



Client Spotlight Canadian Helen Keller Centre

Meet Canadian Helen Keller Centre. They have been part of the Connectability client family since September 2018.

Canadian Helen Keller Centre (CHKC) has been in operation since 1992, providing Canadians who are deafblind with support, training and opportunities. Their vision is to remove the barriers and limitations that individuals with deaf blindness encounter.

CHKC operates a fully accessible and affordable apartment complex in the Willowdale neighborhood of Toronto. This 16 unit facility offers members of the deafblind community the opportunity to live as independently as possible. Also, CHKC runs a Training Centre where Canadians who are deafblind can access programs and services to learn life skills, such as cooking and cleaning, as well as communication courses, technology classes and clubs that provide the opportunity to socialize with peers. CHKC provides up to 24 hours a week of intervenor services for individuals who are deafblind. Intervenors act as the eyes and ears of a person who is deafblind at doctor's appointments, grocery shopping trips and other essential activities.

Connectability has been Canadian Helen Keller Centre's technology partner for almost two years. We oversee their computers, servers, cybersecurity, and backups to ensure that their systems are working efficiently and protected from outside threats. We also provide on-site and remote support to keep their network and computers secured and up to date with the latest security protections.

If you would like to learn more about Canadian Helen Keller Centre, please go to: <https://www.chkc.org/>

August 2020



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



The #1 Mistake Companies Make With Their IT

If you're like many businesses today, there's a good chance you've made this one mistake with your IT security: you don't budget for it.

Or if you do budget for it, it's not enough to *really* protect your business.

Time and time again, business owners decide NOT to invest in IT services. Instead, they go it alone or skip it completely.

Or they might approach an IT services company and ask, "What do you charge for your services?" They don't ask, "What will I get for my money?" or "How can you meet the needs of my company?"

This is a backward approach to IT - and it's a big mistake.

The fact is that a lot of business owners don't take IT seriously. They think that because they haven't been

hit by a data breach or a malware attack that it will never happen to them. That's another big mistake. Just because a business hasn't fallen victim to a cyber-attack DOES NOT mean they're safe.

It's the opposite.

When you hire an IT services company, what *do* you get for your money?

The honest answer is that it depends on your specific needs. Many IT services companies offer everything from basic to advanced network security. You can expect services like:

- Cloud backup
- Data protection
- Data monitoring
- Threat detection
- Technology maintenance
- And more!

Continued on pg.2

Continued from pg.1

Everything is designed to protect you, your network, your technology, your employees and your business as a whole. It's all about giving you the information and resources you need so you can worry less about outside threats and focus on your customers and the success of your business.

When you're invested in good IT security, you shouldn't even know it's there. It runs in the background like a quiet but powerful electric motor. It's there when you need it, and it's there when you're not even thinking about it.

For some business owners, this is a tough pill to swallow. They don't have something tangible in front of them that they can see 24/7. A lot of business owners like to be more hands-on. They like to see what their money is buying.

The great thing is that a good IT services company will provide you with something tangible. If you want to see what is going on behind the scenes of your IT security, they will give you a complete report. Every week (or month or quarter), you can have an email delivered to your inbox that breaks down exactly what your IT services firm is doing for you.

"We can't wait to react until something happens. Because when something does happen, it's often too late."

You can see things like the threats they blocked from getting through. You can see when they performed system maintenance or when your data was backed up. You can customize these reports to your needs. Basically, you can see what you're paying for and how it's working. This is the very definition of "peace of mind."

Today, none of us can afford to skip out on good IT security. We can't wait to react until something happens. Because when something does happen, it's often too late. The cybercriminals have done their damage and moved on. Meanwhile, your business comes to a screeching halt, and you have to pay the big bucks to get everything back on track – if you *can* get back on track.

Some businesses don't get back on track. They are forced to close after a cyber-attack because they don't have the money or resources to recover. The damage is simply too much and the cost too high. If they had invested in IT security upfront, it might be a different story.

Don't get caught off guard by a data breach, malware infection, hacker attack or data loss due to technology failure or natural causes like flood or fire. It's time to take your IT to the next level. Protect your business the right way and avoid the mistake so many others make when they avoid investing in good IT.

Work with an IT services firm that takes your business as seriously as you do.

Are Your Employees Leaving This Back Door Wide Open?

Chances are your employees have wireless networks set up in their homes. Unfortunately, unlike in well-managed office environments, many home users are fairly lax about the security of their wireless networks – leaving a back door open to hackers. Wi-Fi signals often broadcast far beyond your employees' homes and out into the streets. This has left to an epidemic of "drive-by hacking" that has become so popular among cybercriminals today.

So, here are a few tips for securing your employees' Wi-Fi networks:

- Use stronger encryption (WPA2) and a more complex password
- Hide your wireless network name
- Use a firewall

These security measures aren't difficult to set up, but can have a massive impact on your teams security. If you need help setting up a Work From Home solution or have any other technology questions, please call us at (647) 492-4406 or email us at info@connectability.com and one of our Network Engineers will be happy to assist.

Shiny New Gadget Of The Month:



FlexSafe Is Here To Protect Your Valuables

Beachgoers all know the security dilemma that comes with a stray wallet. When it comes time to put on your trunks and head into the sea, do you bury your valuables in the sand? Hide them under a towel? Or leave them be and hope for the best?

