CONSUMER CHOICE AWARD 2022 GREATER TORONTO AREA 5 YEAR WINNER

Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Help Us Celebrate Emmanuel's 3rd Year Anniversary!

Help us congratulate our Projects and Implementation Manager: Emmanuel Thom-manuel on his successful third year at Connectability.

Emmanuel has played a major role in troubleshooting and resolving our client's IT issues, proactively monitoring their network, and help improving their productivity by leveraging technology.

Emmanuel goes above and beyond to ensure projects are successful, in order to meet the expectations of our clients, along with their constantly changing business objectives.

We are very happy to have him on our team and are excited for the years to come!

October 2022

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

Keep Your Information Secure

By Using Strong Passwords

We use passwords for just about everything. Most of us have to enter a password to get into our computers and then enter other passwords to access our email, social media profiles, databases and other accounts. Even our cellphones and tablets can and should be password-protected. In fact, if you aren't securing all of your devices and accounts with passwords, you should definitely start. It could help prevent your business and personal information from becoming compromised.

Why Passwords?

We use passwords to ensure that those who don't have access to our accounts can't get access. Most of our devices hold large amounts of personal information. Think about the potential harm someone could do if they gained access to your personal cellphone. They would immediately be able to see all of your contacts, pictures and applications. They might even be able to log in to your email, where they could obtain your banking information. If this type of access falls into the wrong hands, it could be detrimental to your life. Passwords offer the first line of defence to prevent others from obtaining sensitive information.

This becomes even more important if you own a business. Each of your employees should be utilizing strong passwords to access company information. If your business is not using passwords – or is using simple passwords – you could be opening yourself up to hackers and cybercriminals. If a cybercriminal gains access to your company's private information through a weak password, they will gain access to customer information, which could damage your reputation and open you up to lawsuits. That being said, everyone within your business needs to utilize complex and unique passwords.

Continued on pg.2

Continued from pg.1

Making A Strong Password

Not all passwords are created equal. When it comes to making a strong password, you must think about it. If you use a password that you can't remember, then it's essentially useless. And if you use a password that's too easy to remember, your password probably won't be strong enough to keep cybercriminals out. Your password should be long, have a mix of lowercase and uppercase letters, utilize numbers and special characters, have no ties to personal information and should not be a word from the dictionary.

In the grand scheme of things, it's not enough to just create complex passwords. They also need to be unique. To that end, you should use a different password for each and every one of your accounts to help maximize their effectiveness. Think about it this way: Let's say you use the same password across your business email accounts, social media accounts and bank accounts. If someone decrypts the password for your Facebook page, they now have the password for more valuable accounts. If you can't tell that your social media account was compromised, the cybercriminal could try to use that same password to gain access to more important accounts. It's a dangerous game that can be avoided by using unique and complex passwords for every account you use.

"You should use a different password for each and every one of your accounts to help maximize their effectiveness."

Remembering All Of These Passwords

You may be worried about remembering all of your passwords if you have to create a unique one for each of your accounts. Your first thought may be to write them down, but that might not be the most secure option. If someone gets their hands on your little black book of passwords, they'll immediately gain access to all of your accounts with a handy directory showing them exactly where to go. Instead, you should utilize a password manager to help keep track of all of this sensitive information.

With a password manager, you only have to worry about remembering the master password for your password manager. All of your other passwords will be securely hidden. Password managers also give you the option to create random passwords for your accounts to bolster their security. That way you can have the most complex password possible without worrying about forgetting it. Additionally, password managers can also help you remember the answers to security questions and more so that you never get accidentally locked out of one of your accounts. They're easy to use, convenient and secure.

Passwords are an important part of your cyber security plan. Make sure you and your employees are using complex and unique passwords. It can also help to implement some training so your employees understand the importance of secure passwords. When used correctly, passwords will help deter any would-be cybercriminals from accessing your sensitive information.

Quick Tip: How To Spot A Phishing Email

A phishing email 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

Bril

It might be surprising to hear, but our toothbrushes are some of the dirtiest items in our households. There's a good chance that there are more than a million kinds of bacteria living on your toothbrush right now.

Unfortunately, rinsing your toothbrush after brushing is only so effective. That's why Bril was invented.

Bril is a portable toothbrush case that sterilizes your toothbrush after every use.

It contains an all-natural ultraviolet light that kills 99.9% of germs on contact. It's simple to use as all you have to do is place your toothbrush inside and close the lid. Bril does the rest.

It's the quickest, most effective and easiest way to ensure your toothbrush head stays clean.

Top Tips When Selecting An MSP For Your Business

Technology underpins nearly every aspect of modern business processes. Managing it, however, can be complex and tedious. This is where managed IT services providers (MSPs) can help. Whether your company needs software solutions, network infrastructure management services, or cloud technology, MSPs can provide all this and more.

Selecting the best MSP
While there are numerous MSPs out there, not all of them are equipped to meet your company's unique needs. You can only achieve optimum IT results by selecting the right MSP.

Here are some criteria to keep in mind:

Depth of skills and experience
An MSP should have the skills and experience that go beyond basic software installation, maintenance, and upgrades. They should also have strong expertise in advanced IT functions, such as database management, cloud technology, security, and cross-platform integration, so they can keep pace with your company's growing IT requirements.

