Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: Noventa Energy Partners

Meet Noventa Energy Partners, the newest member of the Connectability client family!

Noventa is a provider of fully engineered technology solutions and developer of renewable energy projects that significantly reduce carbon emissions and manage energy costs. They have over 60 years of collective energy industry experience and continue to develop a diversified portfolio of projects in cities across Canada and the US.

Connectability monitors and manages Noventa's computers, network and cybersecurity protections to ensure that their infrastructure is stable, their team remains productive, and that they are secured against any cyber threats or vulnerabilities. And if they require assistance, we provide unlimited onsite and remote support services. That's how we ensure our clients stay as effective and efficient as possible.

If you would like to learn more about Noventa Energy Partners, please go to: https://www.noventaenergy.com/

May 2021

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

How To Make Cyber Security An Ingrained Part Of Your Company Culture

Your employees are your first line of defence when it comes to protecting your business from cyberthreats. Human error is one of the single biggest culprits behind cyber-attacks. It comes down to someone falling for a phishing scam, clicking an unknown link or downloading a file without realizing that it's malicious.

Because your team is so critical to protecting your business from cyberthreats, it's just as critical to keep your team informed and on top of today's dangers. One way to do that is to weave cyber security into your existing company culture.

How Do You Do That?

For many employees, cyber security is rarely an engaging topic. In truth, it can be dry at times, especially for people outside of the cyber security industry, but it can boil down to presentation. That isn't to say you need to make cyber security "fun," but make it interesting or engaging. It should be accessible and a normal part of the workday.

Bring It Home For Your Team. One of the reasons why people are often disconnected from topics related to cyber security is simply because they don't have first-hand experience with it. This is also one reason why many small businesses don't invest in cyber security in the first place – it hasn't happened to them, so they don't think it will. Following that logic, why invest in it at all?

The thing is that **it will eventually happen**. It's never a question of if, but **when**. Cyberthreats are more common than ever. Of course, this also means it's easier to find examples you can share with your team. Many major companies have been attacked. Millions of people have had their personal data stolen. Look for examples that employees can relate to, names they are familiar with, and discuss the damage that's been done.

Continued on pg.2

Continued from pg.1

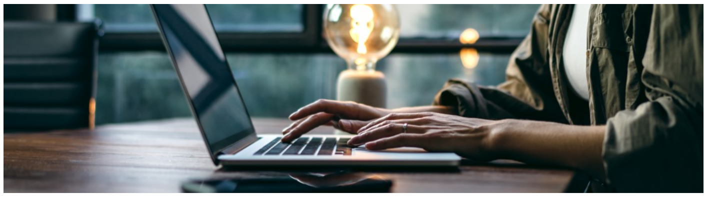
If possible, bring in personal examples. Maybe you or someone you know has been the victim of a cyber-attack, such as ransomware or a data breach. The closer you can bring it home to your employees, the more they can relate, which means they're listening.

Collaborate With Your Employees. Ask what your team needs from you in terms of cyber security. Maybe they have zero knowledge about data security and they could benefit from training. Or maybe they need access to better tools and resources. Make it a regular conversation with employees and respond to their concerns.

Part of that can include transparency with employees. If Julie in accounting received a phishing email, talk about it. Bring it up in the next weekly huddle or all-company meeting. Talk about what was in the email and point out its identifying features. Do this every time phishing emails reach your employees.

Or, maybe Jared received a mysterious email and made the mistake of clicking the link within that email. Talk about that with everyone, as well. It's not about calling out Jared. It's about having a conversation and not placing blame. The focus should be on educating and filling in the gaps. Keep the conversation going and make it a normal part of your company's routine. The more you talk about it and the more open you are, the more it becomes a part of the company culture.

> **"For the day-to-day activities, creating a positive, educational, collaborative environment is the best way to make cyber security a normal part of your company culture."**



Keep Things Positive. Coming from that last point, you want employees to feel safe in bringing their concerns to their supervisors or managers. While there are many cyberthreats that can do serious damage to your business (and this should be stressed to employees), you want to create an environment where employees are willing to ask for help and are encouraged to learn more about these issues.

Basically, employees should know they won't get into trouble if something happens. Now, if an employee is blatantly not following your company's IT rules, that's a different matter. But for the day-to-day activities, creating a positive, educational, collaborative environment is the best way to make cyber security a normal part of your company culture.

Plus, taking this approach builds trust, and when you and your team have that trust, it becomes easier to tackle issues of data and network security – and to have necessary conversations.

Need help creating a cyber security company culture that's positive? Don't hesitate to reach out to your managed services provider or IT partner! They can help you lay the foundation for educating your team and ensure that everyone is on the same page when it comes to today's constant cyberthreats.

Cover Your Webcam!

Here's a disturbing, but very real, tactic for hackers: spying on you via your device's camera. Some simply watch you for fun. Others attempt to catch incriminating photos and then blackmail you by threatening to release the photos or video (which they have) to all your Facebook friends, LinkedIn connections or email address book (which they also have) unless you pay a ransom. If you pay, they can come back and ask for MORE because they now know you care AND that you'll pay. If you don't pay, they will release that picture of you doing, um, well…

As always, follow the various security strategies we send you via our weekly Security Tip emails. As a backup, you can buy stickers that cover your camera with a slider so you can uncover it when you want to actually use it to take a picture or join a web meeting. These are really inexpensive and can be found on Amazon for under $10. Search for "webcam cover slider."

Shiny New Gadget Of The Month:

The Pocket Translator: MUAMA ENENCE

It used to be science fiction, but not anymore! Now, you can translate languages on the go! The Muama Enence is the device that makes it possible. This hand-held "listener" is capable of real-time translation of over 36 common languages from around the globe. Smaller than a smart phone, the Muama Enence breaks language barriers and makes travel easier than ever before, whether you're travelling for business or for vacation.

