any server with this operating system installed will be completely exposed to serious hacker attacks aimed at taking control of your network, stealing 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 10 Point Risk Assessment — a process that's taken us over 15 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 many 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 at 613-594-9199 or email us at sales@neolore.com today.

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. 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

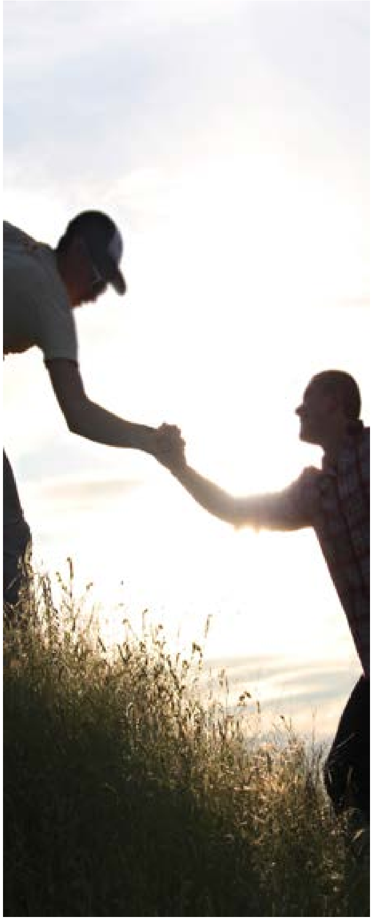
"It Never Hurts To Ask"

We often hear that said. But is it true? Recently someone asked me for a favor. The request came in an impersonal form e-mail. I had some business dealings with this person many years ago. Since then, I had heard from them only once when they asked another favor.

I was being asked to promote something on my social media network. The request did not offer an excerpt, a preview, a sample or any compelling reason why I should offer my assistance and ping the people on my e-mail list.

I thought, "Why should I help?" The implied assumption that I owed this individual something, or that I should help for no reason other than that they asked, seemed a bit off-putting. Have I helped an unfamiliar person before? Yes, there have been circumstances where I was glad to do so. But "Do this for me because our paths crossed" is not a good reason. Sometimes it does hurt to ask. Sometimes it comes across as inappropriate or entitled. Asking someone for a favor when you have no relationship with them is a bad idea. Naturally, most people like to help — but very few people like to waste their time or energy. And nobody likes to feel someone has taken advantage of them.

There's nothing wrong with asking for a favor or assistance. Just make sure you ask the right person for the right reason in the right way. Otherwise, you might damage your reputation and your relationships.



The Lighter Side: Great Starting Salary

Fresh out of business school, the young man answered a want ad for an accountant. Now he was being interviewed by a highly agitated, arrogant little man who ran a small business that he had started from scratch.

“I need someone with an accounting degree,” the man said. “But mainly, I’m looking for someone to do my worrying for me.”

“How’s that?” the would-be accountant asked.

“I worry about a lot of things,” the man said. “But I don’t want to have to worry about money. Your job will be to take all the money worries off my back.”

“I see,” the accountant said. “And how much will my position pay?”

“I'll start you at 85,000,” responded the owner decisively.

“Eighty-five thousand dollars!” the accountant exclaimed. “How can such a small business afford a sum like that?”

“That,” the owner said, “is your first worry. Now get to work.”

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.

Who Else Wants To Win A $25 Gas Card?

The Grand Prize Winner of last month’s Trivia Challenge Quiz is Bob M! He was the first person to correctly answer last months quiz question: True or False: If you use a cloud application they are responsible for storing your data.

Now, here's this month's trivia question (The answer can be found in this newsletter). The winner will receive a $25 gas card!

Question: Name 2 of the 5 most dangerous pieces of information to give in an e-mail

Call (613) 594-9199 right now with your answer!