What's New

Two Became One

The entire B4 Networks team would like to send our congratulations to Alex Vandersteen and Candace Brouwer-Vandersteen on their wedding this past September. May the years ahead be filled with lasting joy.

Welcome!
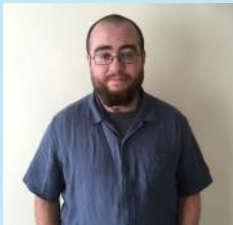
Meet Andrew Vandersteen! If you've called our office in the past few weeks, no doubt you've been greeted by a different voice on the other end of the line. Andrew Vandersteen is our brand-new service technician and is one of the technicians that will answer our phone, and help you with your service requests. Andrew has worked for John Deere for the last 2 years as a hardware technician, and before that with Niagara College for 3 years as a service technician, so he truly understands customer service. He's a real asset, and we're happy to have him on our team. Next time you call in, welcome Andrew to our team.

"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**

The One Attack No Tech Can Stop

You can defend your data with all the latest and best technology. But if just one team member gets tricked into giving away the keys to the castle, it's game over. Hackers know this. And that's why so many use social engineering to break in.

And it's not just the big companies you hear about on the news. On February 3, 2016 a suspect posing as the CEO of Magnolia Health Corp. obtained a spreadsheet with sensitive data about their employees. On February 23, someone posing as an employee of Central Concrete Supply Company obtained confidential records and disappeared with them.

In a 2011 survey, Check Point Software Technologies found that nearly half of the companies surveyed reported one or more social engineering attacks resulting in losses ranging anywhere from $25,000 to $100,000 per occurrence.

Unfortunately, there just aren't any tricks or tools that will automatically prevent a clever "social engineer" (SE) from breaking in. The keys to protection are awareness and vigilance. To help you know what to watch for, here are five common ploys - and how to deflect them:

Familiarity - In this type of scheme, the hacker becomes familiar to an employee. Social networking sites can reveal an employee's schedule and favorite hangouts. The hacker might then frequent the same bar or restaurant. After a drink or two, some key fact may slip out... The best way to bust this ploy is to be careful to not get lulled into a false sense of security around people you haven't thoroughly vetted.

The Consultant - A social engineer poses as a consultant for hire. Once they get the gig they can scoop up all the info they need from you and your team because of their seeming authority. Watch for this especially with IT consultants. Do NOT trust blindly. Vet every consultant, and never give all the keys to the kingdom. Just because someone has the skills to fix your server or network doesn't mean they won't steal your data. Vet thoroughly, and, as Ronald Reagan said, 'trust but verify'.

Piggybacking - The social engineer waits by a secured door for someone to

How Often Do You Really Need To Replace Your Hardware?

There has been a lot of debate as to what your hardware refresh cycle should look like. The answer tends to fall somewhere in the 2 – 4 year range, with recommendations from hardware manufacturers leaning more towards a shorter cycle. But there is no one right answer to this question.

There are actually a few questions you need to ask in order to figure out what best suits your business:

- **What do you need your computers to do?** – If your employees routinely have multiple programs and applications running at the same time, system speed is important. The heavier a computer's typical workload is, the shorter its ideal lifespan.

- **What is the productivity cost of not upgrading?** – Waiting longer to replace older systems saves money, but saving money at the expense of employee productivity could be more costly in the long run. If your staff is forever waiting on lagging software to load so that they can complete basic tasks, it has the potential to affect your business as a whole.

- **What are you willing to spend on support costs?** – The older a piece of hardware is, the more maintenance and upkeep is required to keep it running. More than just the hardware itself failing, there is also the cost and hassle of maintaining multiple versions of operating systems and software. Deciding how long you're willing to juggle these costs is a big factor in figuring out what your refresh cycle should look like.

Some of the cost of upgrading can be offset by choosing lower-end hardware in situations where you know your refresh cycle will be shorter. If you know you can use a cheaper option without it impacting productivity, settling isn't necessarily a bad thing. It's all about getting the most out of your business' technology budget.

Have questions about your business' hardware refresh cycle? Contact us at: **help@b4networks.ca** or **(905) 346-4966.**

Tek Tip of the Month

Have one of your internet accounts been compromised?

