



Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by:
Connectability

Happy Holidays!

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

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 long time to come!

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



December 2022



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



IT News, Trends And Information You May Have Missed In 2022

The year 2022 will soon be on its way out the door. It became a year full of ups and downs for many small businesses, but it still felt more promising than the past couple years in the midst of the pandemic. Many small-business owners used this past year to re-evaluate their IT services. Some needed to strengthen their cyber security defenses while others utilized new advancements to further assist their customer base.

If you're a small-business owner, it's essential that you're aware of the IT news, trends and events that took place in the recent past. In fact, knowing what happened in the previous year can allow you to develop plans for the future so 2023 will be successful for you and your business. You shouldn't continue following old trends, because the competition will quickly leave you behind, and that could open you up to cyber-attacks you didn't know

existed. Don't worry, though; we're here to help. Here are our picks for the most important IT events and trends of 2022.

Refined Artificial Intelligence

Artificial intelligence (AI) has come a long way over the past few years. Many people associate AI with video games or using GPS for travel, but many companies have started to implement AI in new ways to boost their businesses. It's even being used to automate certain tasks, provide insight through data analysis and assist customers with their needs.

AI has proved incredibly beneficial when used to help customers, and this can be seen when looking at various small-business websites. They use AI to answer common questions their customer base has, which provides quick, efficient results for their customers, who leave satisfied with their interaction. Around 37% of

Continued on pg.2

Continued from pg.1

businesses now utilize AI in the workplace, according to a survey conducted by Gartner. Another study by NewVantage Partners found that nine out of 10 leading businesses have investments in AI technologies. So, if you want to get ahead of your competitors, implement AI into your business.

Managed IT Services Providers Continuing To Grow In Popularity

Gone are the days of having an in-office IT person or team. A more cost-effective solution has been gaining traction over the past few years and will continue to do so for the foreseeable future. Managed IT services providers (MSPs) install, support and maintain all the users, devices and PCs connected to your network on a routine basis. MSPs can even prevent common problems such as lost devices, hardware failures, fires, natural disasters and a host of other issues that can interrupt or outright destroy your IT infrastructure and the data it holds. The managed IT services industry is growing immensely. At the end of 2021, the industry was valued at \$239.71 billion, and it's estimated to grow by over 13% annually until 2030. Businesses of all sizes have realized the value of MSPs and are using them to their advantage.

"At the end of 2021, the industry was valued at \$239.71 billion, and it's estimated to grow by over 13% annually until 2030."

Major Cyber-Attacks Of 2022

Cyber-attacks happen all the time. As new cyberthreats emerge, we'll see more frequent and severe cyber-attacks over the next few years. Uber saw another cyber-attack this past September that caused the company to shut down its internal messaging service and engineering systems in order to get to the bottom of the incident. Cryptocurrency storage and blockchain were also high-value targets for cybercriminals. Ronin and Crypto.com suffered severe cyber-attacks that required both companies to reimburse their users for the cryptocurrency stolen in the attack. Ronin was hacked for \$540 million, and Crypto.com was hacked for \$33 million worth of cryptocurrencies.

Small businesses weren't safe from cyber-attacks either. While cyber-attacks on big businesses make national news, small businesses are targeted more often since their cyber security defenses aren't as strong. That being said, it's imperative you ensure your business has efficient cyber security practices in place, so you won't have to worry as much about cyber-attacks.

The IT industry is consistently changing to keep up with new developments and advancements. If you're a small-business owner, it's vital to keep up with the latest news and information so you can best protect your business and its data. When you stay ahead of the trends, it's much easier to prevent potential cyber-attacks and threats.

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 Wi-Fi 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 Wi-Fi network. The more protection you put between the camera and the rest of the digital world, the better.

Shiny New Gadget Of The Month:



The Ekster Parliament Wallet

We carry sensitive information in our wallets. They hold our driver's licences, credit cards, family photos and more. It makes sense that we would want to do everything we can to keep our wallets safe. Now, there's a wallet available to help us. The Ekster Parliament Wallet is a premium-leather, RFID-blocking smart wallet. With the press of a button, the built-in aluminum card holder fans out your cards for easier access. It protects your cards from skimming and is available in 10 brilliant colours. For an additional cost, you can add a tracker card to your wallet so you can find it if you leave it somewhere. There's never been a smarter wallet than the Ekster Parliament Wallet.

