LOGICAL TALK · APRIL 2020 EDITION

WHAT'S NEW?

The year 2020 came in with unprecedented challenges for businesses and communities across the world with global pandemic COVID-19.

Idealogical is committed to complying for the health and well-being of our employees, customers and partners. We are also actively executing the directions from our local health officials, provincial leaders and federal leaders while trying to ensure smooth day-to-day operations for our clients.

Read complete Idealogical COVID-19 Advisory online.

ABOUT THE AUTHOR

This monthly publication provided courtesy of Andre Vittorio, President of Idealogical Systems Inc.

Our Mission:

To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

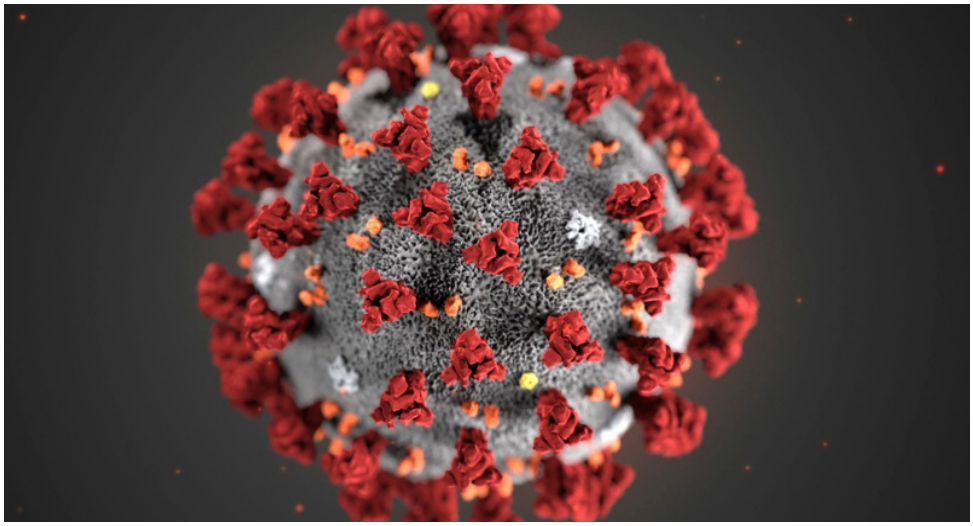

Illustration by CDC, Jan 2020

How To Quickly Shift To A Work-From-Home Business Model Amidst COVID-19

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.

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

Continued on page 2

Continued from page 1

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

1. Avoid asking 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 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 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 Wi-Fi access point. Without a secure Wi-Fi access point, you're essentially leaving a back door open to hackers. That's because Wi-Fi 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' Wi-Fi access points:

- Use stronger encryption and a more complex password
- Hide your network name
- Use a firewall

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, they do keep your home network from being exposed. We have the technology and infrastructure in place, so we are still surprisingly productive.

> **"Our team wants to help your business survive and thrive during today's unique environment."**

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... you should know that 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 additional requirements: http://www.scheduleyou.in/imJu2wqk

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

We are here to support our community affected by the COVID-19 outbreak

What are we doing to support Businesses?
We have introduced a new community support program to help businesses in the GTA who have been hurting due to the spread of COVID-19.

How are we supporting Businesses?
We are offering free services and cost-free sessions with Finance, HR and IT experts.
www.idealogical.com/covid-19-community-support

Additional Support
We are publishing weekly articles in the form of blogs that are focused on making working remotely as secure and safe as possible for you and your team.
www.idealogical.com/resources/blog

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. Stock Markets are being hit hard. People are no longer going out. We're told to quarantine or self-isolate and not engage in groups.

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.

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 emails

Because people are scared and confused right now, it's the perfect time for hackers to send emails with dangerous malware and viruses. At this moment, your inbox is probably filled with "COVID-19" subject lines and coronavirus-focused emails. Always carefully inspect the email and make sure you know the sender.

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

2. Ensure your work-from-home computers are secured

First, ensure 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) or a similar path to access your company data. 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

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.

Avoid inviting more problems by letting your computer and network security slide during these times.

For more detailed description, visit http://bit.ly/3dI2YnJ

Dr. Theresa Tam is Canada's Chief Public Health Officer (CPHO). She is a physician with expertise in immunization, infectious disease, emergency preparedness and global health security.
Dr. Tam provides advice to the Minister of Health, supports and provides advice to the President of the Public Health Agency of Canada, and works in collaboration with the President in the leadership and management of the Agency.

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 anti-virus 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.*

3 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."