Are you concerned your email address and password used to register for websites through the internet has been compromised?

Haveibeenpwned.com will check the entered email address against the list of breaches that have been publicly announced. If it finds anything it will also show you information about the breach and what data was compromised (email, passwords, credit cards etc.)

If you find anything, it's recommended you change those passwords right away.   And if you use that password for your actual email account as well, change your email password as well to a unique password, and don't use it anywhere else.

Alex Vandersteen
Network Administrator

Need Help Right Away? Call our team 24/7 at 905.346.4966.

The One Attack No Tech Can Stop

use their passcode and enters right behind them. Or the Social Engineer struggles with a heavy box and asks a legit employee to hold the door open for them. Being kind and helpful, the employee helps the SE right into the building… free to do as they please. To foil this one, never forget the dangers of allowing a stranger in without proper clearance.

The Interview - Key information often escapes during interviews. A smart social engineer will gain an interview and deftly pick up all the information they need to hack into your network. Make sure any data provided during an interview offers nothing in the way of secrets. Keep the conversation light, or even superficial to avoid leaking critical data.

Angry Man - You may have seen this on TV… Somebody has an angry tone on the phone, or is grumbling to themselves as if they've just had an argument. We all tend to avoid people like that. Enough people avoid them and the way is cleared into the heart of the company - and your data. Don't go along with it. When you see this exploit unfolding, call security.

The key to preventing social engineering attacks is a well-trained workforce. You and your people may be your company's greatest asset. Yet without regular, proper training, human beings can be the weakest link in your company's data defenses.

Here's how to protect your network from a costly cyber attack

As a fellow business owner in the Niagara area, I'd like you to take advantage of my extensive research and experience in protecting data networks for small and medium companies. My business owner's guide, "*The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Cause Total Chaos*" steps you through 10 ways to protect your company from the coming deluge of cyber attacks we can expect over the next several years and beyond.

Call me today at 905-346-4966 or email me at bryan@b4networks.ca to get yours, FREE. We've still got a few of the hard copy versions I'd like to send you, so call or email me now while they're still available. I look forward to sending you this valuable guide right away.

The Top 10 Ways Hackers Get Around Your Firewall And Anti-Virus To Cause Total Chaos

This guide will reveal the 10 most common ways hackers get around your firewall and Anti-Virus to cause you chaos.

You'll Discover:

✓ The 10 most common ways hackers get into your network.

✓ Some tips on how to cover up some of these 10 holes.

✓ What the #1 way hackers use to bypass security protocols.

✓ The #1 way to fight back against new ransomware attacks

To get your copy, email me directly at **bryan@b4networks.ca**, and I'll reply to you with a copy. I promise you won't be spammed or have your information sold. I hate junk mail too!
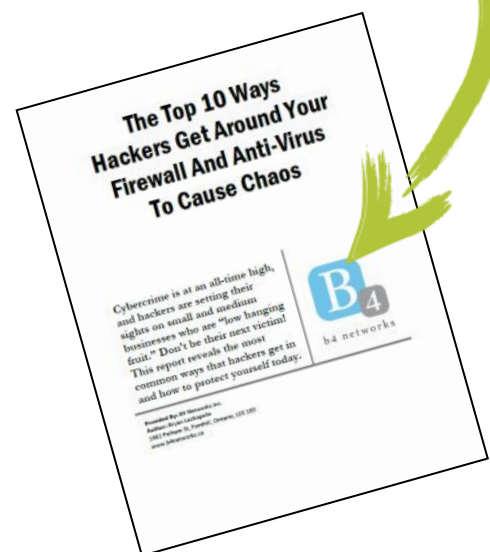
Who Owns Your Domain Name?

Recently, we successfully helped a client retrieve ownership and control of their domain name from their less than co-operative previous web service provider. Unfortunately, this was not the first time we've encountered an issue like this and likely won't be the last. I wanted to take this opportunity to provide some information that will hopefully help educate business owners on the potential pitfalls and security measures related to domain name ownership.

First, let's understand some terminology

- **Domain Name:** The unique URL related to your business. (i.e. tenpine.ca)

- **Registrar:** An organization that manages the reservation of domain names.

