

Questions et réponses : Incident de cybersécurité d'août 2026

Le présent document fournit des informations supplémentaires sur l'incident de cybersécurité du 18 août ainsi que des conseils aux employés. Il sera mis à jour au fur et à mesure que de nouvelles informations seront disponibles.

À propos de l'incident

Que s'est-il passé?

Le 18 août 2026, SCS a subi un accès non autorisé à ses systèmes informatiques et leur chiffrement. Nous avons immédiatement pris des mesures pour contenir la menace, rétablir l'accès à nos systèmes et engager des spécialistes indépendants de la cybersécurité pour mener une enquête.

Qu'a révélé l'enquête?

L'enquête a confirmé qu'un tiers non autorisé a accédé aux systèmes de SCS et en a chiffré les données.

L'enquête n'a pas permis de déterminer si ce tiers a eu accès aux renseignements personnels des clients. Bien qu'il n'existe aucune preuve que les renseignements des clients ont été consultés, copiés ou utilisés à mauvais escient, nous ne pouvons pas complètement exclure un accès potentiel aux dossiers individuels et aux renseignements associés sur les clients.

Des renseignements personnels ont-ils été utilisés à mauvais escient?

Nous n'avons aucune preuve que les informations des clients ont été utilisées à mauvais escient. Cependant, l'enquête n'a pas pu exclure un accès potentiel aux renseignements des clients.

Que fait SCS pour éviter un autre incident?

Nous avons constitué une équipe spécialement chargée de gérer l'incident, composée d'experts internes et externes. Nous sommes en train d'examiner nos systèmes et de mettre en œuvre des mesures de sécurité supplémentaires afin de réduire le risque qu'un incident semblable se produise.

Impact sur les clients et les familles

Pourquoi informons-nous les clients et les familles?

Nous informons les clients et les familles par mesure de précaution et dans un souci de transparence.

Bien que l'enquête n'ait pas pu confirmer que les renseignements sur le client avaient été consultés, elle n'a pas non plus pu exclure cette possibilité. Nous voulons que tout le monde soit au courant de l'incident et prenne les précautions appropriées.

Des renseignements personnels spécifiques ont-ils été volés?

L'enquête n'a pas révélé de preuve que les renseignements sur les clients avaient été consultés, copiés ou utilisés à mauvais escient. Cependant, il n'a pas été possible d'exclure que certains renseignements personnels aient pu être consultés. C'est pourquoi SCS informe les clients et les familles par mesure de précaution.

Quelles précautions puis-je prendre pour protéger mes renseignements personnels?

Bien que nous n'ayons aucune preuve d'une utilisation à mauvais escient des renseignements personnels, nous vous encourageons à :

- **Surveiller les communications suspectes** : soyez prudent face aux demandes inattendues de renseignements personnels ou financiers.
- **Protéger vos mots de passe** : utilisez des mots de passe robustes et uniques, et activez l'authentification multifacteur si elle est offerte.
- **Surveiller les comptes financiers** : vérifiez si des transactions inhabituelles ont été effectuées et signalez-les à votre institution financière.
- **Évitez les liens suspects** : ne cliquez pas sur des liens et n'ouvrez pas les pièces jointes provenant de sources inconnues.
- **Signaler les préoccupations** : communiquez avec ITsecurity@scsonline.ca si vous remarquez une activité suspecte de la part de SCS.

Informations supplémentaires

L'incident a-t-il été signalé aux autorités compétentes?

SCS a informé le commissaire à l'information et à la protection de la vie privée de l'Ontario de cet incident.

Où puis-je obtenir plus d'informations?

Pour toute question concernant l'incident, veuillez communiquer avec ITsecurity@scsonline.ca.