CONSUMER CHOICE AWARD 2020 GTA 3 YEAR WINNER

Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: Origin And Cause

Meet **Origin and Cause!** They've been a part of the Connectability client family since October 2018.

With offices across Canada, Origin and Cause is the largest consulting forensic engineering and fire investigation firm in the country. They have been a trusted leader for over 25 years and provide cross-disciplinary forensic expertise to insurance companies, law firms, independent adjusters, manufacturers and corporate risk managers.

Their team consist of highly trained, extremely skilled professionals with years of hands-on experience.

Connectability has working with Origin and Cause for over a year. Because Origin and Cause operates across Canada, it's important that remote employees have access to company data whenever they need it. We provide support to the entire Origin and Cause team by ensuring they have secure access to company data, and that their technology is protected and operating at peak performance.

To learn more about Origin and Cause and the services they provide, go to: https://origin-and-cause.com/

April 2020

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

Your #1 Threat Of Being Hacked Is INSIDE Your Own Organization

Small businesses are the biggest targets of hackers and cybercriminals. They are targeted because they are less likely to have strong – or any – security in place. But in so many cases, hackers don't need to use malicious code or cracking skills to get what they want. Instead, they rely on your biggest vulnerability: your own employees.

The #1 threat to any business's IT security is its employees. It all stems from a lack of training. Employees don't know how to spot threats, or they don't know not to click unverified links in their emails. Most of the time, these actions are simple mistakes – but mistakes aren't excuses and can result in MAJOR costs to your business.

Here are three things you can do to turn your employees from your biggest IT threat to your biggest IT asset:

Establish Regular Cyber Security Training.

First and foremost, get *everyone* in your business trained up on IT security. Wesley Simpson, the chief operating officer of (ISC)², an international cyber security certification group, suggests thinking about IT education as "people patching." Just as you continually update and patch your software and security, ongoing education serves to update, or patch, your employees. He says, "If you don't get your people patched continually, you're always going to have vulnerabilities."

But don't put the training solely on your shoulders. Work closely with a company that specializes in IT

Continued on pg.2

Continued from pg.1

security. Doing it yourself can be stressful and time-consuming. An experienced IT firm is going to come in with all the education and resources you need to successfully train everyone in your organization on cyberthreats targeting your business today.

Keep Cyber Security Top Of Mind.

While you may have training or educational sessions once a quarter or biannually (regular sessions are recommended), you still need to keep IT security in the minds of your employees on a weekly basis. During weekly meetings, for example, talk about a cyber security topic. Or, if you share news or links with your employees in a weekly, company-wide email, for example, include a cyber security story or tips article. It's all about utilizing systems you already have in place to keep your team informed and this important topic at the forefront.

Emphasize Safe Internet Usage Habits.

This should supplement regular training. Employees should always know the best practices when it comes to using the Internet, email or anything else that brings them in contact with the World Wide Web. Part of it involves keeping the lines of communication open. If an employee sees something out of the ordinary come into their inbox, encourage them to bring it to the team's attention – whether they're telling their direct supervisor, manager or you. The easier the communication between everyone on your team, the easier it is to identify and stop attacks.

> **"The #1 threat to any business's IT security is its employees."**

The goal is to eliminate guesswork. If an employee isn't sure about an email, they should be trained to ask questions and verify. On top of that, you should have a policy in place that prevents employees from installing unverified software, which includes apps and app extensions (such as browser extensions), without permission. And one more thing – stress safe Internet usage habits not just in the workplace but at home as well. This is especially critical if your employees are bringing in their own devices. If that's the case, you should absolutely have a "bring your own device" (BYOD) security policy in place. It's just another wall between your business and potential threats.

How do you get all this started? Good question! It all starts with reaching out. If you're ready to lock down your business and you're serious about educating your employees and turning them into your best defense, we can help. The best IT security you've ever had is one phone call away.

Quick Tip:
3 Essential Rules For Securing Cloud Apps

Are your employees use cloud applications while working from home? If so, you should be concerned about data privacy and security. The company hosting your data is responsible for keeping hackers out of their network, but most cloud breaches are due to user error.

Here are a few things you can easily do to improve security in the cloud:

1) **Maintain a strong password** of at least eight characters with both uppercase and lowercase letters, numbers and symbols. Don't use "Password123!" While that technically meets the requirements, a hacker could easily crack it. Or, use a string of random numbers and letters. The more complex, the harder it is to crack.

2) **Make sure the device you're using is secure.** You'll need professional help installing and maintaining a strong firewall, antivirus and spam-filtering software. Don't access cloud apps on a device you also use to check social media or free email accounts.

3) **Back up your data.** If the data in the cloud is important, make sure you regularly download it from the application and back it up to another safe and secure location. If your account gets hacked, or if the cloud company shuts down your account, you still have a copy.

Want more tips for setting up safe Work From Home networks? Check out our Work From Home FREE Report **https://bit.ly/2xpA8Zb**. And if you have any questions, give us a call at (647) 492– 4406.

Shiny New Gadget Of The Month:

Bringing The Peephole Into The 21st Century: The Ring Door View Cam

As more and more things in the world become digitized and revamped for the smartphone generation, the humble peephole has joined the ranks of IoT-enabled devices. Enter the Ring Door View Cam, a nifty little piece of tech that replaces the fish-eye lens of your peephole with a camera so there's never any question who is at the door.

In addition, you get mobile notifications whenever the device's motion sensor is triggered, enabling you to remotely communicate with a visitor from your phone, even if you're not home. That means no more missed drop-ins, no more packages left out in the open on your doorstep and no more shady, late-night encounters with suspicious strangers.

