



Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by:
Connectability

Is This You?

Are you a small to midsize business in the Toronto area, who wants to turn technology into a powerful tool that can move your business forward, instead of being a problem that costs you time and money? If so, we can help!

Add Our Technology Experts to Your Company's When:

- You want to focus on your business, not the technology
- Your current system seems to hinder business more than it helps
- You know that computer downtime costs you money
- You need to be certain your data is always backed up, period.
- You demand reliability and a HIGHER level of security from your computer network
- You're looking to expand your business, but need to know the technology and costs involved in doing so

Connectability has been providing IT Support Services for over 25 years. We have the expertise to help you experience Trouble-Free IT. Email us at: info@connectability.com or give us a call at (647) 492-4406.

February 2022



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



All across the world, hackers are targeting and exploiting security weaknesses and holding data hostage. In May, the Colonial Pipeline was hit by a cyber-attack that disrupted fuel supplies along the East Coast of the US for several days. The company – and the FBI – paid hackers US\$4.4 million in Bitcoin to regain control of the system.

Colonial Pipeline was not the only corporation that paid hackers an exorbitant amount of money. The NBA, Kia Motors and JBS Foods have also been victimized by cyber-attacks where hackers demanded millions of dollars. CD Projekt RED, a Polish video game developer, was also a victim of a cyber-attack, but since they had backups in place, they never had to pay the demanded ransom.

While these are all big organizations, that does not mean that small businesses are safe. These stories made the news because companies paid millions of dollars to regain control of their data. When a small or mid-size business (SMB) gets attacked, they can't

pay millions of dollars to recover stolen information. Instead, these hackers will usually go after customer and employee information as well as financial records and statements. When a hacker attacks an SMB, it often ends in the business closing their doors for good.

The year 2021 set a record for cyber-attacks, and 2022 is shaping out to be no different. If you're a business owner, you need to wake up to the reality of cyberthreats and cyber security before it's too late.

Here are a couple of the best cyber security practices you should put into place immediately.

Hire A Managed Services Provider For Your IT Needs

Cyber security awareness has grown over the past five years, but there are still plenty of SMB owners who think there is no need for cyber security measures or that they're too expensive. The simple truth is that every business can be a victim of cyber-attacks. If you

Continued on pg.2

Continued from pg.1

think it's too expensive to have your own IT team watching over your cyber needs, think again. Hiring an MSP is one of the best and most cost-effective ways to ensure that your network and information are protected.

MSPs can be incredibly beneficial to any business. They're designed to recognize and fix weak points in your IT infrastructure. MSPs work proactively to ensure that your business is fully protected in the cyberworld. They offer around-the-clock monitoring, data backup and recovery, firewall and network protection, real-time threat prevention and so much more. MSPs provide you with a dedicated team of IT professionals who are available to assist with any IT needs. If you have not looked into hiring an MSP for your business, you should seriously consider it.

If you're interested in hiring an MSP or want more information about the benefits, reach out to us and we will assist with any concerns or questions you may have.

Create A Cyber-Secure Culture

Many cyber-attacks stem from employee error or misunderstanding. You need to make sure that all of your employees are aware of the risks associated with cyber-attacks. When you first hire an employee, train them on cyber security. In addition, your current employees should go through a reminder course at least once a year.

You'll need to inform your employees about the dangers of phishing emails and texts, downloading malware, social media scams and password protection. If you have



employees working remotely, you should ensure that their devices have security measures built into them. If your employees are informed about the risks, they will be more observant so they can spot any potential threats. Your entire team needs to buy into the cyber-secure culture if you want your training to be effective.

In today's day and age, you can never be too careful when it comes to your cyber security. You need to be proactive and put all of the security measures you possibly can into effect. The year 2021 saw cyber-attacks reach new heights, and it's likely that these numbers will continue to rise even further this year. Take preventive action and don't let your business add to the cyber-attack statistics. If you're unsure of where to begin when it comes to buffing up your cyber security practices, give us a call, and we will be glad to help.

'I DIDN'T KNOW'

Unfortunately, That Excuse Doesn't Replenish Your Bank Account, Resolve A Data Breach Or Erase Any Fines And Lawsuits.

It's coming ...

- That day a hacker steals critical data, rendering your office useless
- That day when your bank account or credit card is compromised
- Or that day when your customers' private lives are uprooted



Cybercriminals and hackers are constantly inventing NEW ways to infiltrate your company, steal your assets and disrupt your life. The ONLY way to STOP THEM is this:

You Must Constantly Educate Yourself On How To Protect What's Yours!

Sign up to receive our FREE "Cyber Security Tip of the Week." We'll send these byte-sized quick-read tips to your email inbox.

Call us at (416) 966-3306 to get your FREE "Cyber Security Tip Of The Week"

Shiny New Gadget Of The Month:



Kailo – The Future Of Pain Relief

Nearly everyone has felt pain so intense that they had to take a painkiller to calm the discomfort. Sometimes orally administered painkillers can take too long to be effective, or they simply fail to dull the pain at all. The people at Kailo realized this and made it their mission to help people manage pain with a nanotech patch.

Kailo interacts directly with your brain's electrical system, telling it to calm down and reduce pain. Kailo doesn't use medicine or drugs, and there are zero side effects. In addition to this, it works anywhere on your body, and you'll start feeling the effects within the first minute. If the usual painkillers aren't working for you, give Kailo a try.

How Cyber Criminals Use The Dark Web, And Why It Matters To Your Business

If your password to your bank portal, or email account were breached, how would you know? Well, if you're like most businesses, you wouldn't, unless and until a cybercriminal or malicious actor chooses to use your password for some nefarious purpose.

