TECHNATION CA

COVID 19 & Cybersecurity Vigilance

In the midst of this novel coronavirus pandemic, we are coming together as a nation to 'flatten the curve' by exercising better personal hygiene and social distancing. During this crisis, Canadians and Canadian businesses have embraced technology to stay better connected, adopt alternative work arrangements, and move business activities online. We are seeing technology used more than ever and there are hundreds of information and communications technology (ICT) companies and thousands of workers that are assisting in the national response, keeping us connected and helping keep the economy moving.

Unfortunately, during crises like these, opportunistic cyber attacks increase and, in this case, the Canadian Centre for Cyber Security has noted an increase in healthcare related phishing and malware scams. Such attacks seek to take advantage of both human and system weaknesses during the crisis and cause even further damage and disruption. Cybersecurity teams from all levels of government and the ICT industry are taking additional actions to protect Canadians and Canadian businesses. To help, we should all be vigilant and take some basic steps to keep ourselves and our businesses safe and secure online:

1. **Make sure that you have activated your security products** (firewall, anti-virus, intrusion detection, etc.). Many of these products are free or available at low cost.
2. **Ensure that your operating system is up-to-date and patched.** Don't give threat actors an open door to your systems.
3. **Use strong passwords, and where possible, use encryption and/or multi-factor authentication** when engaged in exchange of sensitive information or in financial transactions. There are many trusted online references on these topics.
4. **Understand what you need to protect (systems, devices, data) and how it should be protected**. If you're not sure talk to your cybersecurity or IT service provider.
5. **Ensure that you regularly 'back up' your critical data in a separate location from your current system.** If you don't have a lot of data, you can do this on a USB, external hard drive or DVD. However, if you have more data, you can leverage Cloud services or discuss your requirements with your internet service or email provider.
6. **Be aware of potential phishing, social engineering, and malware attacks.** Ask your staff, colleagues, clients or loved ones to critically assess emails or information from unknown sources. The Canadian Centre for Cyber Security provides some specific things you and your employees can do whether at work or working from home.
7. **Have a plan to respond to a cyber attack**. Understand actions you need to take and who can help you in responding to and recovering from an attack. If you are hit with ransomware, call local law enforcement who will help guide you in your response.

For further information on keeping yourself safe online, check out the Government of Canada's GetCyberSafe website and, for businesses, check out their guide.

KPMG tenable Canadian Cyber Threat Exchange Informing Canadian Business Échange canadien de menaces cybernétiques Informer les entreprises canadiennes ROGERS eSENTIRE

Microsoft Bennett Jones AMO Association of Municipalities Ontario Deloitte.