BERTIGROUP
MANAGED IT SERVICES

December 2020, Issue #29

In This Issue

"Sorry about this. I wanted to email or text you my list, but she insisted on a picture."

BERTIBRIEF

The Top 3 Tricks And Sneaky Schemes They Use To Hack Your Computer Network That Can Put You Out Of Business

Cybercriminals and hackers are rarely shy about the methods they use to attack their victims. Many of them are more than happy to share how they broke into a business's network or how they walked away with thousands of dollars after successfully extorting a business owner whose company is now destroyed.

There are new stories out there to get your blood boiling as cybercriminals work to ruin people's lives and livelihoods. These criminals don't care what kind of damage they do. They only care about one thing: money. If they can get away with it – and many do – they'll keep on doing it. It's up to the rest of us as business owners (and employees) to stay at least one step ahead of these cyber thugs. The single best way to do that is to **stay educated on the latest threats**. The second-best way is to **stay up-to-date with the latest technology designed to combat cyber-attacks.** Here are three tricks of the trade cybercriminals are using right now in an attempt to get their hands on your money:

Ransomware. This is very common. It's a form of malware, and it can sneak onto your network and into your computers in several different ways:

- **Ad Networks.** These ads can appear on social media sites and familiar websites. Someone clicks a compromised ad or pop-up, and it initiates a file download. It's quick and it can be confusing. This is where anti-malware and anti-ransomware come in very handy.

The Pandemic Has Imposed More Canadians and Canadian Firms Online, Exposing Them to Greater Cyber-risks

This was a key message from the Communications Security Establishment's latest threat assessment, which makes for some pretty chilling reading. The agency said it is "almost certain" that state-sponsored actors will try to steal Canadian intellectual property related to COVID-19. Businesses not involved in vaccine research can't afford to be complacent either, it noted, highlighting the ongoing risk of commercial espionage and ransomware attacks against large companies. Often secretive spy agency for the first time said cyber actors sponsored by China, Russia, North Korea and Iran pose a threat to Canada, by sowing divisions between Canadians and developing the ability to disrupt critical infrastructure. Other notable factors in this report focused on an EVOLVING "cyber threat landscape" are as follows:

- ✓ The potential risk for the physical safety and economic value of Canadians
- ✓ Collection of data will increase privacy risks in the future
- ✓ A pool of advanced cyber tools and skills are conveniently accessible to more threat actors

Internet governance is at crossroads and is "pushing hard to change the accepted approach to internet governance from the multi-stakeholder approach to one of the state sovereignty."

To access the full report you can go to the link: https://cyber.gc.ca/sites/default/files/publications/ncta-2020-e-web.pdf

How Apple shifting Gears Impacts your Mac-based Business Technology? By Adam Berti

If you are an Apple nerd like all of us here at Berti Group, I don't have to tell you that the past month was BIG for Apple. There are two major releases from the company on both the hardware and software front. I won't get deep into my thoughts, but I will just go just far enough to help you understand how this impacts your business and future decision making.

The macOS Big Sur is the latest operating system from Apple and is a recent release. Computers that are managed under our BertiCare platform will currently block you from upgrading. The reason for this is that Apple moves fast and isn't shy about breaking things the first go around. As a business, you turn to us for expected outcomes in your IT, and to ensure these outcomes, as of now we need to block this release. This is nothing new: we do this every year as it isn't clear right at the release of what will and will not work. It could be certain printers, some software you use or other hardware. **We typically don't want a business to be running on Apple's latest macOS until at least 2, sometimes even 3 revisions have shipped.** We expect this to be in Spring 2021. We will of course look at your unique situation and decide on an individual basis when it's right for you.

Apple also made a big jump in their hardware this week with the release of its processors, switching away from Intel. This is a much bigger deal than the aforementioned macOS release, as this new processor means the software needs to be rewritten to take full advantage of the new chips, and sometimes even just to be compatible with the latest machines. Apple knows this is a big jump, and so continues to sell computers with Intel processors. These new computers are shipping with macOS Big Sur and cannot be downgraded. Rest assured, we have already ordered these for learning and testing (and of course just nerding out). Please reach out to us to help us guide you in the decision-making process to ensure compatibility and the best option for your needs. As a reminder, if you are not currently set up with an Apple Online Custom store, we can help you with this as it enables us to support you in your purchasing by creating quotes directly with which you can simply click order.

We love working with Apple because they like to challenge the status quo and aren't afraid to leave behind the past. This works great as a consumer where your efficiency and profitability don't depend on your IT. So as always. please reach out if you have questions or need advice. At last, I would like to wish everyone happy holidays, please be safe and spend time with your loved ones in the close cohort and small groups.

•**Malicious Links.** The cybercriminal sends you a legitimate-looking email, supposedly from your bank or a familiar online store. It may even be disguised as an email from a colleague. The email contains a link or file. If you click the link or file, it installs the ransomware.

•**Hidden Files On Thumb Drives.** This happens way too often where someone brings a thumb drive from home. While the user doesn't know it, the drive has a malicious file on it. When the thumb drive is inserted into a networked machine, the file is installed.