We're Here To Help You Through COVID-19!

The world is in chaos right now. COVID-19 has changed everyone's lives, and no one knows for how long. Businesses around the world are facing unprecedented challenges. Everyone is being asked to self-isolate and practice social distancing, which puts businesses in a tough position. They either have to shut down completely or allow employees to work from home. The answer for this is mostly dependent on the nature of your business, but most companies have opted for the latter.

Connectability is committed to delivering support and services during these tough times. We are helping our clients reduce the exposure and transmission of COVID-19 to maintain the health and safety of our clients, employees, and the overall community.

Working from home often carries an increased cyber security risk. In a traditional office environment, employees work on company owned computers protected by a business-grade Firewall, Antivirus software and a 24/7 remote monitoring and management solution. But many employees who work from home use personal devices which have minimal to no security.

With such short notice, it's challenging to get your ducks in a row. Transitioning to a remote workforce and managing your security and communication needs can be stressful. To ensure your business is secure, you need to determine how your employees are currently accessing company data, what systems you have in place right now, and how your company network and individual computers are being protected.

To help business out, we've put together a variety of resources to help you succeed. If you are moving to a remote work model, but aren't sure how, or if your employees are already working from home, but you want to make sure they are effectively protected against cyber threats, then check out these resources.

We must stick together, now more than ever! We've created guides for collaboration and communication, security checklists and best practices, a disaster recovery planning template, and more! To get these resources, go to: **https://www.connectability.com/covid19/**

Tech Connect Video Series:
Stay Secure While Working From Home

As of March 11th, the World Health Organization (WHO) declared COVID-19 a global pandemic. So, where do businesses go from here? Many brick and mortar businesses have shut down or halted operations temporarily, and the ones that haven't have told their employees to work from home.

Working from home can sometimes increase productivity and focus, but it also presents challenges. To determine if your business is 100 percent ready to work from home, you will need to examine different strategies for remote access, tools for efficient remote communications, and ensure your remote workers are secure from cyber threats.

If you're working from home, watch this video now. You will learn how you can go from a traditional office-centered environment to working entirely remote. To access it, go to YouTube, look up Connectability IT Support and find the video **"Work In The Time of Coronavirus"** OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

Ready To Transform Your Business With Technology? Follow These 5 Truths...

Investing In Tech Is A Must. Investing in your own IT infrastructure is critical, but you get what you pay for. Go cheap, and you'll expect to buy again. Go quality, and you'll be more pleased with the results.

It's Not Easy. Shifting a business mindset from analog to digital is hard, especially if you've been doing things one way for a long time. When you prepare yourself and your team for a challenge, you'll be able to better meet that challenge.

It's Fast-Paced. Tech moves fast. You see buzzwords everywhere – "5G" or "blockchain" – and it can be confusing. You may feel pressure to keep up, but don't jump in without a plan. Do research and make changes that truly apply to your business.

Cyber Security Is Essential. Stay up-to-date on security trends and solutions. Remember that cybercriminals target small business, but when you stay ahead of the curve on IT security, you stay ahead of the bad guys.

Leadership Is As Important As Ever. Technology is only as good as the people who use it. As you learn about new tech or invest in it for your business, make sure your team is learning too. Understand how your customers use technology and be willing to learn and adapt to them. *Inc., July 30, 2019*

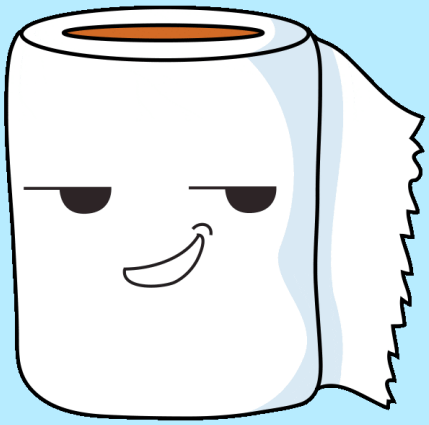
Do These 4 Things To Improve Your Business

Read. There are always new things to learn or perspectives to gain. The top entrepreneurs in the world read every single day. Read books, blogs, articles, anything – but always be reading.

Listen To Podcasts. Podcasts are more popular than ever, and there is a podcast for just about every topic. This is a great way to hear from industry leaders on issues that are affecting them and may be affecting you.

Continue Your Education. How can you improve yourself? Take a class or a seminar! Keep your skills and knowledge base sharp by incorporating continuing education into your year.

Be Open-Minded. Be willing to give and receive feedback and critique on how you work, manage or anything else you want to improve on. The more open-minded you are, the more comfortable your team will be in giving you feedback – and the better you will be at applying it. *Small Business Trends, Dec. 30, 2019*



THANKS TO COVID-19
NOW I AM
THE SH*T!

Daily Bread Food Bank

This month we'll be making our donation to the **Daily Bread Food Bank**.

Founded in 1983, Daily Bread Food Bank is one of Canada's largest foodbanks. Their vision is to end poverty and food insecurity in our communities. They believe that access to food is a basic human right, not a privilege and no one should go hungry, or face barriers in accessing food.

Daily Bread Food Bank takes donations, organizes food drives, and of course runs food banks to provide food to anyone who needs it. Their goal for 2020 is deliver 20% more food to 20 priority neighborhoods that are currently underserved. Given the current crisis, we want to help the Daily Bread Food Bank support those with limited access to food.

If you'd like to contribute to this worthy cause we'd love to hear from you! Email us at: info@connectability.com or call (647) 492-4406 today!