Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Employee Cyber Security Training

Like it our not, the biggest point of entry into your network is your employees.

They mean well, and they may be technically savvy—unfortunately hackers and cybercriminals are often *one step ahead* of average, and even above average computer users.

That's why Cyber Security training is SO critical. With minimal work, you can implement in depth security training for your employees.

Our training program includes a comprehensive Phishing simulation to train your team to recognize email borne threats, and training modules focused on Ransomware, data theft, social media awareness, best practices for remote workers (something almost all businesses should be concerned about), and much more.

Call us today at **(416) 966-3306** to learn how you can educate your team and prevent cyber attacks!

March 2023

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

Keep Your Business Protected By Becoming Aware Of The Most Common Types Of Cyber-Attacks

The rate of cyber-attacks has significantly increased over the past few years. Businesses of all sizes are at risk of becoming victims, which is why it's crucial that every business owner and leader is aware of the most common cyberthreats impacting the business world today. Being aware of common cyberthreats and developing plans to prevent them is the best way to protect your business, customers and employees from cybercriminals.

These criminals' tactics will improve as technology continues advancing, but cyber security defenses will as well. Knowing exactly what you're up against with cyber-attacks and creating the proper safeguards will protect your business. If you're new to the idea of cyber security or need an update on the common threats that could impact your business, we've got you covered. Below, you will find the most common types of cyber-attacks out there and how to protect your business from them.

Malware

Malware has been around since the dawn of the Internet and has remained a consistent problem. It is any intrusive software developed to steal data and damage or destroy computers and computer systems. Malware is an extensive type of cyber-attack, and many subcategories belong to it, including viruses, spyware, adware and Trojan viruses. One type of malware that has lately been used more frequently is ransomware. Ransomware threatens to publish sensitive information or blocks access to necessary data unless a sum of money is paid to the cybercriminal who developed it.

Unfortunately, malware can be detrimental to nearly every operation of your business, so you should do two essential things to prevent it from affecting your company. First, you should install the latest anti-malware programs. If you hire a services provider, they will take care of this for you. If not, you'll need to find anti-

Continued on pg.2

Continued from pg.1

malware that works best for your system. You should also train your team about these risks and ensure they are aware not to click on any suspicious links, websites or files that could be dangerous.

Phishing

Have you ever received an email asking for sensitive information that looked official, but something just wasn't quite right? Chances are it was probably a phishing scam. Phishing occurs when cybercriminals send official-looking messages to individuals, posing as another organization, in an attempt to receive personal information. Falling for a phishing scam can quickly result in you becoming a victim of identity fraud. The results can be substantially worse if a business falls for the scam.

So, how do you best prepare for and protect your team against phishing scams? Utilize employee cyber security trainings so they can spot the warning signs. The actual email will usually line up differently from whom the cybercriminal is trying to represent. Also, most organizations will not request private information over email. Common sense will prevail over phishing scams.

Distributed Denial Of Service

DDoS attacks can bring your business to a standstill. These attacks occur when malicious parties overload servers with user traffic, causing them to lag or shut down since they are unable to handle incoming requests. If your business falls victim to this kind of attack, your employees might not be able to access key functions required to do their jobs, and customers may not be able to use your website or purchase items from you.

> **"Being aware of common cyberthreats and developing plans to prevent them is the best way to protect your business, customers and employees from cybercriminals."**

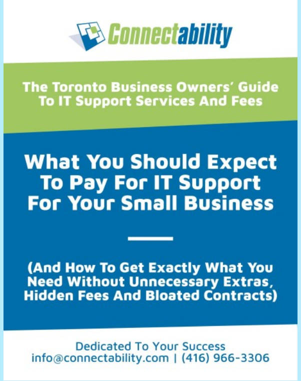
DDoS attacks are very difficult to thwart, and a determined cybercriminal can lock up your websites and networks for days on end. You'll have to identify malicious traffic and prevent access before it can cause damage. Hiring an MSP is your best bet to prevent DDoS attacks. If a DDoS attack is successful, you'll probably have to take your servers off-line to fix the issue.

Password Attacks

If a cybercriminal gets your password or another employee's password, this is the easiest way for them to access your valuable information. They may attempt to guess the passwords themselves or use a phishing scam to gain access. It is vital that you enable multifactor authentication (MFA) for your employees and require complex passwords so you can defend your company against password attacks.

Now that you know the most common forms of cyber-attacks happening today, you can take the necessary precautions to protect your business, employees and customers.

Free Report Download:
The Business Owner's Guide To IT Support Services And Fees



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

You'll learn:

- The three most common ways IT 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 later on that you didn't anticipate

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

Shiny New Gadget Of The Month:

Valve's Steam Deck

Nintendo, Microsoft and Sony are some of the most prominent players in the video game console industry, but there's another name making headlines in these console wars: Valve's Steam Deck. In fact, this is the perfect gaming system for anyone who is looking for a powerful and portable console.

The handheld system is capable of playing the most advanced AAA games available and comes in three different storage sizes. If you've used Steam in the past on your PC, you'll immediately gain access to your library of games and will be able to purchase any other games from Steam directly on the device. Check out the Steam Deck if you're in the market for an affordable, powerful and portable gaming PC.

