CSU Connection

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

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.

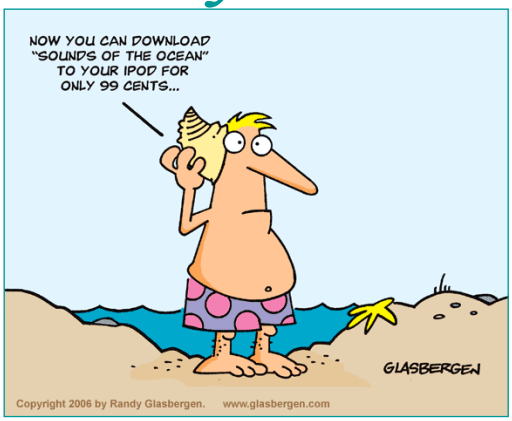
Public Wi-Fi is almost everywhere —in stores, libraries and restaurants and soon on commuter trains and in stations —but so is the danger. The best advice for users is not to be lulled by the convenience of Wi-Fi, to be skeptical and to take your own precautions to secure your computer and information.

"Public Wi-Fi is inherently unsecure. Anyone using it ought to do so with the premise that everything you do is visible to a third-party stranger with access to that hot spot," said Kevin Clark, first assistant Monmouth County prosecutor, an expert in cybercrime. "The chances of you being hacked far exceeds the chances of your home being burglarized. This is a big business."

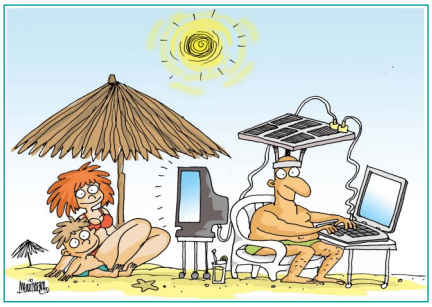
Second, turn off the ability to automatically connect for all of your mobile devices and laptops. You will still be able to connect manually, but it will prevent your laptop or device from connecting to a questionable network without your consent or knowledge.

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.

July 2015



Inside This Issue...



CSU COMPUTER SERVICES UNLIMITED Connection

July 2015

An Urgent Security Warning For Businesses Running Microsoft Server 2003

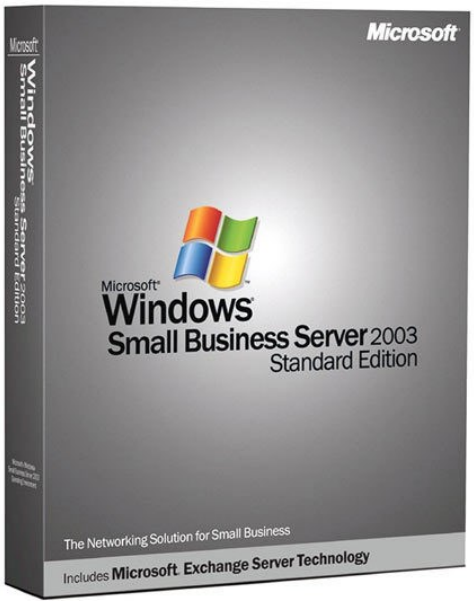
(And A Limited Free Assessment Offer)

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 -Point Risk Assessment — a process that's taken us over 20 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. 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.)*

Microsoft no Longer Supports Server 2003



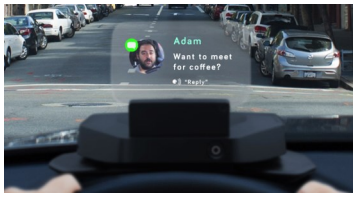
We Recommend Server 2012

Give us a call at (703) 968-2600 or check out our website at www.csuinc.com

CSU COMPUTER SERVICES UNLIMITED Connection

July 2015

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

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!

