CONSUMER CHOICE AWARD 2020 GTA 3 YEAR WINNER

Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Free Executive Webinar The Rise Of Data Breaches

If you've read the news lately, I'm sure you've seen something about a recent, high profile data breach.

Now you might say "Cyber criminals won't bother with my small or medium sized business". Unfortunately, this just isn't true. Cyber criminals aren't discriminating, and time and time again, we've had to remediate the impact of a data breach or cyber-attack on a small business.

Regardless of the size of your business, it pays to be educated. That's why we're hosting a webinar on **Tuesday, November 16th, at 12:00 pm**, titled "***The Rise Of Data Breaches: How A Tidal Wave of Data Breaches Could End Up Costing Your Business, And What You Can Do To Protect Your Data, Your Clients and Your Bank Account***"

To sign up, go to: **www.connectability.com/databreachwebinar** OR call: **(416) 966-3306**.

During the event, you will learn:

- **How Data Breaches Are Changing**
- **The Impact** of a Breach (Downtime, Reputational Damage, Legal Fees, etc.)
- The Future of Data Breaches
- How Data Breaches Can **Disguise Other Types of Attacks**
- **How You Can Protect Your Business and Clients**

November 2021

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

A Proven Method To Secure Your Business's Network

People don't usually think about small businesses when discussing cyber security. The media covers breaches in governmental and big-business security in excess. These entities usually have lucrative targets that attract the attention of hackers but are often backed up with an extremely protective network security system that's difficult to crack. When hackers can't break the big system, they turn their attention to easier targets.

While most hackers want the opportunity to crack a high-risk target, these situations are few and far between. Instead, they turn their attention toward much lower-hanging fruit. This is where small businesses come in; they still have access to money and data but have much lower defence than a governmental entity. Luckily, many average cyber security strategies can keep the would-be hackers away. Their methods are always changing, though, and it helps to be one step ahead of the game.

These are the best current cyber security strategies you can put into place.

Cloud Security

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage and deletion. As more and more businesses switch from hard-drive data storage to remote databases, this practice is becoming more and more commonplace. Methods of providing cloud security include firewalls, penetration testing and virtual private networks (VPN), to name a few. While many people feel that their data and information are better stored on a hard drive on their own network, data stored in the cloud may actually be more secure, depending on the system's defence strategy. Be wary, though: not all cloud securities are made the same. Do your research and pick one that will best protect your data.

Network Security

Network security is the protection of the underlying networking infrastructure from unauthorized access, misuse or theft. This is what your network administrator will need to put into place in order to keep your devices and data secure. The best approach to protecting

Continued on pg.2

Continued from pg.1

your network is to create a strong WiFi password. Random numbers and letters work best for a small business since nobody but those who need it will be able to guess the password. In addition to a strong password, you'll also have to anticipate any type of internal attack.

VPNs And Firewalls

A VPN can help protect your security by masking your IP address. This essentially means that you'll be connected through a different server, making it much harder for the government or websites to pinpoint your location. It also encrypts all network data by creating a secure tunnel. A firewall is simply a shield that protects your computer from the Internet. Firewalls can help restrict access to sites that could be damaging to your network. Both of these tools can be highly effective when used properly, but they do not protect against all threats.

Updates And Upgrades

While it might seem simple, consistently updating and upgrading your technology tools can keep you much more secure. The developers of many of these tools are constantly looking for new threats that pose a risk to their program. They'll issue patches to make sure any holes are filled. You just need to make sure that all of your tools are updated in a timely manner and verify that the updates are installing.

> **"Many average cyber security strategies can keep the would-be hackers away."**

Data Backups

You should always have multiple backups of your business's data. You never know when a power surge or some type of natural disaster might cause your current files to be deleted. You can prevent this issue by regularly backing up your data.

Employee Training

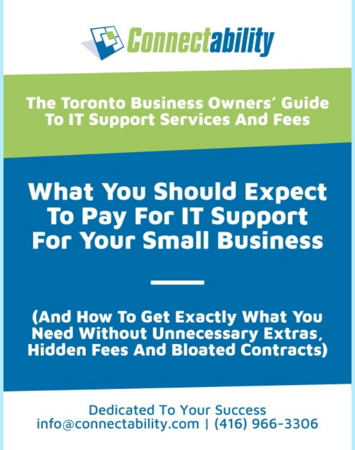
It's important to limit employee access to systems and data owned by your company. Not everyone needs to have access, so only give it to those who can't work without it. There should also be some type of security training for all employees. Phishing schemes and weak passwords create just as many issues as hackers do. Finally, you should make sure everyone in your workplace is security-conscious. A single breach could critically hurt your business. Your employees need to understand this so they can be proactive as well.

No matter which route you take, the most important thing you can do for your small business is protect its network. Governmental entities and big businesses do not suffer from security lapses nearly as bad as small businesses. A security lapse could even stop your business dead in its tracks.

Free Report Download: The Toronto Business Owners' Guide To IT Support Services And Fees

You'll learn:

- The 4 most common ways IT services companies charge for their services, and the pros and cons of each approach
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs that you didn't anticipate



Connectability

The Toronto Business Owners' Guide To IT Support Services And Fees

What You Should Expect To Pay For IT Support For Your Small Business

(And How To Get Exactly What You Need Without Unnecessary Extras, Hidden Fees And Bloated Contracts)

Dedicated To Your Success
info@connectability.com | (416) 966-3306

Claim your FREE copy today at: https://www.connectability.com/itbuyersguide/

Shiny New Gadget Of The Month:

Angel Guard Cookware Prevents Burns

Many people burn themselves every day while cooking in their kitchens. There's a new product on the market that aims to prevent these injuries. After firefighter Eric Le Blanc responded to back-to-back kitchen burns involving children, he knew there had to be a safer alternative. In his research, he found that tipping pots of hot liquid were the world's leading cause of adolescent burns.

