Français

CAPSULE # 1 – March 16, 2020

Cybersecurity Issues

WORKING FROM HOME SECURELY AMIDST COVID-19

Given the current situation, it is important to discuss considerations for working from home securely amidst COVID-19 concerns. Remote workers have access to data, information, and network resources. This will attract imminent attention from bad actors.

Expect an increase in phishing attempts, especially targeted attempts towards VIP credentials. Be wary of requests that break corporate policy.

Be wary of anything “urging you” to access information via a third-party or attachment files, especially if it is related to COVID-19.

CYBERSECURITY CONSIDERATIONS

- **Use precautions when in public; there is increased risk of device and data theft (all connections should be encrypted).**
- **Use only trusted Wi-Fi networks, and be mindful of the risk.**
- **Only use sanctioned company devices and services for handling company data (use a VPN):**
    - Use approved work-from-home technologies.
    - Use a company private network resource (VPN).
    - Do not use third-party services because you can’t access your standard systems.
    - Use approved systems and services to communicate and transfer information. For example, do not use Dropbox to transfer a document to a client because you can’t access your standard security system or service.
- **If you require company devices to work from home, ensure the following:**
    - A formal approval from technology staff to borrow devices.

  - An assurance that required security software is properly installed.
  - Use of VPN and encryption where possible to protect data at rest and in transit, for files, systems, and general communications

- **Personal devices are generally against most organizations usage policies, but if special approval has been provided to perform work tasks, ensure the following:**

  - Systems are completely updated.
  - Systems and software have current and up-to-date antivirus software.
  - Do not store any unnecessary data (even Office documents).
  - Delete company data from the devices as soon as it is unnecessary.

- **Watch for phishing attacks – treat COVID-19 themed emails with great caution:**

  - Be wary of communications provoking a sense of urgency, particularly those with attachments or links that have “added information”.
  - Be wary of the abuse of legitimate brands being used to deliver information related to COVID-19.
  - Be wary of communications purporting to come from the Centers for Disease Control and Prevention (CDC) or World Health Organization (WHO).

NOTE TO THE IT DEPARTMENTS OF THE ORGANIZATIONS CONCERNED.

- **It is strongly suggested that strong authentication be used for remote access and cloud services. This type of authentication, called “multi-factor authentication (MFA)”, consists of using, in addition to a password, a second authentication factor such as a code sent by SMS to the cell phone in order to make your various connections.**

TALK TO US

We are here to listen. To start the conversation, contact your KPMG team of professionals, write us at continuite@kpmg.ca and/or visit our KPMG COVID-19 Resource Centre.

Do not hesitate to contact Francis Beaudoin, Partner and National Leader, Technology Risk Consulting, as well as Yassir Bellout and Guillaume Clément, Partners, Cybersecurity.

USEFUL LINKS

www.quebec.ca/coronavirus
www.canada.ca/coronavirus
KPMG COVID-19 Resource Centre

the KPMG Online Subscription Centre.

At KPMG we are passionate about earning your trust and building a long-term relationship through service excellence. This extends to our communications with you.

Our lawyers have recommended that we provide certain disclaimer language with our messages. Rather than including them here, we're drawing your attention to the following links where the full legal wording appears.

Disclaimer concerning confidential and privileged information/unintended recipient
Disclaimer concerning tax advice