CONSUMER CHOICE AWARD 2020 GTA 3 YEAR WINNER

Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by: Connectability

Happy Holidays!

We are another year older, and hopefully a year wiser! During the holiday season we like to reflect on the past year and say thanks for what we are grateful for.

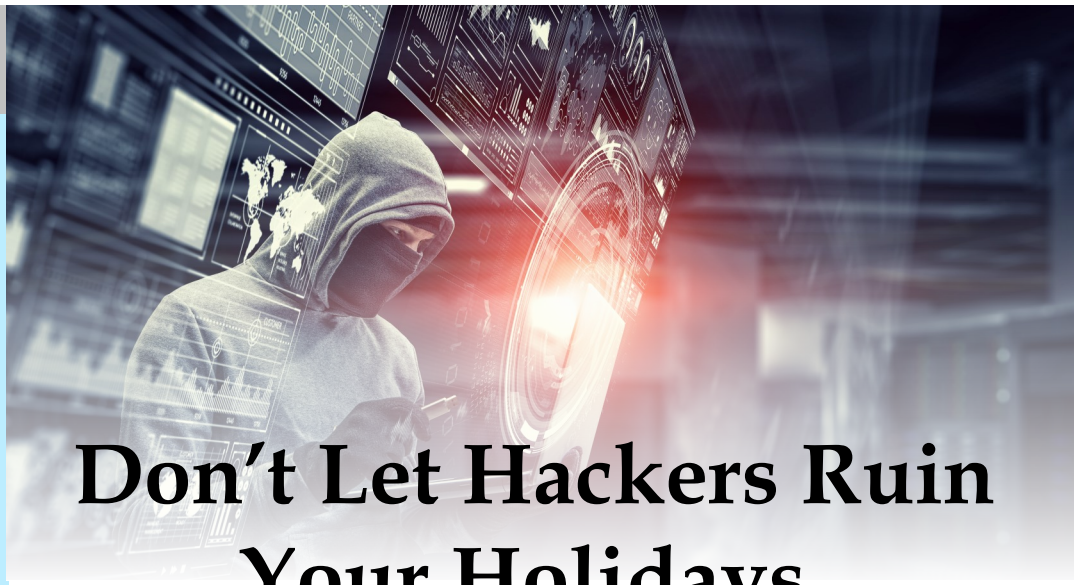
On that note: we would like to thank our customers for being part of the Connectability family! There's a lot of choices out there but you chose us and that means a lot.

We love working together, and we hope to have the opportunity to support your technology, and your business, for a lot longer!

The entire Connectability team sends our warmest wishes to you and your loved ones. Have a wonderful holiday season!

December 2021

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



Don't Let Hackers Ruin Your Holidays

Online shopping has become more popular than ever before. In 2020, more than 2 billion people bought products or services online. Whether they're shopping online because it's more convenient or they're avoiding going to brick-and-mortar retailers during the ongoing pandemic, more people are turning to online retailers every day.

It's not just the convenience or health safety that's drawing people to shop online; shopping this way has become more secure than ever before. That doesn't mean all retail websites are created equal when it comes to safety and security. Hackers and scammers are still out there trying to get your information, but by taking the proper precautions, you have no reason to worry while shopping digitally.

If you plan on buying online this holiday season, here are five tips to ensure your information stays protected.

Use Well-Known And Secure Sites

When looking to purchase a product or service online, you have thousands of options to choose from. To avoid having your personal information stolen, it's best to use familiar sites such as Amazon, Walmart or any of the other major retailers. If you search for a product on a search engine, you may be presented with prices that are extremely low. There's a good chance these are not trustworthy sites. When it comes to online shopping, if it seems too good to be true, something is wrong.

Pay attention to the security of the site where you're trying to make a purchase. Look for a lock icon in the top left of the browser bar. If the website has one, then you should be safe on their site. Another way to tell is by looking at the beginning of the web address. If it begins with "https" instead of "http," you are in good shape, and you can continue using the site. Secure websites help protect your financial information as well as passwords. Shopping at unsecured sites can put your personal information at risk.

Continued on pg.2

Continued from pg.1

Create Stronger Passwords
A strong password can make all the difference between your information remaining secure and someone stealing it. You need to make your passwords as difficult as possible so that hackers and thieves can't hack into your accounts. It's best to use a complex mix of uppercase and lowercase letters while including special characters and numbers. Avoid using common spellings of words and personal information in your passwords because these can be easier to crack.

If you're worried about not remembering a complex password, use a password manager. This tool will remember the passwords for your accounts while also keeping them protected. Utilizing password managers is the best way to create complex passwords since you won't have to personally remember them, and they will still be protected.

Keep Track Of Your Statements
You should always be watching your finances, but it becomes even more important when shopping online. It's a good habit to form and will help you catch overcharges or purchases that you did not make. It's also a good idea to only shop with a credit card when shopping online. If someone hacks into your account and steals your debit card information, they will have direct access to your money.

