CONSUMER CHOICE AWARD 2020 GTA 3 YEAR WINNER

Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight
Northcrest Developments

Meet **Northcrest Developments.** They have been part of the Connectability client family since April 2019.

Founded in 2018, Northcrest Developments is located in Toronto and is in the process of redeveloping the Downsview Airport lands on behalf of the Public Sector Pension Investment Board (PSP Investments).

With the mandate of master planning and developing the Downsview Airport lands, Northcrest delivers financial returns for its shareholders, while also generating public benefits. Northcrest works with local communities, residents, and stakeholders locally and from across Toronto to develop the Downsview site into a sustainable and vibrant community.

Connectability has been Northcrest's technology partner for over a year. We monitor and manage their computers, mobile devices, peripherals like printers and firewalls, and their network infrastructure. We also provide them with a range of cybersecurity solutions to prevent cyber-attacks, data breaches and downtime, and we keep them updated with the latest security protections to ensure their computers and network are always secure. As their technology partner, we provide on-site and remote support, as well as consultative services to ensure Northcrest is operating at maximum efficiency.

If you would like to learn more about Northcrest, please go to: **https://www.northcrestdev.ca/**

September 2020

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

Why Your Business Is The PERFECT Target For Hackers...

And What You Need To Do NOW To Protect Yourself

Everybody gets hacked, but not everything makes the evening news. We hear about big companies like Target, Home Depot, Capital One, and Facebook getting hacked. What we rarely hear about are the little guys – the small businesses that make up 97.9% of employers in Canada. It's these guys who are the biggest targets of cybercriminals.

Basically, if you run a business, that business is a potential target. It doesn't matter what industry you're in, what you sell or how popular you are. Cybercriminals go after everybody. In 2018, a cyber security survey by the Ponemon Institute found that 67% of small and midsize businesses in the U.S. and U.K. were hit by a cyber-attack.

For the cybercriminal, casting a wide net makes the most sense because it gets results. It puts them in a position where they are able to extort money, steal sensitive information and ultimately profit off of destroying the property, prosperity and reputation of others.

Why do cybercriminals love to target small businesses? There are a handful of reasons why small businesses make sense to attack.

1. **Small Businesses Are The Most Vulnerable.** Business owners, entrepreneurs and executives aren't always up-to-date on network security, current cyberthreats or best practices in IT. They have a business to run and that's usually where their focus is. Unfortunately, that means cyber security can take a back seat to other things, like marketing or customer support. This also means they might not be investing in good network security

Continued on pg.2

Continued from pg.1

or any IT security at all. It's just not top-of-mind or they may feel that because it's never happened to them, it never will (which is a dangerous way of thinking).

2. **Small Businesses Don't Take IT Security Seriously.** Coming off that last point, it's true that many businesses don't properly secure their network because they feel that they *aren't* vulnerable. They have the mindset of "It hasn't happened to me, so it won't." Along those same lines, they might not even take password security seriously. According to research conducted by Trace Security, upward of 80% of ALL breaches come down to one vulnerability: weak passwords! Even in 2020, people are still using passwords like "12345" and "password" to protect sensitive data, such as banking information and customer records. Secure passwords that are changed regularly can protect your business!

3. **Small Businesses Don't Have The Resources They Need.** Generally speaking, medium to large companies have more resources to put into IT security. While this isn't always true (even big companies skimp on cyber security, as the headlines remind us), hackers spend less time focused on big targets because they assume it will take more of their own resources (time and effort) to get what they want (money and sensitive data). Many small businesses lack the resources like capital and personnel to put toward IT security, so hackers are more confident in attacking these businesses.

> **"67% of small and medium-sized businesses in the US and UK were hit by a cyber-attack."**

Just because you haven't had any major problems for years – or at all – is a bad excuse for not maintaining your computer systems. Threats are growing in number by the day. While many small businesses might think, "I don't have the time or resources for good security," that's not true! You don't need to hire IT staff to take care of your security needs. You don't need to spend an arm and a leg securing your network. IT security has come a LONG way in just the last five years alone. You can now rely on IT security firms to handle all the heavy lifting. They can monitor your network 24/7. They can provide you with IT support 24/7.