Most businesses understand the importance of cyber-security and invest regularly to strengthen their level of protection. You likely already have a business-grade Antivirus program running on your employee's computers (and your servers), and chances are you also have a business-grade firewall installed on your network to block external attacks.

Unfortunately, what a lot of businesses lack is any kind of cyber security monitoring. Most tools are centered around PREVENTING infections. Unfortunately, hackers are a crafty bunch and are constantly finding new way to break into your computers and network. And the fact of the matter is, there are NO tools out there capable of preventing all infections with 100% certainty. If there were, you can bet there would be far fewer news articles and exposes covering the most recent major data breach.

This is where things tie into *The Dark Web*. The Dark Web is a place where cyber criminals act as buyers and sellers. Some Dark Web sites focus on the illegal sale of physical items like weapons, drugs, and even people, while other sites are more interested in the sale of data.

For example, some Dark Web sites sell stolen credit card information. In fact, they offer multiple options: you can purchase

verified cards, or unverified cards. You can even differentiate between the TYPE of card you want to buy, whether that is personal or business. So, if you're a criminal looking for a verified card with a high credit limit, you can specifically look for business cards, as banks don't monitor spending as closely as they do on personal accounts. These sites also specialize in the purchase of confidential information like usernames, passwords, social insurance numbers, and even bank account numbers.



Ultimately, there are many ways a hacker can gain access to this information. They could access it through a phishing attack, a vendor breach, social engineering, etc. So, while you still need advanced cybersecurity solutions in place now, how would you know if your data WAS breached and accessible on the Dark Web?

This is ultimately the reason the Dark Web matters to your business. Your credentials can be breached in any number of ways, by any member of your team. If just ONE password is breached for a critical account and ends up on the Dark Web, your entire organization could be compromised. If you don't even KNOW you've been breached, how can you take the necessary precautions to secure your business? The simple answer is: you can't.

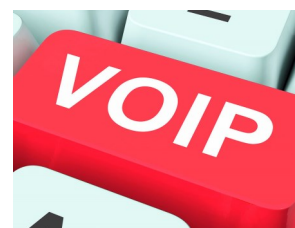
I wrote this article for this specific purpose: to educate business owners and executives of the need for ongoing monitoring. If your data ends up on the Dark Web, you need an early warning system so you can change passwords, engage your IT provider, and determine where you are vulnerable, BEFORE you are breached – not after it's too late.

Tech Connect Video Series: Everything You Need To Know About VoIP

Voice over Internet Protocol (VoIP) phone systems are game-changing, allowing users to make and receive calls from virtually anywhere with an internet connection.

VoIP system can help make your organization more flexible, improve customer service, and make you more efficient – all while saving you money. A VoIP solution may not be the right fit for every business, but it offers many proven benefits that can help businesses to thrive, whether your team is 100% remote, or located entirely in a specific facility.

If you're concerned about your phone systems, watch this video now. To watch, go to YouTube, look up Connectability IT Support and find the video **"VoIP vs. Traditional Phones"** OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".



■ Prepare For A Hack Attack TODAY

Every business owner, big and small, should be prepared for a cyber-attack. It's incredibly likely that hackers will attack your company at some point. Luckily, there are five strategies you can implement to better protect your company from hackers.

1. **Hide Your Data:** Keep your data in multiple online locations and separate data between multiple cloud providers to keep it secure. Hackers are likely to give up if it's too much hassle to get in.
2. **Routinely Check Your Finances:** It can be nearly impossible to recover from a hack if too much time has passed. It's not your bank's or accountant's responsibility to keep up with your finances, it's yours. Get in the habit of regularly checking

your finances.

3. **Utilize Multifactor Identification:** Make sure your employees use multifactor identification to protect company information.
4. **Avoid Phishing Scams:** Train your employees to not open or respond to any suspicious texts or emails.
5. **Watch What You Post On Social Media:** Don't post any information on social media that a hacker could utilize to breach your security.

■ Surviving The Great Resignation

The pandemic completely changed how freelancers function. Previously, full-time employees were the most sought-after employees. With the pandemic and the ensuing labour

shortages, freelancers have been brought further into the corporate world, and it looks like they're here to stay. Now, if you want to attract freelancers to work for your business, you need to entice them.

One of the most desirable things you can offer a freelance worker is flexibility. Don't restrict their hours to the usual 9 to 5 — they want freedom, and with proper communication, flexibility can work to your benefit and theirs. Freelancers often feel disconnected from their team, and you should make an effort to include them as part of the team. Create an inviting atmosphere and encourage them to take part in team-building exercises. Lastly, you need to offer competitive pay and stick to it. If you're not paying them enough, they will find someone who will.

Can You Solve This Sudoku Puzzle?

1	4	2		9				5
7			4				8	9
8		5					2	4
2					4	8		
	3				1	2	6	
	8			7	2	9	4	1
	5		2		6			
	2	8			9	4	1	
	7	9	1		8	5	3	

Call Us At (647) 492-4406 For The Answers!



This month we will be donating to **Soldier On**.

Founded in 2007, Soldier On is a program of the Canadian Armed Forces Transition Group. Soldier On is committed to providing support for veterans and serving members to help adapt and overcome permanent physical injury or PTSD.

Soldier On is dedicated to improving the quality of life of veterans and current serving members through physical activity and sport. Soldier On provides a safe environment and empowers them to adapt and re-integrate with local, community-based activities, and remain active for life.

If you want to contribute to Soldier On, we would love your help! Email: info@connectability.com or call (416) 966-3306.