www.pcmag.com /how-to/how-could-a-data-breach-affect-me

Comment vous protéger contre les violations de données et planifier à l'avance

Un peu d'action préventive et beaucoup de bon sens peuvent vous aider à préserver votre vie privée après une fuite de votre courrier électronique suite à une violation de données.

Kim Key ⋮

Aucune entreprise n'est à l'abri d'une violation de données.
Vous participez sans doute d'une manière ou d'une autre à l'économie mondiale, *vous* n'êtes donc pas non plus en sécurité.
Les violations de données se produisent si souvent qu'elles font rarement l'actualité, en dehors d'actualités majeures comme la violation qui a touché des milliers d'employés de Sony , l' incident de sécurité de Mint Mobile en 2023, ou le géant Mother of All Breaches (MOAB) qui vient juste d'arriver. à la lumière au moment d'écrire ces lignes.
Le volume et la fréquence des violations de données sont légitimement effrayants, mais cela ne signifie pas que vous devez abandonner, refuser de changer et continuer à transmettre vos données privées sans combattre .

Nous sommes là pour vous expliquer les dangers des violations de données et ce que vous pouvez faire dès maintenant pour vous protéger contre la prochaine grande violation.

Pourquoi devriez-vous vous soucier de savoir qui détient vos données ?

Si les attaquants disposent de votre adresse e-mail et de votre mot de passe pour un site ou une application, ils peuvent détenir les clés d'une grande partie de votre vie, surtout si vous utilisez le même mot de passe pour tous vos comptes .
Vous devez vous soucier de l'apparition de vos données lors d'une violation de données, car de mauvais acteurs pourraient utiliser ces informations pour usurper votre identité et publier vos comptes privés .

“ "Ashley Madison ; c'était une sacrée violation de données...
C'est une affaire où des gens se sont suicidés à cause de cela." ”

Troy Hunt est le propriétaire de HaveIBeenPwned , une ressource de sécurité en ligne gratuite utilisée par de nombreux gestionnaires de mots de passe et suites de sécurité pour la surveillance du Dark Web.
Son site Web répertorie les violations de données au fur et à mesure qu'elles sont signalées et permet aux visiteurs de vérifier si leurs informations sont apparues dans l'une d'entre elles.
Hunt a déclaré : « Selon la nature des données, il peut s'agir d'informations que vous ne souhaitez tout simplement pas que d'autres personnes voient. »

Il a poursuivi : « Cela pourrait être quelque chose comme Ashley Madison ; c'était une sacrée violation de données.
Cela pourrait être quelque chose de très profondément personnel.
C’est un cas où des gens se sont suicidés à cause de cela.

À quelle fréquence les violations de données se produisent-elles ?

"Tous les jours. Plusieurs fois.
Chaque jour, sans aucun doute.

Alors qu'il me parlait au téléphone depuis son domicile à Brisbane, en Australie, Hunt a déclaré qu'il venait de terminer le traitement de 545 comptes piratés ce matin-là à partir de rapports de nuit, et qu'il lui restait au moins autant à publier sur son site Web ce jour-là.
Il est l'une des rares personnes au monde à avoir une idée du volume et de la fréquence des violations de données .

