



Avis d'information

Incident de sécurité concernant des données personnelles

1. Que s'est-il passé ?

Un de nos prestataires nous a informé qu'il avait fait l'objet d'un incident de sécurité ayant entraîné un accès non autorisé à notre base de données clients.

2. Quelles sont les données concernées ?

Les catégories de données susceptibles d'avoir été exposées sont les suivantes : nom, prénoms, date de naissance, adresse e-mail, numéro de téléphone, adresse postale, numéro de carte de fidélité et solde de points de fidélité

Aucune donnée bancaire (carte bancaire, RIB), ni aucun mot de passe n'ont été impactés.

Vos points de fidélité restent disponibles sur votre compte.

3. Quelles peuvent être les conséquences pour vous ?

Les données concernées pourraient être utilisées par des personnes malveillantes :

- Pour personnaliser des tentatives de fraude ou d'hameçonnage (« phishing »), notamment
- Par e-mail, SMS, courrier ou téléphone, en se faisant passer pour notre enseigne ou pour un autre organisme connu.
- Pour se faire passer pour vous auprès de tiers ou faciliter le contournement de procédures de vérification d'identité.
- Pour recouper ces informations avec des données provenant d'autres fuites déjà en circulation.

3. Quelles sont les mesures prises par notre enseigne

Dès la prise de connaissance de l'incident :

- Le sous-traitant concerné a immédiatement corrigé la vulnérabilité et renforcé la sécurité de ses accès.
- Une investigation technique approfondie a été menée avec le concours d'experts en cybersécurité.
- La Commission Nationale de l'Informatique et des Libertés (CNIL) a été formellement notifiée dans le délai imparti.
- Nous avons procédé à l'analyse de l'incident et de ses conséquences afin d'identifier et mettre en œuvre les mesures nécessaires pour limiter les risques pour les personnes concernées.

4. Nos conseils et recommandations

Nous vous recommandons d'appliquer les consignes de prudence suivantes :

- **Vigilance face aux démarchages** : méfiez-vous des e-mails, SMS, courriers ou appels téléphoniques suspects se réclamant de notre enseigne ou de tout autre organisme.
- **Ne communiquez aucune donnée sensible** : notre enseigne ne vous demandera **jamais** vos identifiants, codes d'accès ou coordonnées bancaires par téléphone ou par e-mail.
- **Vérifiez les expéditeurs** : avant de cliquer sur un lien dans un e-mail ou un SMS, vérifiez attentivement l'adresse de l'expéditeur et le nom de domaine.

5. Nous contacter

Notre Délégué à la Protection des Données (DPO) est votre point de contact pour toute question relative à l'incident, à ses conséquences ou plus généralement à la protection de vos données personnelles. Vous pouvez le contacter :

- Par courrier électronique : dpo@groupe-novi.com
- Par courrier postal : NOVI – Délégué à la protection des données, 1 rue des Lys, ZAC Astier Val – CS30040 – 24110 Saint Astier
- Par téléphone : 06 59 66 03 26