Exposition de 16 milliards d'identifiants et des mots de passe – que faire ?

20 juin 2025

Selon un média spécialisé en cybersécurité, 16 milliards d'identifiants et de mots de passe dérobés sont accessibles en ligne dans une même base. Ces données peuvent être utilisées pour faciliter des usurpations de comptes en ligne. La CNIL rappelle les bons réflexes à avoir.

Une base massive d'identifiants et de mots de passe

Selon le média spécialisé en cybersécurité Cybernews, 16 milliards d'identifiants et de mots de passe dérobés sont désormais accessibles en ligne. Cet ensemble de données serait constitué d'une agglomération de différentes fuites de données passées. Cela signifie qu'il ne s'agit pas d'une fuite de données nouvelle.

Concrètement, l'existence d'une base aussi massive d'identifiants ne change pas la nature des risques cyber auxquels sont déjà exposés tous les utilisateurs de services en ligne. Elle peut toutefois les accentuer. En effet, elle est susceptible de faciliter le travail des acteurs malveillants qui souhaitent attaquer un site ou usurper des comptes en essayant toutes les combinaisons connues, profitant du fait que beaucoup de personnes continuent d'utiliser les mêmes mots de passe et identifiants sur plusieurs services en ligne.

Comment réagir?

Afin de limiter ces risques, vous pouvez adopter quelques gestes simples :

- **soyez vigilants à l'activité de vos comptes les plus importants** (service de mail, espaces personnels sur des sites publics, site de e-commerce, etc.)
    - la plupart de ces services vous avertissent, souvent par mail, lorsque des connexions inhabituelles se produisent sur votre compte : soyez attentifs à de tels messages ;
    - plus généralement, soyez attentifs aux notifications que vous pourriez recevoir de sites en ligne (notification changement de mot de passe, d'adresse, de RIB, etc.).

      en cas d'événement suspect ou de doute, changez vos mots de passe pour les comptes concernés :

    - en privilégiant des mots de passe forts ;
    - en priorisant les services les plus importants (courriel, impôts, banques, sites de commerce en ligne, etc.) ;

- **évitez d'utiliser le même mot de passe pour différents services** et conservez-les dans un gestionnaire de mots de passe ;

- pour les services les plus importants et de confiance (mail, compte bancaire, etc.), **utilisez l'authentification multifacteur** quand elle vous est proposée (idéalement via une application dédiée sur votre téléphone ou, alternativement via, l'envoi d'un code à usage unique sur votre téléphone pour valider une connexion).
    - certains services vous proposent de reconnaître un de vos appareil comme étant « de confiance », ce qui ne remplace pas une authentification multifacteur mais peut contribuer à vous protéger.

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.

Bonne pratique : partager l'information, c'est protéger les autres

Si vous pensez qu'une **violation de données** peut concerner une personne de votre entourage (famille, amis, collègues), n'hésitez pas à :

- lui transmettre les points de vigilance de la CNIL ou d'autres autorités officielles ;
- lui indiquer des bons réflexes à avoir dans l'immédiat et au quotidien (par exemple : changer ses mots de passe, utiliser une authentification multifacteur lorsque cela est proposé).

Soyez vigilant concernant les personnes vulnérables, en particulier :

- celles n'ayant pas un accès quotidien ou aisé à Internet ;
- les personnes âgées ;
- ou encore celles courant un risque personnel du fait de la fuite de données (par exemple en cas de divulgation de l'orientation sexuelle, de l'opinion politique ou religieuse, d'un état de santé, etc.).

Texte de référence

- Le règlement général sur la protection des données (RGPD)