Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: USW Local 1998

Meet the **United Steelworkers Local 1998**! They have been a part of the Connectability family since January 2016.

Founded in 1998, United Steelworkers Local 1998 (USW 1998) is a union that represents clerical and technical staff at the University of Toronto. USW Local 1998, has brought creativity and enthusiasm to the union and infused Toronto Steelworkers with spirit and diversity.

It all started with about 120 volunteers who were employees of U of T. They began with the goal of gaining a place at the table, rather than having unilateral decisions imposed on them. Now, two decades later, the Union has made significant improvements in working conditions and wages and has grown to be the largest Steelworker Local in Canada. It also has one of the most proactive Steelworker Area Councils, who are always leading the way in the broader labour movement.

Connectability has been USW Local 1998's technology partner for almost 4 years. We monitor their network and computers to guarantee their network and data are safe, and we provide regular remote and onsite support. We are also proactive – so we can predict when issues might occur to prevent downtime, lost productivity and employee frustration.

If you would like to learn more about United Steelworkers Local 1998, please go to: **http://www.usw1998.ca/**

October 2019

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

3 Ways To Prevent Your Employees From Leaking Confidential Information

A lot of businesses need to come to terms with the fact that their employees are their greatest IT threat. As a business owner, you may be aware of cyberthreats to your business, but your employees might not be. They might not know about the threat of cyber-attacks or malware. They might use unsecured WiFi on company equipment. As a result, your employees may be putting your business at serious risk.

What can you do to change that?

1. IT ALL STARTS WITH EDUCATION. One of the biggest reasons why employees put their employer at risk simply comes down to a lack of education. They don't know about the threats targeting businesses or that small businesses are a major target to hackers and scammers.

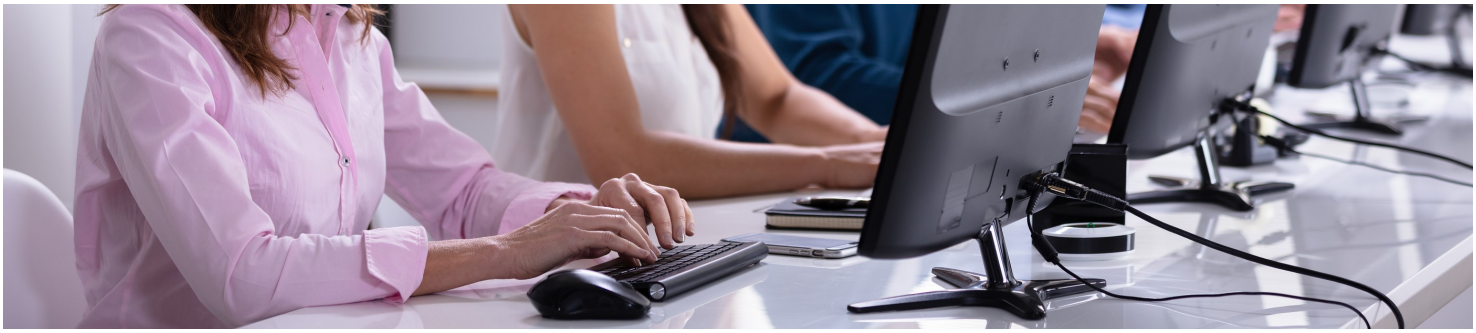
You need to do everything you can to train your employees. Give them the education and resources to be a line of defense rather than a risk. Develop a consistent training regimen. If you need to bring in IT professionals to help, do it. Don't make assumptions about critical IT security training if you aren't sure. Professionals can answer your questions and make sure you and your employees have everything you need to know to keep your business secure.

Another important thing is to ***hold this training regularly.*** Threats evolve, and you need to stay ahead of the curve. Keep IT security on the minds of your employees. When they forget about it, that's when the risk is highest.

2. SAY NO TO UNSECURED, PUBLIC WIFI. This is a big problem for businesses with remote employees, employees who work from home or

Continued on pg.2

Continued from pg.1



employees who use company technology outside of the business walls. According to a Spiceworks study, 61% of employees said they have connected to unsecured WiFi while working remotely.

This is cause for concern. Connecting to public WiFi is like leaving the front door of your home wide-open while posting on social media that you're going to be out of town for a week. You never know who is going to let themselves in and snoop around. Hackers use public hot spots to circulate malware and steal data. Sometimes they even set up fake hot spots with the same name as a legitimate hot spot to trick users into connecting to their WiFi, which makes data theft *even easier.*

Discouraging your employees from using unsecured, public WiFi is a good step to take, but don't be afraid to take it further. Don't let them connect company equipment to unsecured WiFi *at all.* And place a bigger focus on endpoint security – make sure your equipment has up-to-date software, malware protection, local firewalls, as well as a VPN (virtual private network). The more layers of security, the better.

