Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight:
The Gord Downie & Chanie Wenjack Fund

Meet **The Gord Downie & Chanie Wenjack Fund**, the newest member of the Connectability client family!

The Gord Downie & Chanie Wenjack Fund was inspired by the story of Chanie Wenjack, a young Anishinaabe boy who lost his life trying to escape Canada's residential school system. When Gord Downie of the Tragically Hip learned about Chanie, he urged us all to "Do Something" which became a rallying cry to build a better Canada. Through their Legacy Space and Legacy School partnerships, DWF aims to build cultural understanding and create a path toward reconciliation between Indigenous and non-Indigenous peoples. This month, join them in commemorating Secret Path Week from the 17th to the 22nd! This is a meaningful week as October 17th and 22nd respectively mark the dates that Gord Downie and Chanie Wenjack joined the spirit world, and allows us to honour their legacies. Learn more at SecretPathWeek.ca

Connectability monitors their computer, network and VoIP phone infrastructure to ensure their team is able to work productively with no interruptions. We also ensure that their data is backed up, secured and recoverable in an emergency. Connectability provides phone and onsite support to ensure their technology is running smoothly whether the team is in the office or working from home. We have also implemented a number of security protections to help minimize their risks of cyber threats. As The Gord Downie & Chanie Wenjack Fund's technology partner, we respond proactively to IT issues, minimize the possibility of experiencing downtime, and ensure their team is always protect against the latest cyber threats.

If you would like to learn more about The Gord Downie & Chanie Wenjack Fund, please go to: https://www.downiewenjack.ca/

October 2020

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

Employees Are Letting Hackers Into Your Network ...
What You Can Do To Stop It

Cyberthreats are everywhere these days. Hackers, scammers and cybercriminals are working overtime to break into your network – and the network of just about every business out there. They have a huge arsenal of tools at their disposal, from automated bots to malicious advertising networks, to make it possible.

But there is one "tool" that *you* may be putting directly into their hands: your employees. Specifically, **your employees' lack of IT security training**.

While most of us expect hackers to attack from the outside using malware or brute-force attacks (hacking, in a more traditional sense), the truth is that most hackers love it when they can get others to do their work for them.

In other words, if they can fool your employees into clicking on a link in an email or downloading unapproved software onto a company device, all the hackers have to do is sit back while your employees wreak havoc. The worst part is that your employees may not even realize that their actions are compromising your network. And that's a problem.

Even if you have other forms of network security in place – malware protection, firewalls, secure cloud backup, etc. – it won't be enough if your employees lack good IT security training. In fact, a lack of training is the single biggest threat to your network!

It's time to do something about it. Comprehensive network security training accomplishes several things, including:

1. Identifying Phishing Emails Phishing emails are constantly evolving. It used to be that the average phishing email included a message littered with bad grammar and misspelled words. Plus, it was generally from someone you'd never heard of.

These days, phishing emails are a lot more clever. Hackers can spoof legitimate email addresses and websites and make their emails look like they're coming from a

Continued on pg.2

Continued from pg.1

sender you actually know. They can disguise these emails as messages from your bank or other employees within your business.

You can still identify these fake emails by paying attention to little details that give them away, such as inconsistencies in URLs in the body of the email. Inconsistencies can include odd strings of numbers in the web address or links to YourBank.**net** instead of YourBank.**com**. Good training can help your employees recognize these types of red flags.

2. Avoiding Malware Or Ransomware Attacks One reason why malware attacks work is because an employee clicks a link or downloads a program they shouldn't. They might think they're about to download a useful new program to their company computer, but the reality is very different.

Malware comes from many different sources. It can come from phishing emails, but it also comes from malicious ads on the Internet or by connecting an infected device to your network. For example, an employee might be using their USB thumb drive from home to transfer files (don't let this happen!), and that thumb drive happens to be carrying a virus. The next thing you know, it's on your network and spreading.

This is why endpoint protection across the board is so important. Every device on your network should be firewalled and have updated malware and ransomware protection in place. If you have remote employees, they should only use verified and protected devices to connect to your network. (They should also be using a VPN, or virtual private network, for even more security.) But more importantly, your employees should be trained on this security. They should understand why it's in place and why they should only connect to your network using secured devices.

"Every device on your network should be firewalled and have updated malware and ransomware protection in place."

3. Updating Poor Or Outdated Passwords If you want to make a hacker's job easier than ever, all you have to do is never change your password. Or use a weak password, like "QWERTY" or "PASSWORD." Even in enterprise, people still use bad passwords that never get changed. Don't let this be you!

A good IT security training program stresses the importance of updating passwords regularly. Even better, it shows employees the best practices in updating the passwords and in choosing secure passwords that will offer an extra layer of protection between your business and the outside world.

If you or your employees haven't updated their passwords recently, a good rule of thumb is to consider all current passwords compromised. When hackers attack your network, two of the big things they look for are usernames and passwords. It doesn't matter what they're for – hackers just want this information. Why? Because most people do not change their passwords regularly, and because many people are in the habit of reusing passwords for multiple applications, hackers will try to use these passwords in other places, including bank accounts.

