Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: O'Doughs

Meet O'Doughs – a member of the Connectability family!

Founded in 2006, O'Doughs offers delicious and mouth-watering baked goods in Canada and the USA.

Focusing on the love people have for baked goods, and the needs of celiac and gluten-intolerant individuals, O'Doughs provides a wide variety of healthy and soft, high quality gluten-free products. Their products include savoury breads, buns, pizza crusts, and delicious sweet cakes - all with a great taste, soft and wonderful texture, and wholesome, nutritious ingredients.

O'Doughs is baking a difference and are happy to bring you what you want – whether that's great-tasting, healthy baked goods, or gluten free, non-GMO, vegan goods. O'Doughs wants you to feel good about eating, and have buns, breads, and cakes that you and your whole family will enjoy.

You can enjoy one of their mouth-watering products at restaurants such as Scaddabush, Jack Astors, Quiznos, and more, or visit one of the many retail stores that carry their products, located across Canada.

Connectability has been working with O'Dough's since June of 2017. Part of our role is delivering IT services and support, but it doesn't end there. We also provide O'Doughs with consultation services to help identify bottlenecks, areas for improvement, and cost-savings. We're always looking for ways to be proactive, and are regularly evaluating and taking on new security and productivity tools.

To learn more about O'Doughs, the products they offer, and their delicious recipes go to: https://odoughs.com/

August 2019

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

3 IT Investments You Should NEVER Skimp On

What is standing between your business's data, and hackers a world away? What's your plan when your on-site server fails?

When you skimp on technology and IT solutions for your business, the answers to these two questions are simple: 1) There is nothing standing between your business's sensitive data and people who want to take advantage of that data; and 2) There is no plan.

It happens way too often. Businesses cheap out on certain aspects of their technology to save a few bucks upfront. You may even know someone who has done just this. They jump at the chance to outfit their office with a huge monitor and a PC with top specs (even though they don't need it) and then they decide that IT security isn't a priority. They aren't willing to pull out the credit card for a security solution because they don't want to deal with a monthly or yearly cost.

But skimping on security can cost them dearly in time, money, resources and clients.

When it comes to investing in IT, here are three things you never want to cheap out on:

Security. Far too many businesses – from small to large – underinvest in IT security. We touch on this topic a lot because we see it a lot. These are business owners and managers who fall into the mindset of "It won't happen to me." This is a dangerous line of thinking.

For small businesses, a data breach can be devastating. Not only is data compromised and potentially copied or stolen, but your clients will also immediately question whether or not they should trust you. There's a good chance they end up taking their business elsewhere – and they may even sue you.

When IT security isn't a priority and you invest in the cheapest option available, it's like asking hackers to let themselves in. One study by the security firm Imperva found that over 50% of all Internet traffic is made by bots. Many of these bots are looking for security holes. They test websites and networks, looking for a way

Continued on pg.2

Continued from pg.1

in. If they find their way in, they can do some serious damage.

Investing in solid IT security – with an experienced team of IT specialists behind that security – can prevent that damage from ever happening in the first place. It's not only about protecting your business assets but also protecting your clients and giving them another reason why they should trust you.

Backups. You keep all of your data on-site with no backups. It's all stored in one central location and that's it. This is a recipe for disaster if you get hacked, but it can be an even bigger disaster if a hard disk or server fails. Suddenly, you find yourself unable to access client information, invoices, phone numbers – you name it. Having a backup on-site or in the cloud means everything you do has an extra layer of protection. A backup gives you the ability to restore your data should the worst-case scenario occur.

It's even better to go a step further and have a backup for the backup. Make sure you have one on-site solution and one cloud-based solution. Even if the backup to the backup is as simple as a 4TB hard drive from Amazon, it has the potential to save your business should anything go wrong.

Of course, you also need a system in place to make sure data is being regularly and accurately updated. Another mistake businesses make is buying a backup or backup services, but not making the best use of it. For example, they simply never bother to set it up, or it is set up, but isn't configured correctly. Your backup data isn't protected as intended – or it is being backed up too infrequently to be useful.

> **"... when you cut corners and cheap out, you will end up paying for it later..."**

Updates. How old is your technology? Think about the hardware you're running – and the software on that hardware. Letting your technology fall behind the times can spell trouble. Not only are you opening yourself up to security vulnerabilities, but you may also be operating on technology that's no longer supported by the developers.

If the developers are no longer publishing updates or supporting the software, this is a huge security red flag that it's time to update. On top of that, should you or an employee need to troubleshoot a piece of unsupported software, you may find yourself going up against walls. There might be no one to call, and if a Google search doesn't help, you may be out of luck.