3. PROTECT ALL OF YOUR DATA. Your employees should never save personal or business data on portable/external hard drives, USB drives or even as printed material – and then take that data out of the office. The theft of these types of devices is a real threat. An external hard drive is a tempting target for thieves because they *will* search the drive for sensitive data, such as financial or customer information that they can use or sell.

If you have remote employees who need to access company data, put a method in place to do just that (it should be discussed as part of your regular company IT security training). They need to know how to properly access the data, save the data or delete it, if necessary. Many businesses go with a secure cloud option, but you need to determine what makes the most sense for your business and its security.

While these three tips are great, nothing beats helping your employees develop a positive IT security mindset. It's all about understanding the threats and taking a proactive approach to security. Proactivity reduces risk. But you don't have to go it alone. Working with experienced IT security professionals is the best way to cover all your bases – and to ensure your employees have everything they need to protect your business.

> **"It's all about understanding the threats and taking a proactive approach to security."**

Help Welcome Our Newest Member! Emmanuel Thom-manuel

Connectability has grown tremendously in the past few years! So, to better meet the needs of our clients, we continue to grow our team. Please welcome Emmanuel Thom-Manuel to Connectability! Emmanuel is our newest Technical Specialist. His role at Connectability is to troubleshoot and resolve your IT issues, proactively monitor your network, and help improve your productivity by leveraging technology.

Emmanuel has a degree in Computer Network Technologies from Northumbria University in Newcastle, England, and industry certifications from Cisco and Microsoft. With over 8 years of technical support experience, Emmanuel is ready to solve your IT problems, and to help educate you about your technology. Call our office and speak to Emmanuel today for any IT needs!

Shiny New Gadget Of The Month:

The Philips Somneo Sleep & Wake-Up Light

Research suggests that when you wake up naturally (that is, you aren't jolted awake by an alarm or radio), you feel more refreshed and energized during the day.

The Philips Somneo Sleep & Wake-Up Light puts this research to the test. It's designed to simulate a natural sunrise right in your bedroom. You can set it to your specific needs, and it will slowly and steadily brighten when you need to wake up. It can also simulate a sunset for the opposite effect when you're going to bed! You can even use the light as a reading lamp — and it has a built-in radio, too!

The Philips Somneo Sleep & Wake-Up Light is a versatile device, perfect for anyone who wants to get a better night's sleep. Find it at Amazon and many other electronic retailers.

See You Never, Windows 7

On January 14, 2020, we officially bid farewell to Windows 7 and Server 2008. Microsoft announced early in 2018 that they will no longer update or support them after the deadline passes. That means Windows 7 machines will stop receiving security updates and feature enhancements. That doesn't mean that your computer will stop working though. You will still be able to boot up your machine, use your email, access Microsoft Office apps, and browse the web, but you *will* be susceptible to cyber threats.

Hackers work tirelessly to find windows to break into your network – and in this case the "window" is Microsoft (pun intended) announcing that they are discontinuing support for Windows 7 and Server 2008. Traditionally, hackers find a vulnerability and design malware or a virus to exploit it. Once Microsoft or Apple find out, they develop a fix, and release a security update. Unfortunately, since Microsoft is no longer offering support, you're out of luck. If a hacker finds a vulnerability and exploits it, your computer could be infected, and your data could be stolen.

To keep your computer and data private and protected, here's what you should do to prepare. Work with your IT provider to create a plan for your computers. You can either upgrade or replace them – depending on age. If the machine is older than 2.5 years we recommend replacing it. Given the time it takes to perform these updates, it's not worth it for a machine that has less than 2 years of operation left. Plus, some older computers don't have enough performance to support Windows 10. If your computer is less than 2 years old, we recommend that you upgrade the software and replace your machine later.

January 2020 is around the corner, so don't wait until the last minute. When the time comes, its possible that certain software's won't be compatible with Win 7. Programs that you use on a day-to-day basis may suddenly stop working. This will be very disruptive for you, and could have a negative effect on downtime and productivity.

If you value your business, this isn't a choice. With each passing day it becomes even more critical for you to upgrade. If you wait, your IT provider might not be able to help you before the year ends. You will be at the back of a long line, and if you pass January 14 without a solution, you will regret it.

