Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Help Us Welcome Our Newest Team Member: Laurie Ashton

Connectability has grown a lot over the past 5 years. To continue that aggressive growth we've also had to grow our team. Please help us welcome Laurie Ashton to Connectability!

Laurie is our newest Office Manager. Her role at Connectability is to assist our clients and staff to ensure all procedures and operations are followed. Laurie is ready to work with your team and is focused on providing exceptional service.

June 2021

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

Breaking Bad Habits
4 Ways Your Employees Are Putting Your Business At Risk Of Cyber-Attack

Your employees are instrumental when it comes to protecting your business from cyberthreats. But they can also become targets for hackers and cybercriminals, and they might not know it. Here are four ways your employees might be endangering your business and themselves — and what you can do about it.

1. They're Not Practicing Safe And Secure Web Browsing. One of the most basic rules of the Internet is to not click on anything that looks suspicious. These days, however, it can be harder to tell what's safe and what isn't.

A good rule of thumb is to avoid websites that do not have "https" in front of their web address. The "s" tells you it's secure – https stands for Hypertext Transfer Protocol Secure. If all you see is "http" – no "s" – then you should **not** trust putting your data on that website, as you don't know where your data might end up.

Another way to practice safe web browsing is to avoid clicking on ads or by using an ad blocker. Hackers can use ad networks to install malware on a user's computer and network.

2. They're Not Using Strong Passwords. This is one of the worst IT security habits out there. It's too easy for employees to use simple passwords or to reuse the same password over and over again or to use one password for everything. Or, worse yet, all of the above.

Cybercriminals love it when people get lazy with their passwords. If you use the same password over and over, and that password is stolen in a data breach (unbeknownst to you), it becomes super easy for cybercriminals to access virtually any app or account tied to that password.

Continued on pg.2

Continued from pg.1

No hacking needed!

To avoid this, your employees must use strong passwords, change passwords every 90—180 days, and not reuse old passwords. It might sound tedious, especially if they rely on multiple passwords, but when it comes to the IT security of your business, it's worth it. One more thing: the "tedious" argument really doesn't hold much water either, thanks to password managers like LastPass that make it easy to create new passwords and manage them across all apps and accounts.

3. They're Not Using Secure Connections. This is especially relevant for remote workers, but it's something every employee should be aware of. You can find Wi-Fi virtually everywhere, and it makes connecting to the Internet very easy. A little too easy. When you can connect to an unverified network at the click of a button, it should raise eyebrows.

And unless your employee is using company-issued hardware, you have no idea what their endpoint security situation is. It's one risk after another, and it's all unnecessary. The best policy is to prohibit employees from connecting to unsecured networks (like a public Wi-Fi) with company property.

Instead, they should stick to secure networks that then connect via VPN. This is on top of the endpoint security that should be installed on every device that connects to your company's network: malware protection, antivirus, anti-spyware, anti-

"Education is a powerful tool and, when used right, it can protect your business and your employees."

ransomware, firewalls, you name it! You want to put up as many gates between your business interests and the outside digital world as you can.

4. They're Not Aware Of Current Threats. How educated is your team about today's cyber security threats? If you don't know, or you know the answer isn't a good one, it's time for a change. One of the biggest threats to your business is a workforce that doesn't know what a phishing email looks like or doesn't know who to call when something goes wrong on the IT side of things.

If an employee opens an email they shouldn't or clicks a "bad" link, it can compromise your entire business. You could end up the victim of data breach. Or a hacker might decide to hold your data hostage until you pay up. This happens every day to businesses around the world – and hackers are relentless. They will use your own employees against you, if given the chance.

Your best move is to get your team trained up and educated about current threats facing your business. Working with a managed service provider or partnering with an IT services firm is an excellent way to accomplish this and to avoid everything we've talked about in this article. Education is a powerful tool and, when used right, it can protect your business and your employees.

