TECHNOLOGY TIMES

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

What's New

B4 Networks named one of Canada's Top 50 Best Managed I.T. Companies

See pg. 5 for more information

March 2018

"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.

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

5 Ways Your Employees Will Invite Hackers Into Your Network

Whether they're criminals or heroes, hackers in the movies are always portrayed as a glamorous group. When it comes down to the wire, these are the individuals who crack into the ominous megacorporation or hostile foreign government database, hitting the right key just in the nick of time. They either save the day or bring down regimes, empty the digital vault of the Federal Reserve or disable all the power plants in the country. It's always a genius up against an impenetrable fortress of digital security, but no matter what, they always come out on top.

In real life, it's rarely that difficult. Sure, if you look at the news, you might believe hackers are close to their Hollywood counterparts, stealing data from the CSEC and nabbing millions of customer records from Equifax. But the majority of hacks aren't against the big dogs; they're against small to mid-sized businesses. And usually, this doesn't involve actually hacking into anything. A lot of the time – approximately 60% according to the *Harvard Business Review* – an unwitting employee accidentally leaves the digital front door open.

The biggest threats to your company aren't teams of roaming hackers; they're your employees. Here's why.

1 They'll slip up because they don't know any better.

With the proliferation of technology has come an exponential rise in digital threats of such variety and complexity that it'd be impossible for the average person to keep track of it all. Each of your employees' lives are a labyrinth of passwords, interconnected online accounts and precious data. If their vigilance slacks at any point, it not only leaves them vulnerable, but it

Continued on pg.2

Continued from pg.1

leaves your company vulnerable as well. For this reason, most cyber-attacks come down to a lack of cyber security education.

2 They'll let you get hacked on purpose.

It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data to malicious groups. Whether it's info vital for your competitive advantage, passwords they can sell to hacker networks to make a quick buck or sensitive data they can make public simply to spite your organization, it's difficult to protect against a double agent.

3 They'll trust the wrong person.

For many hacks, little code is needed whatsoever. Instead, hackers are notorious for posing as a trusted member of your own team. And if you believe that you'd be able to spot an impostor from a mile away, you may want to think again. Not only is it easier than ever to crack individual users' e-mail passwords and login credentials, and personal info is now littered throughout social media. A simple visit to Facebook can give a hacker all they need to know to "social hack" their way into the heart of your business.

> **"It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data... but there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people."**

4 They'll miss red flags while surfing the web.

Clickbait is more than a nuisance plaguing your social media feeds. It can be a powerful tool for hackers trolling for easy prey. If an employee doesn't understand what exactly makes a site or link look dubious, they may open themselves – and your company – to browser exploits or other types of attacks.

5 They're terrible at passwords.

According to Entrepreneur.com, "3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more." Even more of those passwords are simply weak, inviting easy access for unsavoury elements. Many people brush off the importance of strong passwords, but the risks posed by the password "123456" or "password" cannot be overstated.

When it comes to defending your precious assets against digital threats, it can seem impossible to protect yourself at every turn. But there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people. Through a comprehensive security training program, including specific examples of methods hackers use – particularly phishing – you can drastically minimize the risk of an employee accidentally opening up a malicious e-mail or posting sensitive info. When you make a concerted effort to make the entire organization vigilant against cyber-attacks, you're much less likely to be targeted.

How Does Your I.T. Company Compare?

Our February 2018 Service Key Performance Indicators

90%

8 Business Hour Ticket Resolution

96%

Client Satisfaction

10 mins

Average Response Time

Shiny New Gadget Of The Month:

FIXD

When was the last time you turned on your car, pulled out of the driveway and suddenly noticed the engine light pop up on your dashboard? You probably just ignored it and drove to your destination. Maybe the next day you spent some time trying to get to the bottom of the issue, only to come up short. Everything seems fine, so what's going on?

A new device called FIXD aims to figure that out. After plugging in the $59 USD, palm-sized widget into your car's onboard diagnostics port – the same one mechanics use to find potential issues – it can communicate with a free app to tell you precisely what's wrong with your vehicle. You can determine why your engine light is on, how serious the problem is, and whether it requires emergency repairs, all without risking being ripped off by shady mechanics. If necessary, the device can actually turn off your engine light right from the app, making it a nuisance of the past.

www.fixedapp.com/buy

Cash In On Your Million-Dollar Idea

By Mike Michalowicz

So, you came up with a brilliant idea. A million-dollar idea, even! But right now, that's all it is. The question is, how do you turn that big concept into cold, hard cash?

1. Write it down. How many light-bulb moments do you have at 2:00 a.m. and then forget come 9? Or, worried that your idea will be stolen, you keep it to yourself, promising to chase it down when you finally get the time. If you actually write down every money-making scheme you think up, one of them is bound to be the real deal eventually.