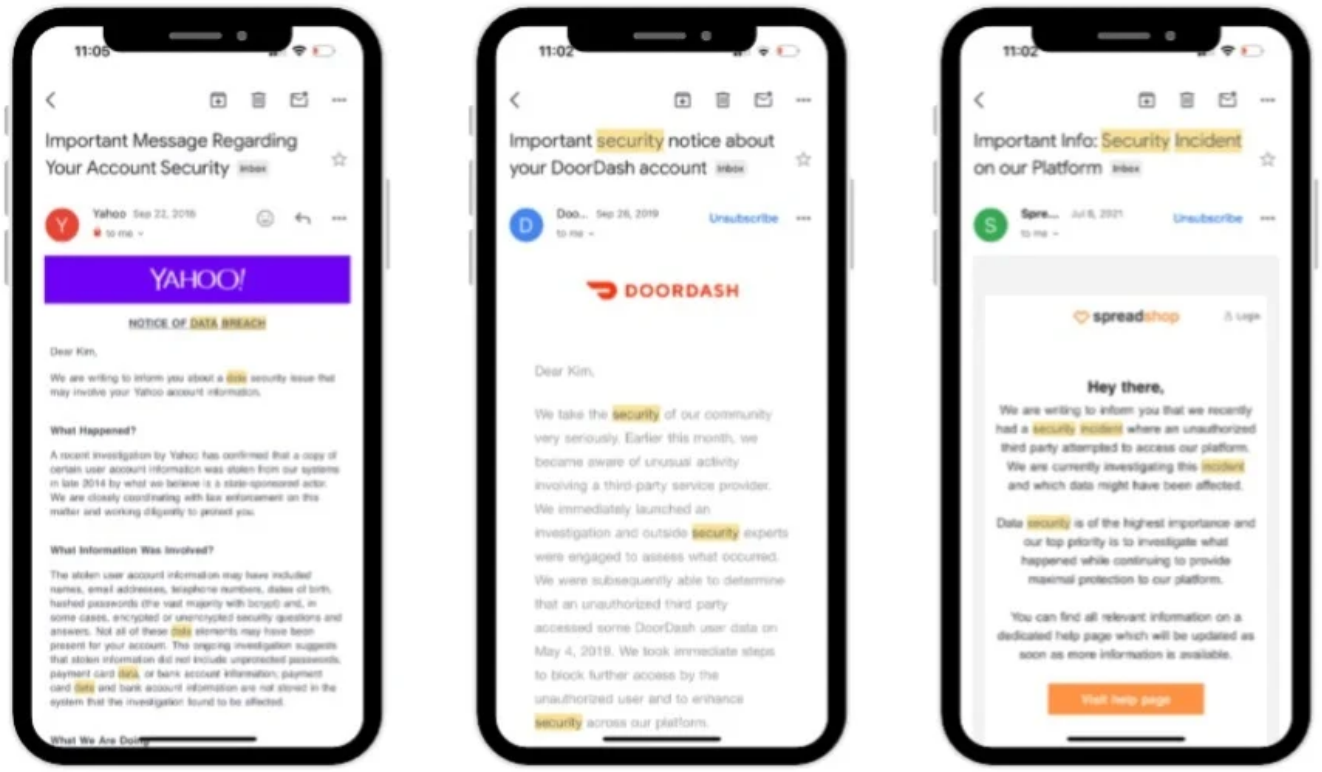
Il est raisonnable de supposer que les services de sécurité des grandes entreprises sont régulièrement mis à rude épreuve, mais 2023 a été une année particulièrement mauvaise en termes de violations de données .
Dans sa liste de prévisions en matière de cybercriminalité pour 2024 , l'Identity Theft Resource Center (ITRC) prédit une augmentation des incidents de vol d'identité après « un nombre sans précédent de violations de données en 2023 par des acteurs menaçants motivés par des raisons financières et étatiques ».
Les clients de Facebook, Yahoo et Amazon ont tous été touchés par des violations de données ces dernières années.
Si ces grandes entreprises ne peuvent pas assurer la sécurité de vos données, n’importe quelle entreprise le peut-elle ?

Comment protéger vos données contre les violations

Hunt m'a dit que l'atténuation des dommages causés par les violations de données dépend de la prise de mesures préventives et de la modification de vos habitudes en ligne.
Vous trouverez ci-dessous quelques moyens simples de modifier vos habitudes Internet et de protéger vos données privées à l'avenir.

Pensez à la façon dont vous partagez vos informations personnelles

Tout le monde connaît quelqu'un enclin à raconter les moindres détails de son existence sur la plateforme de médias sociaux de son choix.
Mais le partage excessif peut également consister à offrir trop de données personnelles privées sur les formulaires d'inscription à un compte ou à publier des photos publiques de vous-même et de votre famille.



