Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

IT Security Services: What You Need To Stay Secure

Cyber security threats pose a serious risk to **businesses of all sizes**. With new sophisticated hacks emerging every day, you can no longer take a "set it and forget it" approach to IT security.

Unfortunately, the owners of many small and medium sized businesses take the perspective that they won't be breached because they are small. Their logic is that hackers and cybercriminals are only focused on stealing from the biggest and most successful companies. Unfortunately, that's far from the reality.

Unless your business is **secured by 24/7** network monitoring, intrusion detection and advanced threat management (at a minimum), **you are leaving yourself vulnerable**.

Protecting your digital assets — from servers, your network, applications, all the way down to individual files — is **multi-layered and complex.** Your IT security needs will look completely different from another company's.

That's why we audit your IT infrastructure and current security protections before devising and implementing your **unique IT security plan**. With custom IT security services from Connectability, you get the attention and level of protection your business needs at an affordable monthly cost.

Give us a call at **(416) 966-3306**, if your are interested in IT Security Services for your business.

May 2022

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

Stay Compliant

By Upping Your Cyber Security Practices

If you own or operate a business, there are plenty of things you must do to ensure success. You have to make the right hiring decisions; develop a product or service that you can sell; build relationships with clients, employees and partners; and much more. One of the biggest responsibilities that comes with owning or operating a business is ensuring that your business is compliant with any guidelines put in place by regulatory bodies.

Every business needs to make an effort to stay compliant, and a big part of that is making sure your cyber security practices are up to standards. With technology rapidly advancing and regulations changing fairly often, you have to stay up-to-date on any changes that should be made going forward. You also need to make an effort to plug any holes in your current cyber security plan.

You can do this by asking yourself a few questions and making the necessary adjustments if you answer no to any of the following:

- Is my business protected by a firewall and antivirus software?
- Do I use backup solutions, and do I have a disaster recovery plan in place?
- Has my storage stayed up-to-date with any technological changes?
- Do I have any content or email spam filtering software?
- What data am I encrypting?

Ensuring that your business stays compliant will be extremely important in maintaining client and employee relationships. If a customer's information gets compromised because your business did not have the necessary cyber security in place, they probably won't come through your doors again. As technology changes and evolves, so do many of the regulations and cyber security practices that you should put in place. It can be difficult to become compliant if your business was lacking previously. Luckily, there are a few steps you can take to help ensure that your business becomes and stays compliant with any

Continued on pg.2

Continued from pg.1

regulating bodies.

First, you should document all of the consumer data your business holds. If a customer asks what information your business has collected on them, then you should be able to give them an honest answer. You might also be obligated to share this information. By keeping and maintaining this information, you will be able to supply your customers with it if they ever do ask.

It can also help greatly to partner with a managed services provider who manages IT needs since they will be able to perform routine IT data checks and work to better protect your customer and the private information within your business. MSPs go a long way toward helping with all of your potential IT needs, but their focus on cyber security—protection and compliance— should not be underestimated. Partnering with an MSP will help get your business on the fast track to becoming cyber-secure.

Another big part of ensuring that your business stays compliant is to introduce cyber security training for all of your employees. Did you know that 95% of cyber-attacks start with human error? If your team has not bought into a cyber-secure culture or does not know the proper cyber security practices, you could be in some trouble. Make sure that cyber security training is part of your onboarding process and continue to train your employees throughout their tenure with your business.

Once your employees are aware of the risks of cyber-attacks and have bought into a cyber-secure culture, it's time to upgrade your cyber security. One of the best things you can do

Cyber security and compliance work right alongside each other.

for your business is to invest in regular software patching. Technology is ever-evolving, and we should make the necessary changes to ensure it continues to cooperate with our network and systems. Put technology in place to cover these holes or partner with an MSP that can help take care of any lapses in your cyber security.

