July 2015

Technology Update

by B4 Networks

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

Inside This Issue…

"As a business owner, I know 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!"
Bryan Lachapelle, B4 Networks Inc.

B4 Networks Inc.
1462 Pelham Street
Fonthill, Ontario, L0S 1E0
Tel: 905.346.4966

Ways To Fortify Your Company's Cyber Security

Many business owners worry that their security technology isn't adequate:

The reality is that it's not just the systems you have in place that are at risk, because one of the weakest security links stems not from the technology you use to secure you network, but your personnel.

Cyber criminals are always coming up with ways to dupe your employees into clicking on something that appears genuine or innocent looking. But, by doing so, these employees have opened the Pandora's Box instead, letting the hacker to perform whatever nefarious deed they have in mind.

Have you provided security training to your employees? If the answer is no, a breach that can ruin and devastate your business is just a click away!

It's time to step up to the plate and ensure your people know what to be on the lookout for and get real about cyber crime.

Let's start with some basics!

- Train Everyone – Each employee performs different tasks and uses different forms of IT media. It's vital you impress on your employees the potential consequences of what a cyber attack could have on your company and their future. It's not something to take lightly. From passwords, email, attachments and encryption protocols, ensure all employees are aware of the most current types of threats and methods hackers use. A good place to start, is having every employee read our newsletter. We pack it full of useful security information each and every month.
- Establish Security Protocols – It's time consuming, but every employee needs to be on the same page when it comes to security. Some of the most minor aspects of your system can be the most vulnerable. If necessary, hire an IT Security Consultant to review your systems and assist you with setting clear security protocols to protect your business.
- Use the Latest Security Technology – Never let your security systems become old or stale, as cyber criminals can always find a weakness and will use it to their advantage. This is especially important if you are using Cloud technology, so apply the latest security IT to strengthen your security, and use it to frustrate a potential cyber criminal at every turn.
- Evaluate Your Security Systems Regularly – Make this an annual review with all department heads. Encourage lower level employees to report any suspicious activity immediately. Take prompt action in evaluating any potential threat. The new approach in security is "real time monitoring" rather than prevention because it's on the front line that a threat can invade your system.

Don't fall prey to a cyber criminal and get all your people on the same page. Contact B4 Networks to help prevent your business from falling victim to cyber crime. Call us today at **(905) 346-4966** or email us at: help@b4networks.ca and we will help strengthen your company's security.

An Urgent Security Warning For All Businesses Running Microsoft Server 2003

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.

You may think no one would bother to "attack" your clinic, after all, your just small potato's in the grand scheme. Unfortunately the reality is, cyber criminals aren't after anyone specifically. They go where they can (where there's a vulnerability), and if that means your network, then so be it. This is a threat that should not be ignored; if you don't want cybercriminals running rampant in your clinics server, you MUST upgrade before that deadline.

It is important to regularly check for and install updates for operational systems and software programs to protect data. Windows 2003 being unsupported by Microsoft means that it is now at risk, and since the upgrade cannot be done easily (it requires a trained IT Specialist to perform this upgrade) don't wait until it's too late, take action before this 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 59-Point Risk Assessment — a process that's taken us over 10 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 businesses 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.)

Tek Tip of the Month

Skip The Recycling Bin

As you know, anytime you delete a file, it goes to the rycycling bin, and doesn't' really delete, unless you also, empty the recycling bin.

Sometimes though, you may just want to delete something you absolutely know you don't need, and don't want it taking up any space on your computer anymore.

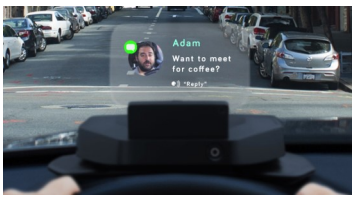
If so, this trick is for you. Be very careful though, this trick can lead you into hot water if you delete something you didn't mean to. :

To skip the recycling bin, do the following: Select the file / files you no longer want, and then simply hold down "shift" key while pushing the delete key. A prompt will appear asking you if you want to **Permanently** the file. Click yes, and presto!

Steve Lamarre
Service Manager

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 B4 Networks Comic Strip

Meet *After Stuff Happens Networks*

After Networks is a fictitious computer company that provides terrible customer service, does everything wrong, takes days to respond to service requests, are very arrogant, talk down to clients, and are anything but helpful. In fact they are downright lazy.

