

**Incident billetterie en ligne Théâtre
Information à destination des personnes concernées**

Madame, Monsieur,

Le 28 juin 2024, notre prestataire de billetterie en ligne SIRIUS nous a informé avoir été victime d'un piratage informatique.

Bien que l'incident soit à présent terminé et la menace levée, certaines de vos données personnelles pourraient avoir été récupérées à des fins malveillantes, entraînant une perte de confidentialité.

Les catégories de données potentiellement impactées sont les suivantes

- Votre nom.
- Votre prénom.
- Votre adresse email.
- Votre numéro de téléphone.
- Votre adresse postale.
- Votre mot de passe de connexion si vous avez créé un compte sur l'espace de vente en ligne.

Les coordonnées bancaires ne sont quant à elles pas concernées.

Les données subtilisées pourraient être utilisées afin de vous contacter par mail, par SMS ou téléphone, notamment à des fins d'hameçonnage (phishing). Elles pourraient également permettre une usurpation d'identité.

Conformément au Règlement Général sur la Protection des Données (RGPD), une notification de violation a déjà été réalisée auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Mesures prises pour remédier à l'incident et atténuer ses effets négatifs

Dès connaissance de l'attaque, tout a été mise en œuvre afin d'en limiter les risques :

- une réinitialisation immédiate de l'ensemble des mots de passe des utilisateurs a été réalisée
- le fichier de configuration ayant fuité a été modifié afin de ne faire apparaître qu'un historique et un mot de passe fictif
- la configuration de l'accès à la base de données a été modifiée afin que les anciennes informations de connexion (identifiant et mot de passe) ne soient plus visibles en clair.
- le code d'accès à la base de données n'est plus enregistré en clair : ce code est désormais chiffré.

Personne à contacter

Pour toute information complémentaire relative la gestion de vos données personnelles, il vous est possible de joindre notre référente par mail sur dpo@ville-poissy.fr ou par courrier à l'adresse suivante : Hôtel de ville, Place de la République, 78300 Poissy.

Recommandations

Suite cet incident, nous vous rappelons également les bonnes pratiques à adopter pour protéger au mieux vos données personnelles.

Pour rappel, les données les plus communément collectées sont celles concernant l'identité : noms, prénoms, date de naissance.

Ainsi, pour tout compte utilisateur nécessitant des identifiants de connexion, pensez à changer votre mot de passe et à vérifier l'exactitude de vos informations personnelles.

Pour vous prémunir de l'hameçonnage

- Vérifiez que le mail vous est réellement destiné.
- Portez attention à l'adresse de l'expéditeur. Faites attention aux expéditeurs inconnus, ou connus mais suspects.
- Soyez attentif au niveau de langage du mail et aux fautes d'orthographe.
- Ne cliquez sur aucun lien présent dans le mail.
- Ne transmettez aucune information à caractère confidentiel par mail (coordonnées bancaires, numéro de sécurité sociale).

Pour vous prémunir d'une usurpation d'identité

- Rendez-vous sur le site cybermalveillance.gouv.fr pour obtenir des conseils.
- Déposez plainte au plus vite auprès d'un commissariat de police ou de gendarmerie.
- Consultez les recommandations de la CNIL « [Comment réagir face à une usurpation d'identité ?](#) ».