4 Things You Should Do To Secure Your Business Against Ransomware

Ransomware is becoming increasingly pervasive. A few years ago, when we spoke to business owners about Ransomware, very few had heard of it. Nowadays, most managers and directors know that Ransomware is a concern, and likely not going away anytime soon.

Ransomware, simply put, involves a hacker accessing your systems, encrypting your data, and demanding payment via untraceable means (often Bitcoin) in order to return it to you. And unfortunately, you never have any guarantee that they will do what they said they will.

Ransomware attacks are often dispersed using phishing schemes, spam emails, Trojans, password-stealers, ad clickers, and so much more.

Once files are encrypted, ransomware prompts the user for a ransom to be paid within a day or two to decrypt the files, or they will be lost forever. Here are 4 things you can do to better protect your computers, data, and business from a ransomware attack.

1. **Back up your data:** Having a regularly updated backup can help defeat ransomware. If you are attacked with ransomware, you can restore your system and not pay the attackers a penny.

2. **Patch your software:** Software developers regularly release security updates. We've all been guilty of pressing the "remind me later" button and putting off updates for as long as possible. But it's something you should avoid at all costs. Cybercriminals can use this hole in your software to gain access to your systems. By patching and updating your computer, you can decrease your chances of a potential ransomware attack.

3. **Check your emails:** Be wary of suspicious emails, especially if they include links and files. Email is one of the popular methods a cybercriminal uses to get into your network. If you are questioning whether an email is authentic and from a trusted source, do not download or click anything and delete it immediately. If you are concerned, pick up the phone and try to call the contact to confirm.

4. **Use a strong security "stack":** By using a good security "stack", you can protect your computer and network from being breached. A good software stack includes antivirus, a business-grade firewall, and email filtering software, at a minimum. These tools look for threats, unsafe links, and can protect you from malicious emails, viruses, and external entry into your network.

By following the 4 tips above, you can avoid becoming the victim of a ransomware attack. These protective measures can go a long way to ensuring your computer and business is protected. If you are interested, we can also conduct a free network assessment to see if your business is truly secured. Call us now at **(416) 966-3306** for your free assessment. It could end up saving you thousands of dollars later!

Tech Connect Video Series:
Think Your Email Is Safe? Think Again!

For most business owners and executives, email is a critical communication tool that they use every day to stay connected with customers, colleagues, and vendors alike. Unfortunately, due to it's wide-spread use, it has become THE SINGLE MOST common attack point hackers and cybercriminal use to gain access to your confidential data and your business network.

What would you do if your mailbox were breached, or encrypted with Ransomware? How long could you and your business survive without access to this data? Could you afford to pay the Ransom? Do you have systems in place to allow you to restore that data, even if it is encrypted by a hacker?

This video will provide answers to these questions and walk you through the various tips, tricks, and tools you can use to secure your email, and your business. To watch, go to **https://bit.ly/3JzoPQs** OR go to our website at **www.connectability.com**, hover over "Resources & Videos" and select "Videos".

2 Selling Strategies Your Business Should Avoid

In the world of business, there are good and bad selling strategies. Strong selling strategies bring your customers back for more and encourage them to refer their friends and family. In contrast, poor strategies will send your customers running for the hills. They'll never look back at your business and will tell everyone about their negative experiences.

If you or your selling team are utilizing any of the following strategies when selling to customers, you should put a stop to it immediately, or your sales will begin to decline.

Not Addressing The Customer's Main Problem: When customers approach you for a specific product or service, they most likely have a reason for coming. Listen to your customers' concerns rather than overexplaining your product or service. If you provide a solution to their problem, you'll likely earn a sale.

Arguing With Customers: Has a customer ever said something unreasonable or completely wrong about your product? You might have been quickly defensive, but starting an argument with a customer will never lead to a sale, even if you're right. Listen to them and figure out where they're coming from before responding.

Become A Better Business Leader By Ditching These Habits

You want to be the best leader possible if you own or operate a business, but you may have developed habits over the years that are preventing you from being your best. As you grow in your role, you must overcome habits and certain ways of thinking that might impede your progress. If you're utilizing any of the following habits, it's time to change the way you're approaching things.

Black-And-White Thinking: There is plenty of grey in the world of business. You can't look at things as being one way or another. There are many different ways to approach each problem.

Your Opinion Matters More: You must listen to your team if you hope to be a great leader. You won't be right with every decision. Hear suggestions from your team and make an informed choice in order to determine the best path for your business.

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!

Which country has the highest percentage of their population online?

A. South Korea
B. Iceland
C. Norway
D. Japan

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

Pathways
to Education

This month we will be donating to **Pathways To Education**.

Pathways To Education was founded in 2001, and its mission is to help youth from low-income communities thrive. They deliver resources and support to help young people graduate from high school, and prepare for a successful future.

Using a breakthrough approach, focused on innovation and community building, Pathways To Education helps students overcome adversity by developing resiliency and skills to succeed. They focus on four important areas – academic, financial, social, and one-on-one services. Pathways To Education has helped students from all over the country graduate from high school, and has put them on the path to one day becoming Canada's leaders.

If you would like to contribute to **Pathways To Education** we would love your help! Email us at: info@connectability.com or call: (416) 966-3306.