Financial stability
With IT being the backbone of your business operations, you need an IT partner who will be there for the long haul. Assess their stability by looking into how long they've been in business. Check how many clients they have and their customer retention numbers. Also, read online customer reviews and testimonials.

Competitive service level agreement (SLA)
An SLA is a contract that dictates the standards that your MSP must meet. It should be able to answer these questions: Do they offer 24/7 support? Can they conduct remote and on-site support? What are their guaranteed response and resolution times? If they fail to meet their committed service levels, do they offer rebates or money-back guarantees?

Third-party vendor partnerships
Pick an MSP with an ongoing relationship with the technology vendors (e.g. Microsoft, CISCO, QuickBooks) whose products you already use in your IT environment. Verify the partnership the MSP has with those vendors. The higher the partnership level, the more vendor experience the provider has, which means they can provide plenty of expertise to your business.

Choosing the right provider is a crucial decision that will impact your business's performance and success. If you want to learn more about how MSPs can support your business, contact us today at (416) 966-3306.

Tech Connect Video Series:
How Zero-Trust Solutions Can Reduce The Risks Of Your Biggest Cybersecurity Vulnerability: Your Staff

When evaluating cybersecurity protections, most businesses focus on external threats like hackers, and cyber criminals. And while these are important risks to consider, one area that few businesses take seriously enough is the risk introduced by their employees. Your team regularly downloads and installs new software, responds to customer emails, and provides confidential company information to colleagues, clients, and vendors. As a result, your employees represent the greatest cybersecurity risk to your organization.

So, what happens if an employee accidentally (or intentionally) installs a malicious program? Do you have technology to notify you or prevent it? How would you even know if someone has breached your systems? If you were infected with Ransomware, how long could you and your business survive without access to your data? These are all questions you will need to answer.

Watch this video to learn how Zero-Trust Solutions can protect you from a cyber-attack. To find out more, go to https://bit.ly/3srPqpn OR go to our website at www.connectability.com, hover over "Resources & Videos", select "Videos" and click on "How Zero-Trust Solutions Can Reduce The Risks Of Your Biggest Cybersecurity Vulnerability: Your Staff".

Take Advantage Of Google Reviews

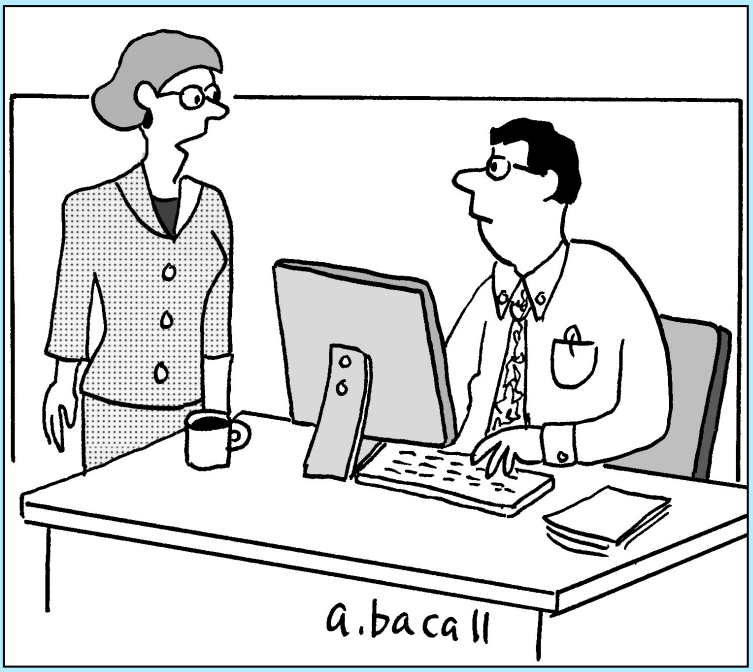
When you are deciding on a restaurant to dine at, you might check the Google reviews to help with your decision. The same thing goes for your business. Before people come in to buy your product or services, they might check your Google reviews – so it's important that your reviews positively reflect your business. If you own a company, you should understand how Google reviews work and do everything you can to encourage customers to leave positive ratings and comments.

If you haven't already claimed your Google business profile, you should do so immediately. It will allow you to add pictures and a description so customers know what to expect from your business. When customers have completed a purchase with you, encourage them to leave a review if they had a positive experience. Some customers may need help with the review process, so teach them how to leave a review if they have never done it before. Make sure you thank customers who leave positive reviews and try to fix the issues explained in your negative reviews. Being a responsive owner will reflect positively on your business. When you use Google reviews to your advantage, you will see a boost in clientele.

3 Easy Ways To Make Your Mac More Secure

Data breaches and malware attacks have been on the rise over the past few years, so you must take the necessary precautions to protect your devices. Below you will find three easy ways to make your Mac more secure.

- Install a mobile device management profile so you can give an administrator remote access to the device. If your Mac is ever stolen, you can locate it and lock it before any of your data becomes compromised.
- Utilize multifactor authentication which will require you to confirm your login on another device. This adds an extra layer of security to your Mac.
- Backup your data to protect yourself from ransomware attacks. Consider buying an external hard drive or a cloud storage solution and backup software to do so.



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

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 (416) 966-3306.