Que faire si un escroc a accès à votre adresse courriel

W. Perry Wortman ⁝

Alors que la cybercriminalité et les tactiques de phishing se perfectionnent, il est toujours possible qu'un escroc accède à votre adresse courriel et crée une situation dangereuse sur le plan de la sécurité, à laquelle vous devez réagir immédiatement.
Si un escroc a accès à votre adresse courriel, quelques mesures simples peuvent minimiser la perte potentielle de confidentialité et de sécurité.

Que peut faire un escroc avec votre adresse courriel ?
Les identifiants volés permettent à un pirate d'envoyer des messages malveillants ou des liens vers des logiciels malveillants à vos contacts, d'extraire des informations personnelles ou financières de vos messages enregistrés ou d'inciter vos amis et votre famille à lui envoyer de l'argent sous de faux prétextes.

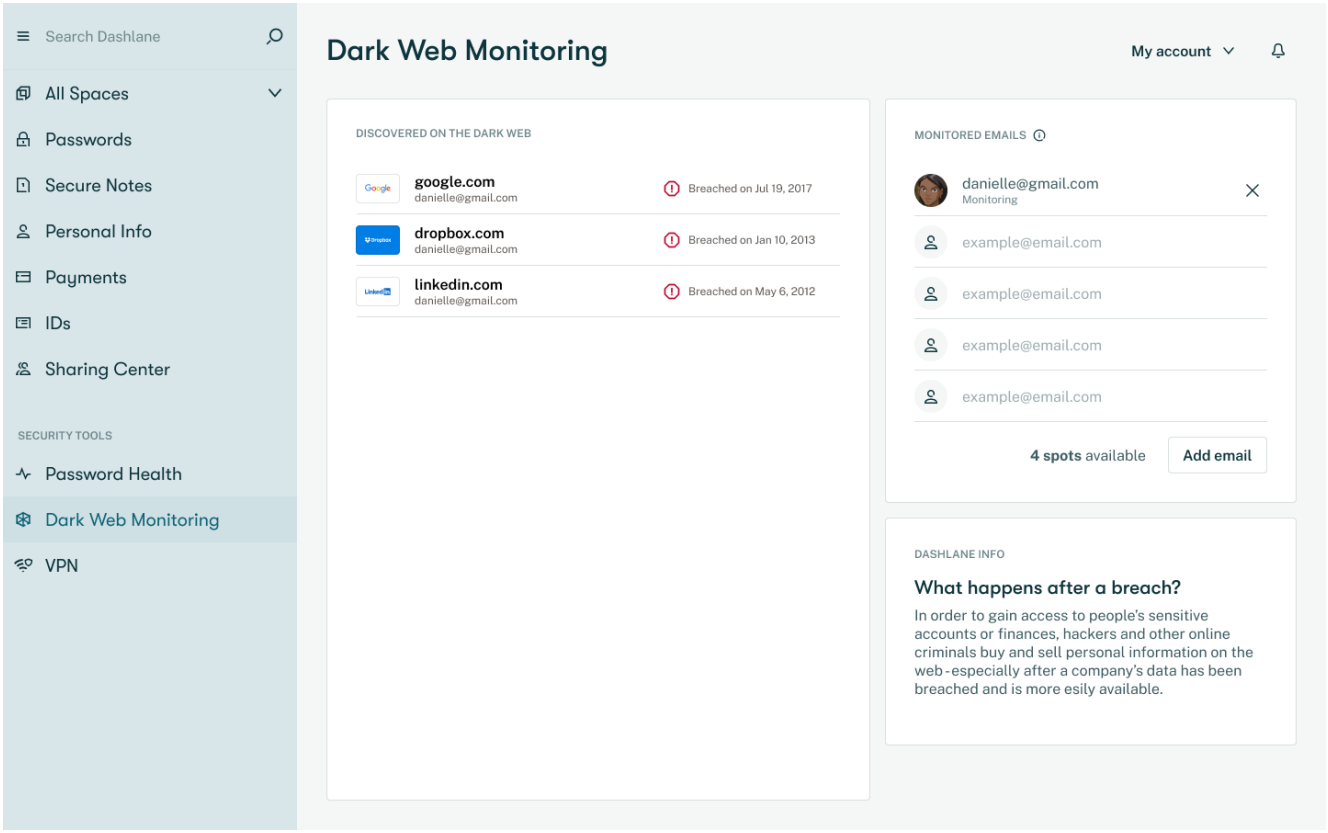
Voici quelques signes indiquant que votre compte de messagerie a été piraté :

