CONSUMER CHOICE AWARD 2020 GTA 3 YEAR WINNER

Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: Dundas Real Estate Investments

Meet Dundas Real Estate Investments from our Connectability family!

Founded in 1997, Dundas Real Estate Investments started as a real estate investment and management firm. Their primary focus is on commercial and retail properties and they take a proactive approach to achieving high levels of satisfaction. They ensure that their clients operations run smoothly and efficiently to gain maximum value and profits.

Dundas Real Estate Investments believes in the importance of tenant relationships, and of balancing the responsibility and service between the owners and tenants. To successfully run properties, they believe in the significance of good relationships with all parties.

Connectability has been Dundas Real Estate Investment's technology partner since June 2016. We oversee their computers, servers, and cybersecurity to ensure that their systems are working efficiently and protected from any 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. Plus, we meet regularly to review service levels, upcoming needs, and budgets to plan for the future.

To learn more Dundas Real Estate Investment and the services they offer, go to: https://www.dundas-realestate.com/

December 2020

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

Cybercriminals Confess:

The Top 3 Tricks And Sneaky Schemes They Use To Hack Your Computer Network That Can Put You Out Of Business

Cybercriminals and hackers are rarely shy about the methods they use to attack their victims. Many of them are more than happy to share how they broke into a business's network or how they walked away with thousands of dollars after successfully extorting a business owner whose company is now destroyed.

There are new stories out there to get your blood boiling as cybercriminals work to ruin people's lives and livelihoods. These criminals don't care what kind of damage they do. They only care about one thing: money. If they can get away with it – and many do – they'll keep on doing it.

It's up to the rest of us as business owners (and employees) to stay at least one step ahead of these cyberthugs. The single best way to do that is to **stay educated on the latest threats.** The second-best way is to **stay up-to-date with the latest technology designed to combat cyber-attacks.**

Here are three tricks of the trade cybercriminals are using right now in an attempt to get their hands on your money:

Ransomware. This is very common. It's a form of malware, and it can sneak onto your network and into your computers in a number of different ways:

- **Ad Networks.** These ads can appear on social media sites and on familiar websites. Someone clicks a compromised ad or pop-up, and it initiates a file download. It's quick and it can be confusing. This is where anti-malware and anti-ransomware come in very handy.
- **Malicious Links.** The cybercriminal

Continued on pg.2

Continued from pg.1

sends you a legitimate-looking email, supposedly from your bank or a familiar online store. It may even be disguised as an email from a colleague. The email contains a link or file. If you click the link or file, it installs the ransomware.

- **Hidden Files On Thumb Drives.** This happens way too often where someone brings a thumb drive from home. While the user doesn't know it, the drive has a malicious file on it. When the thumb drive is inserted into a networked machine, the file is installed.

No matter how the ransomware gets onto your devices, the result is basically the same. The ransomware goes to work and begins encrypting your files. Or it may completely block you from accessing your computer altogether. You'll get a full -screen message: *Pay up or never access your files again*. Some ransomware programs threaten to delete all of your files. Others say they will never restore access.

DDoS Extortion. Short for distributed denial of service, DDoS attacks are a relatively easy way for hackers to take down your business's online presence and wreak havoc on your network. These attacks mimic online users and essentially "flood" your network with access requests. Basically, it's as if millions of people were trying to access your website at once.

Your network simply can't handle that kind of traffic and, as a result, it goes down. The hackers can continue the attacks until you take action. That is to say, until you pay up. If you don't pay up, the hackers will do everything they can to keep you offline in an attempt to destroy your business. If you rely on Internet traffic, this can be devastating, which is why many businesses end up paying.

Direct Attacks. Some hackers like to do the dirty work themselves. While many cybercriminals rely on bots or malware to do the work for them, some hackers will see if they can break through your network security in a more direct way. If successful at breaking in, they can target specific files on your network, such as critical business or customer data.

Once they have the valuable data, they may let you know they have it. Sometimes they'll ask for money in return for the sensitive data. Sometimes they won't say anything and instead simply sell the data on the black market. Either way, you're in a bad position. A criminal has walked away with sensitive information, and there is nothing you can do about it.

Except, that last sentence isn't true at all! There *are* things you can do about it! The answer is preventative measures. It all comes around to these two all-important points:

- Stay educated on the latest threats
- Stay up-to-date with the latest technology designed to combat cyber-attacks

If you do these two things and work with an experienced IT services company, you can change the outcome. You can put the cybercriminals in their place and have a digital defense wall between your business and those who want to do your business harm.

"You can put the cybercriminals in their place and have a digital defense wall between your business and those who want to do your business harm."

Ditch The Old Stuff, And Start New!

New Years resolutions are about getting rid of old baggage and striving to be the best that you can be. So why not apply the same concept to your business? At some point your IT equipment will no longer meet the needs of your business. They will become too slow or the technology will be outdated. It's time for you to take action!

The best indicator of whether it's time to buy new equipment is if your employee's productivity has dropped as a result of the equipment provided to them. If an employee spends a significant portion of their day waiting for files to load due to a computer issue, then the repeated loss of productivity is probably going to outweigh the $1,000 or so to buy a new laptop.

