AVIS DE NOTIFICATION D'UN INDICENT DE SÉCURITÉ

Nous tenons à vous informer d'un incident de sécurité impliquant la protection de renseignements personnels. Si vous êtes un usager du CISSS de la Montérégie-Centre et que vous avez reçu des soins ou des services entre le mois de janvier 2021 et le mois de mai 2023 et que vous avez été sollicité pour effectuer un don à la Fondation de l'Hôpital Charles-LeMoyne, cette communication vous concerne.

Que s'est-il passé? Unimarketing est une entreprise québécoise qui offre des services téléphoniques et d'hébergement informatique pour des partenaires d'affaires. Un de ses clients, Unicause, fournit des services à différentes organisations dans le cadre de mandats d'accompagnement en philanthropie et de campagnes de financement. C'est dans le cadre d'un mandat de publipostage pour une sollicitation de dons que certains renseignements personnels concernant des usagers de l'Hôpital Charles-Le Moyne ont été transmis à Unicause.

Le 8 août 2023, Unimarketing a détecté un bris de sécurité qui a touché ses systèmes informatiques. Grâce à l'assistance d'experts indépendants en cybersécurité et d'un prestataire de services informatiques, nous avons pu rapidement maîtriser la situation, enquêter et évaluer la sécurité de notre nouvelle infrastructure mise en place depuis l'événement.

Nous avons toutefois été informés le 22 décembre 2023 qu'un nombre important de fichiers avait été compromis. Lorsqu'ils ont pu être récupérés, nous avons entrepris un examen approfondi des fichiers concernés, dont la première phase s'est complétée au mois d'avril 2024. Il a été déterminé que des renseignements personnels étaient contenus dans certains des fichiers concernés.

Quels renseignements sont concernés? Les renseignements personnels qui ont été identifiés comprennent une combinaison de ce qui suit: nom, prénom, coordonnées, âges et le département de l'Hôpital Charles-LeMoyne consulté.

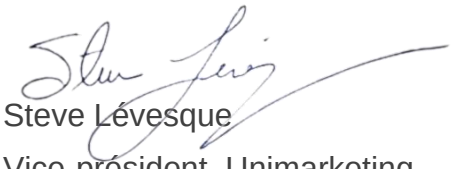
Que faisons-nous? Nous prenons cet événement et la sécurité des renseignements personnels qui nous sont confiés très au sérieux. Dès que nous avons eu connaissance de l'activité suspecte, nous avons immédiatement débuté une enquête externe et pris les mesures nécessaires afin d'y remédier. Les mesures prises dans le cadre de l'enquête ont notamment consisté à évaluer et à sécuriser notre réseau informatique, reprendre les activités, examiner les fichiers concernés et à informer les clients impliqués. Dans le cadre de notre engagement continu envers la protection de la vie privée et la sécurité de notre environnement, nous révisons également nos politiques et procédures internes. Enfin, l'évènement a déjà été rapporté à la Commission d'accès à l'information du Québec et au Commissaire à la protection de la vie privée du Canada.

Que pouvez-vous faire? Alors que nous n'avons aucune indication de fraude ou de vol d'identité découlant de cet événement, nous encourageons les personnes concernées à demeurer vigilantes contre les incidents de fraude par la réception de courriels ou d'appels téléphoniques suspects. Toute activité suspecte doit être rapidement signalée aux autorités concernées.

Pour plus d’informations. Si vous avez des questions additionnelles ou avez besoin d’assistance, veuillez communiquer avec un membre de notre équipe au 1-833-615-1421 ou par courriel à renseignements@unimarketing.ca.

Nous regrettons sincèrement tout inconvénient que cela pourrait causer.

Sincèrement,



Steve Lévesque

Vice-président, Unimarketing