2. Once you settle on the idea you want to pursue, write a pros-and-cons list. What could make your idea truly successful? What could make it a total bust? Once you identify the cons – a too-high initial production cost or a newcomer in a competitive industry – you can start your search for solutions.

3. Determine your audience. Who do you think will buy your product or service? Run business surveys to determine whether there's a market for what you want to sell.

4. Figure out what problem you're solving. Uber eliminated the inconvenience of hailing a taxi and the difficulty of pre-ordering a ride, all for an affordable rate. Apple lowered the cost of technology and made it user-friendly at a time when computers were designed for engineers and tech professionals. If you solve a real problem that exists in the market, consumers won't be able to live without your product.

5. Find a business partner. Although you may want to keep your idea to yourself, remember that it takes two flints to make a fire. How many successful start-ups do you know that were founded by a single person?

6. Start to think about money. If you don't already have some rainy-day funds to dive into, consider crowdfunding, borrowing from friends, credit cards or loans. Know the risks you're taking before moving forward.

7. Create a financial model. If you want to attract investors, a financial model that forecasts the fiscal performance of your business will show them your expected profitability and their return on investment. This makes you a more reliable bet.

8. Develop your prototype or beta test. This will allow you to see if your idea will actually work in the real world.

9. Prepare to be flexible and roll with the punches. Odds are, your initial idea won't be the same as your final product, and that's okay.

10. Keep on the sunny side. There are going to be truckloads of people who try to tear you and your idea down on your road to success. Stick to your guns – it's your baby and your investment of time and money, so make sure you believe in it.

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 www.mikemichalowicz.com.*

The "Not Me!" Problem…And Why This Is Almost Guaranteed TO Happen To You Security this, password that – now they want a password with 14 characters with two symbols? And I have to change it every three months? As difficult as it is to remember 24 different passwords, four PIN numbers and a slew of new cyber security processes, we still manage to instantly recall most of the tangible things in our lives. The code for the company door and alarm system, the passcode to our phones, the garage code, the other garage code – you get the idea. But these numbers are based upon a time when the most "real" threat seemed to be someone busting in our door and threatening our families in the middle of the night. In 2018, those kinds of physical threats are far less statistically prevalent than cybercrime. In fact, data breaches and identity theft are occurring at three times the rate that home burglaries occur in the U.S. according to a 2016 study by the University of Kentucky.

Don't succumb to the "Not me!" approach to the shift in crime. Understand that it can happen to you, and approach all aspects of physical and electronic security with the attention they deserve.

7 Things Mentally Strong aders Never Do Leaders need to stay mentally sharp to effectively lead their teams. Here are seven things that truly strong leaders never, ever do.

1.They don't mask their insecurities, but instead maintain their humility and acknowledge their mistakes and weaknesses.

2. They don't go overboard with their emotions. Instead of suppressing their feelings, real leaders stay aware of how their emotions influence their behavior.

3. They accept criticism with open arms. Instead of protecting a fragile ego, mentally strong leaders take unfavourable feedback and use it to improve their processes.

4. They take responsibility for their actions. When a good CEO messes up, they apologize with sincerity and accept the consequences of their behavior.

5. They don't mistake kindness for weakness. Offering extended bereavement leave isn't letting your employees take advantage of you – it's a common courtesy.

6. They don't confuse confidence with arrogance. Though they're sure of themselves, a good leader recognizes the necessity and competence of their team. They don't put themselves over others.

7. They don't fear other people's success. When someone else is doing great things, they know that it doesn't diminish their own accomplishments.

Inc.com 12/12/2017

March Fun Days of the Month

- March 1st • **World Book Day**
- March 2nd • **Employee Appreciation Day**
- March 8th • **International Women's Day**
- March 17th • **Saint Patrick's Day**
- March 20th • **First Day of Spring**
- March 25th • **Waffle Day**
- March 31st • **World Backup Day**

Client Spotlight: **The Mentholatum Company of Canada, Ltd.**

The Mentholatum Company was founded in the USA in 1889 and opened its Canadian head office originally in Fort Erie in 1904. Mentholatum Canada is a small Health & Beauty/ Pharmaceutical company, now located in St. Catharines, Ontario. Mentholatum Canada competes in multiple product categories with internationally recognized brands such as Oxy (acne care), Deep Relief (topical pain relief), Softlips (lip balms), as well as smaller brands such as pHisoderm (facial wash), Provacare (anti-fungal), and their original product Mentholatum Natural Rub (cough and cold). They currently manufacture and sell cosmetics, medical devices, natural health products and over-the-counter drugs. They are dedicated to providing effective solutions for your health and well-ness and prides itself in offering high quality innovative products that delight their customers and exceed their expectations.

