Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: Origin & Cause

We're thrilled to welcome **Origin and Cause** to the Connectability family!

With offices across Canada, Origin and Cause is the largest consulting forensic engineering and fire investigation firm in the country.

Origin and Cause has been a trusted leader for over 25 years, and provides cross-disciplinary forensic expertise to insurance companies, law firms, independent adjusters, manufacturers and corporate risk managers.

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

April 2019

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

What Is Managed IT Services…And Why Should You Demand It From Your IT Services Company?

In today's constantly shifting technological landscape, where fresh viruses and the new security patches designed to protect against them arrive by the week, it takes a proactive approach to stay abreast of all the changes. This is why, in 2019, more small to midsize businesses (SMBs) are ditching their outdated break-fix strategies and making the switch to a managed services provider (MSP) for their IT needs. But for those of us still coming to terms with the new rapid-fire reality of business in the digital age, it can be difficult to determine which approach is right for your organization, or even what a managed services provider actually does.

Here's a breakdown of the managed services strategy versus the traditional break-fix approach and how it applies to your business.

MANAGED SERVICES ARE DESIGNED FOR UP-TO-THE-MINUTE IT UPKEEP.

Maintaining the integrity, efficiency, and security of your business network is a lot like taking care of your car. You don't buy the equipment with the expectation that it'll be good to go forever; you know that it'll take regular upkeep to stay in tip-top shape. For a car, of course, that means regular oil changes, rotating the tires, checking the alignment, checking and replacing the fluids, ensuring adequate tire pressure, changing your spark plugs, flushing the transmission – the list goes on and on. If you don't bother with basic preventative maintenance of your vehicle, it'll fail you sooner rather than later. We're guessing most of our readers wouldn't drive 30,000 kilometers without checking the oil, for instance. Many of these tasks can be taken care of with some savvy and time investment, but others require the expertise of a seasoned professional, especially when serious problems arise.

It's the same with your network. Business technology is notoriously

Continued on pg.2

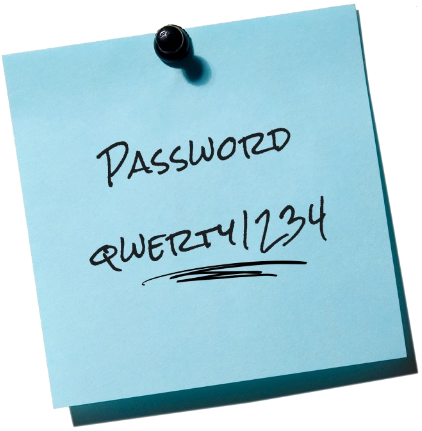
Continued from pg.1

finicky. It'll work perfectly for months and, in rare cases, for years – until suddenly it doesn't, at which point it's likely too late. Suddenly all your data is locked down behind some nasty new ransomware, or your server decided to give up the ghost without warning, leaving key customer information swinging in the wind. We constantly hear about Fortune 500 companies shelling out millions for high-profile data breaches, but when these attacks come to SMBs, they often fold the company completely. What was once a thriving small business is now an empty storefront, buried under the never-ending progress of modern technology.

The old break-fix approach to IT management attempts to address the digital risks facing SMBs only *after* problems arise. Is your server down? Is malware giving you a headache? Is your e-mail not working for some reason? If so, they're on the scene. Otherwise, they're hands-off. The idea behind this strategy is the classic adage "If it ain't broke, don't fix it." Business owners look to cut costs on IT by only addressing the most serious technological crisis after they've already happened, rather than shelling out funds for regular preventative maintenance.

Unfortunately, just like how this approach doesn't make sense in the context of your car, it certainly doesn't make sense for your network. A break-fix strategy can save money in the short term, sure, but it results in more network downtime, a much higher frequency of issues and a ton of dollars spent on damage control down the line.

> **"You don't buy the equipment with the expectation that it'll be good to go forever; you know that it'll take regular upkeep ... "**



Instead, you should demand that the IT professionals responsible for the backbone of your business provide managed services. This means they're in the guts of your network every day, mastering and locking down every aspect of your technology long *before* anything goes wrong. They'll detect issues before they cost you money and fix them without hesitation. You might be reluctant at the initial subscription fee, but if you run the numbers, you'll quickly see how much money it will save you in the long run.

An investment in an MSP is an investment in the future of your business. You wouldn't drive your car mindlessly until it breaks down; it's arguably even more dangerous to do the same with your network. Take a proactive approach, demand managed services and breathe a sigh of relief knowing your network is in the hands of professionals well-versed in the ins and outs of your business's specific needs.

Help Us Welcome Our Newest Team Member: Abarnaa Arunaruban

Connectability has grown a lot over the past 5 years. To continue that aggressive growth we've also had to grow our team. Please help us welcome Abarnaa Arunaruban to Connectability! Abarnaa is our newest Marketing Associate and Sales Representative. Her role at Connectability is to ensure our brand is communicated consistently across different media platforms, and to craft and deliver valuable content to our customers.

Abarnaa is a recent graduate of Ryerson University, with a major in Marketing Management, and minors in both e-Business, and Professional Communications. With years of Marketing and customer service experience, Abarnaa is ready and willing to go above and beyond for our customers!

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.

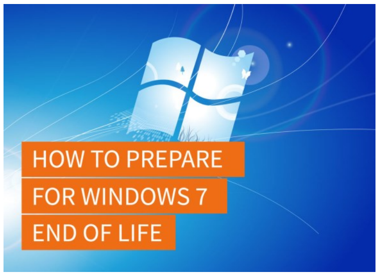
Support for Windows 7 is ending

All good things must come to an end, even Windows 7 and Windows Server 2008. On January 14, 2020, Microsoft will be **discontinuing support** for PC's running Windows 7, and servers running Server 2008.