"In 2020, more than 2 billion people bought products or services online."

Most credit cards have protections in place for fraud, so you won't be at fault for any errant charges on your account.

Protect Your Information
When entering a new website, you should be wary if they ask for any personal information upfront. No online retailer should ever ask for your Social Insurance Number unless you are applying for a credit card on their site. Be cautious if they ask for your birthday as well. Hackers can use this information in conjunction with your credit card number to wreak havoc on your life.

Don't Shop On Public WiFi
While it might seem like a good way to keep yourself entertained while enjoying a coffee at a local café, shopping on public WiFi can leave you at risk of being hacked. Public WiFi is often not very secure, and entering your personal information while using it can give hackers easy access. It's much safer to bookmark the item and wait until you're home or no longer using WiFi to make the purchase.

Shopping online can be as safe and reliable as shopping in a store – as long as you take the proper precautions. Take some time to ensure that you are following the right security measures before making purchases or entering any information.

Top Tips On How To Prevent Your Smart Cameras From Being Hacked

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. That issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

1. **Regularly update your passwords.** Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password – you name it. Changing your passwords every three months is an excellent way to stay secure. Every password should be long and complicated.

2. **Say no to sharing.** Never share your smart camera's login info with anybody. If you need to share access with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

3. **Connect the camera to a SECURE network.** Your smart camera should only be connected to a secure WPA2 encrypted, firewalled WiFi network. The more protection you put between the camera and the rest of the digital world, the better.

Shiny New Gadget Of The Month:

Travelmate Robotics

Tired of the usual, old-fashioned luggage? Travelmate Robotics is trying to change the luggage game. With these suitcases, you never have to worry about the safety of your items. It comes standard with a secure Bluetooth-enabled lock and GPS tracking if your bag ever goes missing. The suitcase also comes with a scale so you'll never have to worry about overpacking. The best part? The suitcase is entirely autonomous and will follow you around through a Bluetooth connection. The "Follow Me" function as well as the obstacle avoidance system sets Travelmate Robotics ahead of the competition. It's the ideal suitcase for any businessperson or frequent flyer.

3 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 solid 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 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.

3. **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.

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.

Tech Connect Video Series:
The Rise Of Data Breaches

If you've read the news lately, I'm sure you've seen something about a recent, high-profile, data breach. In fact, in the first half of 2021 alone, more than 118 million people were impacted by data breaches, data exposures and data leaks. Now you might say "Those are all large multi-national companies. Cyber criminals won't bother with my small or medium sized business". Unfortunately, this just isn't true. Cyber criminals aren't discriminating, and time and time again, we've had to remediate the impact of a data breach or cyber-attacks.

If your data is breached, do you know what the costs to your business would entail? Do you know how long it could take to recover or restore your data? What are your disclosure requirements? Do you have copies of that data, or is it gone forever? What would be the impact on your clients, and would they continue to use your services after a breach? These are all questions you should be asking yourself.

Watch our Webinar now to learn about the rise of data breaches and how you can protect your business. To watch, go to YouTube, look up Connectability IT Support and find the video **"The Rise of Data Breaches"** OR go to our website at **www.connectability.com**, hover over "Resources & Videos" and select "Videos".

Netflix Reveals The Formula That Led To Its Success

For the past 20 years, Netflix has steadily taken over the home entertainment industry. It went from a struggling DVD-to-home mailing company to an entertainment powerhouse that produces its own big -budget shows and movies in addition to its large library of third-party releases. Netflix co-founder Reed Hastings attributes the company's success to three areas: building talent density, increasing candour and reducing controls.

Hastings was forced to lay off a third of his staff during the dot-com burst in 2001. This left him with the highest-performing employees who truly loved their jobs. He encouraged these fantastic employees to openly speak their minds so they could make the best possible decisions to boost business and loosened his control by creating a more relaxed environment that would inspire innovation. Previous procedures delayed action, so he threw the rule book out and creativity began to surge. By gathering the best possible staff – and allowing them the freedom to do what they did best – Netflix's stock and popularity grew to unprecedented levels, where they remain to this day.

The Real Reason Your Team Isn't Ready To Work

The pandemic caused many employers to allow their employees to work remotely. As we enter the second winter during COVID-19, fewer people have returned to the workplace, and many wonder if they will ever return to the pre-pandemic work environment. The truth is that the virus has caused many uncertainties for people. There's no telling if there will be more mandates in the future that will cause employees to stay working remotely. Many have changed how they handle childcare and would need time to make new arrangements if asked to return to work. Microsoft recently dealt with this, announcing a "return to work" date for its employees to eliminate any uncertainties. The company wants to find ways to ease people's minds before bringing them back into the workplace. The more comfortable your employees are, the better they will perform and the more likely they will be to stay with the company.

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!

What popular social networking site was sold to News Corp. for $580 million in 2005?

a) Twitter
b) Myspace
c) Facebook
d) Snapchat

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

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**.