The potential headaches don't end there. If you're running unsupported software on shiny, new hardware, you may be voiding the warranty of that hardware (always check your warranties and the fine print of any hardware you buy).

Alternatively, if you're trying to run brand-new software on old hardware, chances are you're going to run into compatibility issues. That wonderful piece of software might not work, or work the way you expected it to, all because you didn't want to update your old hardware.

It's not always fun to reach into your pocketbook to invest in good IT security, cloud backup storage or new hardware, but when you cut corners and cheap out, you will end up paying for it later, one way or another. When that bill comes, it's going to be a lot bigger than if you had committed to those IT investments in the first place.

It's More Than Just A Pop Can Tab!

Connectability is finding more ways to give back to our community. With all the hot weather we've had recently, our staff are enjoying some cold cans of pop to keep them cool. To give back, and put these pop cans to good use, we've decided to start a new initiative in the office. We are now collecting the pop tabs and donating them to March of Dimes Canada to be recycled at a local scrap metal company. March of Dimes Canada provides a range of services to people with physical disabilities throughout the country.

Our pop can tabs will be donated to their Pop Can Tabs Collection program. March of Dimes Canada recycles the tabs, and with the revenue generated from the recycling, they fund their Assistive Devices Program and their DesignAbility Program. The Assistive Devices Program helps buy, repair, and maintain a wide variety of mobility and assistive equipment (including wheelchairs), and the DesignAbility Program modifies and custom builds products for the physically disabled. Connectability is aiming to donate *a ton* of pop tabs, by collecting them all-year round.

If you want to learn more about this initiative and how to start it in your business, call us now at (416) 966-3306, or visit https://www.marchofdimes.ca for more information.

Shiny New Gadget Of The Month:

Drone X Pro

People are constantly looking for creative ways to express themselves, document their daily lives, share their adventures with their loved ones, and immortalize the most precious memories…

Nowadays, it's not so easy to stand out from the crowd, but there's finally one assured way to do it – and we call it DroneX Pro!

DroneX Pro was created with simplicity in mind so that everyone could use it. There's no need for heavy, bulky devices anymore – DroneX Pro's well-thought-out and ultra-compact design allows you to carry it wherever you go since it can easily fit in your pocket!

Despite the DroneX's size and portability, it provides you the most valuable features of high-quality drones and turns the process of taking pictures into an incredibly fun and entertaining experience!

DON'T Underestimate The Importance Of Software Updates

Over the past decade, cybercriminals have been a major threat to businesses around the world over. And to be frank, things are only getting worse. There are numerous hackers looking to get their hands on your confidential information. Some hold your data hostage until you pay up, while others are looking to take out their frustrations on your business. They might publish your client list, share your client's credit card info, or send data to a competitor.

Regardless of their goals, there are many ways a cybercriminal can get a foothold in your computing infrastructure. One of the most common methods of access is through phishing attacks. While these attacks are still widely successful, they've evolved into "spear-phishing" attacks, which are targeted, and more successful than traditional attacks.

Phishing scams aren't the only type of attack you need to be concerned about. There is also Ransomware, viruses, malware, spyware, and about a million other entry points to your network and confidential data. That said, hackers are always looking for the low hanging fruit. They aim for the easiest entry points to your network. One vulnerability we frequently see hackers take advantage of is unpatched computers.

Here's a quick story. Arizona Beverages, one of the largest soft drink suppliers in the U.S., was compromised and hit with Ransomware back in March. Their computers and servers were wiped clean, because a cybercriminal was able to gain entry through unpatched servers. They were running old and outdated operating systems that hadn't received any security patches in years. The result? Arizona had to shell out hundreds of thousands on new hardware, software, and recovery costs. And those costs don't include the sales they lost over the week they were inoperable, or the cost of downtime for hundreds of staff who were unable to work. Could your business survive this kind of disaster? If you aren't sure, you should update your computer and call your IT provider now.

The story above illustrates just why it is so important to do the little things – like updating your computers regularly. Having a firewall and a professional grade antivirus solution is a good start, but it will take a lot more than that to stop a seasoned hacker. Here are a few security tools and solutions that you can use to protect yourself and your business.

