

Diffusion de données piratées à la suite d'une cyberattaque : quels sont les risques et les précautions à prendre ?

26 septembre 2022

La CNIL constate une nette progression des notifications de violation de données dont près de la moitié résultent d'une attaque par rançongiciel. Dans certains cas, les données personnelles des usagers peuvent être mises en ligne par les pirates. La CNIL répond aux questions des personnes potentiellement concernées.

Vous êtes informé(e) que vos données ont été compromises et/ou mises en ligne

Si une violation vous concerne, l'organisme responsable doit vous en informer dans les meilleurs délais.

Lorsque la violation de données est susceptible d'engendrer un risque élevé pour les droits et les libertés, les organismes responsables ont l'obligation d'informer directement les personnes concernées du fait que leurs données ont été compromises et publiées en ligne. Cela peut être le cas si des [données de santé](#), par définition sensibles, ont été divulguées et en nombre important.

Le rôle de la CNIL est de s'assurer que cette communication est faite, dans les plus brefs délais, afin que les personnes concernées puissent prendre les précautions qui s'imposent.

La CNIL n'est cependant pas en mesure de vous dire si vos données sont impactées par une violation.

Attention : certains sites web indiquent détenir les données et pouvoir vous dire si vous êtes ou non concerné(e). La CNIL déconseille de les utiliser.

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

Les principaux risques

L'hameçonnage (phishing) ou l'usurpation d'identité

L'[hameçonnage](#) consiste à vous envoyer un courriel ou SMS frauduleux qui vous paraîtra plus réaliste du fait de l'utilisation des données récupérées grâce à la fuite de données (un soi-disant courriel de votre médecin ou de la sécurité sociale par exemple).

N'ouvrez surtout pas les pièces jointes, n'y répondez pas, ne consultez pas les liens et supprimez le message immédiatement. Pour [repérer une tentative d'hameçonnage](#) dans votre messagerie, et pour vous prémunir contre l'usurpation d'identité en ligne, soyez vigilants :

- vérifiez que le message/courriel vous est réellement destiné ;
- faites attention aux expéditeurs inconnus ;
- soyez attentif au niveau de langage du courriel ;
- vérifiez les liens dans le courriel ;
- méfiez-vous des demandes étranges et ne transmettez rien de confidentiel ;
- portez une attention particulière sur l'adresse de messagerie source.

Si vous pensez être victime d'une [usurpation d'identité](#) à la suite de la divulgation d'informations vous concernant, vous pouvez :

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

D'une manière générale, soyez vigilant lorsque vous saisissez des données sur le web ou lorsque vous recevez des courriels vous demandant de fournir ou de mettre à jour des données vous concernant.

Perte de confidentialité d'un mot de passe à la suite d'une fuite de données

Des mots de passe peuvent également être présents dans une fuite de données. Si vous êtes concerné(e), l'organisme devra vous en informer.

Afin de limiter les risques, et sans attendre cette information de l'organisme, vous pouvez adopter quelques gestes simples :

- **changez vos mots de passe** des services web que vous utilisez :
 - en [privilégiant des mots de passe forts](#) ;
 - en priorisant les services les plus importants (courriel, impôts, banques, sites de commerce en ligne, etc.) ;
- **évit**ez l'utilisation d'un même mot de passe pour différents services ;
- **utilisez** les [authentifications multifacteurs](#) quand elles vous sont proposées par des services de confiance (par exemple l'envoi d'un SMS à usage unique sur votre téléphone pour valider une connexion).

Comment la CNIL peut-elle vous accompagner ?

Si vous observez une utilisation frauduleuse de vos données, vous pouvez adresser une réclamation auprès de la CNIL afin que celle-ci intervienne auprès de l'organisme :

- soit sur le site internet de la CNIL :
 - dans certains cas déterminés, par le [téléservice de plainte en ligne](#) ;
 - dans les autres cas non prévus par le téléservice, par le service « [Besoin d'aide](#) ».
- soit par courrier postal en écrivant à : CNIL - 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07

Dans tous les cas, la CNIL n'est pas compétente pour accorder une indemnisation aux personnes ayant subi un préjudice.

Vous pouvez saisir les tribunaux civils qui statueront sur l'existence et l'évaluation de votre préjudice pouvant mener à indemnisation.

Le rôle de la CNIL en matière de cybersécurité

La CNIL accompagne les administrations et les entreprises dans la prise en compte de la sécurité informatique. L'obligation de sécurité, inscrite dans la loi depuis plus de 40 ans, a été renforcée par le RGPD et complétée de nouveaux outils comme [la notification des violations](#), [l'analyse d'impact sur la protection des données](#) ou [les codes de conduite](#).

Quelques chiffres

- + **79 %** de notifications de violation de données en 2021 par rapport à 2020 (5037 en 2021)
- + **de 2150 notifications** de violations résultant d'une attaque par rançongiciel reçues en 2021, soit 43 % du volume total
- **1/2 des sanctions** prononcées par la CNIL visent des manquements à l'obligation de sécurité des données

Texte reference

Pour approfondir

- > [Tous les contenus de la CNIL sur la cybersécurité](#)
- > [Spam, phishing, arnaques : signaler pour agir](#)
- > [Phishing : détecter un message malveillant](#)
- > [Comment réagir face à une usurpation d'identité ?](#)
- > [Les conseils de la CNIL pour un bon mot de passe](#)
- > [Comment lutter contre les spams par SMS ou MMS ?](#)
- > [Les chiffres sur la cybersécurité pour l'année 2021 \(PDF, 803 ko\)](#)