

TECHNOLOGY UPDATE

"Inside Tips To Make Your Business Run Faster, Easier and More Profitably"

What's New

**B4 Networks welcomes
Château des Charmes
as our newest client**

See Page 5 for more information

Girls in STEM

How B4 Networks is empowering tomorrow's women—today!

See Page 5 for more information

Win an iPad

See Page 4 to see how!

October 2017



"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

**170 Hwy 20 W. Unit 3A, Box 249
Fonthill, Ontario, L0S 1E0
Tel: 905-346-4966**



You're Better Off Giving Your Employees A \$1,000 Bonus Than Being Cheap With Technology

Imagine, for a minute, that you're the CEO of a scrappy, promising new start-up. In the beginning, it was just you and two other employees working on dinky PCs out of a 12-by-12-foot office, but times are picking up and the company is heading into the uncharted waters of rapid growth.

As the business moves into the public eye — and, in turn, the hungry eyes of potential hackers — it's become obvious that you're going to need to lock down your data. At this critical stage, a cyber-attack could mean the death of everything you and your team have built.

But the budget is looking lean. Everything you've done so far has been

by the skin of your teeth, so why should security be any different? You put one of your more tech-savvy employees on the case, tasking him with finding the cheapest cyber security solutions available. Sure, he may not be an expert, but he understands computers. What could go wrong?

He scours the web, perusing dozens of "Top 5 Cheap Firewall Software" articles, and, with the help of a scrappy how-to guide, installs what seems to be the best of the lot on your servers and across all your computers. The entire process takes 10 hours, and costs the company next to nothing.

Potential crisis averted, you turn your attention to other matters. We'll revisit

Continued on pg.2

Get More Free Tips, Tools and Services At Our Website: www.b4networks.ca

Continued from pg.1

our cyber security later, you think, once we have a little more financial wiggle room.

Across the following year, the company's success skyrockets. The phone is ringing off the hook, new business is flooding in and your profit margin is exploding. You even ended up snagging a feature in *Entrepreneur* magazine. Your company is the envy of all your peers.

That is, until the day that you get hacked. One morning, an advanced strain of ransomware easily sidesteps your free antivirus and starts wreaking havoc. It slithers through your systems and locks you out of *everything*, from client data to basic Word documents, and encrypts it behind a paywall, demanding \$50,000 in Bitcoin or you'll lose access to all of it — forever.

You couldn't make room in your budget for a robust cyber security solution. Well, how does that \$50K ransom strike you?

"The fact is, when your time, money and business are on the line, it simply doesn't pay to be cheap when choosing your cyber security technology."

Think of it this way. Say, with your free antivirus, you're "saving" \$100 a month. Lo and behold, a virus manages to punch its way through and causes chaos throughout the company server. Even if you're lucky and it isn't ransomware, by the time you've managed to expunge the stubborn virus from your business, you'll have put in countless man-hours, guaranteed to cost you more than that \$100 a month. Instead of throwing those thousands of dollars down the drain, you'd be better off giving each of your employees a \$1,000 bonus!

Free antivirus software, giveaway cyber-protection, or a \$5 firewall seems like a great idea, until a hacker cuts through your company's defenses like a warm knife through butter. These guys *love* when they see these outdated, cheapo barriers guarding your priceless data — those are the paper-thin defenses that keep hackers in business.

You wouldn't buy a rusty, secondhand old lock for your house, so why are you installing primitive cyber security software to protect your most precious company resources?

In today's world of rampant cybercrime, it's inevitable that somebody will come knocking at your digital door. When that day comes, do you want a free piece of software that you saw on LifeHacker, or a tried-and-tested, up-to-the-minute, comprehensive security solution?

Don't be shortsighted and risk everything just to save a quick buck. Invest in your company's future, and protect yourself with the most powerful tools on the market.



Just one ransomware attack can result in a serious financial blow if you're not prepared.

