# Connectability Corner

## PUTTING THE PIECES TOGETHER.

*Powered by:* **Connectability**

CONSUMER CHOICE AWARD 2020 GTA — 3 YEAR WINNER

## May 2020

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

# 3 Ways To Stop Cybercriminals Cold In Today's Crazy Times

You've seen it. You've probably even experienced it. For what feels like forever now, just about everyone has been forced to modify priorities. As a business owner, you've probably been focused on shifting your business to accommodate this world crisis. You may even be investing more of your time in retaining customers and generating new cash flow. If you're like most people out there, you've barely even had time to think about cyber security and protecting your important data.

Maybe you've heard the saying "Never let a crisis go to waste." It's as if cybercriminals wrote it because that's exactly what they're thinking right now. In fact, they're probably working overtime right now to craft new malware while our lives have been turned upside down. Yes, as you're focused on your business, hackers are finding new ways into your IT network. Their objective is to steal data and passwords, compromise your clients' private information and even demand large ransoms.

Did you know that cybercrime is expected to cost $6 trillion (that's a 6 followed by 12 zeroes!) by the year 2021? But, now is when hackers are expected to do their absolute most damage.

Here are three strategies you can use right now to help protect your business data, money and productivity during these unusual times.

**1. Guard Your Inbox.** People aren't paying as much attention as they usually do, which makes it the perfect

time for cyber-attackers to send emails with dangerous malware, worms and viruses. Always carefully inspect every email received and make sure you know the sender.

Here's another tip: avoid clicking links in the email unless it's abundantly clear where they go. Also, don't ever download an attachment unless you know who sent it and what it is. While it takes a few extra seconds, double check by calling the person who sent you the attachment. Better safe than sorry. Make sure you communicate these safeguards to everyone on your team, especially if they are working from home.

**2. Secure Your Company-Based Technologies.** During crises like this one, your passwords are a critical first line of defense. Don't wait for your company's finance data to be compromised. Make a point now to reevaluate your passwords and direct your team to create stronger passwords. Too many employees are guilty of using the same password across multiple applications. Use a unique password for every single application.

Your team may tend to save your passwords in their web browser. Don't do this. A skilled hacker can bypass the PIN required to access your saved passwords. Once they have the password or PIN to access your web browser, they can steal as much as they want – credit card information, customers' private data and more!

**"Did you know that cybercrime is expected to cost $6 trillion (that's a 6 followed by 12 zeroes!) by the year 2021?"**

We recommend our clients use a password manager. It's convenient, but more importantly, it's far more secure.

**3. Secure Your Home-Based Technologies.** With the coronavirus pandemic, far more businesses are encouraging their employees to work from home. That means a lot of people are working from the living room or kitchen without giving a second thought to security. This negligence is an invitation to new cybercrimes.

Here are a few tips to ensure your work-from-home employees are keeping your network and data secure: make sure your employees and contractors are not using their home computers or devices when they are working from home. Add a firewall to ALL computers and devices that will be utilized at home. Finally, your network and data are not truly secure unless your employees utilize a VPN (virtual private network), or log in through a remote access tool.

There's no need to invite more problems in by letting your computer and network security slide during these times. We would be happy to help you create or even improve your work-from-home environment.

While this coronavirus scare has negatively affected countless businesses, we are proud to say we are open and continuously servicing our customers. If you need additional security advice or would like to have a consultation to discuss how to keep your data safe or how we can help you work more effectively, simply connect with us today.

## Connectability Is Toronto's #1 IT Provider!

For the third year in a row, Connectability has been recognized by Consumer Choice Awards as the Best Managed Service Provider in Toronto and the Greater Toronto Area. We are very honoured to receive this award, and we couldn't have done it without our amazing customers!

Consumer Choice Award promotes business excellence in small and medium sized business across Canada. Connectability was chosen because of our commitment to providing high quality, responsive, and consultative IT services and support. Our services include Managed Services, VoIP solutions, cybersecurity services, backup and disaster recovery, and more. We work our clients to minimize downtime, reduce IT costs, and resolve frustrating and time-consuming technology issues that leave you pulling your hair. Our aim? To maximize our clients productivity and profitable by delivering Worry-Free IT.

In our 25 years in business we've worked with hundreds of companies across a wide range of industries, so we have the insight and experience to understand your business needs, technology issues, and strategic direction, so we can propose the most appropriate solution for YOU. If you want to work with Toronto's Best Managed Service Provider call us at (647) 492– 4406.

## Shiny New Gadget Of The Month:

### Zepp Golf 2
### Swing Analyzer

Improve your golf game with a device smaller than a golf ball. The Zepp Golf 2 is a remarkable piece of tech that attaches to the back of any golf glove. It's packed with sensors and delivers real-time analysis of your game.

Using Bluetooth, the Zepp Golf 2 pairs with your smartphone. As the data is analyzed, it's displayed on the accompanying app. It tracks your club speed, backswing positioning, hip rotation, consistency and much more. The Zepp Golf 2 also has a long-lasting battery – up to eight hours – so it will definitely make it through your next game without a hitch. The Zepp Golf 2 is compatible with both iPhone and Android devices. Learn more at Amazon or Zepp.com.

