Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Client Spotlight: Express Gold Refining

Meet Express Gold Refining Ltd. They have been part of the Connectability family since January 2018!

Express Gold Refining is a fourth-generation family business with roots going back all the way to 1915 in the middle east. Since 1994, Express Gold Refining has been servicing the precious metals industry from downtown Toronto.

Express Gold Refining is your one stop – honest, reliable and quick - precious metals dealer and refiner. They partner with Jewellers, manufactures, wholesalers, pawnshops, refiners, precious metals dealers and dental labs in Ontario and across North America. EGR provides the fastest service available in the industry. They use the latest technologies to analyze and determine the quality of your metal. To be productive and efficient EGR uses industry best practices to handle your metals.

EGR has professionally trained staff that have over 100 years of combined experience. This allows them to handle different materials and answer any of your questions.

Connectability has been Express Gold Refining's technology partner for almost two years. We monitor their computers and server infrastructure, and maintain and secure their network to ensure that their business is protected. We also provide backup and security services. We proactively monitor their environment for IT issues, in order to reduce downtime and help their business operations run smoothly.

If you would like to learn more about Express Gold Refining, please go to: https://www.xau.ca/

December 2019

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

Cybercriminals Are Taking Aim At Your Business … Is Your Network Protected?

Cybercriminals love to test your defenses. They love to see how far they can get into the networks of businesses all over the globe. Cybercriminals really love going after small businesses because they can all too often sneak onto a network, copy data and move on. Through the use of ransomware, they can hold your data hostage and refuse to cooperate until you pay them some amount of dollars – and if you don't pay up, they threaten to delete all your data.

But protecting yourself is not as hard as you might think. While cybercriminals and hackers are an everyday threat to businesses, you can take steps to significantly reduce that threat and take the target off your back.

The first thing you need to do is understand why cybercriminals target small businesses and what makes your particular business vulnerable. There are many things small businesses do and don't do that open them to attack and data theft. These may include not having enough (or any) security in place or not training employees on security protocols.

Realistically speaking, the biggest threat to your business does, in fact, come from your own employees. This doesn't mean they are intentionally harming your business or leaving your network exposed to outside threats. It means they don't have the proper training and knowledge to protect your business from a cyberthreat.

For instance, your team needs to be trained to use strong passwords, and those passwords *must* be changed periodically (every three months is a good rule of thumb). A lot of people push back on strong, complicated passwords or use the same password for everything, but this is just asking for trouble and should not be allowed at your company.

Once strong passwords are in place, enable two-factor authentication (2FA) on everything you possibly can, from network access to every account you and your employees use. This is an additional layer of security on top of standard password protection. This feature is generally tied to a mobile number or secondary e-mail, or it

Continued on pg.2

Continued from pg.1

may be in the form of a PIN. For example, when 2FA is enabled, after you've put in your password, you will be prompted for your PIN for the associated account.

Another thing you must do to get that target off your back is to get anti-virus software installed. Every workstation or device should have some form of this protection. Not sure what to use? This is when working with a dedicated IT company can come in handy. They can help you get the right software that will meet your specific needs without slowing you down. They will install software that is compatible with your PCs and other networked equipment. Plus, they will make sure anti-virus software is working and is regularly updated.

> **"You can take steps to significantly reduce that threat and take that target off your back."**

On top of this, you want to have an active firewall in place. Every business should have its network protected by a firewall; like anti-virus software, firewall security comes with a number of different settings, and you can customize it to fit the needs of your network. Firewalls help keep attackers and malicious software off your network. When paired with a good anti-malware software, your layers of security are multiplied. The more layers, the better protected you are.

Finally, with all of this in place, your employees need to know what it all means. Keep your team up-to-date on your business's security protocols. This includes items like your password policy, virus/malware protection policy and proper e-mail and web-surfing etiquette. The bad guys are never going to stop attacking, but you have the power to protect your business from those attacks.

Shiny New Gadget Of The Month:

HD Mask Surveillance Camera USB Spy Cam

Sometimes, you don't want security cameras in plain sight or you don't even want to go to the trouble of installing cameras. Meet the HD Mask Surveillance Camera USB Spy Cam. This device makes video monitoring easier than ever.

