



Connectability Corner

PUTTING THE PIECES TOGETHER.

Powered by:
Connectability

Help Us Welcome Our Newest
Team Member:
Keenan Magnuson

Connectability has grown a lot over the past few years. To continue that aggressive growth we've also had to grow our team. Please help us welcome Keenan Magnuson to Connectability!

Keenan is our newest Office Administrator. His role at Connectability is to assist our clients and staff, and to ensure all procedures and operations are followed. Keenan is ready to work with your team and is dedicated to providing exceptional service.

Keenan was born and raised in Toronto and holds broad reaching interests, from Cinema and Ancient Philosophy to Mixed Martial Arts and Game Collecting. Keenan is a University of Toronto Humanities graduate who brings 7+ years of varied experience in areas of Customer Service, HR, and Office Administration to his role with Connectability.

Keenan's unique skillset allows him to provide Connectability's customers with the best customer experience possible.



August 2022



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



Internet Safety Tips For Parents

In today's climate, is there anything more prevalent than the Internet? In fact, we've grown so accustomed to using it that the Internet now seems to help us meet any need or want. Unfortunately, we don't often think about the effect that has on our kids, who have never known a world without this level of technology.

For the most part, the Internet is an incredible boon to our children. They can look up anything they're curious about and will be met with more information than previously fathomed. Many of us remember visiting the library to research topics, and even then, resources were limited compared to what can easily be found online today.

While the Internet offers many benefits for kids, there are risks.

That's why it's important to keep your children protected. Before your kids get a social media account or dive headfirst into the web, take the following security measures.

Parental Restrictions

Nearly every device that can connect to the Internet has some level of parental control. With computers and laptops, you can restrict what websites and apps your children visit. You can also specify which websites you want totally blocked. This is an option on many tablets and smart phones as well. With those, you can actually set time constraints and limits that make it so your child can only use the device for a certain amount of time, and you can even completely restrict usage at night.

Continued on pg.2

Get More Free Tips, Tools and Services At Our Website: www.connectability.com
(416) 966-3306

Continued from pg.1

Potential Risks

When your children first start using the Internet, you must ensure they understand any potential risks. We all know people aren't always who they say they are on the Internet. Similarly, not all information found online is true. When your kids visit websites or use apps, remind them not to share any personal information about themselves. They should never give out their address, school information, phone number or even their email address to anyone online. Even if the person requesting this information claims to be someone they know, they might not be. If your child is using social media, inform them not to accept friend requests from people they don't know. It's important that kids understand all of the risks to ensure they stay safe in the digital and physical world.

Get Familiar

If your children are using the Internet, you should become familiar with the websites and applications they use. Make sure all websites have the little padlock icon by them, which indicates they are safe websites. Look through the apps and websites your



children frequent to ensure they're safe for them to use and do not contain any inappropriate content.

Lead By Example

Your children's first interactions with the Internet will most likely stem from you, so do your best to set a great example for them. This is your opportunity to model positive online habits for your children. Your social media posts should also be appropriate and not break any of the online rules you set for your own child. In their eyes, it won't be fair if you or someone else in the family can do things they cannot.

Our children are some of the most important people in our lives, so it makes sense that we would do everything in our power to keep them protected. Just make sure your protective efforts extend from the physical world into the digital world as well.

"Your children's first interactions with the Internet will most likely stem from you, so do your best to set a great example for them."

Free Report Download:

What Every Small Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain, non-technical English common mistakes that many small business owners make with their computer network that cost them thousands in lost sales, productivity, and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration of these oversights.

You'll Discover:

- The single most expensive mistake most small business owners make when it comes to protecting their company data.
- The universal misconception business owners have about their computer networks, and how it can end up costing between \$9,000 to as much as \$60,000 in damages.
- 6 Critical security measures every small business should have in place.
- How to greatly reduce – or even completely eliminate – frustrating crashes, slow performance, and other annoying computer problems.
- How to avoid expensive computer repair bills and get all the computer support you need for a low, fixed monthly rate.

Get your FREE copy today:

<https://www.connectability.com/protect/>



Shiny New Gadget Of The Month:



Oura Ring Generation 3

For the past few years, fitness trackers have become all the rage. Between Fitbits and the Apple Watch, nearly everyone has or is familiar with fitness trackers. One of the most common complaints about many fitness trackers is comfort. Oura decided to take the wristband out of the equation with the Oura Ring. The Oura Ring is a fitness tracker that you wear on your finger. It tracks sleep, activity and readiness measurements. This device is even more accurate than other fitness trackers since the finger is a better spot to record heart-rate data. Through temperature sensors, a library of informational resources and much more, the Oura Ring is the perfect fitness tracker for just about anyone who is looking to improve or maintain their physical health.

