Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: Pontifical Mission Societies

Meet **Pontifical Mission Societies**! They have been part of the Connectability client family since May 2019.

Founded in 1922, the Pontifical Mission Societies have been the official missionary arm of the Church. The four societies include: The Pontifical Society for the Propagation of the Faith, Saint Peter the Apostle, the Holy Childhood, and Pontifical Missionary Union. The main purpose of the four societies is to promote a universal missionary spirit and a spirit of prayer and sacrifice among all baptized Catholics to gather support for the worldwide missions of the Church. They oversee the work of evangelization and charitable works throughout the world. In Canada, they have offices in Toronto and Montreal.

They have offices within 1120 districts in Asia, Africa, Oceanic, Pacific Islands and Latin America. Each provides support to special projects such as building of churches and chapels, the work of Religious communities in health care and education and for communication and transportation needs.

Connectability has been Pontifical Mission Societies technology partner for almost a year. We provide support and security tools to keep their confidential information protected. We monitor their workstations and servers to ensure they are operating smoothly and at peak performance. We take care of their IT needs, so they can focus on promoting the missionary spirit, and growing support for the goals of the church.

If you would like to learn more about Pontifical Mission Societies, please go to: https://www.missionsocieties.ca/

March 2020

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

5 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 of businesses to choose from, and many don't invest in good IT security. Plus, many business owners and their employees have bad cyber security habits. They do things that increase their risk of a malware and cyber-attack. 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 deleting cookies Cookies are digital trackers. They are used to save website settings and to track your behavior. For example, if you click a product, cookies are logged in your browser and shared with ad networks. This allows for targeted advertising. There's no good way to tell who is tracking you online. But you can use more

Continued on pg.2

Continued from pg.1

secure web browsers, like Firefox and Safari. These browsers make it easier to control who is tracking you.

In Firefox, for example, click the three lines in the upper right corner, go into the Options menu and set your Privacy & Security preferences. Plus, every web browser has the option to delete cookies – which you should do constantly. In Chrome, simply click History, then choose "Clear Browsing Data." Done. You can also use ad-blocking extensions, like uBlock Origin, for a safe web-browsing experience.

3. 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.

4. 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.

> **"Good IT security can be the best investment you can make for the future of your business."**

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.

5. You believe it will never happen to you This is the worst mentality to have when it comes to cyber security. It means you aren't prepared for what can happen. Business owners who think hackers won't target them are MORE likely to get hit with a data breach or malware attack. If they think they are in the clear, they are less likely to invest in good security and education for their employees.

The best thing you can do is accept that you are at risk. All small businesses are at risk. But you can lower your risk by investing in good network security, backing up all your data to a secure cloud network, using strong passwords, educating your team about cyberthreats and working with a dedicated IT company. Good IT security can be the best investment you make for the future of your business.

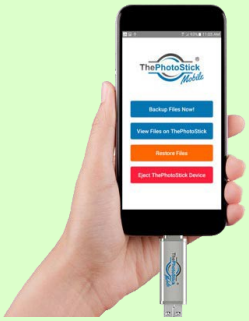
Help Us Celebrate Abarnaa's Anniversary!

Help us congratulate our Marketing Associate & Sales Representative: Abarnaa Arunaruban on her successful first year at Connectability. Abarnaa has played a major role in promoting Connectability across various media platforms and delivering valuable content to our customers.

Her first year has involved a lot of growth for both Connectability and Abarnaa. Here's what she had to say: "Working for Connectability has helped me grow and develop my skill set significantly! I've learned so much about IT, marketing best practices, and cybersecurity. I've had the opportunity to meet and connect with a lot of great people, including my colleagues, and of course our clients! I'm excited for the next step in this journey, and to continue to be a valuable member of the Connectability team."

Abarnaa goes above and beyond to create promotional messages to drive our business. She prepares and promotes engagement and communication programs, including weekly communications, campaigns, newsletters, and webinars. We're very happy to have her on our team!

Shiny New Gadget Of The Month:



ThePhotoStick Mobile

Never worry about running out of memory on your smart phone again! It happens to all of us – you're trying to take a picture or record a video and you get a message saying your phone's storage is full. You don't want to buy another new smart phone, so what can you do besides delete old photos and uninstall apps?

That's where ThePhotoStick Mobile comes in. It's a memory stick compatible with most Android and iPhone devices and will boost your phone's memory without having to buy a new phone. It also acts as an insurance policy against lost photos and videos.

ThePhotoStick Mobile gives you more control. While most smart phones work without a hitch for years, you never know if something might happen or if you'll run out of memory. ThePhotoStick Mobile plugs into your device and allows you to copy photos over. You can keep them on ThePhotoStick or transfer them to another device. To learn more, go to: GetPhotoStickMobile.io!

Why Secure Passwords Need Length!

The truth is, no matter how many times we see a warning about protecting our online identity, we take the easy route. It's like the verification box we're forced to check accepting the terms and conditions when we create a new online account, whether it's for a Facebook or bank account. At most, we skim through the agreement and hope that nothing bad happens. And this mentality applies to *everything*. Unfortunately, that means that most people take the same approach when creating passwords. Creating strong and hard to guess passwords is difficult, so most of us instead opt to keep it simple and hope for the best!

Passwords are an extremely important component of protecting your online identity. They are the first line of defense against unauthorized access to your accounts and confidential information. The more complex your password is, the more difficult it is for hackers to break in.

Traditional password practices include selecting a word and adding numbers, uppercase letters, and special characters. For instance, it could be your cat's name: Chl0e25@. Now, most of us would agree this password is complex, regardless of its length. However, the FBI has chimed in and clarified that longer passwords which include simple words and constructs, are better than short passwords with special characters.