No matter how the ransomware gets onto your devices, the result stays the same. The ransomware goes to work and begins encrypting your files. Or it may completely block you from accessing your computer altogether. You'll get a full-screen message: *Pay up or never access your files again*. Some ransomware programs threaten to delete all of your files. Others say they will never restore access.

DDoS Extortion. Short for distributed denial of service, DDoS attacks are a relatively easy way for hackers to take down your business's online presence and wreak havoc on your network. These attacks mimic online users and essentially "flood" your network with access requests. It's as if millions of people were trying to access your website at once.

Your network simply can't handle that kind of traffic and, as a result, it goes down. The hackers can continue the attacks until you take action. That is to say, until you pay up. If you don't pay up the hackers will do everything they can to keep you off-line in an attempt to destroy your business.

Direct Attacks. Some hackers like to do the dirty work themselves. While many cybercriminals rely on bots or malware to do the work for them, some hackers will see if they can break through your network security more directly. If successful at breaking in, they can target specific files on your networks, such as critical business or customer data. Once they have valuable data, they may let you know they have it. Sometimes they'll ask for money in return for the sensitive data. Sometimes they won't say anything and instead simply sell the data on the black market. Either way, you're in a bad position.

However, there are things you *can* do about it! The answer is preventative measures. It all comes around to these two all-important points:

✓Stay educated on the latest threats

✓Stay up-to-date with the latest technology designed to combat cyber-attacks

If you do these two things and work with an experienced IT services company, you can change the outcome. You can put the cybercriminals in their place and have a digital defence wall between your business and those who want to do your business harm.

TOP 5 WAYS TO OVERCOME SETBACKS AND GROW

After you encounter a setback, it can be hard to start again. But simply believing in yourself is the best way to get back on track.

1. Recognize when failure is your fault and when it isn't. Some setbacks are entirely out of your control. Learn to recognize the difference in your faults and what you can't control, then move forward.

2. Learn from your mistakes and don't repeat them. Immediately letting go of the regret of making a mistake can be hard, so instead, focus on what caused the mistake, then learn from it.

3. Focus on your new goal. Failure often comes from going after something we don't truly want. Discover what you want so you understand what you need to work on.

4. Celebrate small wins. You don't have to wait to celebrate, even if you haven't reached your end goal. Validate yourself for completing smaller tasks, and you'll empower yourself to keep going.

5. Find the right mentor. This is someone who believes in you, even when you don't believe in yourself, and who can support you in reaching your goals. Find someone with the right knowledge and experience to learn from. *Business Insider, Sept. 16, 2020*

TOP BUSINESS APPS TO GET YOU ORGANIZED

If you're struggling to stay on top of your work tasks, there are some great apps available to help out.

Asana helps your business improve communication and collaboration. You can view all tasks and projects and follow progress on a communal board so you can communicate without having to rely on email

Proven helps organize your hiring process by posting listings to multiple job boards with one click. You can also review and sort applicants with ease.

Boxmeup organizes and tracks your packages, containers and bulk storage items to make storing and shipping a breeze.

Evernote keeps all your notes organized in one place and allows you to easily share notes and lists with co-workers.

Trello tracks your team's workflow. Whenever you make a change to a project or task, the app notifies each team member involved so you don't have to.

KanbanFlow helps managers visualize overall workflow. It gives overviews of work status, tracks progress and assigns tasks to team members.

Nerdwallet, April 21, 2020

Ottawa Unveiled Changes to Canada's Privacy-Protection Laws As an Attempt to Bring Them In-line with Digital Transformation and Growing Tech

The current pandemic has transformed us Canadians navigate our day-to-day lives. We live, work, access information and connect every day from home and remote, positioning technology to the front and centre of our daily consumption. A primary factor why the Canadian government is ensuring the security of Canadians, their personal information, and their privacy in the digital space.

On November 17, 2020, the Honourable Navdeep Bains, Minister of Innovation, Science and Industry, introduced the proposed Digital Charter Implementation Act, 2020, modernizing the framework for the protection of personal information in the private sector. Modernizing this legislation is going to be the key contributor to ensuring Canadians are safeguarded under the current and responsive law. Also, innovative businesses will benefit from clear rules, even as technology continues to evolve. This includes enhanced transparency and control and when companies are handling personal information about Canadians' ;

- ✓ greater control and freedom to securely migrate their details from one organization to another.
- ✓ the enhanced authority with privacy commissioner, to be able to force compliance, stop the collection of data, and use personal information.
- ✓ ensuring that Canadians have the right to demand their information to be destroyed.
- ✓ serious penalties among G7 privacy laws- with fines up to 5% of the revenue for the most serious offences.

The proposed Digital Charter Implementation Act is an initial step towards a vital reform of Canada's privacy framework. This initiative helps to build trust between citizens, companies and government while ensuring the innovators and businesses benefit from a modernized privacy framework. The Government of Canada is also proposing to modernizing the *Privacy Act*, which applies to the federal public sector and which the Privacy Commissioner of Canada also oversees. *By Sumit Munjal- Berti Group, Dec, 2020*