Don't let your employees become your biggest liability. These are just a few examples of how comprehensive IT and network security training can give your employees the knowledge and resources they need to help protect themselves and your business. **Just remember, you do not have to do this by yourself! Good IT training programs are hard to find, and we are here to help.**

Welcome The Newest Member Of The Connectability Team!

Connectability is growing! So, to better meet the needs of our clients, we continue to develop our team. Please welcome Chris Barnes! Chris is our newest Network Engineer. His role at Connectability is to troubleshoot and resolve your IT issues, proactively monitor your network, and help improve your productivity by leveraging technology.

Chris is a graduate of Humber College and specialized in micro computer management and technical support. Chris enjoys the challenges that digging into computer problems provides and gets a great deal of satisfaction from fixing a complex issue. With over 16 years of technical support experience, Chris is ready to solve your IT problems, get you back to work, and help you and your team get the most of our your technology!

Shiny New Gadget Of The Month:

Ovo Portable Steam Iron And Garment Steamer

The **Ovo Portable Steam Iron And Garment Steamer** is much smaller than your average iron, yet capable of so much more. It's an iron *and* a steamer—the perfect companion for when you're travelling and want to look sharp. Or keep the Ovo at home to save space!

The Ovo fits easily in your hand. It's lightweight and won't take up much space in your luggage. Plus, it holds enough water to create up to 10 minutes of steam. You can quickly switch from the metal ironing plate to the brush attachment to add finishing touches to delicate fabrics (and remove any lint or pet hair). It even comes with a heat-resistant travel case. Learn more about this mini-marvel at https://bit.ly/2FwBSE8!

Stay Safe From Text Message 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 now 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 a few 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 asking you 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 incoming text message:

1. Contains a clear 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, consider it as a phishing text.

2. Pay Attention to Odd Behaviour

Be wary if the message sounds strange. For instance, if the originator of the message 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 for you. That's why you need to be aware of SMS scams. To protect yourself from phishing texts, you should 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:
3 Ways To Protect Your Mobile Devices

Everyone lives on their mobile phones. It's the first thing you check in the morning and the last thing you put down before bed. Most businesses today use mobile devices to some degree or another. Any why wouldn't you? Mobile devices have become like minicomputers for your employees. They can use their phone to access emails, company data, financial documents, join meetings, and so on.

Businesses embrace mobile technology to improve collaboration, communication, and ultimately, productivity, but these advancements come with a cost: Your Security. If you or your employees use mobile devices to access confidential company data, then it's important that you consider the security implications, and have a process in place for securing your data and ensuring it doesn't fall into the wrong hands.

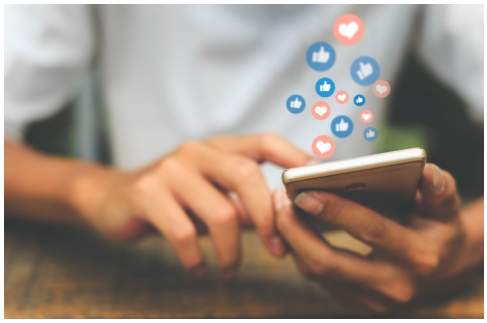
Watch this video to learn 3 tips you can use to secure your team's mobile devices against cyber threats. To find out more, goto YouTube, look up Connectability IT Support and find the video "3 Ways To Protect Your Mobile Devices" OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

Do These Things To Protect Your Business From Getting Hacked

1. Train Employees. Your team needs to know how to identify and handle today's IT security threats. Cybercriminals often rely on your employees' lack of training to break into your network. Ongoing training gives employees tools and resources to overcome this and many other IT security challenges. Make training a top priority!

2. Hold Employees (And Yourself) Accountable. Training and company guidelines don't mean much without accountability. When you set rules, follow them, just as you follow industry and government rules and regulations when operating your business. Be willing to hold anyone who does not accountable.

3. Have A Disaster Recovery Plan. Things happen. When you store sensitive data, you need to have a plan in place to recover and restore that data should anything happen. This doesn't just include data loss from malicious attacks but other types of disasters, including hardware failure, fire and flood. How is your data being backed up and saved? Who do you notify in the event of a breach? Who do your employees call in the event of disaster? *SmallBiz Technology, Dec. 26, 2019*



4 Tips To Get Projects Done On Time With A Small Team

1. Give Them The Tools And Resources They Need
We all need tools to get things done – project management software, content creation tools, messaging apps, virtual private network access and more. Have a conversation about what each team member needs to maximize productivity and work closely with them to meet that need.

2. Set Aside Time For Proper Research
Don't jump headfirst into a project without jumping into research first. Information is a powerful tool to get things done efficiently and effectively.

3. Assign Accordingly
Before the team goes to work, make sure assignments or responsibilities are delegated properly and check in with everyone on a regular basis to make sure things are going smoothly (or to see if they need help).

4. Plan And Plan Again
Plan out the project before you set to work. Give yourself and your team a map to follow as you work through the project. As with any project, expect obstacles along the way and be willing to update your map accordingly. *Small Business Trends, July 4, 2020*

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 HACKERS CYBERSECURITY
DATA ANTIVIRUS PHISHING
RANSOMWARE FIREWALL HUNTRESS
FOOTHOLDS

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 2020 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 we'd love to hear from you! Email us at: info@connectability.com or call (647) 492-4406 today!