Additionally, you should invest in some content-filtering software. There are plenty of toxic websites with nefarious intent that can wreak havoc on your cyber security if accessed by an employee on your network. Content filtering allows you to restrict certain websites. It also goes a step further by recognizing patterns in websites that have malicious codes and blocking those websites that might pose a risk.

Cyber security and compliance work right alongside each other. If you're trying to ensure that your business stays compliant, you need to beef up your cyber security practices. There are many methods you can take to do this, but if you're unsure of where to begin, give us a call. We would be glad to help you take the next steps toward creating a cyber-secure business.

Do You Safeguard Your Company's Data And Your Customers' Private Information?

You are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – Social Insurance Numbers, credit card numbers, birthdates, home addresses, emails, and many other important details

Don't kid yourself. cybercriminals and hackers will stop at NOTHING to steal your credentials. And once they have your password(s), it's only a matter of time before they destroy your business, scare away your customers and ruin your professional and personal life.

Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

Our 100% FREE and 100% confidential, exclusive Dark Web Scan is your first line of defense. To receive your report in just 24 hours, give us a call. Hopefully it will be ALL CLEAR and you can breathe easy. If your company, your profits and your customers are AT RISK, we'll simply dig a little deeper to make sure you are protected.

Don't let this happen to you, your employees and your customers. *Reserve your exclusive Dark Web Scan now!*

Get your free Dark Web Scan TODAY
Call Us At (416) 966-3306

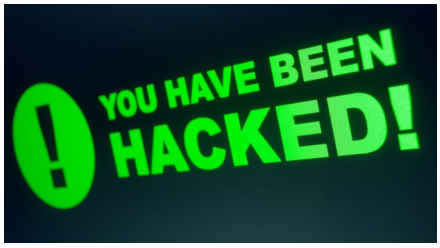
Shiny New Gadget Of The Month:

Bird Buddy

Birdwatching from your home has never been easier. Bird Buddy is the newest development in the world of birdhouses. Bird Buddy looks like your normal birdhouse but has so much more to it. It has a built-in camera that will send a push notification to your phone whenever a bird is visiting. Bird Buddy comes standard with artificial intelligence bird recognition so you'll know exactly what types of birds visit your home. It's easy to install and can even be mounted to the outer walls of your house or on fence posts. It's built from incredibly durable materials; you won't have to worry about inclement weather or squirrels destroying your birdhouse. Bird Buddy is the most advanced birdhouse on the market and is available for pre-order now.

3 Signs You're About To Get Hacked — And What You Can Do To Prevent It

Hackers love to go after small businesses. There are tons to choose from, and many don't invest in solid IT security. Plus, many business owners and their employees have bad cyber security habits. They do things that increase their risk of malware and cyber-attacks. Here are **five bad habits that can lead to a hack** and what you can do to reduce your risk.



1. **Giving out your email**: Just about every website wants your email address. If you share it with a vendor or e-commerce site, it's usually not a big deal (though it varies by site – some are more than happy to sell your email to advertisers). The point is that when you share your email, you have no idea where it will end up – including in the hands of hackers and scammers. The more often you share your email, **the more you're at risk and liable** to start getting suspicious emails in your inbox.

   If you don't recognize the sender, then don't click it. Even if you do recognize the sender but aren't expecting anything from them and do click it, **DO NOT open links or attachments.** There's always a chance it's malware. If you still aren't sure, confirm with the sender over the phone or in person before clicking anything.

2. **Not checking for HTTPS:** Most of us know HTTP – Hypertext Transfer Protocol. It's a part of every web address. However, most websites now **use HTTPS, with the S meaning "secure."** Most browsers now automatically open HTTPS websites, giving you a more secure connection, but not all sites use it.

   If you visit an unsecured HTTP website, any data you share with that site, including date of birth or financial information, is not secure. You don't know if **your private data will end up in the hands of a third party**, whether that be an advertiser (most common) or a hacker. Always look in the address bar of every site you visit. Look for the padlock icon. If the padlock is closed or green, you're secure. If it's open or red, you're not secure. You should immediately leave any website that isn't secure.