The Muama Enence is super-easy to use and ultra-portable. All you need to do is press a button, and it does the rest. Plus, with excellent audio quality, you'll be able to hear the translation, even when things get busy around you. Learn more – and get your own – at **bit.ly/37hhn8R**.

3 Ways Systems Can Be Breached

When it comes to business IT security, many small- and medium-sized businesses struggle to protect their systems from cyberattacks. But, like many things, the first step is awareness. Here are three common ways your systems can be breached.

1. You are tricked into installing malicious software

There are countless ways you can be tricked into downloading and installing malware. One is by downloading software from torrent websites. When you visit these sites, you are told to download software in order for the site to load properly. Once downloaded, the malware that came with the software infects your system. In other cases, hackers send emails with a malware-infected attachment.

Luckily, there are steps you can take to avoid accidentally installing malware:

- **Never download files from an untrusted source**. If a website is asking you to download something, make sure it's reputable and reliable. Double check the URL of the website as well, as hackers can spoof legitimate websites and use similar but slightly altered URLs, such as "www.g00gle.com" instead of "www.google.com." If you are unsure, it's best to avoid downloading and installing the software.

- **Always look at the name of the file before downloading**. A lot of malware is often deliberately given names similar to those of legitimate files, with only a slight spelling mistake or some unusual wording. If you are unsure about the file, don't download it. If you know the sender, you may contact them to verify the file's authenticity.

- **Always scan a file before installing it**. Use your antivirus scanner to check downloaded files before opening them.

- **Stay away from sites with torrents, adult content, or those that stream pirated videos**. These sites often contain malware, so avoid them altogether.

2. Someone physically accesses your computer

Your system can also get infected with malware or your data can get stolen because someone physically accessed your systems.

Let's say you leave your computer unlocked when you go out for lunch. Someone can just walk up to it and plug in a malware-infected USB drive, which can infect your system. They can also manually reset the password, thereby locking you out.

An easy way to defend against this is to secure your computer with a password. You should also lock, turn off, or log off of your computer whenever you step away from it. You can also disable drives like CD/DVD and connections like USB if you don't use them. Doing so will limit the chances of anyone using these removable media to infect your computer or steal data from it.

3. Your password is compromised

Passwords are typically the main verification method businesses use to access their accounts and systems. The issue with this is that many people have weak passwords that are easy to crack. To make matters worse, many people even use the same password for multiple accounts, which could lead to a massive breach.

It is therefore important to use strong and different passwords for your accounts. It's best to also utilize multifactor authentication, which requires users to present more than one way to verify their identity such as a password plus a fingerprint or a one-time code.

If you want to learn more about securing your systems, contact us today.

Tech Connect Video Series
Is Your Cloud Data REALLY Backed Up?

The cloud has grown tremendously since its inception, and more and more businesses are using it to store their data. This includes documents stored in Google Docs, emails that you send and receive through Gmail or O365, files you share on Dropbox, and pictures you post on Facebook and Instagram.

Your data is vital to everything you do. Without it, your business wouldn't exist. That's why its so important to backup your cloud data. If your staff accidentally deletes a file, or you get hit with Ransomware, or your data gets corrupted, you need to be able to recover it quickly. Without an effective backup solution, it may take weeks or even months before you get it back, or it might be deleted permanently.

If you're concerned about your data security, watch this video now! You will learn why you need to backup your cloud data, and how you can implement an effective backup solution for your business. To find out more, go to YouTube, look up **Connectability IT Support** and find the video **"Is Your Cloud Data REALLY Backed Up? Find Out How You Can Protect and Secure Your Confidential Information"** OR go to our website at **www.connectability.com**, hover over **"Resources & Videos"** and select **"Videos".**

How To Know It's Time To Start Scaling Your Business

Creating a business that is scalable isn't easy, but it's necessary if you intend to grow – and grow some more. There are three simple ways to tell if you've created a business that is scalable.

You Have Positive Cash Flow Figured Out. You've successfully built a reliable month-to-month revenue stream. It's money that you can use to invest further into your business – whether it's to pay for additional employees, technology, systems and processes or all of the above.

Everything Has Been Delegated. Delegating is hard for many entrepreneurs. You want to have a hand in everything. But when your team keeps everything running – and everything runs even when you're not there – you're in a great place to scale up.

You Have More Control Over The People You Get To Work With. Basically, you can start to shape your client base. If there is someone you want to say no to (say you don't have the full resources to fulfill their needs or they're just not a great fit), you can move on guilt-free.

If you have these three things in place, you have the foundation to scale up safely and to create the business you've always wanted. *Forbes, Feb. 11, 2021*

How To Build A Forward-Thinking Customer Culture In Your Small Business

How well do you know your customers and clients? If you want to deliver a stellar customer experience and have a forward-thinking customer culture within your organization, you need to know your customers. What makes them tick? What do they love? Why do they make the decisions they make?

More than that, you need to go after the customers who make the most sense to your business. As you grow, you have more opportunity to be picky, so be picky! Develop the customer base you really want. That makes it easier to market to them, because you're all on the same page.

Finally, when you know who you want to target, stay consistent in your messaging. The entire customer experience – from online marketing to your storefront – should all be uniform. Consistency helps build your brand and anchors customers to the overall experience. *Forbes, Feb. 15, 2021*

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!

Google's first tweet on Twitter was a message encoded in binary that read what?

a. Don't be evil
b. I'm feeling lucky
c. Do the right thing
d. Is this thing on?

Call us right now with your answer!
(647) 492-4406

Food Banks Canada Banques alimentaires Canada

This month we'll be making our donation to **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!