Visit www.b4networks.ca/dodge TODAY or call 905-346-4966 by October 31st for a

FREE Data Recovery Review
(ordinarily a \$300 Service)



- ▶ We'll provide you with a complete on-site assessment of your current backup system to check for and safeguard against any gaps that could prove financially lethal to your business.

A Diverse Team Is More Productive



Guest Article by Mike Michalowcz

Everyone knows the saying, "If you build it, they will come," from the 1989 film *Field Of Dreams*. Well, the same rule applies to the type of work environment you create, and, as a result, how diverse your team becomes.

Diversity may not happen overnight, but you can be sure that a diverse team means a broader range of perspectives brought to the problem-solving table. When employees feel accepted and comfortable in their workplace, you can expect them to take more chances on out-of-the-box thinking and creativity, not to mention increased productivity.

But you can't expect your employees to feel safe expressing their identities, and thus their ideas, if you don't first create an inclusive environment for them. But how do you create a space in which your team feels safe drawing from their unique perspectives?

One way to make your employees feel more visible and heard is through **diversity networks**, groups that come together based on shared identities, like single moms, veterans, LGBTQ individuals, Asian-Americans, the disabled or Latinx. These networks help individuals support and learn from one another, share resources and discuss the challenges and stereotypes facing this facet of their identity and how to address them. If you're worried that this could divide the office more than unite it, don't be. These networks empower individuals to share their experiences with the broader team, allowing everyone to learn from each other.

You also need to make sure you **allow opportunities for team members to express themselves**. The quickest way to make an employee feel uncomfortable and unaccepted is to have their co-workers interrupt or speak over them. Provide moments for individuals to talk about the projects they are working on, their goals and their struggles.

Diversity training can be helpful in the office. The fact is, everyone has a bias, and it's usually subconscious. Diversity workshops can be a great way to unpack our biases and privilege. Being able to listen and empathize is a vital skill in any business setting, and will improve not only communication between your employees, but their customer service skills as well. A diversity workshop should not be a lecture, but rather an opportunity for honest conversation and learning.

Institute an open-door policy so that your employees feel safe coming to you and their other bosses about issues of discrimination, sexism, racism, homophobia and more. First and foremost, listen. Don't invalidate their experiences by immediately questioning them or taking a side in the conflict. This, plus literally keeping your door open as often as possible, will instill a feeling of trust in your office.

Show that diversity is important to you by hiring employees who come from a variety of backgrounds. Your work team should ideally represent the full diversity of your customer base, enabling them to relate and appeal to your clients on a personal level. Representation also works as a strong motivator. When individuals can see themselves in their role models — bosses, podcast guests, interviewees, etc. — they'll be more likely to imagine higher goals for themselves.



MIKE MICHALOWICZ (pronounced mi-KAL- o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford—a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small business columnist for *The Wall Street Journal*; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book *The Toilet Paper Entrepreneur*. His newest book, *The Pumpkin Plan*, has already been called "the next E-Myth!" For more information, visit



Shiny New Gadget Of The Month

Picture Keeper Connect *The Best Way To Back Up Photos On The Go*



Nothing feels worse than having to delete an old favourite to make room for some new photos. The Picture Keeper Connect solves both of these issues, providing easy-to-use backup for your phone or tablet.

The Picture Keeper Connect, which looks a lot like a conventional flash drive, is designed specifically to back up photos, videos and contact information with just a couple of button presses. It plugs into your phone and gets to work. Even better, it can do all of this without the need for WiFi or network connection. It keeps your photos in their designated album, meaning you won't end up with a cluttered mass of photos when you transfer them to a new device.

Simple, functional, and portable, the Picture Keeper Connect is a must for any avid smartphone photographer.

