Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: Nature's Source

Meet Nature's Source! They have been part of the Connectability family since November, 2018.

For over 20 years, Nature's Source has been serving customers across the GTA. They and are one of Canada's leading "Health Food Stores", and a full-service Natural dispensary. By partnering with Naturopathic physicians they deliver the ideal natural health products, and quality supplements for all your needs.

The Nature's Source team includes in-store staff with educational backgrounds in Homeopathic and Naturopathic Medicine, and other specialties. This allows them to provide customers with knowledgeable advice, and recommendations that fit their needs.

Connectability has been Nature's Source technology partner for over a year. We are responsible for monitoring their computers for performance, investigating and recommending tools that provide additional security, and configuring and deploying Firewalls and other security solutions at each of their locations. We support their business to ensure that they are always operational, and their data is secure and confidential. We guarantee their IT equipment is running smoothly, so their business can be productive and profitable!

If you would like to learn more about Nature's Source, please go to: https://www.natures-source.com/

February 2020

This monthly publication provided courtesy of Ted Shafran, President of Connectability

If You Think Your Business Is Too Small To Be Hacked ... You're A Cybercriminal's #1 Target

Many cybercriminals look at small businesses like blank checks. More often than not, small businesses just don't put money into their cyber security, and hackers and cybercriminals love those odds. They can target small businesses at random, and they are all but guaranteed to find a business that has no IT security – or a business minimal security that is set up incorrectly.

At the same time, cybercriminals send e-mails to businesses (and all their employees) with links to phishing websites (websites designed to look like familiar and legitimate websites) or links to malware. They hope employees will click on the links and give criminals the information they want. All it takes is ONE employee to click on the link.

Or, if the business doesn't have any security in place, a cybercriminal may be able to steal all the data they want. If you have computers connected to the Internet and those computers house sensitive business or customer data – and you have NO security – cybercriminals have tools to access these computers and walk away with sensitive data.

It gets worse! There are cybercriminals who have the ability to lock you out of your computer system and hold your data hostage. They may send along a link to ransomware, and if you or an employee clicks the link or downloads a file, your business could be in big trouble. The criminal may request a sum of money in exchange for restoring your PCs or data.

However, as some businesses have learned, it's not always that simple. There are businesses that have paid the

Continued on pg.2

Continued from pg.1

ransom only for the cybercriminal to delete all of their data anyway. The criminal walks away with the money and the business is left to die.

And that's not an understatement! Once cybercriminals have your data and money, or both, they don't care what happens to you. Cybercriminals can do more than just minor damage to small businesses; their actions can literally destroy a company! We're talking about the costs of repairing the damage and the cost of losing customers who no longer want to do business with you. You're looking at a public relations nightmare!

This goes to show just how critical good IT security really is, but business owners still don't take it seriously. Even as we enter 2020, there are business owners who don't consider cyber security a high priority — or a priority at all. It's a mindset that comes from before the age of the Internet, when businesses didn't face these kinds of threats. And many business owners become complacent. In other words, "It hasn't happened yet, so it probably isn't going to happen." Or "My business isn't worth attacking."

Cybercriminals don't think like this. It's a numbers game and only a matter of time. Business owners need to adapt to today's online landscape where just about everything is connected to the Internet. And if something is connected to the Internet, there is always going to be some level of risk.

"The reality is that cyber security should be a normal, everyday part of any business."

But you can control your level of vulnerability! You can be cheap or complacent and do the bare minimum, putting your business and customers at risk. Or you can take it seriously and put cyber security measures in place – firewalls, malware protection, secure modems and routers, cyber security insurance and working with a dedicated IT security company. There are so many options available to secure your business.

The reality is that cyber security should be a normal, everyday part of any business. And anyone thinking about starting a business should be discussing cyber security from the very beginning: "What are we going to do to protect our business and our customers from outside cyberthreats?"

When it comes down to it, not only do you need good cyber security, but you also need a good cyber security policy to go along with it. It's something you share with your team, customers, vendors, investors and anyone else who puts their trust in your business. Transparency about your cyber security practices is a great way to build and maintain trust. If you don't have IT security in place, why should anyone trust you?

