

[REDACTED]

---

**De:** [REDACTED]  
**Envoyé:** 31 juillet 2019 08:31  
**À:** [REDACTED]  
**Objet:** INFORMATION - Entrevue Éric Caire

Bon matin !

Entrevue intéressante de Éric Caire, Ministre délégué à la Transformation numérique gouvernementale, à l'émission *Puisqu'il faut se lever* avec Louis Lacroix ce matin.

<https://www.985fm.ca/extraits-audios/faits-divers/238013/entrevue-avec-eric-caire>

- Gouvernement a identifié plus de 500 bases de données existantes
- Travaux de consolidation des données en cours
- Processus de catégorisation des données en cours
- Importance des mesures de sécurité physique et technologique
- Intention de recourir au cloud
- Données sensibles (20 %) seront en cloud privé avec contrôle des données
- Données non sensibles (80%) seront en cloud public
- Gouvernement actuellement en appel de qualification pour les fournisseurs selon les plus hauts standards



[REDACTED]

[www.hydroquebec.com](http://www.hydroquebec.com)

# Vol de renseignements personnels: une série noire appelée à se poursuivre

**Les systèmes de sécurité du gouvernement et des entreprises dépassés, selon des experts**



**JEAN-MICHEL GENOIS GAGNON**

Jeudi, 8 août 2019 00:00

MISE À JOUR Jeudi, 8 août 2019 00:00

Après le Mouvement Desjardins et Capital One, Revenu Québec a annoncé avoir été l'objet d'une fuite de données personnelles, et la série noire est loin d'être terminée, selon des experts. Ils jugent «dépassés» les systèmes et les mesures de sécurité du gouvernement.

Hier, l'agence a annoncé dans un communiqué que les renseignements personnels de 23 000 de ses employés, notamment des numéros d'assurance sociale, avaient fait l'objet d'une fuite.

### **Urgence**

Tout comme le fondateur du Groupe Vigiteck, l'expert en sécurité informatique Steve Waterhouse estime que le gouvernement devrait «rapidement» refaire ses devoirs pour mettre en place des mécanismes plus rigoureux afin de mieux protéger les données personnelles des citoyens.

«En peu de temps, les Québécois se sentent directement affectés par un manque de rigueur à l'intérieur de différentes organisations. Là, c'est le gouvernement du Québec qui est touché, dit-il. Au gouvernement, il y a encore des gens qui ne réfléchissent pas à la sécurité de façon omniprésente et constante. Cela donne ces résultats», ajoute-t-il.

Selon l'expert, après l'annonce de Desjardins le 20 juin dernier, «Revenu Québec aurait dû mettre en place des changements radicaux pour éviter ce genre d'incident. Je crois que l'agence n'a pas fait ses devoirs», poursuit-il.

- **ÉCOUTEZ Mathieu Fortier, conseiller financier, à l'émission *Avocats à la barre*, à QUB radio:**

Chez Revenu Québec, on souligne que des changements concernant les mesures de sécurité à l'interne ont été apportés au cours des dernières semaines, notamment concernant l'accès des clés USB non sécurisées. Un comité a aussi été mis sur pied en juin afin de discuter des procédés en matière de sécurité.

### **Des cas récents**

- Le 20 juin, le Mouvement Desjardins a été victime d'une fuite à l'interne. Au total, 2,9 millions de membres et d'entreprises ont été touchés.
- Le 29 juillet, un vol de données personnelles chez Capital One a touché 106 millions de clients, dont 6 millions au Canada.



***En vedette  
cette semaine***

**ÉCOUTEZ NOS SÉRIES BALADOS**

Publié le 07 août 2019 à 16h03 | Mis à jour le 07 août 2019 à 16h30

## Une demande d'action collective déposée contre Capital One



Capital One a indiqué que près de six millions de personnes au Canada auraient été touchées par la brèche de sécurité et qu'un million de numéros d'assurance sociale figuraient parmi les informations confidentielles divulguées.

PHOTO JOHANNES EISELE, ARCHIVES AGENCE FRANCE-PRESSE

La Presse Canadienne  
Toronto

Un cabinet d'avocats ontarien a déposé une demande d'action collective au nom des Canadiens touchés par l'énorme vol de données dévoilé par Capital One le 30 juillet.

La poursuite de Diamond & Diamond réclame une indemnisation pour les Canadiens ayant demandé des cartes de crédit à Capital One entre 2005 et 2019.

« Ce vol de données pourrait avoir des conséquences très graves pour les personnes concernées en ce qui concerne leurs finances futures », a affirmé Jeremy Diamond, associé directeur du cabinet, dans un communiqué.

La demanderesse principale est Rina Del Guidice, de Bolton, en Ontario. Elle a obtenu une carte MasterCard du détaillant Costco

auprès de Capital One.

La poursuite note que Capital One exploitait également des cartes de crédit proposées par d'autres marchands, notamment la Compagnie de la Baie d'Hudson.

Darryl Singer, l'avocat principal du cabinet pour cette poursuite, a indiqué dans une déclaration que les informations volées pourraient constituer un risque de vol d'identité pendant des années.

« Ce qui rend cette brèche si choquante, c'est qu'elle comprend des informations d'identification telles que le nom d'une personne et son numéro d'assurance sociale, qui ne peuvent pas être modifiées. »

La déclaration demande que la poursuite soit certifiée en tant qu'action collective et réclame plus de 350 millions en indemnisation financière et autres formes de réparation pour les plaignants.

Capital One a indiqué que près de six millions de personnes au Canada auraient été touchées par la brèche de sécurité et qu'un million de numéros d'assurance sociale figuraient parmi les informations confidentielles divulguées.

La brèche a également révélé les données d'environ 100 millions de clients américains, dont environ 140 000 numéros d'assurance sociale et 80 000 numéros de comptes bancaires liés.

Capital One a précisé qu'elle commencerait à informer les Canadiens touchés par la violation cette semaine par l'entremise de lettres ou de courriels, mais pas par appel téléphonique.

Le Commissariat à la protection de la vie privée du Canada a indiqué la semaine dernière qu'il avait ouvert une enquête sur le vol de données.