- **Vous ne parvenez pas à vous connecter.**
  L'une des premières choses qu'un escroc peut faire s'il accède à votre compte de messagerie est de modifier votre mot de passe.
  Si vous êtes certain d'avoir saisi vos nom d'utilisateur et mot de passe correctement, et que vous ne parvenez toujours pas à vous connecter, cela pourrait vous mettre la puce à l'oreille.
- **Votre compte envoie des courriels que vous n'avez pas écrits.**
  Le réveil peut être brutal lorsqu'un contact ou un proche vous demande si vous lui avez envoyé un courriel qui ne lui semble pas familier.

Est-ce que ce courriel est une escroquerie ?

Si on vous rapporte que votre compte de messagerie envoie soudainement des liens mystérieux ou des messages indésirables (spam), il se peut qu'il ait été compromis.

- **Vos dossiers ont été vidés ou modifiés.**
  Votre fournisseur de messagerie ne supprime pas, ne déplace pas et ne réorganise pas les fichiers ou les messages enregistrés.
  Si vous remarquez un quelconque changement dans la structure de vos fichiers et que vous n'avez partagé le mot de passe de votre compte avec personne, il se peut qu'un pirate vous ait rendu visite.
- **Votre appareil se comporte de manière étrange.**
  Un compte courriel compromis ne provoquera pas à lui seul le ralentissement ou le comportement étrange de votre ordinateur ou de votre appareil.
  Cependant, un pirate peut avoir déjà installé un logiciel malveillant sur votre appareil pour accéder à votre compte de messagerie, ce qui pourrait expliquer la baisse de performance.
- **Vous recevez une alerte de sécurité.**
  Les employeurs, les fournisseurs d'accès à Internet et les applications de cybersécurité vous enverront souvent une alerte de sécurité si les informations de votre compte sont compromises.
  Il faut toujours prendre ces alertes au sérieux et changer immédiatement votre mot de passe si vous avez été victime d'une violation de données.
- **Vos informations apparaissent sur le dark Web.**
  Malgré votre vigilance, vous ne pouvez pas toujours vous rendre compte que votre compte de messagerie a été compromis.
  La surveillance du dark Web est un outil précieux qui scrute les moindres recoins d'Internet à la recherche de vos données personnelles et de vos identifiants.
  Par exemple, la fonctionnalité Surveillance du dark Web de Dashlane alerte immédiatement les abonnés si leur(s) mot(s) de passe ou leurs informations de compte sont détectés et doivent être modifiés.



Que faire si un escroc a accès à votre courriel ?

Lorsque votre compte courriel est compromis, cela signifie qu'un escroc y a accès.
Il pourrait déjà être en train d'envoyer des messages frauduleux ou des liens vers des logiciels malveillants à vos contacts.
Informez un maximum de vos contacts en utilisant une autre adresse courriel, par SMS ou par téléphone.
Une fois la menace immédiate maîtrisée, suivez les conseils suivants pour contrecarrer le pirate et minimiser son action :

1. **Ignorez-le s'il vous contacte**
   L'une des pires façons de réagir face à un escroc est d'entrer dans son jeu.
   Il peut essayer de vous contacter, même en utilisant votre propre adresse courriel, mais lui répondre ne mettra pas fin à son comportement et ne le découragera pas. Au contraire, toute réponse ne fera que confirmer un autre contact existant à exploiter.
   Veillez à marquer les courriels de l'escroc comme spam.
2. **Changez le mot de passe et les questions de sécurité de votre courriel**
   Changer ses mots de passe à intervalles prédéfinis n'est plus considéré comme une bonne pratique.
   Le NIST déconseille même ces réinitialisations périodiques, car les changements mineurs apportés aux mots de passe existants ont peu de valeur et sont facilement devinés par les pirates.
   Toutefois, si votre compte courriel a été compromis, vous devez changer votre mot de passe et vos questions de sécurité immédiatement.
3. **Vérifiez que votre appareil ne contient pas de logiciels malveillants**
   Toutes les modifications que vous apportez à votre compte n'ont que peu d'intérêt si votre appareil a été infecté par un logiciel malveillant.