Think about that question and think about the security you have in place right now. How can you make it better? If you need to reach out to an IT security firm, do it! It will only make your business better and prepare you for the threats that are looming right now. No business is too small or too obscure to be hacked.

Webinar: Strengthen Your Cybersecurity Defenses

This month we will be hosting a webinar focusing on the importance of "stacking" your cybersecurity protections. The cyberworld isn't safe anymore. To fully protect your business from a cyber attack requires more than one tool. You need an advanced stack of security tools that complement each other. Without it, your business is more susceptible to data loss, Ransomware, and downtime.

The Webinar is titled: **"Why Antivirus Isn't Enough And How You Can Close Security Holes Hackers Use To Get Into Your Company Network"** and takes place on **Wednesday, February 26th, 2020** from **10:00-11:00 am**.

During this Webinar You'll Discover:

- Why you need a "stacked" approach to cyber security
- How cyber security protections can prevent downtime, and save you time, money and frustration
- What you can do now to reduce your companies' risk, and strengthen your defenses
- How Threat Hunting works, and why it's the missing piece to the security puzzle

If you're concerned about your security protections, and want to avoid a cyber security disaster, then you should definitely attend! To register, visit **www.connectability.com/threathunting** or call: **(647) 492-4406** and we will save you a seat.

Shiny New Gadget Of The Month:

M&R Digital Counting Coin Bank

Many of us still keep a coin jar to toss our spare change into. Even with the growing popularity of apps like Apple Pay and Google Pay, coins remain a big part of our lives. Of course, when you're tossing coins into a jar at the end of the day, you have no idea how much you've collected until you count it or take it to the bank.

The M&R Digital Counting Coin Bank solves this problem. You never have to count change again. Every time you drop coins into the bank, it counts and adds them to the total. The digital readout keeps you updated on how much you've saved. It's a remarkably simple piece of technology that eliminates the hassle of keeping track of change.

Stay Safe From SMS Fraud

Hackers are taking phishing schemes to a whole new level. Rather than sending an infected email, or prompting you with a pop-up, hackers are sending phishing texts to your smartphone. And because anyone can send you an SMS, it's very difficult to stop them.

Text messages come in several varieties:
The first are messages you receive from someone in your contact list that you are actively connecting with. For example, a family member or a friend asking you "what time is dinner tonight" or a colleague confirming that they've sent information over to a client.

On the opposite end of the spectrum are text messages that are clearly spam. These messages come from unknown numbers and are generally ripe with spelling errors. They also ask you to take some ridiculous action. For instance, Canada Revenue Agency sends an SMS indicating you have received a refund of $120.52 and to enter your banking information to deposit it. Most people can tell right away that this is a fraudulent message.

Now the *real* issue are the texts that look like they could be legitimate. These messages are usually from businesses and services that you are aware of and might have given permission to message you. They might appear to be from a supplier providing an update on an order, or they might be from your bank indicating that there has been fraud on your account. They're generally ask you to take action: click a link, reply back with some information, etc.

So, how do you know if the message is legitimate? Here are 3 rules you can follow to help identify a fraudulent text message:

1. **Don't Respond to a Call to Action**
   This is a BIG red flag. The message requests you to take some type of action. This could be to click on a link, call or text a number, enter payment details, or simply reply. Regardless of the action, when an unknown number asks you to do something fishy, treat it as a phishing text.

2. **Pay Attention to Odd Behaviour**
   Be wary if the message sounds strange. For instance, if the originator has your name, but greets you with "Hello, friend", or "Dear client" then be cautious about replying. Also, lookout for any grammatical/spelling errors. This could be as simple as the name of your bank with a zero instead of an O (e.g. BM0).

3. **Do Some Research First**
   You might still be wondering if the message is real. What if you don't respond? Will your package be put on hold? Will your bank account be disabled? That's what hackers pray for - doubt. What if the message IS legitimate? Well, do your research first. Call the supplier or your bank directly, check their online portal (if they have one), or look up the number to see if it has a history of spamming. Always verify the SMS through official channels first!

If a cybercriminal gains access to your phone, they can review your messages and emails, get banking information, and stir up a whole lot of trouble. That's why you need to be aware of SMS scams. To protect yourself from phishing texts, turn on the "Block Unknown Sender" feature on your device. This will help filter senders with numbers that are not in your contact list and appear to be fraudulent. You can also utilize an anti-spam service. Finally, any time you get a fraudulent text, you should go into your contacts and block the number. This won't prevent them from spamming you from a different number, but it will prevent recurring spam from that number. Protect yourself now to prevent a breach later!