B4 Networks Named One of Canada's Top 50 Best Managed I.T. Companies

B4 Networks has been named one of Canada's Top 50 Best Managed I.T. companies for 2018. The event is hosted by TechnoPlanet, an international channel marketing and communications company that specializes in the technology industry. The recipients of the awards are chosen by a panel of eight established and independent judges within the industry. The winners were selected based on an in-depth review of the best practices that are used to run their business spanning over 12 different categories.

View our Press Release Online: www.b4net.ca/best50

Do You Know Someone That Needs Computer Support?

In our opinion, referrals from very happy clients and their employees are the greatest form of flattery. We love it when you're so pleased with our services, that you're willing to recommend us to other business owners you have a relationship with!

If you know someone who is looking for computer support for their company, you will receive $100 for every referral you send our way.

If your referral becomes one of our managed clients, you will receive a cheque to the amount of one month of their signed agreement. That could be up to $5000 in your own pocket!

For full details about our referral program and to submit your referral, please visit www.b4networks.ca/referral-program today and get us in contact with your friends today!

The Comprehensive Guide to Understanding and Stopping Ransomware

Cybercriminals are everywhere. Both domestically and around the world, countless hackers work day in and day out to penetrate the digital defenses of businesses just like yours, using a variety of proven, effective, and ever-evolving methods. Whether they infect your system with malware hidden in a seemingly innocuous email attachment or con an unsuspecting employee out of vital information through social engineering, the end results are the same: data loss, financial damages, lawsuits, reputational damage, bankruptcy, and worse.

Our team of certified system professionals understand how serious the modern threat of cybercrime is to businesses in your industry, which is why we've developed this whitepaper as a vital resource to show you how hackers think, what methods they use, and how you can stop them from victimizing your business. Without the right knowledge, tools, and technology to prevent hackers from stealing your information, your business is left prone to a major data breach.

A recently popular type of malware is the "ransomware" variety, which encrypts a victim's files (making them unreadable) and only offers the key to recover them after a ransom has been paid. The unfortunate reality is that when it comes to your business' vulnerability to ransomware and other types of malware, it's not a matter of IF, it's a matter of WHEN. There are simply too many varieties of ransomware to guarantee total safety for your business.

IT security can be a complicated and scary subject when it comes to modern cybercrime tactics such as ransomware.
Most business owners cannot confidently claim that their business' network is secure. Can you?

When it comes to ransomware, the most important consideration is email security, and often, it can be as simple as ensuring that you and your staff know what to look for.

What makes a victim a victim?

The short answer is lack of awareness. Almost no hacking attempt can be a success without the victim playing at least some role in the process, such as:

- Visiting a malware-infected, unsecured website, either via an email, inappropriate browsing habits, or otherwise.
- Opening an untrustworthy attachment in an email from a hacker that's disguised as coming from a sender such as a business contact, employee, client, government agency, etc.
- Downloading files that include a stow-away malware program or virus.
- Conducting any of the above while logged in with administrator rights provides even greater access to the hacker that's infecting the system.

The bottom line is that digital security begins and ends with the user. Regardless of how modern, expensive or well-recommended your security software is, one wrong move by a single employee can be all it takes to infect your system. But that's not the only threat to your security.

Is your technology making you an easy mark?

Outdated, unsecured, and just plain faulty technology is just as likely to make you an ideal target for hackers as an unsuspecting employee is. A major part of the investment in new technology is that it comes prepared to handle all previously identified hacking threats and security loopholes. The older your technology is, the more vulnerable it is to new hacking techniques.

Here are three vital considerations you should keep in mind

Don't take our word for it. Here's what a client is saying about us:

"The personal service is bar none, the best I've ever seen, the service is just phenomenal."

Our old provider was very frustrating. They meant well, but it was very hard to get service. We would be down for hours, and sometimes days, or even weeks before things would get taken care of. Now with B4 Networks, the service is phenomenal. Our staff is never unhappy, B4 Networks is here sometimes before I am. If they spot a problem, they will be waiting in the driveway before I even get here. The personal service is bar none, the best I've ever seen, the service is just phenomenal.

Pamela St. Jean, Administrator,
Thorold Auto Parts

(Continued from page 6)

when evaluating your current technology:

- **Patch regularly, and patch often:** Did you know that the most common way cybercriminals get into a network is through loopholes in popular third-party programs? That means the computer programs you rely on to get work done every day could be leaving you vulnerable to security breaches if you fall behind on updates. That's why patch management is such a crucial part of proper IT security, in order to help you stay ahead of the non-stop tide of oncoming digital threats.
- **End of Life (EOL) is FINAL:** As good as it is to run a frugal business, it's important to keep in mind that you're not a college student trying to make an old, beaten up laptop last until you can afford a new one. You're running a business, with much more to invest in and much more to lose. When your software reaches EOL, it will no longer receive the vital security patches it needs to keep you safe. At that point, as much as you may like the current operating system, you have to let it go and replace it with the new, secure version.
- **Legacy technology isn't worth the risk:** Legacy software is often the gap in an otherwise capable suite of digital armor. Your business may have a brand new infrastructure, top-of-the-line security technology, and fresh-out-of-the-box desktops, but in the end, your unpatched, out of date legacy web browser

What is malware, exactly?