If you would like us to help create a plan for your business, call us at **(647) 492-4406** or email info@connectability.com, and we would be happy to assist!

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 survive. 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 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 about 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".**

These Are The Biggest Privacy Threats You Face Online Today

Webcam Access – While it's rare, there are known exploits that allow others to access your webcam (such as malicious software or software security flaws). Putting electrical tape over your webcam isn't a bad idea, but more webcams are coming with kill switches and shutters for peace of mind.

Phishing Scams – Don't ever expect these to go away. People still fall for them. NEVER click links in e-mails from anyone you don't know (and even if you do know them, verify that they sent you a link — e-mail addresses can be spoofed).

Web Browser Plug-ins – Vet every browser plug-in and extension you install. Many extensions collect your browsing history and sell it. Read the terms of service before you click install (a good rule of thumb for software in general).

Ad Tracking – Web ads (and web ad providers, such as Facebook and Google) are notorious for tracking users. They want to know what you like so they can cater ads directly to you in the hopes that you'll click the ad, which gives them ad revenue. It's one of the many reasons why people use ad blockers.

Device Tracking – If you have a smartphone, chances are it's being used to track your every move. Again, it comes back to delivering ads that are relevant to you so you'll click on them. For companies like Facebook and Google, users are the product. *Inc., 7/19/2019*

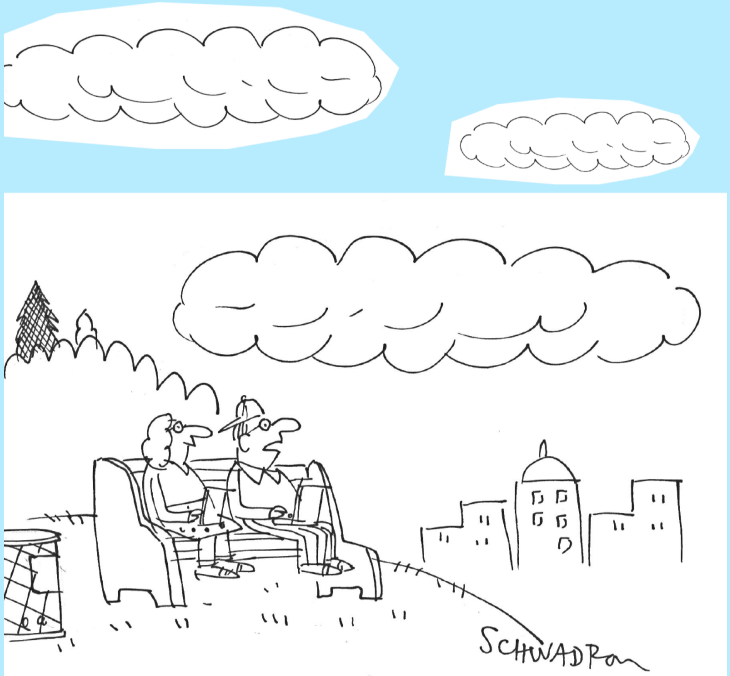
Capitalize On This Strategy To Improve Your Bottom Line

Want to boost your bottom line? The answer may be in cashless payments. It's all about taking your current systems and updating them to current trends.

Outside of the U.S., particularly in Europe and much of Asia, cashless payments are king. More people are relying on smartphones as payment processing tools (both in the consumer and business worlds). Of course, you don't want to rely on cashless — you want to be able to accept any money your customers are spending, whether it's cash, card or electronic.

Look at your point-of-sale system — is it ready for cashless? If not, look into it, research your options, ask around and see what option makes sense for your business (and bottom line). *Small Business Trends, 6/26/2019*

"Okay, everything is stored in the cloud– BUT, what happens if it's a sunny day?"



Children's Wish Rêves d'enfants | Make-A-Wish FAIS UN VŒU CANADA

This month we will be donating to the **Children's Wish Foundation of Canada.**

Founded in 1985, Children's Wish Foundation is a charity committed to granting wishes to Canadian children who are diagnosed with a life-threatening illness. Children's Wish Foundation of Canada is the largest and only all-Canadian charity and has granted more than 25,000 children and their families with their wishes.

There are offices and staff in every province, and every family has a dedicated Wish Coordinator, who can accomplish the wish to meet the needs of the child and their family. The Children's Wish Foundation enhances the quality of life for children between the ages 3-17, and their families, by making their heartfelt wish come true and creating hope and happiness.

If you want to contribute to the Children's Wish Foundation of Canada, we would love your help! Email: **info@connectability.com** or call **(647) 492-4406**.