FREE REPORT: The 7 Urgent And Critical Protections Every Small And Medium Sized Business Must Have In Place NOW

You will learn:

- The #1 threat to your business that even the BEST firewalls and anti-virus software can't protect against (and what you need to do NOW to remedy it).
- The biggest security risks with cloud computing and what you need to do to stay safe if you store client data, confidential data and financial information in the cloud.
- A common misconception about business bank fraud that will shock you – and 3 simple things you can do to protect your bank account from unauthorized access and theft.
- How to keep your network secure with the increasing proliferation of mobile devices, cloud applications, email, social media sites and internet-connected devices accessing your computer network.

Claim your FREE copy today at
https://www.connectability.com/7protections/

Shiny New Gadget Of The Month:

Cancel Stress With Cove

Wouldn't it be nice if you could just press a button and your stress would melt away? Well, now it's possible, and it's thanks to Cove. The first of its kind, Cove is a wearable device (like a pair of headphones) designed with "stress cancellation" in mind.

Cove rests on your ears and wraps around the back of your neck. It uses subtle vibrations behind your ears to soothe your stress. Over 90% of those who participated in clinical trials reported a marked decrease in stress, and 91% reported sleeping better.

If you're looking for a new and innovative way to help manage your stress, Cove may be the answer. Due to its compact, lightweight design, it can be used anywhere, anytime. Learn more at **FeelCove.com**.

Stay Safe From SMS Fraud

Hackers are taking phishing schemes to a whole new level. Rather than sending an infected email, or prompting you with a pop-up, hackers are sending phishing texts to your smartphone. And because anyone can send you an SMS, it's very difficult to stop them.

Text messages come in several varieties:
The first are messages you receive from someone in your contact list that you are actively connecting with. For example, a family member or a friend asking you "what time is dinner tonight" or a colleague confirming that they've sent information over to a client.

On the opposite end of the spectrum are text messages that are clearly spam. These messages come from unknown numbers and are generally ripe with spelling errors. They also ask you to take some ridiculous action. For instance, Canada Revenue Agency sends an SMS indicating you have received a refund of $120.52 and to enter your banking information to deposit it. Most people can tell right away that this is a fraudulent message.

Now the *real* issue are the texts that look like they could be legitimate. These messages are usually from businesses and services that you are aware of and might have given permission to message you. They might appear to be from a supplier providing an update on an order, or they might be from your bank indicating that there has been fraud on your account. They're generally ask you to take action: click a link, reply back with some information, etc.

So, how do you know if the message is legitimate? Here are 3 rules you can follow to help identify a fraudulent text message:

1. **Don't Respond to a Call to Action**
   This is a BIG red flag. The message requests you to take some type of action. This could be to click on a link, call or text a number, enter payment details, or simply reply. Regardless of the action, when an unknown number asks you to do something fishy, treat it as a phishing text.

2. **Pay Attention to Odd Behaviour**
   Be wary if the message sounds strange. For instance, if the originator has your name, but greets you with "Hello, friend", or "Dear client" then be cautious about replying. Also, lookout for any grammatical/spelling errors. This could be as simple as the name of your bank with a zero instead of an O (e.g. BM0).

3. **Do Some Research First**
   You might still be wondering if the message is real. What if you don't respond? Will your package be put on hold? Will your bank account be disabled? That's what hackers pray for - doubt. What if the message IS legitimate? Well, do your research first. Call the supplier or your bank directly, check their online portal (if they have one), or look up the number to see if it has a history of spamming. Always verify the SMS through official channels first!

If a cybercriminal gains access to your phone, they can review your messages and emails, get banking information, and stir up a whole lot of trouble. That's why you need to be aware of SMS scams. To protect yourself from phishing texts, turn on the "Block Unknown Sender" feature on your device. This will help filter senders with numbers that are not in your contact list and appear to be fraudulent. You can also utilize an anti-spam service. Finally, any time you get a fraudulent text, you should go into your contacts and block the number. This won't prevent them from spamming you from a different number, but it will prevent recurring spam from that number. Protect yourself now to prevent a breach later!