It's a word you've probably heard a lot. You know it's bad, and that you have software (anti-malware) designed to help you stop it. But in the end, if you don't really understand how the enemy operates, how can you expect to defeat it?

Malware comes in many different forms and is used by hackers in a number of different ways. It can be used to steal information, locate vulnerabilities in your IT systems for a secondary attack, or simply to cause damage. While cybercriminals continue to innovate new forms of malware and the ways they use it, there are currently three main types that you should be familiar with:

- **Malicious Scripts:** This type attacks when you or a member of your staff visit the wrong web page. With the right conditions (user with admin rights, an outdated browser, lack of anti-malware software), simply loading the wrong web page is enough to infect your system.
- **Embedded Media:** While this form also attacks from a web page, it is through an infected media that is embedded in the site, such as a video or audio file. If your browser media player isn't up to date (which is extremely common among today's users), simply playing the media file can lead to a malware infection.
- **Infected Files:** The oldest form of the three is also the simplest. By downloading and running files (media codecs, screensavers, desktop images, etc.) that they haven't properly inspected ahead of time, or that contain a hidden malicious file, the user openly invites malware into the system.

How Can You Keep Your Business Safe From Ransomware?

When developing your ransomware defense, keep these recommendations in mind:

- Make a considerable investment in a comprehensive backup data recovery solution so that you can restore your data at a moment's notice when necessary.
- Test your backup and cybersecurity measures thoroughly and regularly; create dummy files and then delete them to see how fast they can be restored, or schedule a day to literally unplug your critical systems to find out how long it takes to get online again.
- Be sure to make the most of the available resources (both provided online and through expert IT consultants) to ensure that you're not overlooking vulnerabilities in your IT security methodology.
- Employ email filtering, encryption, and continuity solutions to ensure that your lines of communication are secured.
- Equip your business with industry-tested security solutions like firewalls, antivirus, antimalware, and network monitors to keep your systems safe from external threats.
- Make sure your software and browsers are updated and patched on a regular basis.
- Train your employees in best practices for safe browsing and email conduct so that they don't click the wrong link or download the wrong file.

Seems like a lot, right?

That can be a lot to handle for a business owner like yourself. You have clients to see to, employees to manage, and more on your plate every single day; should you really be expected to also oversee regular maintenance of your cybersecurity all on your own?

Of course not!

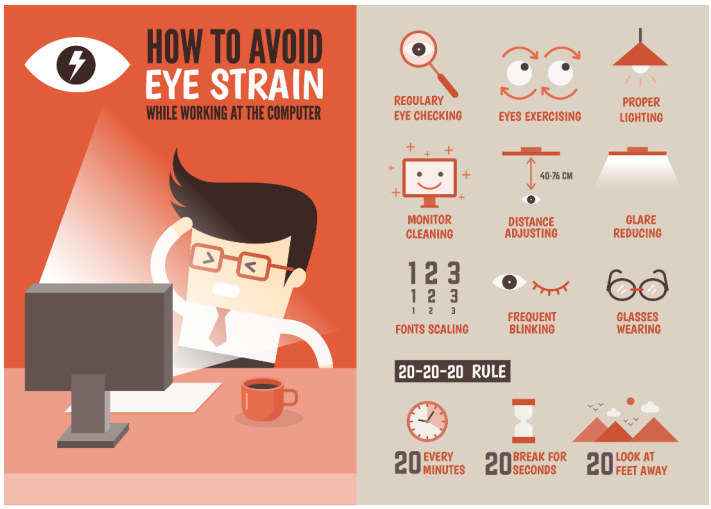
The best way to ensure that your business is kept safe is by outsourcing your cybersecurity management to a reliable and experienced Managed Services Provider like our Information Systems experts. For an easily budgeted monthly flat rate, you can enjoy the peace of mind that comes with knowing your business is safe from the whatever modern cybercriminals may throw at it.

Technology is a critical ingredient in your recipe for success. Don't neglect your technology solutions.
Call (905) 346-4966 or email us at help@b4networks.ca today

TekTip

Photo Album

- To avoid eye strain while working at your computer, follow the 20-20-20 rule. Every 20 minutes, look at something 20 feet away for 20 seconds.



- If you're sick of YouTube ads playing while you're mid-video, download *Adblock for YouTube* from the Chrome webstore and say goodbye to those interruptive ads forever!

- Press F2 immediately to rename a file without having to double click the file.

- If Google Chrome freezes, hit Shift + Esc. Chrome has an inbuilt Task Manager to follow you to force quit the application.