The HD Mask is a tiny camera disguised as a USB charger. At a glance, you would have no idea it was a camera. Even better, it actually works as a USB phone charger, which really sells the disguise. It records as soon as it's activated with motion and has many practical purposes, from keeping an eye on pets to monitoring certain areas of your office for security purposes. You can access the footage right on your smartphone and watch in real time. Learn more at HDMask.com.

The Clock Is Ticking—End Of Windows 7 Is Near!

Pull up a chair and read this carefully!

Microsoft is discontinuing support for Windows 7 and Server 2008 as of January 14th, 2020, leaving your business susceptible to serious security threats. After January 14th, any systems running Windows 7 or Server 2008 will no longer receive support, security updates, or feature enhancements – leaving you and your business vulnerable.

Your computers won't stop working on January 14th. BUT your business will be more exposed to security threats. That's why it's so important for you act immediately and put a plan in place ASAP.

So, here's what you can do now:

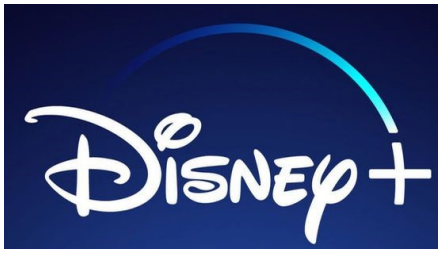
Assess the age of your equipment. If the machine is older than 2.5 years, we recommend replacing it. The software upgrade alone is $160, never mind the time it takes to upgrade the machine. That's why computers of this vintage are generally not worth upgrading. Instead, we recommend replacing them. If your computer is under 2 years old you can simply upgrade it.

Don't wait until it's too late – your security depends on it. 2020 is right around the corner. So, if you don't have a plan in place for your business, call us at (647) 492-4406 or email info@connectability.com and we would be happy to help.

Disney+ Accounts Are Already Being Hacked. Your Business Is Next!

Security used to be simple. 10-15 years ago, if you had antivirus software, a firewall, and some physical security measures like an alarm system or camera, you were safe. But since then things have changed dramatically. You can't go one week without seeing another news article about the latest high-profile cyber attack. Hackers are working tirelessly to get into your systems, steal your data, and make you pay. Here's a little story that will some shed light on how hard cybercriminals are working to steal your data, and why cybersecurity is so important for your business.

If you haven't already heard, on November 12th Disney released a subscription video on-demand streaming service called **Disney+.** If you're a die-hard Disney, Marvel, Pixar, or Star Wars fan, you probably didn't waste much time subscribing to the service. Since it first launched 4 weeks ago there are already millions of customers. Unfortunately, cyber criminals didn't waste much time either. Disney+ user accounts were being hacked *hours* after the service launched.



Almost immediately, some users began to complain that they were not able to stream their movies and shows. But, that's not all! Many subscribers reported that their accounts were hacked, and they were being logged out on all their devices. They received emails notifying them that their account information had been altered, and when they researched further, users realized that their passwords and emails had been changed. The owner of the account was locked out for good.

What's shocking is the speed at which cybercriminals hijacked and monetized the accounts. Breached credentials were put up for sale on hacking forums. Accounts were on sale from around $3 to $11 (which by the way, is higher than the original cost for the service, which is $7). The forums also had ads that offered Disney+ account credentials to be shared amongst the hacker community for free. The original owners of the accounts were contacted, and they confirmed that the credentials were theirs and still active.

So, how did this happen?!

One of the common mistake's individuals make is reusing the same passwords across accounts. If you are guilty of this, then it's time to start creating unique passwords. Once a hacker finds out your go-to password, they can easily hack into all your accounts. BUT, that's not the only way hackers breaking into your Disney+ accounts. There is the possibility that hackers gained access to accounts through machines infected with keyloggers or malware.