# How To Secure Your Work From Home Business

Businesses around the world are facing unprecedented challenges. Everyone is being asked to self-isolate and practice social distancing, which puts businesses in a tough position. Do you shut down completely, or allow employees to work from home? It obviously depends on your business, but most companies have opted for the latter.

Most business owners want to know how they can keep their teams productive, grow their revenue and continue to build their business while managing a dispersed workforce. One of the best ways you can do that is to help your employees create a successful environment to work in from home. And while it sounds simple, an effective remote work environment takes more than just ensuring your employees have a laptop and phone. It's important that you determine what technologies they need, how you can keep their networks and computers secure, and how you can help them set up a comfortable and productive environment.

For now, "business as usual" is going to involve a major shift. To adjust to a work from home model, you need to do three things:

1. **Don't allow employees to use home computers or devices**
   Your company computers and network are secure and protected from malware, viruses and cyber attacks while personal computers may not be. Personal devices are used to downloaded music, videos and more, which increases your businesses exposure to cyber threats. To keep your business safe, provide your employees with a secured company device to use at home. And make sure you have an Acceptable Use Policy (AUP) so employees know what they can and cannot do with those machines.

2. **Ensure your Wi-Fi Network is Secured**
   If your employees Wi-Fi networks aren't password protected, then their personal info and your company info are accessible to all manner of hackers. To properly secure your employees Wi-Fi networks, they must use WPA2 level encryption along with a complex password. That password should be long and random so it can't be cracked by a determined hacker. To take security to the next level, they should also enable the firewall on their router, and hide their network name.

3. **VPN must have two factor authentication**
   The employees' virtual private network (VPN) must use multi-factor authentication. This means that there is an additional layer of security for your business. Your employee will have to verify themselves with a code that is sent to their phone each time they access your network.

Adapting from a traditional office centered environment to working from the comfort of your home can be a challenge. You need to have the right tools and infrastructure in place to be productive and secure. If your business needs some extra assistance right now, or a solution to allow employees to work from home, we are here to help. Give us a call at (647) 492-4406 and someone from our office will assist you.

---

### Tech Connect Video Series:
#### Build Strong Habits And Create A "New" Normal

So much has happened over the past few months. Everyone has been hiding out in their homes and trying to avoid human contact as much as possible. While working from home can be a great for your team, it can also make it more difficult for people to develop and stick with their habits.

Working from home is the new normal and you must define where your work life ends and where your personal life begins. To remain productive and effective you need to establish a new routine and form habits. We've put together a video with 4 tips you can use to build a consistent routine and stick with it.

If you've had a challenging time transitioning to a remote work environment and want to get back on track, watch this video now. To access it, go to YouTube, look up Connectability IT Support and find the video "**How To Maintain Strong Habits While Working From Home**" OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

## Do These 3 Things To Make Sure You Don't Get Hacked

**Train up.** Get your entire team trained on IT security fundamentals and best practices. They should know how to create strong passwords, how to safely access the web and how to securely use email – including how to identify phishing scams. They should have a clear understanding of today's threats and how to be proactive in addressing those threats.

**Invest in good tech.** You should be invested in solid malware protection, including antivirus software and firewalls. All of your data should be backed up to the cloud and expertly secured using encryption software. You should also be invested in threat monitoring.

**Establish relevant systems and processes.** Have standard operating procedures (SOP) in place to train employees, respond to threats and access networks. For example, are employees connecting with unverified devices from home? Establish rules on what can and cannot happen. Another example: are your cloud backups set up correctly? Is someone checking it? Again, have SOP in place to address these kinds of issues. *Small Business Trends, Feb. 13, 2020*

## 3 Ways To Grow Your Business Without Spending A Dime

**Follow a thought leader in your industry.** Whether you follow them on social media or their blog, keep up-to-date with the issues they're talking about. Then do further research into those issues. This keeps you in the know and more likely to learn something you can easily apply to your own business.

**Use your best testimonials.** If someone posts a great review on Google, for example, reach out and ask about using it in your marketing. Or reach out to customers who you already have a good relationship with and ask if they're willing to give you a testimonial. It builds credibility.

**Partner up.** It pays to develop partnerships with existing vendors or other businesses that are adjacent to yours. That is to say, look for opportunities to share customers. If you have a customer who's looking for a specific service you don't offer, point them to someone who does (your partner). And your partner will do the same. Reach out into your business community and see what kind of relationships you can form. *Business Insider, Feb. 13, 2020*



"Say what you like about Cloud Computing, but the technical support is amazing"



This month we'll be making our donation to the **Food Banks Canada.**

Food Banks Canada is a national charitable organization dedicated to helping Canadians living with food insecurity. They support several Provincial Associations, affiliate food banks, food agencies, and provide support at the community level to relieve hunger.

Food Banks Canada offers programs to help food banks collect a safe and stable supply of nutritious food and distribute it to people in their communities. They also have a community garden program that provides food banks access to fresh food. They serve approximately 85% of the Canadians who turn to their community food bank or food program for help.

If you'd like to contribute to this worthy cause we'd love to hear from you! Email us at: info@connectability.com or call (647) 492-4406 today!