

Montréal, le 24 novembre 2022.

À tous nos clients(es),

Nous avons été victimes d'une cyberattaque impliquant l'accès non autorisé à notre serveur informatique. Après vérification par nos experts des dommages et du degré d'intrusion, il semble que la totalité du contenu de notre serveur soit encryptée via un rançongiciel.

Nous tentons actuellement de récupérer nos données historiques sur nos disques de sauvegarde.

Pendant que nous travaillons à résoudre cette situation, nous avons mis en place des mesures pour redémarrer nos opérations en toute sécurité :

- Nous avons embauché des consultants spécialistes en cybersécurité pour nous proposer des mesures additionnelles afin de protéger davantage nos systèmes informatiques;
- Nous avons vérifié chacun de nos postes de travail pour éliminer les virus actuels et en dormance;
- Nous procédons au renforcement de nos systèmes informatiques pour éviter de futurs incidents;
- Nous sommes présentement à reconstruire les dossiers qui ont été endommagés;
- Nous avons fait appel aux autorités policières, qui font présentement enquête;
- Nous avons avisé la Commission d'accès à l'information du Québec;
- Nous avons avisé notre Ordre professionnel et nos assureurs.

Par souci de transparence et comme l'exige la réglementation concernant la protection de la vie privée, nous faisons cette annonce pour vous informer de notre situation.

Même si nous avons pris des mesures au cours des dernières années pour renforcer la sécurité de notre parc informatique, ceci nous rappelle que nous devons toujours avoir une longueur d'avance sur le cybercrime, qui est devenu un enjeu omniprésent

mondialement et ce, dans tous les secteurs d'activités et peu importe la taille des entreprises visées.

Afin d'éviter que de mauvaises mains accèdent à vos données, nous vous suggérons de changer immédiatement vos mots de passe sur vos applications, notamment l'accès à votre ordinateur, vos mots de passe à la banque et aux gouvernements.

Et s'il vous plait, rappelez-vous de continuer à suivre les consignes importantes de protection de vos ordinateurs et de leur contenu, notamment :

- N'ouvrez pas les courriels dont vous ne connaissez pas la provenance;
- Ne communiquez jamais d'informations sensibles à un étranger;
- Soyez prudent en cas de courriels inhabituels et évitez l'ouverture de pièces jointes rattachées à ces courriels; Utilisez un antivirus et un antipourriel (antispam) et maintenez vos systèmes et applications à jour;
- Utilisez des mots de passe différents et complexes et modifiez-les régulièrement;
- Augmentez votre niveau de sécurité, par exemple en utilisant l'application de l'authentification à deux facteurs (Multi-factor solutions «MFA»);
- Consultez des spécialistes en cybersécurité afin de vous donner les meilleurs conseils pour votre sécurité.

Soyez assurés que nous prenons cette situation très au sérieux. Si vous avez des inquiétudes face à cette situation, contactez-nous pour en discuter.

Cordialement,

Les associés de Beaudoin Doray Tremblay S.E.N.C.R.L.

Montreal, November 24, 2022.

To all our clients,

We were victims of a cyberattack involving unauthorized access to our computer server. After verification by our experts of the damage and the degree of intrusion, it seems that the entire content of our server is encrypted through a ransomware.

We are currently attempting to recover our historical data from our backup discs.

While we work to resolve this situation, we have put measures in place to safely restart our operations:

- We hired consultants specializing in cybersecurity to suggest additional measures to further protect our computer systems;
 - We checked each of our workstations for current and dormant viruses;
 - We are strengthening our IT systems to avoid future incidents;
 - We are currently rebuilding the files that were damaged;
 - We called on the police authorities, who are currently investigating;
 - We have notified the Commission d'accès à l'information du Québec;
 - We have notified our Professional Order and our insurers.

For the sake of transparency and as required by privacy regulations, we are writing this letter to inform you of our situation.

Although we have taken steps in recent years to strengthen the security of our IT infrastructure, this reminds us that we must always be one step ahead of cybercrime, which has become a pervasive issue worldwide and in all sectors of activity, regardless of the size of the companies targeted.

In order to prevent from accessing your data, we suggest that you immediately change your passwords on your applications, in particular the password allowing access to your computer, as well as your bank and government passwords.

And please remember to continue to follow important guidelines to protect your computers and their contents, including:

- Do not open emails of which you do not know the source;
- Never give sensitive information to a stranger;
- Be cautious of unusual emails and avoid opening attachments in such emails; Use antiviruses and antispam and keep your systems and applications updated;
 - Use different and complex passwords and change them regularly;
- Increase your level of security, for example by using the application of two-factor authentication (Multi-factor solutions “MFA”);
 - Consult cybersecurity specialists to give you the best advice for your security.

Be assured that we are taking this situation very seriously. If you have any concerns about this situation, please contact us to discuss it.

Regards,

The partners of Beaudoin Doray Tremblay S.E.N.C.R.L.