The Tech chronicle

What's New

The series of events during March 2020 will never be forgotten. From a business perspective, owners and C-level executives have had to make decisions that will impact the future of their company and the landscape of their industry.

We have created a webpage to keep you updated for you to make informed business decisions. www.haycorsolutions.ca/covid-resources/

Haycor's goal to stay in constant communication through virtual interactions and public announcements and keep you informed about Cybersecurity.

April 2020

This monthly publication provided courtesy of Jason Wachtel, President of Haycor Computer Solutions Inc.

Our Mission: To build strong, long-lasting relationships that surpass professional formalities by catering our services to each customer's specific needs.

How To Quickly Shift To A Work-From-Home Business Model To Maximize Productivity In Today's Coronavirus Environment

As a business owner today, you are now facing unprecedented challenges to help deal with the coronavirus pandemic. You are asked to self-isolate and practice social distancing to "flatten the curve." You are asked to allow your employees to work from home to reduce possible exposure and slow the spread of COVID-19.

These are all reasonable requests. However, as a business owner you also need to maximize productivity, bring in revenue and try to grow your business in these demanding times. How can you accomplish these goals when your office is now a ghost town and productivity has fallen off a cliff?

The answer lies in setting up your office to function remotely. If you've never implemented a work-from-home policy before, it may seem like a whole different world. Managing an entirely remote workforce goes far beyond giving your employees a laptop and reminding them to check in every once in a while. After all, there are many factors most business owners haven't ever had to consider, such as:

- What technologies do I need?
- How can my employees work from home without compromising the security of our network?
- How can I make this new work environment as easy, comfortable and productive as possible?

We understand these are unique times. We know that "business as usual" is going to be quite different for an undetermined amount of time. But together we can help you adjust to today's new normal by giving you the tools, technologies and insights to create a secure and productive work-from-home business environment.

Continued on pg.2

Continued from pg.1

Here are three important considerations to getting you set up and running a successful work-from-home business:

1. Don't allow employees to use home computers or devices. Their mindset may be, "Well, I'm working from home so I may as well use my home computer." This is a dangerous mistake. Our team works hard to ensure your company computers and network are secure and protected from malware, viruses and cyber-attacks. Their home computers and devices could be littered with tons of downloaded music, videos, images and more. Because it's more exposed, it can invite malware into your network. Rather, provide a company-approved and secured computer/laptop for employees to use at home.

2. Secure their WiFi access point. Without a secure WiFi access point, you're essentially leaving a back door open to hackers. That's because WiFi signals are often broadcast far beyond your employees' homes and out into streets. Yes, drive-by hacking is popular among cybercriminals today. A few tips for securing your employees' WiFi access points:

Use stronger encryption and a more complex password

Hide your network name

Use a firewall

These security measures are not difficult to set up. But if you have any questions or need assistance, we will be happy to help get your employees set up remotely.

3. Use a two-factor authentication VPN. VPN stands for virtual private network. It's essentially a private, encrypted tunnel that goes direct to your IT network in your office. Ideally, you'll want your VPN to support two-factor authentication. This means it's doubly secure because your employees will need to call in to access the network. If you don't have a VPN for your employees to use, you can consider other services, such as GoToMyPC or Zoho. While these products are not as secure, at least they keep your home network from being exposed.

As business owners ourselves, we too are having to pivot and work differently than we ever have before. However, because we have the technology and infrastructure in place, we are still surprisingly productive.

Our team wants to help your business survive and thrive during today's unique environment. If you and your IT team need extra hands right now…or solutions to help your employees work SECURELY from home…we have software tools, expert staff and resources we'd like to offer you to keep your business as productive as possible.

Here's a link to my personal calendar if you wish to book a quick call to discuss:
https://www.scheduleyou.in/n4YC3b

Please know that this is not a sales call but simply an outreach to help a fellow CEO stay afloat.

