Assurance responsabilité professionnelle Barreau

PRÆVENTIO

Août 2023 | Volume 24 | Nº 4

Ce que tu décides de ne pas faire est tout aussi important que ce que tu décides de faire.
Steve Jobs

Service de Prévention

Judith Guérin, avocate
aux activités de prévention

Aurélie Lompré, avocate
aux activités de prévention

Votre mot de passe est-il robuste?

Nous connaissons tous l'importance d'avoir des mots de passe robustes, mais nous négligeons cela trop souvent.

À l'ère du numérique, nos ordinateurs contiennent nos dossiers, nos courriels, nos données personnelles, celles de nos clients ainsi que de nombreuses autres informations privilégiées et confidentielles.

Du fait de ses obligations professionnelles et déontologiques, l'avocat doit assurer la confidentialité des renseignements concernant le client, ses affaires et ses activités en lien avec la relation professionnelle[1].

Afin d'éviter des tentatives d'accès non autorisé à votre ordinateur, ce dernier est-il protégé par un mot de passe adéquat? Quant à vos accès en ligne, détenez-vous des mots de passe suffisamment robustes pour résister aux potentielles attaques de cybercriminels?

La plupart d'entre nous cherchent des mots de passe faciles à retenir. Certains vont jusqu'à utiliser le même mot de passe pour différents accès.

Or, si le mot de passe aisément mémorisable contient des informations personnelles, telles que le nom de nos enfants, de nos animaux de compagnie ou le lieu de nos dernières vacances, celui-ci sera facile à trouver. Par exemple, « pensez au nombre de fois où vous avez publié des photos de votre chien ou d'articles y faisant référence sur les réseaux sociaux.[2]»

Par conséquent, si un même mot de passe utilisé pour accéder à différents comptes est découvert par un cybercriminel, ce dernier pourrait l'utiliser à plusieurs reprises afin de pirater ces différents comptes!

---

[1] Voir notamment les articles 60 à 70 du *Code de déontologie des avocats,* RLRQ, c. B-1, r.3.1.

[2] *Votre mot de passe est-il suffisamment robuste? Voici cinq façons de l'évaluer*, Pensez cybersécurité, Gouvernement du Canada, 15 janvier 2020 : https://www.pensezcybersecurite.gc.ca/fr/blogues/votre-mot-de-passe-est-il-suffisamment-robuste-voici-cinq-facons-de-levaluer

Voici quelques suggestions relativement aux mots de passe :

- Si votre mot de passe est compromis ou découvert, changez-le immédiatement;
- Ne divulguez jamais votre mot de passe;
- Créez un mot de passe distinct pour chacun de vos comptes;
- Choisissez des mots de passe neutres (aucune information personnelle);
- Utilisez un gestionnaire de mots de passe sécurisé. N'écrivez pas vos mots de passe dans un calepin physique qui risque de se perdre, voire de tomber dans de mauvaises mains;
- Un mot de passe long est plus difficile à déchiffrer : favorisez une phrase plutôt qu'un mot « une phrase de passe est un amalgame de mots disparates qui n'ont de sens que pour vous. Idéalement, une phrase de passe est constituée d'au moins quatre mots et au moins 15 caractères. »[3]
- Différents caractères doivent se retrouver dans le mot de passe : majuscules, minuscules, chiffres, symboles. De plus, un indice peut vous aider à retrouver votre mot de passe en cas d'oublis. Par exemple, l'indice pourrait être « Fonds » et le mot de passe : @$$uranceRepons@b!l!té#2023 (= Assurance Responsabilité 2023);
- Changez régulièrement (chaque mois[4]) votre mot de passe;
- Favorisez la double authentification, si possible;
- Mettez en place une procédure interne à votre cabinet quant à la création et à la gestion de mots de passe afin de vous assurer d'une sécurité additionnelle[5].

Nos mots de passe sont une porte d'entrée donnant accès à des informations de grande valeur, il est primordial de protéger celles-ci en adoptant des mesures adéquates.

En effet, le 10 mars 2022, Statistique Canada indiquait qu' « environ un cinquième (21 %) des entreprises canadiennes ont déclaré avoir été touchées par des incidents de cybersécurité en 2019. La même année, les entreprises canadiennes ont déclaré avoir dépensé un total de 7 milliards de dollars directement en mesures visant à empêcher, à

---

[3] *Supra*, note 1.
[4] « Guide des TI Gestion et sécurité des technologies de l'information pour l'avocat et son équipe », Barreau du Québec, mise à jour en janvier 2016, p.7 : https://www.barreau.qc.ca/media/2331/guide-ti.pdf
[5] "Password Security Tips", Lawyers Mutual Liability Insurance Company of North Carolina : https://nmcdn.io/e186d21f8c7946a19faed23c3da2f0da/556712d9bf0f4cb2a916cc810687d52b/files/risk-management-resources/articles/Password-security.pdf

détecter et à se remettre de tels incidents.[6] » Malheureusement, ces chiffres n'ont cessé de croître au cours des dernières années.

En conclusion, prenons les mesures nécessaires pour gagner la course contre les tentatives d'accès non autorisé à nos divers comptes et ordinateurs : À vos mots de passe, prêts, partez!

[6] *Les risques liés à la cybersécurité ont des répercussions sur les entreprises canadiennes*, Statistique Canada, 10 mars 2022 : https://www.statcan.gc.ca/o1/fr/plus/514-les-risques-lies-la-cybersecurite-ont-des-repercussions-sur-les-entreprises-canadiennes