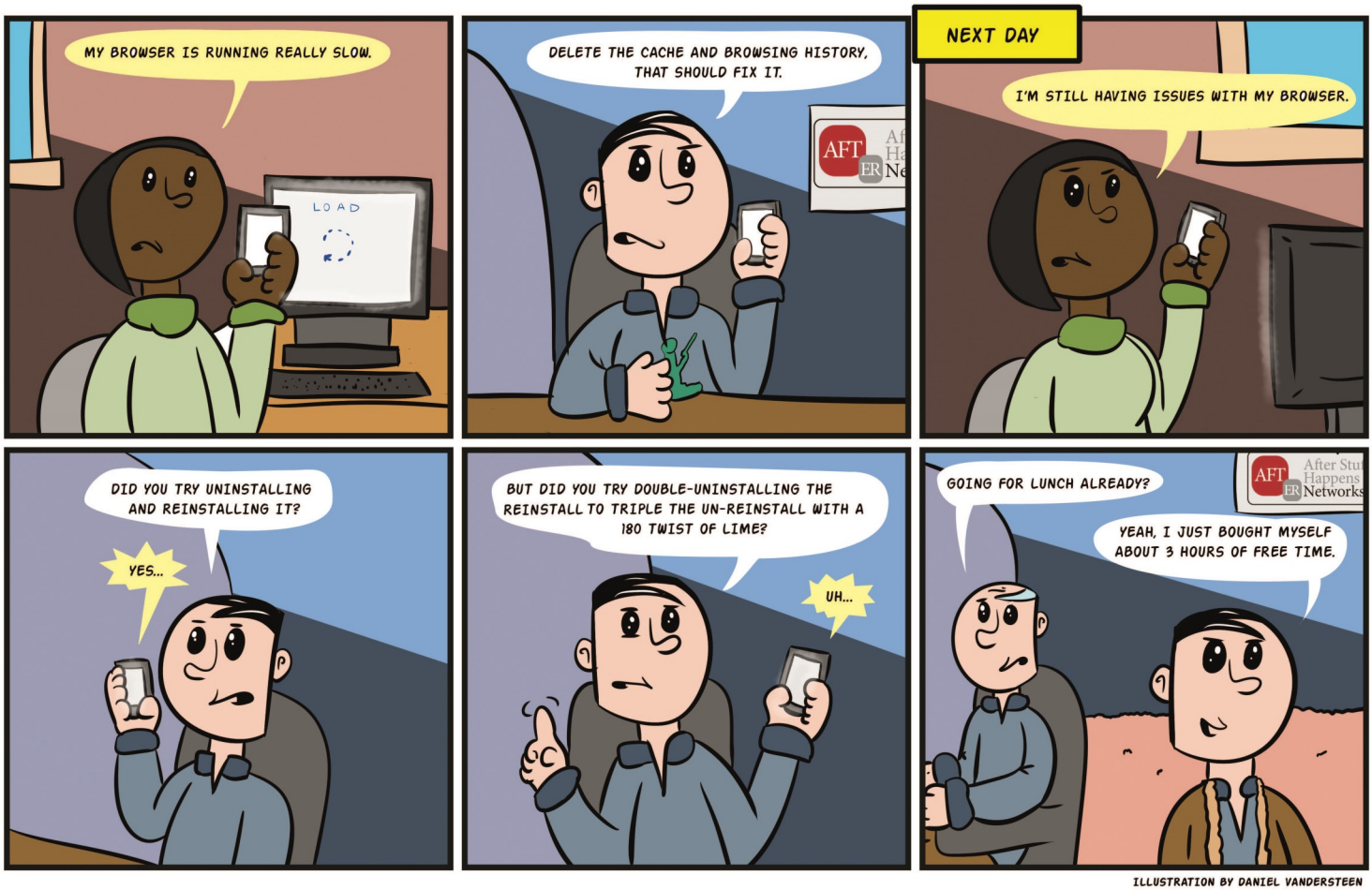
This company does not actually exist. No one we know of is this bad at delivering their service. But we've all at one time or another run across a company that has one of these poor traits. If you struggle with your IT firm, call us for a second opinion. 905-346-4966

Note: The comic strip is not meant to insult or make fun of anyone. We decided to make this comic strip series to try and bring a little light and awareness to some of the situations we've come across, and hopefully affect some change within the IT industry. Not all of the comics are real situations that have occurred, but all of them do address a particular issue we have encountered.

After Networks doesn't fix issues, and tries to get the customer to do all the work.

Nothing is more frustrating than having to repeatedly get something repaired. While it does happen on occasion that the initial attempted fix won't solve the problem, however that should be the exception rather than the rule.

A great IT Company will explain everything that they are going to attempt without complicated jargon meant to confuse. If they are going to try several things one at a time, they should clearly communicate that so you know what to expect. They will also do the work themselves rather than tell you what to do, after all, isn't that why you called them?