3. **Saving passwords in your web browser:** Browsers can save passwords at the click of a button. Makes things easy, right? Unfortunately, this method of saving passwords is not the most secure. **If a hacker gets your saved passwords, they have everything** they could ever want. Most web browsers require a password or PIN to see saved passwords, but a skilled hacker can force their way past this if given the chance.

   Protect yourself with a dedicated password manager! These apps keep passwords in one place and come with serious security. Password managers can also suggest new passwords when it's time to update old passwords (and they remind you to change your passwords!). LastPass, 1Password and Keeper Security Password Manager are good options. Find one that suits your needs and the needs of your business.

Tech Connect Video Series:
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. In fact, in the first half of 2021 alone, more than 118 million people were impacted by data breaches, data exposures and data leaks. Now you might say "Those are all large multi-national companies. 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-attacks.

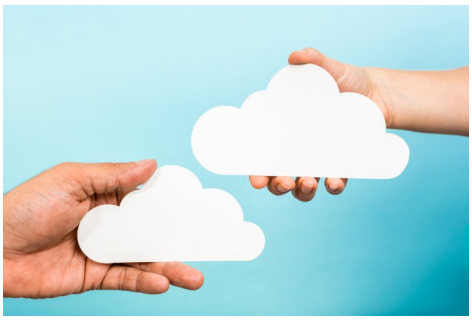
If your data is breached, do you know what the costs to your business would entail? Do you know how long it could take to recover or restore your data? What are your disclosure requirements? Do you have copies of that data, or is it gone forever? What would be the impact on your clients, and would they continue to use your services after a breach? These are all questions you should be asking yourself.

Watch our Webinar now to learn about the rise of data breaches and how you can protect your business. To watch, go to YouTube, look up Connectability IT Support and find the video **"The Rise of Data Breaches"** OR go to our website at **www.connectability.com**, hover over "Resources & Videos" and select "Videos".

Using Multiple Public Clouds In Your Business? Try Out Cross-Cloud

Public clouds are commonplace among businesses these days. A public cloud is an IT model where on-demand computing services and infrastructure are managed by a third-party provider and shared with multiple organizations using the public Internet. About 73% of businesses are currently using two or more public clouds. This is becoming a problem because most public clouds are not designed to operate alongside other cloud systems.

Almost half of technology executives report that their cloud structure is increasingly complicated, but they are looking to increase consistency across their public cloud environments. The cross-cloud operating model is aimed at fixing any inconsistencies between clouds and making them more compatible with each other. With cross-cloud, operators can deploy, monitor and manage apps for every cloud. This will allow businesses to spend more time working on their business and less time trying to manage multi-cloud dilemmas. The VMware Cross-Cloud services portfolio is an industry-first, multi-cloud architecture that unifies app and cloud infrastructure, development and operations.



The Worst Month For The Stock Market Since The Pandemic Began

The stock market saw a very rough start to kick off 2022. Some stocks that saw rises throughout the past two years suffered from the opposite effect in January. Vaccine maker Moderna, one of last year's top-performing stocks, started the year down nearly 40%. This drop is believed to be caused by research suggesting that the firm's booster shot is less effective against the Omicron variant.

Another company that experienced a big drop is Netflix. They had poor fourth-quarter earnings and saw their shares drop 37% in January. With higher prices announced for every streaming package on Netflix, it seems unlikely that their stock is in for an immediate bounceback. Other stocks that had a major negative trend in January are Etsy, Advanced Micro Devices, Nvidia, Caesars Entertainment and Domino's Pizza. Stocks have swung wildly since the year began, and only time will tell if things return to a level of normalcy for many companies that had stock increases throughout the pandemic.

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!

What company did the founders of YouTube work for before starting up YouTube?

a) PayPal
b) Google
c) Disney
d) Amazon

Call us right now with your answer!
(416) 966-3306

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.