WORK FROM HOME GAMEPLAN

"The Ultimate Small Business Guide To Setting Up A "Work From Home" System For Your Staff"

Secrets Every Business Owner Must Know Before Installing A 'Virtual Network' To Allow Employees To Work From Home, On The Road, Or From A Remote Office

Free "Work from Home Gameplan" Report

Written before the outbreak, Haycor Computer Solutions released a free "Work from Home Gameplan" report. The report addresses 1. What "telecommuting" is and why so many small and medium sized businesses were rapidly implementing work from home programs before the COVID 19 outbreak. 2. The single most important thing you MUST have in place for every remote office initiative. 3. How to get a FREE "Home Office Action Pack" ($97 Value).

To receive this report, you can visit **https://www.haycorsolutions.ca/workfromhome/, call us at 905-707-6775 ext 227, or** email **cory@haycorsolutions.com** requesting the report.

How to Clean your Mouse and Keyboard

Now is a great time to ensure your commonly used devices are being cleaned on a consistent basis. If you haven't cleaned either your mouse or keyboard in a while, we recommend following the instructions below:

How to Clean Your Mouse:

1. Unplug the mouse
2. Moisten a cotton cloth with rubbing alcohol, and use it to clean the top and bottom of the mouse.
3. Reconnect the mouse once it is dry

How to Clean Your Keyboard:

1. Unplug the keyboard
2. Turn the keyboard upside down and gently shake it to remove dirt and dust
3. Use a can of compressed air to clean between the keys
4. Moisten cotton cloth or paper towel with rubbing alcohol and clean the tops of the keys.
5. Reconnect the keyboard to the computer once it is dry

Cybercriminals Are Counting On You Letting Your Guard Down During This Global Pandemic—Here's How To Stop Them

The world is slowing down during this COVID-19 pandemic. The economy is has been hit hard. People are no longer going out. We're told to quarantine or self-isolate and not engage in groups.

You can bet there's one group that's not slowing down at all. In fact, they're probably working overtime while the rest of us have our lives turned upside down. Cybercriminals and hackers know there's no better time to strike than during a global crisis. While you are distracted and spending your time trying to make sense of this new normal, they are finding new ways into your IT network so they can steal data and passwords, compromise your clients' private information and even demand large ransoms.

Cybercrime is already on the rise and is expected to cause $6 TRILLION in damages by 2021! But, if history repeats itself, hackers will be out in full force throughout this coronavirus scare. We fully expect in the upcoming weeks that headlines will change from stories about COVID-19 to accounts of a frenzy of cyber-attacks on corporations and small businesses.

Here are solutions you can implement now to help protect your business data, money and productivity:

1. Be more suspicious of incoming e-mails.
Because people are scared and confused right now, it's the perfect time for hackers to send e-mails with dangerous malware and viruses. At this moment, your in-box is probably filled with "COVID-19" subject lines and coronavirus-focused e-mails. Always carefully inspect the e-mail and make sure you know the sender. There have been numerous reported scams across Canada ranging from e-mails, phone calls, text messages, etc.

Avoid clicking links in the e-mail unless it's clear where they go. And you should never download an attachment unless you know who sent it and what it is. Communicate these safeguards to everyone on your team, especially if they are working from home.

2. Ensure your work-from-home computers are secure.
Another reason we expect a rise in cyber-attacks during this pandemic is the dramatic increase in employees working from home. Far too many employers won't think about security as their team starts working at the kitchen table. That's a dangerous precedent.

First, make sure your employees are not using their home computers or devices when working. Second, ensure your work-at-home computers have a firewall that's turned on. Finally, your network and data are not truly secure unless your employees utilize a VPN (virtual private network). If you need help in arranging your new work-from-home environment, we would be happy to get your entire team set up.

3. Improve your password strategy.
During crises like the one we are all facing right now, your passwords could mean the difference between spending your time relearning how to grow your business and trying to recoup finances and private data that's been hacked. Make a point now to reevaluate your passwords and direct your team to create stronger passwords.

