

Piratage de votre boîte mail, quelles peuvent être les conséquences sur votre vie personnelle

✕	Piratage de votre boîte mail, quelles peuvent être les conséquences sur votre vie personnelle
---	---

Votre boîte mail est souvent la clé qui permet d'accéder ou de vous inscrire aux services en ligne. Raison de plus pour la sécuriser au maximum !



Pour votre boîte mail : un mot de passe solide

Vous devez utiliser un mot de passe propre et unique pour vous connecter à votre webmail et surtout ne pas l'utiliser pour un autre compte.

Pourquoi c'est important ?

Utiliser le même mot de passe pour votre compte de messagerie et votre compte de réseau social est une pratique risquée. Si votre fournisseur de réseau social est victime d'une fuite de données comprenant vos moyens d'authentification, une personne mal intentionnée pourrait les utiliser pour non seulement accéder à votre compte de réseau social mais aussi pour accéder à votre messagerie.

De plus, une fois l'accès à votre messagerie obtenu, il deviendra possible de voir la liste des messages d'inscriptions à vos comptes sur différents sites (si vous ne les avez pas supprimés de votre boîte). Il sera ainsi possible de connaître certains de vos identifiants de compte et d'utiliser la fonction d'oubli de mots de passe pour en prendre le contrôle.

Cette absence de sécurité ou l'utilisation d'un mot de passe faible vous expose à des risques :

- Usurpation de votre boîte mail pour piéger votre liste de contacts ;
- Ajout d'une redirection de mail (souvent indétectable après la compromission d'une boîte mail) : vos emails continuent de fuiter malgré tout changement de mot de passe ultérieur...
- Connexion du pirate à vos sites et applications tierces ;
- Utilisation de vos coordonnées bancaires pour payer ;
- Usurpation d'identité grâce aux données collectées dans votre boîte mail ;
- Demande de rançon suite à des données compromettantes retrouvées dans votre boîte mail ;
- ...

[CONSEIL] – En parallèle d'un bon mot de passe :

- Il est déconseillé d'utiliser sa boîte mail en tant qu'espace de stockage, notamment pour les données qui peuvent vous paraître sensibles et notamment, les bulletins de paie, les justificatifs d'identité envoyés qui peuvent notamment contenir votre adresse postale personnelle, ou les mots de passe échangés en clair. Attention également aux photos qui permettent de vous ré-identifier sur des sites de réseaux sociaux et donnent la possibilité à une personne malveillante de se créer une fausse identité.
- Il convient de supprimer les emails reçus, envoyés ou enregistrés en tant que brouillon qui paraissent avoir une importance particulière ou de chiffrer les documents que vous mettez en pièce jointe.
- Enfin pour protéger votre identité, il est recommandé d'utiliser une boîte mail sous pseudonyme pour l'inscription à des services que vous jugez intrusifs, ou particulièrement sensibles (site de jeux concours, site de rencontre ...).

L'initiative

haveibeenpwned est un site conçu par Troy Int, informaticien indépendant. Il recense tous les mails compromis à l'occasion de fuite de données massive. L'utilisateur n'a qu'à entrer son email pour savoir s'il figure dans une base de données piratée et si ses mots de passes sont potentiellement entre les mains de personnes malveillantes.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous accompagner dans vos démarches de mise en conformité avec la réglementation Européenne relative à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus

d'informations

sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article