Le Blanc developed the world's first tip-proof cookware: Angel Guard Cookware. This cookware removes risk by including a removable stem that slides underneath the burner grate and locks the cookware into place. Now parents no longer have to worry about their child getting hurt after removing a pot from the stove.

Are Your Printers Safe?

When most people think about hackers and protecting their equipment, they think about their desktops, laptops and servers, while overlooking other equipment that they have in their office or home workspace. But what about your printer? Just like your computers and servers, printers are also an entry point that a cybercriminal can use to access your network. Your business may have cybersecurity protections in place for your computer infrastructure, but are you securing the rest of your network, including your printers?

Here are 3 tips to protect your printer:

1. **Update your printer's operating system**
   It's important to update your printers so that software updates or patches are applied. This makes it more difficult for a cybercriminal to get in. Printer manufacturers regularly release software updates, so keep an eye out for those. You should also change the default password when you configure your printer. Most networked printers can be accessed remotely with a password. By making the default password more complex, you are adding an extra layer of security.

2. **Set up a firewall**
   You can restrict printer access by applying security protections. One protection you should include is a firewall. This will block threats from outside your company network. Another simple way to protect your business is to unplug your printer from your network. If the printer is not connected to your network, then there is no way a hacker can access it remotely.

3. **Wipe the drives**
   Your printer/scanner stores your company's documents, faxes, files, images, etc. that are going to be, or have been printed. Ensure that you wipe the drives to remove all confidential data, or your business may get into some legal trouble. Also, use an encrypted network when printing sensitive information. When you use an encrypted network the print job can't be stopped or interrupted because your information is converted into a code that can't be easily broken by a cyber criminal.

Printers have poor network security measures, which make them more susceptible to cyber attacks. That's why it's important for you to take the necessary precautions to protect your systems. These 3 tips will help secure your printer from viruses and attacks, reducing your chances of experiencing an expensive data breach . If you are concerned about your printer security, we are happy to help. Give us a call at (647) 492-4406 or email info@connectability.com.

Tech Connect Video Series:
Multi Factor Authentication Is More Important Now Than Ever!

Cybercrime is on the rise. Hackers are using all the tools and resources at their disposal to find your login credentials, access your accounts, and steal your company and personal data. Most people tend to use weak, easy-to-guess passwords (like birthdays and pet names) or use the same password for all their accounts. By using simple passwords, you can be a victim of a security breach. That's why it's important to have an additional layer of protection to put a stop to hackers.

MFA immediately increases your account security by requiring multiple forms of verification to prove your identity when signing into an application. By using multi-factor authentication (MFA), you make it more difficult for cybercriminals to exploit and obtain your sensitive data – even if they have your password.

Watch this video to learn 3 benefits of multi-factor authentication and how it can protect you and your business from a cyber-attack. To find out more, goto YouTube, look up Connectability IT Support and find the video **"Multi Factor Authentication Is More Important Now Than Ever!"** OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

Is Your Data Secure?

In today's culture, data security is more important than ever. It would be horrific for many if their personal information was compromised. Unfortunately, your data may not be anywhere near as secure as you might hope.

The Pegasus Project is an exposé that revealed that a piece of spyware can exploit a user's Apple or Android devices to take control of the user's device. A list of 50,000 victims was published that included government officials, business executives and royal family members – proving that nobody is safe.

Tech companies usually write extremely secure codes initially, but as new features roll out, holes are created in the defence that hackers can exploit. Pegasus proved that, in the software world, if an adversary is well-motivated, they will find a way in.

The key to staying protected from these breaches is depth. Multiple lines of defence are more protective, so don't stop at one. Though one security tech may have plenty of gaps, another could fill those and strengthen your security.

New security technologies are continuing to advance the security field. There are plenty of actions you can take to ensure that your data remains secure.

Storytelling Is More Important Than Building A Presence Online

Social media has become an ever-important tool in the business world. It can help build customer loyalty while also being an essential marketing strategy. However, simply having an account is not enough.
In order to grow, you need to understand your customers and what motivates them. Provide them with an experience they won't be able to obtain anywhere else. Be sure to do this while also making your social media content relevant. If your account does not focus on your products or services, it will prove useless.

Build connections with and focus on your customers. Without trying to approach a specific type of customer, your message can get lost. It can be difficult to attract all of your customers at once.

More important than the rest is to make your presence authentic and accessible. Keep the big picture in mind and don't get lost in the weeds.

Can You Solve This Sudoku Puzzle?

1	4	2		9				5
7			4				8	9
8		5					2	4
2					4	8		
	3				1	2	6	
	8			7	2	9	4	1
	5		2		6			
	2	8			9	4	1	
	7	9	1		8	5	3	

Call Us At (647) 492-4406 For The Answers!

Covenant House TORONTO

This month we will be donating to the **Covenant House Toronto**.

Founded in 1982, with only 30 beds, Covenant House Toronto has now grown to provide hope and opportunity for more than 95,000 young people. Covenant House Toronto is committed to supporting vulnerable youth. They serve youth who are homeless, trafficked or at risk.

As Canada's largest agency serving youth to ignite their potential and reclaim their lives, the Covenant House offers a wide range of 24/7 services to about 350 young people each day. They focus on public policy, leading awareness and prevention programs, and building and sharing knowledge.

Covenant House offers housing options, health and well-being support, training and skill development, all with unconditional love and respect. Their team is dedicated to supporting and building one-on-one relationships with youth, advocating for change in the community, and forming programs.

If you want to contribute to the Covenant House Toronto, we would love your help! Call: (647) 492-4406 or email: info@connectability.com.