That's the great thing about technology today – while many hackers are doing everything they can to use technology against us, you can use it against them too. Work with a dedicated and experienced IT security firm. Tell them your business's network security needs, and they'll go to work fighting the good fight against the bad guys.

Quick Tip: How To Spot A Phishing Email

A phishing e-mail is a bogus email that is carefully designed to look like a legitimate request (or attached file) from a site you trust, in an effort to get you to willingly give up your login information to a particular website, or to click and download a virus.

Often these emails look 100% legitimate and show up in the form of a PDF (scanned document) or a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, etc. That's what makes these so dangerous – they LOOK exactly like a legitimate email. So, how can you tell a phishing email from a legitimate one? Here are a few telltale signs…

First, hover over the URL in the email (but DON'T CLICK!) to see the ACTUAL website you'll be directed to. If there's a mismatched or suspicious URL, delete the email immediately. In fact, it's a good practice to just go to the site direct (typing it into your browser) rather than clicking on the link to get to a particular site. Poor grammar and spelling errors are another telltale sign. An equally concerning warning sign is that the email is asking you to "verify" or "validate" your login or asking for personal information. Why would your bank need you to verify your account number? They should already have that information. And finally, if the offer seems too good to be true, it probably is.

Shiny New Gadget Of The Month:

Weber Connect Smart Grilling Hub

Grilling can feel like guesswork. You throw the food on the grill and keep a close eye on it, hoping for the best. Say goodbye to guesswork and overcooked steaks with the Weber Connect Smart Grilling Hub.

The Weber Connect takes the thermometer and timer into the WiFi era. It monitors your food and sends updates to your smartphone. It lets you know when to flip the burgers or steaks – and then notifies you again when it's time to take them off the grill. You can even have the Weber Connect tell you when your meat of choice has reached your ideal level of doneness. It's great for those who are new to grilling or don't grill often, and it works with every grill! See more at **bit.ly/3eTL69Y**!

The Evolution of the Internet of Things (IoT)

Picture this: You are on your way to the airport, ready for your business trip, when you realize you forgot to turn down your air-conditioning at home. Luckily, there's no need to stress. You take out your phone, and with a click of a button, you set the thermostat to 20 degrees.

This one has probably happened to more than a few of you: your son or daughter arrives home from school and realizes they forgot their house key. What do you do? Nowadays, you can just grab your phone and unlock the front door. Simple as that.

Or what if you are away on vacation and want to check in with your teenager to make sure they aren't throwing a wild party? Easy. Just open the webcam app on your smartphone and you can see what is going on in your living room from the light bulb in your celling.

Ten years ago, all of these ideas sounded unbelievable, but things have changed. These technologies all exist today! This is the evolution of the IoT.

The Internet of Things was originally designed to connect stand alone devices to the internet. The purpose of these devices is to leverage the technologies we already have in place, to control things that are ordinarily not considered high-tech devices. IoT devices include fridges, televisions, thermostats, door locks, cars, camera systems, baby monitors, music systems, printers, and so on.

The future holds even greater promise! Some staggeringly innovative IoT products will be released over the next few years. Some include:

- Facial Recognition Door Lock
- Smart Diapers
- Smart Wallet
- Self-driving cars
- Intelligent Toilets
- Smart Alarm Clocks
- Connected Mirrors
- Ingestible Sensors

The use of these internet connected devices will become more and more common, as they offer a variety of benefits. However, like all good things, there are drawbacks. The biggest drawback to IoT devices is your security and privacy.

Having multiple interconnected devices can make you more susceptible to a security disaster. If one device is compromised, then your entire network is exposed – allowing a cyber criminal to gain access to your most critical systems. That's why it's so important to make sure you are protected and secure. Call us now at (647) 492-4406 to evaluate your security risks and vulnerabilities and determine how to best close those security gaps.

Tech Connect Video Series:
3 Signs That Your Mac Is Infected

Whenever people think of viruses or malware infections, they tend to picture a Windows computer. That's because there is a pervasive myth that Macs aren't vulnerable to viruses. Unfortunately, this is far from the truth. Cybercriminals work hard to find security holes and vulnerabilities, and they will attack *anything*. That's why it's important to implement security tools and best practices to protect your computer regardless of the operating system it uses.

Your Mac can be infected with ransomware, viruses, and malware just as easily as a Windows device. The question is: how do you tell if your Mac is compromised? By being aware of the signs, you will be able to identify if your computer is infected and take immediate action.

