Dernière mise à jour le 22 mars 2024

France Travail : la CNIL enquête sur la fuite de données et donne des conseils pour se protéger

France Travail a été victime d'une cyberattaque ayant conduit à une fuite de données susceptible de toucher 43 millions de personnes.

Quelles données personnelles sont concernées ?

Le 8 mars, France Travail (anciennement Pôle emploi) et Cap emploi ont informé la CNIL avoir été victime d'une intrusion dans leurs systèmes d'information. Cette attaque aurait potentiellement permis l'extraction de données de 43 millions d'usagers. Ce nombre, à confirmer, concerne les personnes actuellement inscrites sur la liste des demandeurs d'emploi ou qui l'ont été au cours des 20 dernières années, ainsi que des personnes ayant un espace candidat sur francetravail.fr.

Les données personnelles ayant fuité sont les noms et prénoms, les numéros de sécurité sociale, les identifiants France Travail, les adresses mail et postales ainsi que les numéros de téléphone.

Selon les informations dont dispose actuellement la CNIL, les mots de passe et les coordonnées bancaires ne sont pas concernés par cet acte de cyber malveillance.

Comment savoir si cette violation de données vous concerne ?

France Travail informera individuellement, dans les jours à venir, l'ensemble des personnes susceptibles d'avoir été touchées par cette fuite de données.

La CNIL n'est pas en mesure de vous indiquer si vous êtes concerné(e).

Que pouvez-vous faire si vous êtes concerné(e) par cette violation de données ?

Si vous êtes une personne concernée, la CNIL vous conseille :

- d'être particulièrement vigilant par rapport aux messages (SMS, mails) que vous pourriez recevoir, notamment s'ils vous invitent à effectuer une action en urgence, telle qu'un paiement ;
- ne communiquez jamais vos mots de passes ou coordonnées bancaires par messagerie ;
- si vous avez un doute, n'ouvrez pas les pièces jointes ; ne cliquez pas sur les liens contenus dans des messages qui vous invitent à vous connecter à un espace personnel ; accédez plutôt au site officiel correspondant directement via votre navigateur habituel ;
- vérifiez périodiquement les activités et mouvements sur vos différents comptes ;
- rendez-vous sur le site cybermalveillance.gouv.fr pour obtenir des conseils pour vous prémunir d'actions visant à usurper votre identité - le parquet de Paris a déjà ouvert une enquête, les personnes souhaitant faire un dépôt de plainte sont invitées à le faire par l'intermédiaire de cybermalveillance ;
- assurez-vous que vous utilisez, pour votre messagerie, vos comptes bancaires et autres services importants (impôts, sites

de commerce en ligne, etc.), des mots de passes suffisamment robustes.

Bien que, selon les informations dont la CNIL a actuellement connaissance, la fuite de donnée ne concernerait ni les mots de passe, ni des coordonnées bancaires, il est possible que les données ayant fait l'objet de la violation soient couplées, par des acteurs malveillants, à d'autres informations provenant de fuites de données antérieures. La vigilance est donc de mise, dans les prochains jours, mais aussi et surtout à plus long terme.

L'action de la CNIL

Devant l'ampleur de la violation, la présidente de la CNIL a décidé de mener très rapidement des investigations afin de déterminer notamment si les mesures de sécurité mises en œuvre préalablement à l'incident et en réaction à celui-ci étaient appropriées au regard des obligations du Règlement général sur la protection des données (RGPD).

Communiqué CNIL du 13 mars 2024.

https://www.legisocial.fr/dossiers-synthese/protection-donnees-rgpd.html »