Now for the scary part: cybercriminals can *easily* obtain access to your business through your Disney+ accounts. By identifying your email and passwords, they can repeat the same passwords, or variations of them, and gain access to your computer, your network, or even your bank account. And if you were infected by malware or a keylogger, you have a bigger problem! Hackers can damage your devices, steal your data, and even encrypt your computer in exchange for a "ransom". If you are breached, your confidential data could be held hostage until you pay the ransom. Here's what you should do to protect your accounts:

1) Implement multi-factor authentication (MFA) on *all* your accounts. This will help prevent attacks that occur from people reusing the same passwords. 2) Ensure you have an **anti-virus tool** and a dark web monitoring solution. **Dark web monitoring** acts as an early warning signal that your credentials have been compromised, and that someone might be attempting to steal your identity. If your credentials are found on the dark web, you will be alerted immediately. That way you can change your password right away, BEFORE they can be used by a malicious cyber attacker.

If you signed up for Disney+ and are worried that your account might be breached, or if you are concerned about your business's security, we're here to help. Call us at 416-966-3306 or email us at info@connectability.com and we can help give you the peace of mind that comes with knowing that your business secure.

Tech Connect Video Series

It's Time To Protect Your Cloud Data!

Your data is everything – and like most businesses you probably have data stored in the cloud. If you share documents using Google Docs, work on files in Dropbox, share photos on Facebook, or send emails through Office 365 or Gmail then you are using the cloud. Now, if your data were accidentally, or intentionally, deleted by an employee, or held for Ransom by a hacker, you could lose all your private business data and might have to close shop for good. That's why it is so important to have a backup solution for your business.

Cloud storage means your data can be accessed from anywhere, so long as you have an internet connection. Unfortunately, Cloud STORAGE does NOT equal Cloud BACKUP. Cloud backup stores your data in the cloud with the express intent of being able to restore it in the event of data loss, hardware failure, disgruntled employees, or a disaster.

If you're concerned about the security and recoverability of your data, then watch this video now! You will learn about Office 365 and why you should be backing up your cloud-based data. To find out more, go to YouTube, look up **Connectability IT Support** and find the video **"Protect Your Cloud Data"** OR go to our website at **www.connectability.com**, hover over **"Resources & Videos"** and select **"Videos".**

4 Ways Technology Can Improve Your Business

It boosts productivity. Technology like task management software can change how you work through a day. Everything is listed out, and you can check it off as you go. You can even make dependent tasks so tasks are automatically created for anyone who may be next in line to work on a project.

It's crucial to marketing. You need online and social media marketing. This is where people are. Understanding how social media marketing works can increase the number of people who know about your company, which increases your customer base.

It's essential for security. Technology and security go hand in hand. As your business relies more on technology, you need to rely more on security to protect your networked equipment, like all of your employees' PCs and your many servers.

You can't communicate without it. With things like e-mails, VoIP phone services, and direct messaging through social media sites, technology has made communication easier than ever. When you know how to use all these forms of communication, it puts you above the competition. *Pixel Productions Inc., 7/20/2019*

10 EASY WAYS TO DEFEAT STRESS AT WORK

1. Take a walk. A 15-minute walk will refresh your mind.

2. Work outside. Weather permitting, working in the sun can boost your mood.

3. Meditate. Use a meditation app like Calm or Headspace to lower blood pressure and de-stress.

4. Take deep breaths.

5. Make a checklist. Write it out and focus on one task at a time.

6. Talk to a friend. Have a conversation about a problem. Talking it out can change your perspective.

7. Watch an informative video. It can be on anything. Videos are a great distraction for 5-10 minutes.

8. Listen to soothing music.

9. Take a 20-minute nap. Nothing does wonders for stress like a power nap — just be sure to set a timer!

10. Trust your instincts. If you feel you need a break, take it. Don't push yourself if it isn't necessary. *Small Business Trends, 7/19/2019*

"If you didn't have Facebook when you were a kid, how did you know who your friends were?"

This month we will be donating to Soldier On.

Founded in 2007, Soldier On is a program of the Canadian Armed Forces Transition Group. Soldier On is committed to providing support for veterans and serving members to help adapt and overcome permanent physical injury or PTSD.

Soldier On is dedicated to improving the quality of life of veterans and current serving members through physical activity and sport. Soldier On provides a safe environment and empowers them to adapt and re-integrate with local, community-based activities, and remain active for life.

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