Picturekeeper.com

Highlights of the Month

-  **October 1st**
International Coffee Day
-  **October 9th**
Thanksgiving
-  **October 18th**
Chocolate Cupcake Day
-  **October 22nd**
CAPS LOCK DAY
-  **October 29th**
Internet Day
-  **October 31st**
Halloween

BONUS INFO

Like and Share
our page on
Facebook by
October 31st for a
chance to win an
Apple iPad!

facebook.com/b4networks



Girls in “STEM”



In honour of Women's Empowerment Day, B4 Networks proudly hosted their first “Girls in STEM” fun and educational robotics mini-camp. The 2-hour activity was for girls aged 8-10 years old led by a local Niagara teacher. B4 Networks completely subsidized the event to make it a free event for the participants. The goal of the event was to empower tomorrow's women – today! It was a great success and everyone involved had a great time!



Château des Charmes—B4 Networks' Newest Client

Château des Charmes was founded in 1978 by Paul Bosc, a fifth generation French winegrower. Paul and his young family arrived in Niagara in the 1960's with the idea that growing their own grapes was the best way to make fine wine. More than ever, they believe in this Estate Winery model and they make their wine only from grapes they've grown themselves.

They believe they are custodians of the land. From the beginning they have been committed to using sustainable practices and are charter members of Sustainable Winegrowing Ontario. Paul and his team are meticulous. They use modern science and a lot of TLC to coax the best out of every vine. And with more than 30 vintages in their vineyards they think they now know which varieties grow best in which spot. But there is always more to learn. They believe their groundbreaking research with unique grape varieties will blaze a trail to the future of their industry.



Client Spotlight

Thorold Auto Parts & Recyclers is in the business of supplying garages, repair facilities and private individuals with quality recycled vehicle parts. But that's not all Thorold Auto Parts & Recyclers is up to in 2017.

Frank Serravalle, the owner of Thorold Auto Parts & Recyclers, says he and his team are working hard to upgrade and enhance their facility so they can serve their clients better than ever.

A member of the Ontario Automotive Recyclers Association, Thorold Auto Parts is one of the largest auto recyclers in southern Ontario with a huge inventory of auto parts throughout its 23-acre property. Thorold Auto Parts has over 200,000 recycled parts in stock at any one time. That includes a wide range of foreign and domestic models—everything from Honda and Mazda to Jeep, Nissan and Chevrolet.

Thorold Auto Parts has been part of the Niagara business landscape for well over 30 years now. Frank's father Lenny originally established

Thorold Auto Parts back in 1982, and passed the family business on to Frank in 2000. Since that time, Frank has made several enhancements to his operation. For instance, just a few years ago, Thorold Auto Parts doubled its recycling capacity by adding four new recycling bays and 4,000 square feet to its vehicle dismantling facility.

But the updates haven't stopped there. This past fall, Thorold Auto Parts began the first stages of an ambitious new expansion project, adding 10,000 square feet to their building to allow more room for parts storage and vehicle processing.

“We're always looking for ways to expand our clientele,” Frank says. “In order to do that, we're constantly improving ourselves and the way we do business—and our brand new expansion will be a big help in that department.”

Thorold Auto Parts and Recyclers is located at 1108 Beaverdams Road in Thorold. For more information, please call 905.227.4118 or visit www.thoroldautoparts.com.



8 Ways to Prevent Phishing Attacks

Phishing attacks are deadlier than ever. Here's how to train your employees to watch out for them.



Phishing schemes send duplicitous emails to businesses in an attempt to infect computers with malware. They're successful when an employee clicks a suspect link/attachment, or gets tricked into giving up financial information. When it comes to data security, phishing threats get less attention than more "active" malware attacks—And that's too bad, because today's phishing schemes are deadlier than ever. **A successful phishing attack could cost your company anywhere from thousands to millions of dollars.**

Protect your business—Here are eight tactics to put in place.

1. Encourage Suspicion.

Studies reveal that employees fall for phishing scams because they're trained to always be "nice." As a result, they comply with email requests from "clients" without any question. Experts advise taking a suspicious approach to all emails. If an email message "feels wrong, listen to your gut." Train your employees to follow their instincts when it comes to suspect emails.

