TECHNOLOGY TIMES

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

By Computer Networks of Roanoke, Inc.

Serving Roanoke and surrounding areas since 2006

Volume 8, Issue 7 July 2015

"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!"

Hank Wagner, Owner/Founder
Computer Networks of Roanoke

IT Guru, Published Author, and Trusted Advisor to Medical Practice Administrators and Business Owners

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.

See Alert Page 2

INSIDE THIS ISSUE

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.

See Most Dangerous Page 3

Alert continued from Page 1

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. ❖

OPM Loses Millions

Thehill.com
By Cory Bennett - 06/24/15 11:35 AM EDT

House Oversight Committee Chairman Jason Chaffetz (R-Utah) suggested Wednesday that the largest federal hack in history could ultimately put as many as 32 million people at risk.

Chaffetz based his estimate on the Office of Personnel Management's budget request, submitted in February. OPM officials have acknowledged that two separate breaches laid bare millions of federal workers' information to hackers thought to be based in China.

"Let me read to you what you wrote on Feb. 2 of this year," Chaffetz said to OPM Director Katherine Archuleta during the Wednesday hearing, noting that the OPM claimed it was "a proprietor" of personally identifiable information on 32 million federal employees and retirees.

"Are you here to tell me that information is all safe? Or is it potentially 32 million records here that are at play?" Chaffetz asked.

"We're reviewing the number and scope of the breach," Archuleta replied.

In recent days, it's been reported that 18 million people — including federal workers, military and intelligence community personnel, as well as friends and family named in background investigations — are potentially affected by the breach.

In her opening testimony at the Oversight Committee hearing, Archuleta indicated this number may fall short of the total, calling it "a preliminary, unverified and approximate number."

"It is a number I am not comfortable with at this time because it does not represent the total number of affected individuals," she added.

Chaffetz pressed Archuleta several times on the scope of the hack.

"I'm asking you for a range," he said. "It could be as high as 32 million?"

"I'm not going to give you a number I'm not sure of," Archuleta said. ❖

Editorial Comment

If you think that this cannot happen to you, because you are too small, or not on the Internet that much, or don't do business with the government, or whatever other fantasy reason you can come up with, then you are flirting with disaster. And if you are managing a business for someone else, then you are placing their business and livelihood (salary/future/family) in jeopardy.

This can happen to any business, regardless of the size of the business. Criminals do not just target the big boys and girls like Anthem, Target or the OPM; in fact, smaller businesses are more prone to blowing off computer, Internet and network security, which makes them an easier target. Car thieves don't just steal high-end cars, they take what is available.

Network hacking is most often a crime of opportunity. The crooks send out thousands of emails with malware, Trojans, or viruses and the folks that open them unknowingly become the next victims of identity theft, which leads to people filing false tax returns in your name, opening up new credit accounts in your name, seeking medical treatment under your insurance, and similar things.

Protect your computers now with up to date software and hardware. ❖

Last Call…
You Don’t Have To Go Home, But You Can’t Stay Here

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 exposed to potentially 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.

If this sounds familiar, it is. We did this last year with Windows XP Pro.

This is a threat that should not be ignored; some regulatory agencies may require you to upgrade to avoid fines and penalties.

If you don’t want cybercriminals trying to run your company’s server, talk to us about an upgrade to Server 2008 or Server 2012. ❖

Hank Wagner
757-333-3299 x232
hank.wagner@computernetworksinc.com

David Rourk of Rourk Public Relations has rebranded his business to better describe his current work with web sites. We use them for Search Engine Optimization (SEO) which helps get our website on Page 1 of Google’s search results.

Visit them at http://www.businesswebsiteexperts.com/ to see more about their services, and how they may help your business.

Welcome to
Business Website Experts

Patience does not exist on the internet. If your website is not polished, professional, and easy to navigate your potential customers will quickly click to the next website to find what they need.

Our client websites drive lead$.
We can help you too!

Most Dangerous continued from Page 1

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! ❖

Remote access threats are imminent

Posted on Jun 25, 2015
By *Gary Glover, Security Metrics*

Remote access makes doing business extremely convenient. However, it’s critical to understand that with this ease, comes vulnerability. Insecure remote access is the number one attack pathway used by hackers today.

Remote access technology is an incredibly valuable business tool – as long as there is an Internet connection, it allows workforce members to easily access the office network from anywhere. However, insecure remote access gives hackers a pathway to compromise organization networks and gain access to medical records.

Remember Target’s massive data compromise in 2013? It is believed that the incident began when a hacker gained access to one of Target’s systems via a remote access account belonging to an HVAC company. Hackers were able to use that access to gain a foothold on an internal system and then leapfrog to other systems inside the retailer’s network.

How do hackers do it?
Many healthcare organizations open up their networks to vendors, partners, suppliers, and other business associates to streamline processes and enable better service and support. Few implement processes governing third-party access.

It’s no coincidence that the exploitation of improperly configured remote management tools is the plan of attack most frequently used by hackers. If not properly secured, remote access puts organizations at a severe security disadvantage by allowing attackers to bypass the firewall and most other system security measures and remotely gain access to the POS or other systems in the payment environment.

It’s simply that easy for hackers, especially because while there tend to be rules in place for employees using remote access, the same rules are not always applied to external parties.
According to preliminary Security Metrics forensics investigation data of breached organizations during 2014, insecure remote access played a role in 93 percent of cases. ❖

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.” ❖

Predictable Results For a Predictable Fee

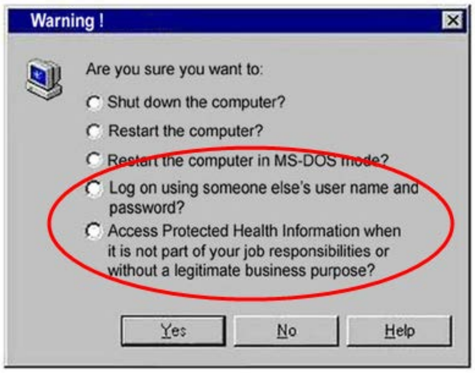
We do it all…HIPAA Security Risk Analysis, Backup and Disaster Recovery (required for HIPAA Compliance), Network Administration, Help Desk, Hardware Sales/Service, Hardware Refreshes/Installs, IT Consulting.

And, we do that for businesses with as few as 10 PCs.

We are looking for a select number of new clients in the medical and professional services fields.

If you are dissatisfied with the level of service you are getting from your current IT Vendor, pick up the phone, call me, Hank Wagner, at 757-333-3299 x232, or email me: hank.wagner@computernetworksinc.com and we can chat a bit about your needs. ❖

Umm, No.



Warning !

Are you sure you want to:

○ Shut down the computer?

○ Restart the computer?

○ Restart the computer in MS-DOS mode?

○ Log on using someone else's user name and password?

○ Access Protected Health Information when it is not part of your job responsibilities or without a legitimate business purpose?

THIS IS MY FIRST TIME HERE. DON'T I NEED TO FILL OUT SOME FORMS?
WE'VE ALREADY DOWNLOADED YOUR INFORMATION.
PATIENT CHECK IN