Tech Connect Video Series

Remove Security Holes Once and For All

Cybercriminals are working their magic to access your computers, steal your data, and cost you a fortune. Cyber security is asymmetric. Even with near perfect defenses, businesses can experience Ransomware attacks, data breaches, trojans, malware, phishing scams and more.

To keep your business safe, it's critical that you have the following tools in your business: business-grade antivirus software, multi-factor authentication, an enterprise firewall with active security licenses, anti-spyware software, and so on. BUT, that's not all. To fully protect your business, you need to find the root cause of the vulnerabilities. By using an Advanced Threat Detection tool like Huntress, you can "hunt" for footholds in your network, remove any vulnerabilities, and close your security holes for good.

If you're concerned about your company's security, watch this video now! You'll learn how an MSP can help you build the perfect cyber security "stack" for your business. To find out more, go to YouTube, look up Connectability IT Support and find the video "Antivirus Isn't Enough—Hunt For Vulnerabilities Instead" OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

7 Things To Do So You DON'T Get Hacked When Shopping Online

1. Verify the URL is safe. Many browsers have a little padlock in the URL bar. If the padlock is closed, the URL is safe. If it's open, you may want to avoid the site.

2. Verify the URL is accurate. Many scammers register fake websites using misspelled URLs or extra numbers to look like the real deal. If the URL looks odd, it's probably a scam.

3. Use a secure web browser. Firefox and Chrome, for example, always navigate to HTTPS (Hypertext Transfer Protocol Secure) websites. These websites are more secure than their HTTP counterparts.

4. Don't click suspicious links or attachments. Never click a link if you can't verify it first. In fact, it's better to delete any e-mail you don't recognize.

5. Always bookmark authentic websites. When you bookmark real websites, you never have to worry about mistyping or clicking scam links.

6. Rely on a password manager. It's hard to remember strong passwords, but with a password manager, you don't have to. Never use a bad password again!

7. Use the official mobile apps for online stores. If you download the official app of your favourite online stores, such as Amazon or eBay, you don't have to worry about accidentally navigating to a scam website. Just make sure the app is verified by Google or Apple. *Lifehacker, Nov. 19, 2019.*

Top Tips For Scaling Security For Your Small Business

Put a greater emphasis on passwords. As businesses grow and adopt more technologies, such as cloud-based apps and mobile apps, they also have to deal with more passwords. The more passwords employees have to remember, the less likely they are to have strong passwords and the more likely they are to use the same password for everything. Another problem is password sharing. A team of people may share a single license for a piece of software, which means they share a single password. Password managers like LastPass can save a lot of hassle while still protecting your accounts, and many password managers are scalable.

Rely on multi-factor authentication (MFA). MFA adds another layer of security on top of firewalls and malware protection. It's like adding an extra password on top of your existing password, though only you can enter it. However, some employees skip MFA because it adds extra steps to the login process. But an extra 15 seconds to log in is worth it for the security. There are many MFA options available for different-sized businesses. Make it a part of your cyber security policy. *Small Business Trends, Nov. 1, 2019.*

"This figures. My file on politicians has become corrupt."

Covenant House TORONTO

This month we will be donating to the **Covenant House Toronto**.

Founded in 1982, with only 30 beds, Covenant House Toronto has now grown to provide hope and opportunity for more than 95,000 young people. Covenant House Toronto is committed to supporting vulnerable youth. They serve youth who are homeless, trafficked or at risk.

As Canada's largest agency serving youth to ignite their potential and reclaim their lives, the Covenant House offers a wide range of 24/7 services to about 350 young people each day. They focus on public policy, leading awareness and prevention programs, and building and sharing knowledge.

Covenant House offers housing options, health and well-being support, training and skill development, and with unconditional love and respect. Their team is dedicated to supporting and building one-on-one relationships with youth, advocating for change in the community, and forming programs. If you want to contribute to the Covenant House Toronto, we would love your help! Call: (647) 492-4406 or email: info@connectability.com.