2. Scrutinize URLs and Addresses.

You should always carefully examine all email addresses and URLs. With phishing emails, they tend to be a bit "off." The URL won't match the directions given in the message, or it won't be the real web address, rather a similar one. The same is true of email addresses, and company logos, watermarks, and signoffs. If you simply glance at this information, you may be fooled. If you take closer look, you'll realize it's a counterfeit. Train employees what to look for if they come across an unexpected email and to always pay attention to the details.

3. Think about the Message and Logo.

Phishing scams can be very subtle. Advanced phishing attempts may take over email clients to send messages from what appear to be very reputable sources. This is why it's essential to stop and think before taking action—*especially when money or sensitive information is involved*. Train your employees to examine the message. Is it unusual? Is it unexpected given what they know about the project or client? If they get a message that says, "Wire \$5,000 right away for patent rights or we will lose this market," this should raise warning bells—Why didn't this person make a call or explain this in person? Any emails that focus on a disaster or emergency like this should be immediately suspected.

4. If You Don't Know the Person, Stay Away from the Email.

Don't recognize who the email is from? Then don't do anything. This policy protects employees from phishing emails that get through your spam filters. If the email is from an address they don't recognize, they should ignore the message. If necessary, they should forward it to the appropriate account manager and ask if it's legitimate. It's always worth taking a little extra time to confirm messages, rather than falling for a phishing scheme.

5. Call for Confirmation.

It's amazing how many people don't do this, even with extraordinary requests. Successful phishing emails *depend on you not calling the sender and asking what's going on*. Calling the sender can destroy the most careful phishing attempts. (At the highest level, phishing may include fake phone numbers or rerouting, but this is quite rare.)

6. Stay on Top of the Latest Phishing Schemes in Your Industry

Phishing schemes vary between industries (based on how much money can be conned out of particular businesses). Research the phishing schemes trending in your industry, and what warning signs to look for. A variety of services offer intelligence reports for this very purpose. You can also visit security zines and forums that focus on your industry. These are typically updated with the latest cyberattacks.

7. Block Access.

Eventually, companies reach a size where trusting employees to avoid phishing attacks becomes very difficult. It's important to use strong firewalls and updated security filters to block access to any dangerous or illegitimate sites (the same goes for downloads, etc.). This is essential to mitigate damage once phishing emails are opened. Phishing scams can't hurt your business if they can't upload malware.

8. Adopt Email Authentication Standards

Email authentication standards are improving all the time. They provide an excellent way for companies to stop spoofing attempts both to and from your organization. Basically, it authenticates senders and makes sure that an email really did come from that sender. This tactic also makes it more difficult to spoof emails from your company. The current standard is DMARC (Domain-based Message Authentication, Report and Conformance). So, if your business is a target of phishing scams, look into adopting this standard for added protection.

Need help protecting your business in Niagara from Phishing attacks?

B4 Networks is ready to help.

Contact us at help@b4networks.ca or call us at **905-346-4966** for a no-obligation, complimentary consult.

News Brief

NEVER Throw Your Boarding Pass Away, Not Even After Your Flight

Everybody knows that a boarding pass is mandatory in order to board a plane. While we're in the airport, we keep a close eye on our boarding passes, clutching them in our hands like they're precious gems. But after we land, pretty much everyone ditches the ticket, whether it's lost on the floor, compacted in the washing machine or thrown directly into the trash. This may seem innocent enough, until you realize the abundance of personal information encrypted on your pass. You'd be amazed at the information a person can glean just by scanning the QR code on the ticket: your home and e-mail addresses, your phone number and even your bank information! When you get rid of your next boarding pass, shred it. Your bank account will thank you.