- **Registrant:** The person, company or entity who owns or holds a domain name.

- **Administrative Contact:** The individual who is authorized by the registrant to interact with the registrar.

So, who owns your domain name?

Let me make it clear that when you pay to have your domain name registered, whether that be directly to a domain registrar or to your web service provider (who handles the domain registration on your behalf), you own that domain name. Even if you do not have access to the domain name and even if you're not listed as the domain Registrant, there are systems in place to protect you.

Even in the worst case scenario, where your relationship with the Registrant has become adversarial, all hope is not lost. The organization that oversees domain names, www.ICANN.org, has developed a "Uniform Domain-Name Dispute-Resolution Policy" for such cases. Under this policy, a company that owns a domain name that's completely unrelated to its core business may have a hard time holding onto it. For example, if "Walters Web Services"

owns the domain name BillsExpertPainting.com, and Bill wants to take over ownership of that domain name when Walter has become unresponsive, common sense will play a major role in resolving the dispute.

How to avoid the hassle

Hopefully the above is a nice comfort for you, and that you are now more aware of your rights and options in terms of domain name ownership. However, the best way to deal with domain issues, is to avoid them altogether. If you're looking to be protected, there are two options we recommend:

1. Register your domain name directly. You can create an account with a company like Hover.com, or NetworkSolutions.com to register your domain name yourself. You would be responsible for payment and annual renewals, but this would be your safest bet to make sure your domain name is under your control. You can always provide your web service provider the login credentials to access the domain name when needed (such as when it's time to point the domain name to make your completed website live).

TIP: Make sure to use an email address

that you will always use and have access to when setting up the domain name. All renewal & update notices will be sent to the email address that the Registrar has on file, and in the event of a possible dispute or simply an account password recovery, this email address will play a significant role.

2. Have your web service provider put the domain in your name. They can still be the ones responsible for the management of the domain name, and you can still pay your web service provider to look after the domain name. However, if you're looking for more peace of mind, you can have them make sure your information is listed as the Registrant of the domain name.

TIP: Also be aware who is the Administrative contact of your domain name. The Administrative contact is the one who approves any requested changes to the domain. So, although the Administrative contact is not the legal owner, they do have significant power.

In many cases, such as is the case with Tenpine, clients are very comfortable allowing their web service provider to register and control the domain name on their behalf. They prefer the hands off approach and would rather an experienced professional handle as much as possible. However if you're the type of person who understandably wants full control over things, or if you've recently lost trust in your current web service provider, at least you know there are options no matter what stage of the process you're currently in.

If you have any specific questions relating to website or domain name ownership that weren't covered above, please do not hesitate to contact me and I'll be happy to provide some insight.

Is it time for you to re-evaluate your website? **Email myles@tenpine.ca or call 905-401-3685 to speak with Myles at Tenpine Web Development.** Tenpine is a full service Web Development Firm located in Niagara.

Testimonial From A Great Client

"Get off the fence, the grass IS greener with B4"

"The biggest benefit for us since moving to B4 Network's is that I'm no longer the IT guy, trying to figure out every problem myself. I direct all those technical issues to B4 and they get handled, and as a result I'm now able to get more usable time out of my day. Compared to all the other IT firms I've worked with in the past, B4 Networks responds very quickly and more importantly efficiently. If you're looking to make a change in your IT, get off the fence, the grass IS greener with B4 "

- Jamie Treschak., Operations Manager, Treschak Enterprises

Guest Article:
The Myth Of Multitasking… And What To Do Instead

"My kids are natural multi-taskers!" a friend exclaimed. She bragged that they could listen to music, watch TV and do their homework all at the same time. She might have been proud of their efforts, but she wasn't accurate about their abilities. Research has concluded that it will take her kids longer to do their homework and likely they won't do it as well.

We think of multitasking as the ability to successfully perform more than one activity at the same time. It has become a seemingly ubiquitous phenomenon like walking in the park while talking to a friend. But there is a difference: walking doesn't require our cognitive attention, so we are free to concentrate on our conversation. Other situations are more complex. For instance, it's a different matter to read a book and listen to a lecture.

In reality, what we commonly refer to as multitasking is the rapid shifting of attention from one task to another that creates the illusion we are performing them concurrently.