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.



Tech Connect Video Series: Why VoIP Is Better For Your Business

When your workforce is remote, communication with your partners, clients, team and vendors is more important than ever. Unfortunately, many businesses struggle to stay connected with their remote teams. If you're finding communication a challenge, a VoIP phone system might be the answer.

VoIP is short for Voice Over Internet Protocol and it uses the internet to make and receive phone calls. There are many benefits of a VoIP system that are hard to ignore. They are heavily customized and with its many innovative features you can increase the effectiveness of your remote team.

If you would like to learn why VoIP is better for you than a traditional landline, watch this video NOW! To find out more, go to <https://youtu.be/i9v4lpd8B1I> or to our website at www.connectability.com, hover over "Resources & Videos" and select "Videos".



4 Ways To Better Protect Your Personal Information

Most people keep their personal information as secure as possible. They don't post their passwords on social media or share Social Insurance Numbers with untrustworthy sources. These practices seem obvious, but there are smaller things we can do to provide better protection. You'll find four of those tactics here.

Dangers Of Unsecured WiFi –

Hackers can use this connection to download malware on your devices.

Password Manager – You shouldn't use the same password between multiple accounts. Utilizing a password manager will help you keep track of different passwords.

Breached Companies – When a company's security is compromised, all of its customers' personal information can be exposed. Avoid working with these companies until they've offered improved security.

Think Before Posting – Be careful about what you share on social media. Revealing too much personal information can leave you vulnerable to a cyber-attack.

Tech Trends To Improve Customers Loyalty

If you want your business to succeed, you must build a solid customer base. Over the past few years, advancements in technology have made it easier for companies to improve their relationships with their customers. One such way is through

the use of AI chatbots. If someone has a question about your service or product, you don't want to leave them waiting for an answer. Chatbots can be programmed to answer common questions until a live representative is available, if they're even needed.

Additionally, you should make an effort to monitor content created by people outside your company. If someone is spreading false information about your business, you need to combat it. If disinformation is allowed to fester, it can quickly sink a small business. Simply replying to misinformed reviews or reporting inappropriate content about your business can go a long way toward becoming a more trustworthy source in your industry.

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | S | Y | T | S | T | R | O | P | P | U | S | T | I |
| E | R | A | W | M | O | S | N | A | R | E | R | K | A |
| T | M | R | H | A | C | K | E | R | S | T | K | R | E |
| R | C | Y | B | E | R | A | T | T | A | C | K | S | Y |
| A | R | P | P | Y | R | O | L | Y | R | Y | T | E | E |
| I | C | L | O | U | D | S | E | R | V | I | C | E | S |
| V | R | S | A | T | B | L | U | E | I | D | A | T | C |
| O | R | Y | V | O | I | P | R | B | S | C | B | M | R |
| C | Y | B | E | R | S | E | C | U | R | I | T | Y | U |
| R | E | M | A | I | L | S | E | C | U | R | I | T | Y |
| C | C | A | C | W | K | S | B | I | M | S | E | P | S |
| C | C | B | C | D | D | R | U | S | S | N | I | I | P |
| C | Y | B | E | R | C | R | I | M | I | N | A | L | S |
| A | S | C | I | E | A | O | I | R | N | S | E | S | A |

CLOUD SERVICES
CYBERSECURITY
CYBERCRIMINALS

VOIP
HACKERS
CYBER ATTACKS

IT SUPPORT
RANSOMWARE
EMAIL SECURITY

REXNIHL
breast cancer

This month we will be donating to **Rethink Breast Cancer**.

Rethink Breast Cancer empowers young individuals globally who are concerned about and affected by breast cancer. It is a young women's breast cancer movement, that focuses on ground-breaking education, support, and advocacy primarily for millennials.

Rethink focuses on thinking differently about breast cancer, with a breakthrough approach by prompting bold, stylish, fear-free awareness, while simultaneously dismissing the myth that breast cancer is only an "old lady disease". Rethink provides care and relief for young women with breast cancer to make their journey a little bit easier.

If you would like to contribute to Rethink Breast Cancer we would love your help! Email: info@connectability.com or call: (647) 492-4406.