Also, while it's so convenient to save your passwords in your web browser, it also lessens your security. Because web browsers simply require their own password or PIN to access saved passwords, a skilled hacker can bypass this hurdle. Once they access your saved passwords, they can steal as much as they want – credit card information, customers' private data and more.

Instead, you should consider a password manager to keep all of your passwords in one place. These password managers feature robust security. A few options are LastPass, 1Password and Keeper Security Password Manager.

You, your team and your family have enough to concern yourselves with in regards to staying healthy, living a more isolated lifestyle and keeping your business strong. There's no need to invite in more problems by letting your computer and

4 Cyber Security Myths Business Owners Need To Know

Myth: Cyber-attacks only come from external sources.
Reality: Upward of 60% of data breaches can be traced back to employee error. They may leave sensitive data on unsecured hardware rather than behind digital walls. They may open malicious files that copy and send data to an external location. Employee IT security training goes a long way to fix this.

Myth: Simple antivirus software or firewalls are enough to protect your business.
Reality: Cybercriminals use sophisticated tools to get what they want. The fewer security solutions you have in place, the easier it is. Antivirus software can't do anything to stop a motivated hacker, and firewalls should never be considered a primary line of defence. Web scanning and malware detection software can give you more protection on top of these.

Myth: Your business is too small or niche to be a target.
Reality: Cybercriminals don't care about the size or type of your business. They target everyone because they know they'll eventually break through somewhere. Small businesses are more appealing because they often lack serious cyber security solutions.

Myth: You don't collect payment or financial data, so you aren't worth targeting.
Reality: They aren't just looking for credit card details. They want usernames, passwords, email addresses and other personal identifying information they may be able to use elsewhere because people have a bad habit of reusing passwords for other accounts, including online banking. *Inc., Dec. 16, 2019*

Top Tips For Making The Most Of Your Small-Business Technology

Embrace mobile. Your customers use mobile, so your business needs to work in the mobile space too. Optimize your website for a better mobile experience.
Good copy goes far. From blogs to social media posts, compelling, well-written copy can go a long way. Share personal stories and success stories and create a narrative for your business online.

Instagram it. If your business isn't on Instagram, it should be. Many of your current and future customers are there. It's a great place to share photos, tell stories and foster connections.

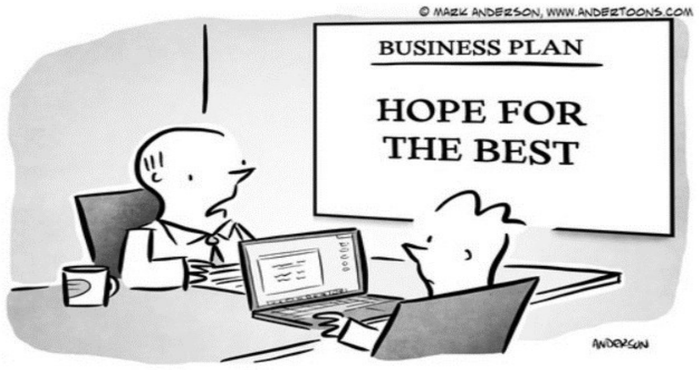
Get more out of SEO. Good header tags, for instance, are a must for good overall SEO. Learn how to get more out of headers and you'll be able to drive more traffic to your website or related web pages. *Small Business Trends, Dec. 1, 2019*

Things Mentally Strong People Don't Waste Time Doing

Overthinking – They look at their situation and take decisive actions. Some look at all the available information and go. Others rely more on their gut. Either way, they keep things moving forward.

Regretting – It's natural to want a different outcome than the one you got or to think, "I should have done X instead of Y." But these thoughts can hold you back and lead to second-guessing yourself later.

Complaining – It can be healthy to complain. It gets your thoughts into the open where they can be discussed. But you have to discuss and arrive at solutions. Complaining for the sake of complaining – or complaining to people who can't help – is unproductive. *Business Insider, Dec. 17, 2019*



"Well, it's not the worst I've seen."