Si vous n’avez pas encore installé de logiciel antivirus ou anti-malware, il est grand temps de le faire. Lancez dès que possible une analyse complète de votre système afin d’isoler et de supprimer tout fichier infecté.

4. **Signalez l’escroc à identitytheft.com**
   Les escrocs qui se cachent dans le cyberespace et changent fréquemment d’adresse peuvent être difficiles à repérer, mais il faut tout de même les signaler. Des services gratuits comme identitytheft.com vous aident à désactiver les comptes concernés, à vous inscrire à un service gratuit de surveillance du crédit et à apprendre comment signaler une adresse courriel frauduleuse.
5. **Créez une nouvelle adresse courriel**
   Pour être tout à fait sûr, vous pouvez suivre les étapes ci-dessus, puis repartir à zéro avec une toute nouvelle adresse courriel.
   Étant donné qu’une personne moyenne aux États-Unis possède entre 100 et 150 comptes liés à son adresse e-mail, vous devrez également les localiser et les mettre à jour.

Comment empêcher les escrocs d’accéder à votre courriel

Comme le dit le proverbe : mieux vaut prévenir que guérir.
La meilleure façon de gérer un compte de messagerie piraté est d’éviter qu’il ne le soit en premier lieu.
Ces conseils et astuces supplémentaires vous aideront à vous prémunir contre de futures violations :

- **Utilisez la double authentification ou l’authentification multifacteur**

La double authentification (2FA) renforce la sécurité de votre compte de messagerie en demandant un deuxième identifiant, tel qu'un code unique envoyé par le biais d'une application ou d'un SMS.
Cela peut ajouter quelques secondes à votre temps de connexion, mais il sera pratiquement impossible pour un escroc d'accéder à votre compte sans disposer de votre appareil.
L'authentification multifacteur (MFA) utilise deux ou plusieurs identifiants, parfois des facteurs biométriques tels que les empreintes digitales ou la reconnaissance faciale.

- **Vérifiez votre méthode de contact de secours**

La plupart d'entre nous ne pensent pas à leur adresse courriel de récupération ou à leur méthode de contact de secours et ne les mettent pas souvent à jour, voire pas du tout. Assurez-vous que l'adresse courriel et le numéro de téléphone que vous fournissez sont actifs et à jour.
Ces méthodes de sauvegarde deviennent importantes lorsque vous êtes bloqué sur votre compte et que vous devez réinitialiser votre mot de passe ou recevoir des alertes de sécurité.

- **Soyez attentif aux attaques d'hameçonnage (phishing)**

Comment les adresses courriel sont-elles piratées ?
Une attaque de phishing, qui prend souvent la forme d'un courriel non sollicité, est une tactique d'ingénierie sociale utilisée pour inciter les destinataires à partager leurs informations de compte ou leurs mots de passe.
Certaines contiennent également des liens vers des logiciels espions ou des enregistreurs de frappe (keyloggers) qui interceptent les communications privées.
Des fautes de grammaire ou d'orthographe, et des URL qui ne correspondent pas au site Web de l'entreprise peuvent être les signes d'une attaque d'hameçonnage (phishing), mais ces indications ne sont pas toujours présentes : les tactiques de phishing et d'ingénierie sociale sont de plus en plus perfectionnées.

- **Utilisez un gestionnaire de mots de passe**

Un gestionnaire de mots de passe protège tous vos comptes importants en chiffrant les mots de passe et les informations relatives à vos comptes, et en stockant vos données dans un coffre-fort sécurisé.
Vous pouvez ainsi déjouer les tactiques de piratage, telles que le credential stuffing, les attaques par force brute et le phishing, qui s'appuient sur des mots de passe de compte de messagerie trop faibles.
Un gestionnaire de mots de passe vous permet également d'enregistrer, de partager et de mettre à jour tous vos mots de passe les plus importants à partir d'une seule et même application sécurisée.