1. **Automated Patch Management:** Automating patch management allows you to focus on what's really important. You can schedule updates and reboots, plus you can analyze computers and servers to display the software version and patch status of each device.
2. **Datto Business Continuity and Data Recovery Appliance**: This device backs up your data locally, and to the cloud. That way, if you do experience a Ransomware attack, or you are compromised, you can boot up your server from the appliance. And, god-forbid, if you ever experienced a fire, a flood, or theft of your office computers you could boot your server directly in the cloud.
3. **Dark Web Monitoring:** in general, most businesses and individuals aren't aware that their credentials have been breached until it's too late. That's why you need Dark Web Monitoring. It scans thousands of dark web sites and forums for your credentials, and if it finds anything, you are notified so you can change your password immediately. This is especially important for those who have a tendency to use the same password for everything.

Ensuring your computers are patched can be the difference between business as usual, and a major cyber security breach.

Why Email Matters More Than Ever

In this month's **Tech Connect** video, Ted discusses everything you need to know about Office 365 and cloud hosted email. Email is the backbone of many businesses, and over the past 5 years it has evolved tremendously.

When email first appeared in commercial settings, it was hosted on an in-house server. That meant that you needed a third party, or an internal team to configure and maintain your infrastructure. If your server crashed, you would be without email until your physical hardware was back up and running. And unless you have a perfect image of your server configuration, AND a new piece of hardware ready to go, your email could be down for days. Without email your staff can't work, you can't fulfil current orders, and you can't take new orders. In the situation above, you'd be lucky if you were up and running in a couple of days.

To relieve these concerns, and reduce the barriers to entry, many companies moved to hosted email at other providers. One of the major providers is Microsoft with Office 365. Office 365 is hosted on Microsoft's own infrastructure, so you no longer need to maintain your own in-house server, PLUS it includes tools and updates for several office applications we use on a daily basis.

Watch this video NOW to learn about the different Office 365 options out there, and to discover the top 3 reasons you should be using Office 365. To learn more, go to YouTube, look up **Connectability IT Support** and find the video "**How Office 365 Makes Your Business Better**" OR go to our website at **www.connectability.com,** hover over **"Resources & Videos"** and select **"Videos".**

Do You Have These 3 Things Every Business Needs To Be Successful?

You have a solid team. People are everything in business – that includes your employees. You strive to hire the best team (who match your core values and company culture and who bring top-notch skills to the table) and you train them well (they understand your systems and processes). On top of that, they're happy!

You have purpose behind what you do. We all need purpose to not only be happy but also to thrive. When your team knows what they're working toward and understand the value of their work, that gives them purpose. You've clearly laid out the objectives and everyone is on the same page. When your employees know why they do what they do, they're happier and more productive for it.

You are passionate. You don't just love what you do, you love the people you work with and you love the difference your business makes in the community or the world. When you have passion, it's infectious. It inspires people around you. When your team is inspired, they'll go the extra mile and your business will find success like it's never found before.
Inc.com, 5/20/2019

What The Heck Is An AUP... And Why Do You Want It?

With so many access points, from cellphones to laptops and home computers, how can anyone hope to keep their network safe from hackers, viruses and other unintentional security breaches? The answer is not "one thing" but a series of things you have to implement and constantly be vigilant about, such as installing and constantly updating your firewall, antivirus, spam-filtering software and backups. This is why clients hire us – it's a full-time job for someone with specific expertise (which we have!).

Once that basic foundation is in place, the next most important thing you can do is create an Acceptable Use Policy (AUP) and train your employees on how to use company devices and other security protocols, such as never accessing company email, data or applications with unprotected home PCs and devices (for example). Also, how to create good passwords, how to recognize a phishing email, what websites to never access, etc. NEVER assume your employees know everything they need to know about IT security. Threats are ever-evolving and attacks are getting more sophisticated and cleverer by the minute.

If you'd like our help in creating an AUP for your company, based on best practices, call us. You'll be glad you did.

Who Else Wants To Win A $25 Gift Card?

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!

Which of the following is a "text-only" web browser?

A) Internet Explorer
B) Firefox
C) Netscape Navigator
D) Lynx

Call us right now with your answer!
(647) 492-4406

Canadian Cancer Society

This month we will be donating to **The Canadian Cancer Society**.

Founded in 1938, The Canadian Cancer Society is a national, community-based organization of volunteers, whose mission is to eradicate cancer and enhance the quality of life for all people living with cancer. Their vision is to create a world where no Canadian fears cancer.

The Canadian Cancer Society takes a comprehensive approach against cancer and are the only national charity that supports all Canadians living with all cancers across the country. The Canadian Cancer Society is committed to improving and saving lives. They are always looking for new and innovative ways to prevent cancer, find it early, and to treat it more successfully. They offer people with cancer the help and support they need to lead a more fulfilling life.

If you want to contribute to The Canadian Cancer Society, we would love your help! Email: info@connectability.com or call (647) 492-4406.