That means they will no longer be providing security updates, or support services—leaving you and your business **vulnerable** to security threats.

If you're still using Windows 7, you need to replace or upgrade to Windows 10 to ensure you are getting the most up-to-date security and feature updates from Microsoft.

So, how can you tell if your computer is still running Windows 7? Click the "Start" button on your taskbar and search "This PC". Right click on it, and press "Properties". A window will pop up with information about your computer—including your current Windows edition.



Now it's time to decide whether to upgrade, or replace your computer.

If the machine is older than 2.5 years we recommend replacing it. Microsoft charges $160 for the software, and then there's the time it takes to install it and configure the machine. It's just not worth it for a machine that only has 1 - 1.5 years left in it.

If your computer is less than 2 years old you can upgrade now and replace your machine later when the time comes.

The end of 2019 may seem like a long way away, but if you have more than a couple of computers running Windows 7 you should **act now**!

Replacing and updating computers is a time consuming and disruptive process. The more you plan this out in advance the less impact it will have on your organization.

We encourage you to work with us to develop a replacement schedule. That way you can spread the cost out as much as possible. It's cheaper and less disruptive for you, and it's easier for us because we can plan and schedule resources in advance.

Remember, 2020 is right around the corner, and it is critical to ensure all of your computers are getting regular security updates and feature enhancements. Not only will your computers work better, they will also be less vulnerable to security threats. Book an appointment now to discuss your options - don't wait until it's ***too late***. We will do whatever we can to meet this timeline, but keep in mind, the sooner you plan this the better.

Your security depends on this, so don't wait—act now and ensure your business stays secure.

Cybersecurity Video Series:

Reduce Your Risk With Employee Training

In this months **Cyber SecuriTip**, Ted provides 5 tips you can use to reduce your chances of data breaches, hacker attacks, and Ransomware. If an employees loses their laptop or smartphone, what does that mean for your business? Can you wipe them remotely, or do they belong to your employee? If you don't know the answer to that question then you could be in trouble if someone malicious gains access to a lost or stolen device.

An Acceptable Use Policy **(AUP)** and regular employee training could very well be the difference between someone losing their phone, and a full-fledged data breach!

To learn more, go to YouTube, look up **Connectability IT Support** and find the video ***"How You Can Reduce Cyber Security Risk Through Employee Training"*** OR go to our website at **www.connectability.com,** hover over **"Resources & Videos"** and select **"Videos".**

The #1 Way Hackers Access Your Network (And How To Prevent It From Happening)

It's easy to imagine the hackers attacking your network as a team of computer masterminds. But in reality, the vast majority of data breaches don't occur from some genius hacking into the mainframe. According to Trace Security, a full 81% of breaches happen as a result of poorly constructed passwords.

Luckily, avoiding this is pretty simple. Ensure every member of your team uses strong passwords, over eight characters in length and comprised of letters, numbers and symbols. Keep the numbers and symbols away from each other, and definitely avoid the common, obvious passwords like "123456789" or "password." You might also consider implementing two-factor authentication in your system, which is several degrees of magnitude more secure than ordinary passwords, but it can be a headache to set up without an expert on your team. *SmallBizTrends.com, 1/3/2019*

There Is One Thing That Separates Successful People From Everyone Else

Steve Jobs was a notoriously exacting boss. He constantly held himself to the highest standards of business and creativity and drove himself, and those around him, to greatness. But in his own words, one of his greatest strengths wasn't the quality of his mind, but his strength of belief. As he put it, "You can't connect the dots looking forward; you can only connect them looking backward. So, you have to trust that the dots will somehow connect in your future. You have to trust in something – your gut, destiny, life, karma, whatever. This approach has never let me down, and it has made all the difference in my life."

Of course, he's not talking about faith in some divine purpose; he's talking about faith in your own ability to make things work. Instead of developing some "perfect" master plan where every detail is accounted for, we always have to work with imperfect information and step into uncharted territory. Being comfortable with this, according to Jobs, is one of the biggest secrets to success. *Inc.com, 1/2/2019*

Who Wants To Win A $25 Gift Card?

Our last quiz question was: **Which of the following types of attacks do hackers use to gain information from you without the use of specialized computer programs?**

The answer was: **D) Social Engineering**

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a $25 gift card to Starbucks. Ready? Call us right now with your answer! **The QWERTY keyboard has basically been in use since the late 1870s. How could you tell that the keyboard in front of you uses the QWERTY layout?**

A) The first 6 letter keys on the top row spell QWERTY
B) The middle 6 keys on the keyboard spell QWERTY
C) The last 6 letter keys on the top row spell QWERTY
D) The function keys above the letter keys spell QWERTY

Call us right now with your answer! 416-966-3306

pancreatic cancercanada

This month we will be making a donation to **Pancreatic Cancer Canada.**

Pancreatic Cancer Canada is committed to improving pancreatic cancer survival by fostering research and creating hope through awareness, education and patient support. Their focus continues to be: supporting research, raising awareness, providing support, and advocating for increased funding.

Since its inception in 2006, Pancreatic Cancer Canada has invested nearly $4 million in research at cancer centers across Canada; funding scientific projects in early detection, treatment and improving patient outcomes.

If you want to contribute to Pancreatic Cancer Canada, we'd love your help! Email: **info@connectability.com** or call **(416) 966 3306**