Tech Connect Video Series:
Beware Of Phishing Attacks!

You probably spend a lot of time emailing clients, vendors, partners and colleagues. It's your main tool to communicate. Unfortunately it's also a hacker's prime target. Hackers use a method call "phishing" to convince you to open malicious links or attachment, send funds to random bank accounts, or provide confidential information about you or your company. Cybercriminals can then get your passwords, install programs on your computer and network, and steal your confidential data.

Cybercriminals are working diligently to get into your computer, infect your backups, and install Ransomware across your network. That's why your business needs to invest in solutions and training that can help your team spot phishing attacks, and prevent them from arriving in your inbox to begin with.

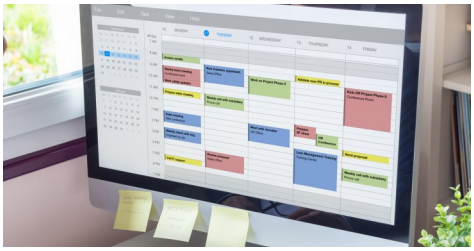
If you would like to learn more about improving your security and preventing your business from becoming a victim of a phishing attack, watch this video NOW! You will learn 3 tips to improve your email security. To find out more, go to **YouTube**, look up **Connectability IT Support** and find the video "**Beware Of Phishing Attacks! 3 Tips To Improve Email Security" OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".**

Eliminate Workplace Distractions To Maximize Your Productivity

While most of us accept that distractions will be a part of our day, if your intention is to get things done and to stay productive and focused, you'll need to minimize those distractions. No, we'll never be able to eliminate them 100%, but we can certainly try. Here's what you can do to cut distractions.

Block Time On Your Calendar (And Stick To It). Use your calendar to its full advantage. Mark time off for emails, for *all* projects, phone calls, Zoom calls, you name it! If it's part of your normal day, put it on your calendar. Even throw on time for miscellaneous stuff. Then share it with all relevant parties and stick to it. If you're working on a project between 1:00 p.m. and 3:00 p.m., that's the word.

Use Sound To Your Advantage. A common source of distraction is sound: it can be office chatter in the background or even neighborhood sounds (for those working from home). Find a sound that complements your workflow. It might be chill music or the sounds of rain or a babbling brook. Find the right sound that helps you zone in and blocks disruptive sounds.
Forbes, March 15, 2021



The 2 Best Investments You Will Ever Make

Practically every successful person has something in common with every other successful person. Millionaires and billionaires share these habits – habits that are absolutely crucial if you want to achieve the success that's on your mind.

1. Read, Read And Read Some More. Warren Buffett and Bill Gates are prime examples of this, but it's one of the most common traits among the most successful businesspeople in the world ... They are constantly reading: books, blogs, newspapers, magazines and anything else that enriches their personal and professional lives.

2. Get Educated. Whether you hire a private coach, take courses (like continuing education) or hire consultants, there are pros who can teach us more about what we do (or want to do) and how to improve ourselves or our businesses. While we may be good at what we do, there is always room for improvement – you just have to be open to it.
Inc., Feb. 24, 2021

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!

Daily Bread Food Bank

This month we'll be making our donation to the **Daily Bread Food Bank**.

Founded in 1983, Daily Bread Food Bank is one of Canada's largest foodbanks. Their vision is to end poverty and food insecurity in our communities. They believe that access to food is a basic human right, not a privilege, and no one should go hungry, or face barriers in accessing food.

Daily Bread Food Bank takes donations, organizes food drives, and of course runs food banks to provide food to anyone who needs it. Their goal for 2021 is deliver 20% more food to 20 priority neighborhoods that are currently underserved. Given the current crisis, we want to help the Daily Bread Food Bank support those with limited access to food.

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