LuxuryAndGlamour.com 2/5/2016

Are You Missing This One Critical Component In Your Business? If So, You Are GUARANTEED To Be Losing Sales

As Inc. writer Rohit Arora puts it, "It may be 2017, but many companies are still conducting business like it's the 20th century." According to data collected in a recent CNBC report, close to half of small businesses don't even have a website, and even fewer — around 36% — use a website to stay in touch with their customers and prospects. But if we can learn something from Nick's Pizza & Deli in New Jersey, it's that even the smallest companies can leverage new technologies to dramatically increase sales. The restaurant partnered with a company called The Block, a business that builds websites for small businesses, granting them online ordering capabilities. As a result, Nick's owner estimates an increase in annual revenues of around 15% to 20% in only six months. When you make it easy for your customers to pay, you drive further sales. It's that simple.

Inc.com 8/6/2017

Here is what a client is saying about us:

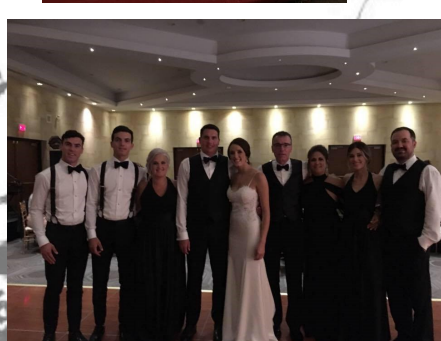
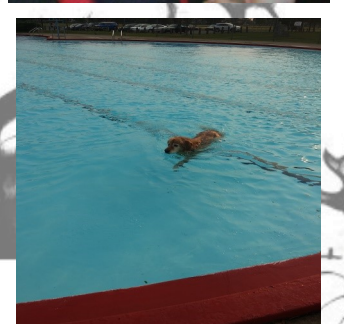
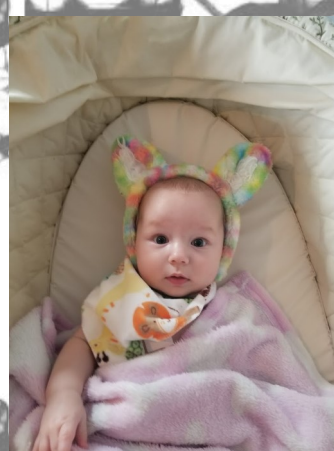
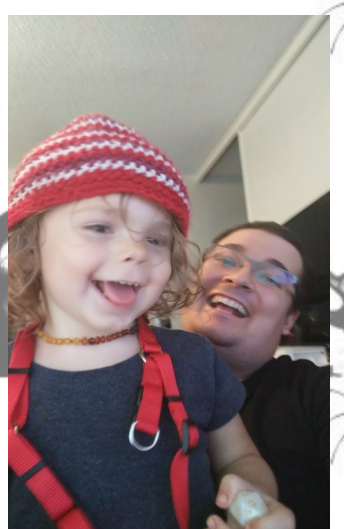
"We have recently started working with B4 and their response time and quality of work has impressed our team. As one of the primary projects, we switched from our old host provider to Office 365 and they were able to help us with little to no delay time in our operations. They are a great team and I would recommend people to use B4 for all IT needs."

Vlad Cojacari—Nuvest Management Services



Get More Free Tips, Tools and Services At Our Website: www.b4networks.ca

Photo Album



TekTip

Create A PDF on your phone



Instead of making PDF files with your phone's camera and scanner, here's a tip on how to create a PDF with the files you have already saved on your phone.

If you use an Android (process may vary depending on the device), simply click on the three dots in the top-right corner of the screen and select print. When asked to select a printer, choose *Save as PDF* and choose where you'd like it stored on your phone.

For iOS 10- when there is a message or page open— select the Share menu icon and select print. A print preview will appear and by putting your fingers on the screen and pinching outward, a PDF document will be created. Simply tap on the Share menu icon one more time to send or store the new file.

B4 Networks is the trusted choice when it comes to staying ahead of technology developments and can provide you with tips, tricks and news.

Contact us at **905-346-4966** or send us an email at help@b4networks.ca for more information.