

Saint-Ouen, le 17 mars 2023

Information importante

Chère Madame, Cher Monsieur,

Malgré les mesures de sécurité mises en place et une vigilance constamment accrue en matière de cybersécurité, l'Espace Numérique de Travail (« l'ENT ») de la Région Ile-de-France a été victime d'une intrusion malveillante qui a conduit à un incident de cybersécurité. L'attaquant a eu accès et a extrait des données de l'annuaire de l'ENT ;

Il en résulte qu'un tiers non autorisé a pu accéder à des données personnelles vous concernant (notamment email, date de naissance, adresse, numéro de téléphone) et qu'il pourrait les utiliser à des fins d'usurpation d'identité, de tentative d'hameçonnage (phishing), de prospection commerciale non sollicitée, de démarchage à domicile.

Dès la connaissance de ces faits, la Région Ile-de-France, en lien avec les autorités académiques, a demandé à ses prestataires de prendre toutes les mesures techniques permettant de sécuriser le système d'information. Elle a également fait appel aux services d'experts indépendants afin qu'ils procèdent à toutes les investigations nécessaires.

La Région Ile-de-France a déposé une plainte auprès du procureur de la République et se tient à la disposition des services enquêteurs.

Conformément à ses obligations en matière de protection des données personnelles, la Région a également notifié la violation de données à la Commission nationale de l'informatique et des libertés (Cnil), qu'elle tient informée des évolutions de la situation.

Nous vous rappelons les recommandations de vigilance pour se prémunir de toute utilisation frauduleuse de vos données personnelles :

- rester attentif et vigilant en cas de réception de courriels, SMS ou d'appels inhabituels, y compris lorsqu'ils ont l'apparence d'un expéditeur ou émetteur officiel ;
- ne jamais fournir d'informations confidentielles (bancaires, mots de passe etc.) ;
- faire preuve de vigilance si le ton du message ou de votre interlocuteur est pressant, qu'il vous pousse à l'action ;
- ne pas ouvrir la ou les pièces jointes ou les liens hypertextes d'un courriel ou SMS suspect ;
- changer vos mots de passe au moindre doute ;
- disposer de mots de passe suffisamment longs et complexes sur tous les services que vous utilisez, et en activant si possible une double authentification.

Si vous pensez être victime d'une utilisation frauduleuse de vos données, vous pouvez consulter le site : cybermalveillance.gouv.fr et déposer plainte auprès d'un commissariat de police ou d'une brigade de gendarmerie.

De manière générale, vous pouvez signaler aux autorités judiciaires tout élément suspicieux que vous estimeriez être en lien avec cette attaque.

Pour toute question complémentaire, nous vous invitons à contacter notre Délégué à la protection des données à l'adresse email suivante : dpo@iledefrance.fr.

Nous regrettons sincèrement le désagrément que cet incident pourrait occasionner et mettons tout en œuvre pour en limiter les conséquences pour chacun.

Nous vous prions de croire, Chère Madame, Cher Monsieur, en l'assurance de notre considération distinguée.

David BONNEAU
Directeur Général des Services
Région Ile-de-France

A stylized, handwritten signature in black ink, consisting of a large, flowing 'D' followed by a smaller, more complex mark.

Stéphanie VELOSO
Secrétaire Générale de la région
académique Ile-de-France

A stylized, handwritten signature in black ink, featuring a large, bold 'S' followed by a series of fluid, connected strokes.