This also goes for other equipment in your office including routers, printers, switches, firewalls, and servers. If you're consistently spending time worrying about, or dealing with IT issues, then it's time for an upgrade.

Slow and outdated computers and IT equipment cost you money in productivity and downtime. Start the new year right, by spending more time with your loved ones and less time dealing with technology headaches.

If you would like to know if it's time for your business to upgrade its IT equipment call us now at: (647) 492-4406.

Shiny New Gadget Of The Month:

SelfieSpin360 For GoPro

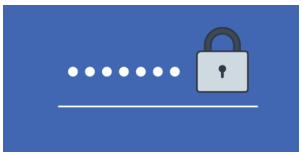
A GoPro camera is great for a crystal-clear, wide-angle video of yourself or your subject, and you can attach it to the end of a selfie stick for some nice static shots, too. But if you're ready to take things up a notch and capture even more truly awesome moments, then you need the SelfieSpin360.

It's all there in the name: the SelfieSpin360 gives you a way to get incredible 360 degree footage of yourself in any setting. You attach your GoPro or smartphone to the end of a sleek and secure base, which is attached to a long cord with a handle for camera controls on the end. Hit Record, then start swinging the device up and around your head lasso-style to capture a unique version of yourself in a special moment. The SelfieSpin360 kicks boring old selfies to the curb. Visit SelfieSpin360.com to purchase yours.

Your Passwords May Not Be Secure — Update It Now!

There is an ongoing battle between technology and security, and it's one that you may never win. To keep information confidential, people depend on a web of passwords, pins, and security codes.

They include passwords for your email, online banking, computer, network, and credit cards. BUT, that's not all: sites like Facebook, Amazon, eBay, Instagram and LinkedIn also require you to have a personal account and password. With so many different accounts, a lot of people end up using the same password for everything. If you are one of these people, I'm warning you! You are making a VERY big mistake.



If a cybercriminal breaks into one of your accounts, they can now access all your other accounts. By using the same password for everything, a hacker can get into your bank account, take your funds, and even steal your identify.

As we end the year, it's time to take an extra step to protect your sensitive information. Here are **4 tips** that will help prevent hackers from getting into your accounts:

1. Don't use simple, easy to guess passwords. For instance, your child's name or the name of a pet. And if you use a familiar password, use a combination of upper- and lower-case letters, numbers and special characters to make it harder to guess. For instance, if your name is Joey, try using J0ey20@.

2. Don't use the same password for everything. You can use different passwords based on the site. For low-security sites like YouTube and LinkedIn, you can use the same password. For online banking, use a different and more difficult password.

3. Change your passwords regularly. The more you change your passwords, the less vulnerable you are to breaches.

4. Use a password manager. Don't use sticky notes, Word documents, or emails to store your passwords. These methods are inherently risky. Instead use a password manager to keep your passwords encrypted and in one location. When you use a password manager, all you need to remember is your master password.

If you use simple passwords, or you use the same password for everything, then you are putting your business at risk. Start the new year on the right track by changing your passwords and storing them in one, secure location.

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".**

Get Organized And Back On Track

Top Business Apps To Get You Organized

If you're struggling to stay on top of your work tasks, there are some great apps available to help out.

- **Asana** helps your business improve communication and collaboration. You can view all tasks and projects and follow progress on a communal board so you can communicate without having to rely on email.
- **Proven** helps organize your hiring process by posting listings to multiple job boards with one click. You can also review and sort applicants with ease.
- **Boxmeup** organizes and tracks your packages, containers and bulk storage items to make storing and shipping a breeze.
- **Evernote** keeps all your notes organized in one place and allows you to easily share notes and lists with co-workers.
- **Trello** tracks your team's workflow. Whenever you make a change to a project or task, the app notifies each team member involved so you don't have to.
- **KanbanFlow** helps managers visualize overall workflow. It gives overviews of work status, tracks progress and assigns tasks to team members. *Nerdwallet, Apr. 21, 2020*

Top 5 Ways To Overcome Setbacks and Grow

After you encounter a setback, it can be hard to start again. But simply believing in yourself is the best way to get back on track.

1. Recognize when failure is your fault and when it isn't. Some setbacks are entirely out of your control. Learn to recognize the difference in your faults and what you can't control, then move forward.

2. Learn from your mistakes and don't repeat them. Immediately letting go of the regret of making a mistake can be hard, so instead, focus on what caused the mistake, then learn from it.

3. Focus on your new goal. Failure often comes from going after something we don't truly want. Discover what you really want so you understand what you need to work on.

4. Celebrate small wins. You don't have to wait to celebrate, even if you haven't reached your end goal. Validate yourself for completing smaller tasks, and you'll empower yourself to keep going.

5. Find the right mentor. This is someone who believes in you, even when you don't believe in yourself, and who can support you in reaching your goals. Find someone with the right knowledge and experience to learn from. *Business Insider, Sept. 16, 2020*

HAPPY HOLIDAYS!

"'Season's Greetings' looks O.K. to me. Let's run it by the legal department."

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, especially over the holidays, we'd love to hear from you! Email us at: info@connectability.com or call (647) 492-4406 today!