A general rule of thumb is that your password should be at least 15 characters. The issue here is trying to remember multiple 15-character passwords. That's why we recommend using passphrases. Passphrases are a string of words, that make it harder for cyber criminals to crack, while also making it easier for you to remember. A passphrase uses spaces and symbols. It also doesn't have to be a proper sentence or grammatically correct. For example, it could be Chloe Luvs Her Yarn! What you use is entirely up to you but using passphrases can be a good way of locking down your accounts to prevent unauthorized access. In addition, to help remember all your passwords, you should consider using a password management program. There are many inexpensive and free password managers that use the same encryption as major banks.

To keep your business protected, it's important to use long and complex passwords. A password is the first "lock" on the front door of your business. If a hacker cracks this open, they can rummage through your personal information and cause chaos. Don't take the easy way out – use passphrases NOW!

Antivirus Isn't Enough– Stack Your Defenses

The cyberworld isn't safe anymore. It doesn't matter whether you are a billion dollar multi-national or a small mom and pop shop - your business is at risk. Cybercriminals are constantly finding new methods to get into your network and cause chaos. To protect your business, you need to establish and maintain strong cyber defenses.

If your business is not protected, a hacker can remain in your network undetected for days, months, or even years. That's why you need to layer your defenses to stay ahead of threats. No single tool is effective at defending against all kinds of attack. To fully protect your business, you need to include a number of traditional tools such as have a business grade firewall, anti-virus software, and email filtering. But you also need to have an advanced threat detection tool to help identify the hackers entry points into your network.

If you're concerned about cybersecurity, watch this video now. You will learn why your business needs to "stack" its security solutions, and how Threat Detection can help. To access it, go to YouTube, look up Connectability IT Support and find the video **"Why Antivirus Isn't Enough & How To Close Security Holes Hackers Use To Get Into Your Company"** OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

Don't Make This Critical Mistake In Your Business

Upward of 41% of companies don't train their HR staff on data security. This is from a recent survey from GetApp. On top of this, 55% of HR staff don't see internal data security as an issue.

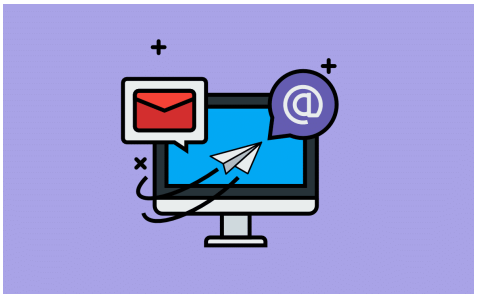
HR departments often handle sensitive data and should take IT security very seriously. If a hacker were to get ahold of employee data, it could be potentially devastating to affected employees and to the company as a whole – and it could set up the company for a major lawsuit on the part of the employees.

The liability by itself isn't worth it and neither is taking on the risk by not investing in data security. Data protection needs to be in place – along with employee training. Everyone, including HR, should be on the same page, and every company should adopt strong data security and policy to go along with it. *Small Business Trends, Nov. 30, 2019*

Follow This One Rule When Sending E-mails

We all use email, and we all spend too much time reading and responding to these messages (one estimate cited by Inc. suggests the average office worker spends 2 1/2 hours per day reading and responding to e-mails).
Wasn't email supposed to save time? It can if you follow one important rule. It's all about streamlining your process. That rule? The CC rule.

It works like this: If you expect a reply from a recipient, you put their name in the "to" field. If you want to add more people to read your message but don't need a reply from them, put them in the "CC" field.



However, for the rule to work, everyone in the email has to know how it works. If the email is addressed "to" you, respond. If not and you're just CC'd, do not respond. *Simple. Inc., Dec. 10, 2019*

FIND THE WORDS!

F	A	Y	R	C	T	T	O	H	A	R	E	H	E
O	N	V	Y	T	H	S	E	M	A	S	H	A	H
O	T	R	T	T	H	R	E	A	T	S	H	H	G
T	I	A	I	T	P	H	I	S	H	I	N	G	R
H	V	N	R	F	T	G	E	A	I	U	U	S	A
O	I	S	U	A	S	S	H	H	H	S	R	T	T
L	R	O	C	Y	S	N	R	A	G	W	W	S	A
D	U	M	E	I	E	B	O	C	L	E	Y	A	D
S	S	W	S	H	R	U	A	K	A	I	Y	S	R
I	H	A	R	A	T	I	I	E	N	I	Y	Y	S
T	L	R	E	S	N	F	U	R	N	U	O	N	H
M	H	E	B	R	U	W	O	S	B	I	T	R	I
C	N	H	Y	R	H	F	I	R	E	W	A	L	L
H	R	A	C	U	I	R	C	T	L	L	E	R	R

THREATS
DATA
RANSOMWARE
FIREWALL
FOOTHOLDS
CYBERSECURITY
PHISHING
HUNTRESS
HACKERS
ANTIVIRUS

YOUTH ASSISTING YOUTH YAY

This month we will be donating to **Youth Assisting Youth**.

For over 40 years, Youth Assisting Youth has been dedicated to supporting the leaders of tomorrow and changing the lives of at risk individuals. Youth Assisting Youth builds mentoring relationship with vulnerable youth and families across the Greater Toronto Area and York Region.

The youth mentorship program are young adult volunteers aged 16-29, who are partnered with youth ages 6-15 to offer a helping hand and encourage a healthy lifestyle.

Since 1976, they have helped over 30,000 kids do better in school, stay out of trouble, and help them become better individuals who give back to their community.

Youth Assisting Youth, doesn't only help mentees. The mentors also go through their own transformations, developing leadership and social skills to become outstanding professionals and community members.

If you want to contribute to Youth Assisting Youth, we would love your help! Email: info@connectability.com or call (647) 492-4406.