For all of those who find each of these options less than ideal, there's FlexSafe. It's a handy, personal, portable safe designed to stave off thieves, wherever you are. Water-resistant, slash-proof, RFID-blocking and equipped with a heavy-duty three-digit combination lock, it turns you from an easy target to a walking fortress. The bag-shaped design clips into itself, allowing you to secure it to a beach chair, umbrella or any other unwieldy surface and go on your merry way without worry. At \$59.99, it could be a sound investment for those of us finding ourselves leaving our valuables exposed on the regular.

Are Your Printers Safe?

When most people think about hackers and protecting their equipment, they think about their desktops, laptops and servers, while overlooking other equipment that they have in their office or home workspace. But what about your printer? Just like your computers and servers, printers are also an entry point that a cybercriminal can use to access your network. Your business may have cybersecurity protections in place for your computer infrastructure, but are you securing the rest of your network, including your printers?



Here are 3 tips to protect your printer:

1. Update your printer's operating system

It's important to update your printers so that software updates or patches are applied. This makes it more difficult for a cybercriminal to get in. Printer manufacturers regularly release software updates, so keep an eye out for those. You should also change the default password when you configure your printer. Most networked printers can be accessed remotely with a password. By making the default password more complex, you are adding an extra layer of security.

2. Set up a firewall

You can restrict printer access by applying security protections. One protection you should include is a firewall. This will block threats from outside your company network. Another simple way to protect your business is to unplug your printer from your network. If the printer is not connected to your network, then there is no way a hacker can access it remotely.

3. Wipe the drives

Your printer/scanner stores your company's documents, faxes, files, images, etc. that are going to be, or have been printed. Ensure that you wipe the drives to remove all confidential data, or your business may get into some legal trouble. Also, use an encrypted network when printing sensitive information. When you use an encrypted network the print job can't be stopped or interrupted because your information is converted into a code that can't be easily broken by a cyber criminal.

Printers have poor network security measures, which make them more susceptible to cyber attacks. That's why it's important for you to take the necessary precautions to protect your systems. These 3 tips will help secure your printer from viruses and attacks, reducing your chances of experiencing an expensive data breach. If you are concerned about your printer security, we are happy to help. Give us a call at (647) 492-4406 or email info@connectability.com.

Tech Connect Video Series: Beware Of Phishing Attacks!

You probably spend a lot of time emailing clients, vendors, partners and colleagues. It's your main tool to communicate. Unfortunately it's also a hacker's prime target. Hackers use a method call "phishing" to convince you to open malicious links or attachment, send funds to random bank accounts, or provide confidential information about you or your company. Cybercriminals can then get your passwords, install programs on your computer and network, and steal your confidential data.

Cybercriminals are working diligently to get into your computer, infect your backups, and install Ransomware across your network. That's why your business needs to invest in solutions and training that can help your team spot phishing attacks, and prevent them from arriving in your inbox to begin with.

If you would like to learn more about improving your security and preventing your business from becoming a victim of a phishing attack, watch this video NOW! You will learn 3 tips to improve your email security. To find out more, go to **YouTube**, look up **Connectability IT Support** and find the video "**Beware Of Phishing Attacks! 3 Tips To Improve Email Security**" **OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".**

■ The 'Not Me!' Problem ...

Remembering 24 different passwords, memorizing four PIN numbers and installing updates all the time is frustrating enough. Many of us also have to remember the code for the door, the alarm code for the alarm panel next to the door, the secret password to tell the alarm company, the passcode to your phone, the garage code ... You get the idea.

This logic is based on a time when threats were more "real," like the idea of someone robbing our house. In 2020, these types of threats are statistically less likely to happen than virtual threats like fraudulent credit card charges, data loss and identity theft. In fact, cyberattacks occur three times as often as home burglaries in the United States, according to a 2016 study by the University of Kentucky.

It's important to avoid the "Not me!" approach to this shift. Businesses say

this all the time: "I'm too small for anyone to want to steal my data. I have a good firewall, hourly backups and a great IT support partner – no one will steal my files."

But the truth is that businesses with under 100 employees are low-hanging fruit for cybercriminals – yes, that's a lot of you! It can happen to you, so you must approach all aspects of physical and electronic security with the attention they deserve in today's business world.

■ Do You Have The Right Business Insurance To Protect Your Company?

There are several types of business insurance on the market. Each one serves a different purpose, and getting the right insurance can save you the major headache that comes with not having insurance or having the wrong type of coverage. While we can't list them all here (there are too many!), here are a few examples:

Commercial property insurance –

This is one of the most important forms of insurance. It protects equipment in the business against damage or loss.

General liability insurance – This is another important one. It helps cover injury and legal expenses should someone get hurt on your business's premises.

Cyber-insurance – This offers protection should you fall victim to malware, cyberattacks and other digital threats. Basically, if your business is connected to the Internet, you need extra protection.

Umbrella insurance – This is another layer of protection on top of existing insurance. Exact details vary by plan, but it can often protect you if you need to pay legal fees or costs related to building or equipment damage.

Small Business Trends, May 13, 2020

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 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, all 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.