Nancy K. Napier Ph.D., in her article, The Myth of Multitasking said, "…much recent neuroscience research tells us that the brain doesn't do tasks simultaneously, as we thought (hoped) it might. In fact, we just switch tasks quickly. This rapid switching of tasks makes us prone to error and ends up consuming more time than if we undertook one task at a time.

Workplace demands often create the perceived need to continually switch tasks. That makes people less effective. The ability to do a thing well and quickly requires full attention, and the myth of multitasking prevents that from occurring.

Success in any area is a function of the capacity to pay attention. Isaac Newton, for example, credited his success and discoveries as "owing more to patient attention than to any other talent."

So what can you do? Here are some suggestions:

Stop fooling yourself. You're not truly multi-tasking, you're task switching. And that's fine if that's what you want to do. But there is a better way.

Block uninterrupted time to work on important projects. Aim for at least 30-60 minutes without phone calls, walk-ins or other distractions.

Choose to focus your attention on one thing at a time. For example, at your next meeting, try listening to others rather than glancing at your smartphone or jotting unrelated notes.

Give people your undivided attention. While it sounds cliche, it is difficult to do, but the payoffs are big. Not only will you improve the interaction, but you'll demonstrate the regard you have for the other person.

Consciously avoid demanding others to multi-task. Don't interrupt a colleague involved in another activity to make a request. Pick (or schedule) times to interact when the other person isn't distracted by competing demands.

Read Cal Newport's book, Deep Work. It is one of the best books I've read in recent years and will provide many insights and tactics you can use to beat the myth of multitasking.

Mark Sanborn, CSP, CPAE, is president of Sanborn & Associates, Inc., an idea studio dedicated to developing leaders in business and in life. Mark is an international best-selling author and noted authority on leadership, team-building, customer service and change. Mark is the author of 8 books, including the best seller The Fred Factor: How Passion in Your Work and Life Can Turn the Ordinary into the Extraordinary, which has sold more than 1.6 million copies internationally. Learn more about Mark at www.marksanborn.com.

Do You Know Someone That Needs Computer Support?

Did you know we have a referral program where you can earn $100 for each referral you send us. See **www.b4net.ca/referral** for more details. **You don't have to be a client to benefit either.**

RECEIVE A
$100
FOR EACH FRIEND
YOU HAVE REFERRED
TO US.

Random Images From The B4 Networks Families

Congratulations to Alex and Candace on a great Wedding

Nate (Bryan's son) had his birthday in September and was surprised with this!

September is also Aiden's (Bryan's youngest) Birthday, and he was taken out for a special breakfast at IHOP!   Yum, followed by some fun in the Falls. (below)

We rocked the escape room!   Go team!

Client Spotlight

VanZanten Greenhouses was established in 1988 when Jan Sr. with his wife and 3 young children emigrated from the Netherlands to Canada's beautiful Niagara region to start growing cut flowers. Experimenting with a variety of different cut flowers he settled on freesias, which they have been growing for over 20 years!

Along with their valuable employees, both Jan Sr. and now Jan Jr. are still actively involved in the growing and managing of this most beautiful, fragrant crop. Currently they have over 60,000 square feet of greenhouses dedicated to year round production and availability of freesia. The remaining 20,000 square feet is in production of cut hydrangea, something they started in 2007. This is a seasonal crop

where fresh flowers start in June, and then to beautiful antique greens and reds in autumn. Using advanced computer climate control systems, as well as a watering system designed to minimize water usage, and the use of biological beneficial insects to curtail our spraying; Vanzanten is also doing their best to protect and maintain our environment.

"We are always looking at ways to continually improve our quality and production techniques with a blend of traditional hard work and modern technology" says Jan, with the hope that every year more people can enjoy the beauty and joy that flowers can bring.

Services We Offer

- Fixed Monthly Fee Worry Free IT
- Peace of Mind Security Services
- No Hassle Backup and Business Continuity Solution
- Disaster Planning and Prevention
- Network Design & Implementation
- Server Planning and Deployment
- Project Management
- General Computer / Network Repair and Troubleshooting

B4 networks

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

Need Help Right Away? Call our team 24/7 at 905.346.4966.