The Dangers Of Password Autofill

Modern web browsers and password managers come with a feature called password autofill. This helps users store and automatically use their account credentials to access websites and other applications. While password autofill is convenient, it comes with security risks.

Why password autofill is so dangerous

Modern web browsers and password managers have a feature that enables usernames and passwords to be automatically entered into a web form. This feature isn't completely safe, however. If you enable this feature and hackers gain access to your computer or web browser, it will be easier for them to infiltrate your accounts because the autocomplete feature will fill in all saved credentials.

Tricking a browser or password manager into providing saved information is incredibly simple. All a threat actor needs to do is place an invisible form on a compromised webpage to collect users' login information. Once the browser or password manager enters the user's information, the hacker will gain access to that data.

Using autofill to track users

Shrewd digital marketers can also use password autofill to track user activity.

For instance, they can track people based on the usernames in hidden autofill forms they place on websites and sell the information they gather to advertisers. While they don't intend to steal passwords, there's always the likelihood of exposure.

One simple security tip

A quick and effective way to improve your account security is to turn off autofill.



Here's how to do it:

- **On Microsoft Edge** – Open the Settings window, click *Profiles*, and then select *Passwords*. Disable "Offer to save passwords."
- **On Google Chrome** – Open the Settings window, click *Autofill*, and disable "Offer to save passwords."
- **On Firefox** – Open the Settings window, then click *Privacy & Security*. Under the Logins and Passwords heading, untick the box next to "Autofill logins and passwords."
- **On Safari** – Open the Preferences window, select the Auto-fill tab, and turn off all the features related to usernames and passwords.

Having good password security habits can significantly protect your sensitive data. For 24/7 cybersecurity support that goes far beyond protecting your privacy, call us today at (416) 966-3306.

Tech Connect Video Series: The Rise Of Data Breaches

If your data is breached, do you know the costs to your business? Do you know how long it could take to recover or restore your data? ***Do you know whether your data can be recovered at all?*** 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, and items we'll be addressing in this video.

In this video, you will learn:

- How Data Breaches Are Changing
- The **Impact** of a Breach (Downtime, Reputation Damage, Legal Fees, etc.)
- The Future of Data Breaches
- How Data Breaches Can Disguise Other Types of Attacks
- **How You Can Protect** Your Business and Clients

Watch our Webinar now to learn about the rise of data breaches and how you can protect your business. To watch, go to <https://bit.ly/3Y0Xeww> OR go to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".

2 Challenges E-Commerce Businesses Face And How To Overcome Them

With the Internet came a new digital marketplace that allowed people to purchase specific products they couldn't find in their hometowns. These days, most businesses offer a way to buy their products or services online, whether it's through their personal website or an e-commerce marketplace like Amazon. Despite this, selling online brings new challenges you don't often see when selling from within a brick-and-mortar location. Here are some challenges to watch for and solutions to overcome them.

Payments

Oftentimes, e-commerce businesses need to deal with chargebacks. This happens when a customer disputes a charge on their credit card statement, causing you to lose out on the sale and the item. To avoid this, have a clear

and concise return policy. You should also keep detailed records of all transactions and shipments to prove the customer received their order.

Shipping

Shipping delays can leave customers feeling frustrated, even if they aren't the company's fault. You can't do anything to control hazardous weather, but you can set a reasonable range of time for your customer to receive their item. You don't have to promise two-day shipping just to compete with Amazon. It can also help to utilize shipping management software to automate your shipping processes.

Coping With Stress

Nearly everyone deals with stress at some point in their lives, and most business leaders struggle with it regularly. The good news is that you don't need to live with extreme levels

of stress. There are simple solutions to help you cope better. Below you'll find three ways to lessen the amount of stress in your life.

- Be aware of how much stress you take on. You need to know how much stress your body and mind can reasonably take on before you start to struggle.
- Set boundaries and say no when needed. You can't agree to do every task or help every person without adding more stress to your plate. Know how much is too much, and don't take on tasks that are too demanding for your current state of mind.
- Meditate, breathe deeply and exercise to relax your body and mind. Stressors won't feel so drastic when you're relaxed.

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!

Which search engine almost bought Google in the 1990s?

- A. Yahoo
- B. Lycos
- C. AltaVista
- D. Excite

Call us right now with your answer!
(416) 966-3306



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 (416) 966-3306.