Have you experienced something similar with your current provider? Do you want to work with an IT provider that responds quickly to your business needs, and fixes things right the first time? Call us today @ 905-346-4966 - www.b4networks.ca

Compliance With Ontario's Personal Health Information Protection Act (PHIPA)

Cyber Security is something that should be taken very seriously especially those that are in the Health sector. Right now, extremely dangerous and well-funded cybercrime rings in China, Russia and the Ukraine are using sophisticated software systems to hack into thousands of small businesses like yours

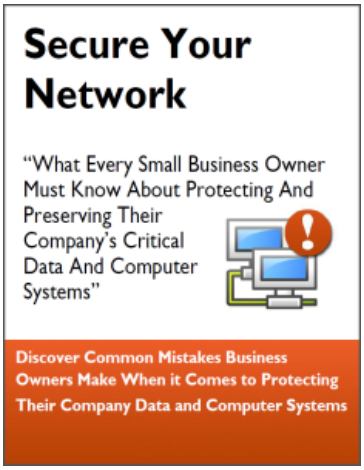
Ontario's PHIPA laws require that helth providers implement technical safeguards to protect you patients personal information, this includes encryption of health information (especially when taken off site), periodically changing passwords, requiring unique logins/passwords to access information, installing and keeping antivirus protection software updated, as well as ensuring security updates on all desktops and servers are performed in a timely basis.

Because I want to do my part in stopping cybercrime, I've put together a report titled **"Secure Your Network—What Every Small Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems"**

This report is brief, concise and contains simple steps you can easily implement – many at no cost – to protect your business. You can instantly download this report for free at www.b4networks.ca/free-technology-reports or you can call my office at **905-346-4966.**

This report reveals:

- The single most expensive mistake most small business owners make when it comes to protecting their company data.
- The universal misconception business owners have about their computer networks, and how it can end up costing thousands in damages.
- 6 Critical security measures every small business should have in place.
- How to greatly reduce – or even completely eliminate – frustrating crashes, slow performance, and other annoying computer problems.



Need help to implement an effective Security Plan for your business?

Call our office now: **905-346-4966** or email me directly here: **bryan@b4networks.ca**

4 Powerful Reasons Businesses Use VoIP to be More Productive…

VoIP is simply an acronym for Voice Over Internet Protocol and can be a vital solution to unify all your business communications.

This service allows you to communicate from anywhere in the world simply by using an Internet connection. Every company that switches to VoIP will see immediate benefits to their business, including:

1. Save Money

VoIP can save your company a lot more money on your phone bill because you pay a fixed amount per month rather than having to pay per individual call. If you have branches spread through the country or agents working about the globe, the cost savings can be enormous as you're making and receiving calls over the Internet.

2. Multiple Users

New lines can easily be set up without the need to purchase and maintain additional hardware. Plus, conference calls or team meeting using VoIP can be an easy way to make your meetings more productive and cost efficient.

3. Numerous Features

Some of the great features with VoIP services include Voicemail, Caller ID, and many other traditional services. Other features, which make VoIP a very powerful tool, include Conference Calling, Desk-to-Desk Calling, Automated Attendant, Music-on-Hold, and much more.

4. More Mobility

Many companies are allowing employees to work from home, rather than at the office. VoIP makes this both convenient and possible so your business can build and grow at it own unique pace. Use your VoIP line via a traditional system or on your smartphone for enhanced flexibility.

Client Spotlight

New Client Announcement:

We are proud to welcome aboard HearAgain Balance & Hearing Clinic as a client of B4 Networks.

Trust your hearing to a Doctor of Audiology.

At HearAgain Balance and Hearing Clinics all hearing testing and hearing aid fittings are performed by an Audiologist who is registered by the College of Audiologists and Speech and Language Pathologists of Ontario. All of the audiologists have either attained or are in the process of completing a Doctor of Audiology degree. Audiologists have both the training and expertise to help people cope with the challenge of hearing loss. Book an appointment today at one of their three Niagara locations. **St Catharines: 905-684-0100**

Niagara Falls: 905-354-2757, For Erie: 905-871-4242

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 insurance 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!

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."

TRIVIA CHALLENGE

The Winner of last month's Trivia Challenge Quiz is **Maryann Sheets** from **Ontario Environmental & Safety Network**

This months winner will receive a $50 Gift Card to a Fonthill Restaurant

This month's trivia question is:

Who was the month of June named after? Goddess of:

a) marriage and childbirth
b) fruit and trees
c) religion
d) love and beauty

To enter email me your answer: **bryan@b4networks.ca** or visit the site below

www.b4networks.ca/trivia

Submit your entry by the 25th of the month, and if your answers are correct, your name will be added to the draw for a $50 Gift Card.
*See website for full trivia rules

The B4 Networks Family

It seems our staff is a little shy this month, so we'll be featuring Bryan's family trip.

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 Wi-Fi and NEVER a public one. We recommend investing in a personal MiFi device that acts as a mobile Wi-Fi 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.

Services We Offer

- General Computer / Network Repair and Troubleshooting
- Network Design & Implementation
- Backup and Business Continuity Solutions
- Disaster Recovery Planning
- Anti Spam & Email Solutions
- Network Security / Firewall Solutions
- Fixed Fee Monthly Services Plans
- Remote Monitoring and Diagnostics, Troubleshooting and Repair
- Project Management
- Technology Consulting
- Hosted Exchange Service
- Cloud Services
- Virus and Spyware Protection

b4 networks
1462 Pelham Street
Fonthill, Ontario, L0S 1E0
905-346-4966
www.b4networks.ca
We Make Technology Work!