CSU COMPUTER SERVICES UNLIMITED Connection

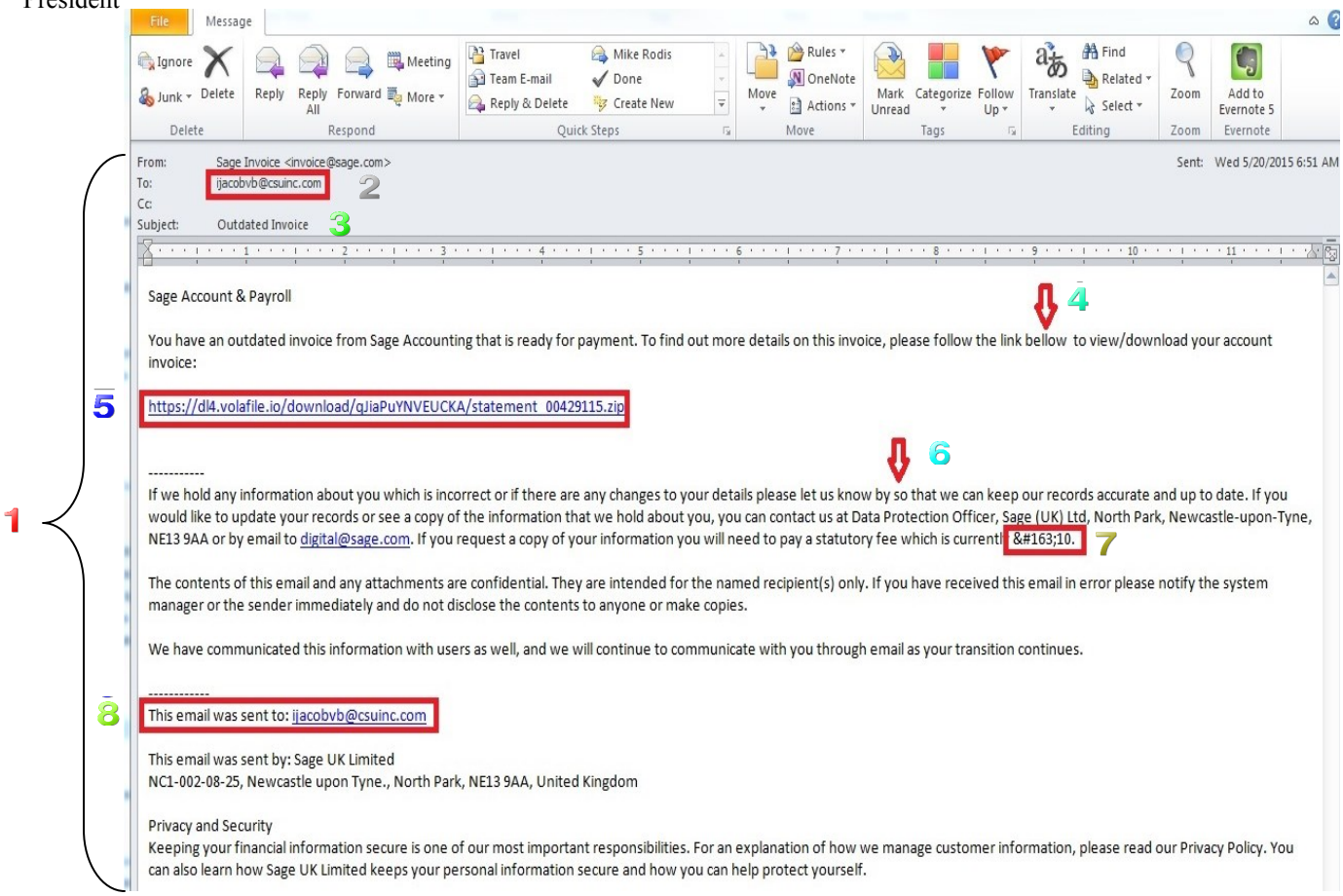
July 2015

Michelle Sherman
President

"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!"

Final Thought for this month

I thought I would let you know that you are not alone when it comes to receiving bogus, evil emails. These kinds of emails make my blood boil and I really wish that I could do more about them than simply just delete them. The only thing that I can do is educate you on how to spot them. Here is an example that I received recently:



From: Sage Invoice <invoice@sage.com>
To: ijacobvb@csuinc.com 2
Cc:
Subject: Outdated Invoice 3
Sent: Wed 5/20/2015 6:51 AM

Sage Account & Payroll

You have an outdated invoice from Sage Accounting that is ready for payment. To find out more details on this invoice, please follow the link bellow to view/download your account invoice: 4

5 https://dl4.volafile.io/download/qJiaPuYNVEUCKA/statement_00429115.zip

6

If we hold any information about you which is incorrect or if there are any changes to your details please let us know by so that we can keep our records accurate and up to date. If you would like to update your records or see a copy of the information that we hold about you, you can contact us at Data Protection Officer, Sage (UK) Ltd, North Park, Newcastle-upon-Tyne, NE13 9AA or by email to digital@sage.com. If you request a copy of your information you will need to pay a statutory fee which is current £10. 7

The contents of this email and any attachments are confidential. They are intended for the named recipient(s) only. If you have received this email in error please notify the system manager or the sender immediately and do not disclose the contents to anyone or make copies.

We have communicated this information with users as well, and we will continue to communicate with you through email as your transition continues.

8 This email was sent to: ijacobvb@csuinc.com

This email was sent by: Sage UK Limited
NC1-002-08-25, Newcastle upon Tyne., North Park, NE13 9AA, United Kingdom

Privacy and Security
Keeping your financial information secure is one of our most important responsibilities. For an explanation of how we manage customer information, please read our Privacy Policy. You can also learn how Sage UK Limited keeps your personal information secure and how you can help protect yourself.

1

1. We don't order Sage Software, so there is no reason for Sage to be invoicing my company.
2. While csuinc.com is the correct domain name, what is in front of the @ sign does not represent anyone in my company.
3. "Outdated Invoice" -really? Who says, 'outdated invoice'. Normally, we say past due or overdue invoices.
4. You will notice that the word below is misspelled.
5. The link that they want you to click on has no reference to Sage at all. Big Time Clue. Somewhere in the link it should have sage.com
6. Know by when?
7. Just how much is that statutory fee?
8. Once again they remind me that they sent the email to someone who is really no one in my company.

Really what has happened here is that some jerk sitting in Russia, China, or Uganda somewhere has typed up a bogus email and put a malicious link in it. Then he or she put it into translation software and it didn't really do a very good job of translating. They are counting on someone being new on the job, or young and curious enough to click through the link.

Once the link is clicked through, I'm sure the link would have tried to install malicious software on my system, possibly even my server. We have as much protection set up as possible against these attacks. Not everyone is up to date on their virus patches, please pass this on to your employees, friends and family members. The only way to fight these criminals is to know how to spot them.