Comment Dashlane protège votre adresse courriel des escrocs

Dashlane offre une fonction de génération de mots de passe transparente qui permet de garantir que tous vos identifiants sont forts, uniques et à l'abri des pirates.
Un coffre-fort sécurisé chiffre et protège vos mots de passe, et l'architecture « zero knowledge » vous assure que personne, pas même Dashlane, ne peut accéder à vos informations.
Notre fonctionnalité de Surveillance du dark Web analyse les tréfonds d'Internet à la recherche de vos identifiants, y compris jusqu'à cinq adresses courriel, et vous alerte si vos mots de passe ou vos informations de compte sont détectés et doivent être changés.

Les conséquences d'un piratage, comme la compromission de comptes de messagerie et la présence de logiciels malveillants, sont parfois inévitables.
Nous avons rencontré un hacker « white hat » (l'un des gentils) pour savoir comment minimiser

l'impact de ces menaces.
Découvrez les propos de Rachel Tobac**.**

Références

1. Dashlane, « 6 Things a Safe Username Should Always Do », février 2023.
2. Dashlane, « 5 choses à savoir avant de partager vos mots de passe avec votre partenaire », février 2021.
3. Dashlane, « What the Hack Is Malware? », février 2020.
4. Dashlane, « What is a Security Alert ? » (Qu'est-ce qu'une alerte de sécurité), décembre 2019.
5. Dashlane, « Changez toujours vos mots de passe après une faille de données », mars 2020.
6. Dashlane « Percer l'obscurité du dark Web », juin 2022.
7. GovTech, « Hacked or Scammed ? », juillet 2022.
8. NetSec News, « Summary of the NIST Password Recommendations for 2021 » (Résumé des recommandations du NIST concernant les mots de passe pour 2021), novembre 2022.
9. Dashlane, "How Strong Is Your Password & Should You Change It?" août 2022.
10. Dashlane, « Résistez aux piratages grâce au générateur de mots de passe de Dashlane », 2023.
11. Dashlane, « Nom de jeune fille, film préféré… Du bon usage des questions de sécurité », septembre 2021.
12. Cybernews, « How to find all accounts linked to your email to protect your privacy » (Comment trouver tous les comptes liés à votre adresse e-mail pour protéger votre confidentialité), février 2023.
13. Dashlane, « Le guide de double authentification du débutant », août 2022.
14. Dashlane, « A Complete Guide to Multifactor Authentication », novembre 2022.
15. Dashlane, « 4 Steps to Secure Your Google and Gmail Accounts » (4 étapes pour sécuriser vos comptes Google et Gmail), novembre 2021.
16. Dashlane, « Pourquoi Dashlane ne vous demandera jamais d'identifiants dans un e-mail ? (parce qu'il s'agit là d'une technique d'hameçonnage) », novembre 2021.
17. Norton, « Spyware: What is spyware + how to protect yourself », décembre 2021.
18. Dashlane, « Password Management 101 » (Les bases de la gestion de mots de passe), 2023.
19. Dashlane, « Le credential stuffing, c'est quoi ? », septembre 2020.
20. Dashlane, « La sécurité avant tout : comment Dashlane protège vos données », janvier 2023.
21. Dashlane Dark Web Monitoring: Your Employees Are Likely Using Compromised Passwords », juillet 2022.
22. Dashlane, « You Asked, A Hacker Answered: 7 Questions With Rachel Tobac », octobre 2021.
23. Dashlane, « Top 8 Most Important Passwords to Change » (Les 8 mots de passe les plus importants à modifier), avril 2023.
24. CrowdStrike, « Keyloggers : How They Work and How to Detect Them » (Keyloggers : comment ils fonctionnent et comment les détecter), février 2023.
25. PCMag, « The Best Malware Removal and Protection Software for 2023 » (Les meilleurs logiciels de protection et de suppression des logiciels malveillants pour 2023), décembre 2022.

Recherche et mise en page par:
Michel Cloutier

CIVBDL
20231016
"C'est ensemble qu'on avance"