Watch our video to learn 3 signs that indicate your Mac may be compromised. Mac cyber attacks may not be as common, but they're still a serious threat you need to prepare for. To find out more, go to **YouTube**, look up **Connectability IT Support** and find the video "**3 Signs That Your Mac Is Infected" OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".**

Back To Basics

A lot of time is spent staying protected from the newest type of scam or the newest cybercrimes, but as is true with many things, remembering the basics is the entire foundation of making sure you, your company and your clients remain safe.

Everyone in the company or organization should know basic security principles. Security principles and policies should be documented and part of every new employee training. Strong password requirements, Internet usage guidelines and only connecting remotely over VPN are examples of some common security policy items. Strict penalties for violating the security policies should be detailed.

It's not a good habit to save files onto your computer if there is a location on the network or on your server where they can live. They're much less likely to be backed up on your computer, whereas they'll reliably and regularly be backed up if they are saved on the server.

If you use websites or software that do not require regular password changes, set a calendar reminder to change the password yourself every other month.

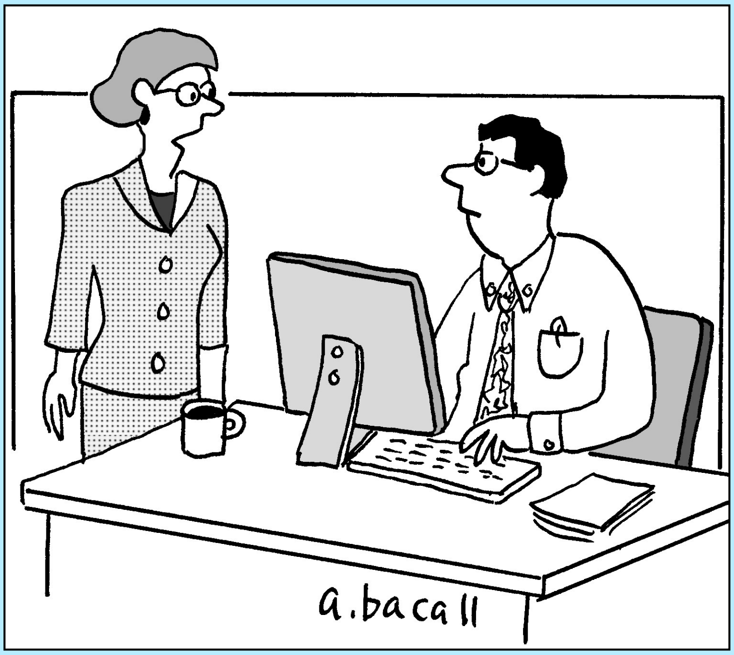
As with other things, a little prevention goes a long way – remembering the security basics, and asking about them if you don't know what they are, is the single best thing you can do to protect yourself and protect the company.

3 Email Productivity Tricks You Need To Know

Turn Off Notifications. Every time you get a ping that you have a new email, it pulls your attention away from what you were doing. It's a major distraction. Over the course of a day, you might get dozens of pings, which can equal a lot of time wasted. Set aside a block of time for reading and responding to emails instead.

Use Filters. Many email programs can automatically sort incoming emails. You define the sources and keywords, and it does the rest. This helps prioritize which emails you need to respond to soonest and which are most relevant to you.

Keep It Short. Most of us don't like to read e-mails – and so we don't. Or we quickly scan for relevant information. Your best bet is to just include the relevant information. Keep it concise and your recipients will appreciate it, and as a recipient, you'll appreciate it as well. *Small Business Trends, April 23, 2020*



"Tech support says your anti-virus software did not catch the problem since it is not a virus. It's a bacterium."

Food Banks Canada Banques alimentaires Canada

This month we'll be making our donation to **Food Banks Canada.**

Food Banks Canada is a national charitable organization dedicated to helping Canadians living with food insecurity. They support several Provincial Associations, affiliate food banks, food agencies, and provide support at the community level to relieve hunger.

Food Banks Canada offers programs to help food banks collect a safe and stable supply of nutritious food and distribute it to people in their communities. They also have a community garden program that provides food banks access to fresh food. They serve approximately 85% of the Canadians who turn to their community food bank or food program for help.

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!