(Crédit : Kim Key)

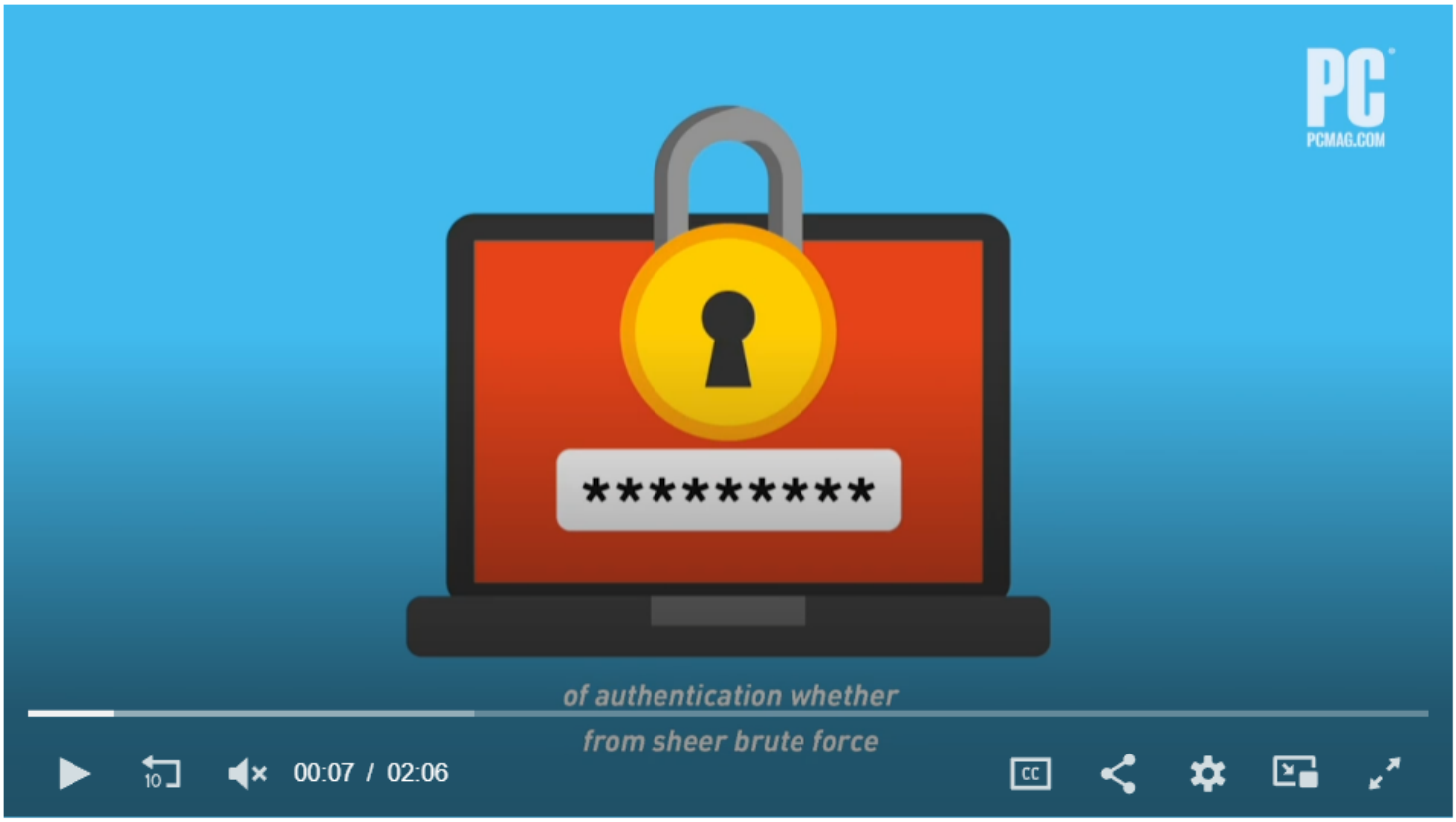
Se fixer des limites sur Internet peut être difficile, car une grande partie de notre vie sociale et professionnelle se déroule entièrement en ligne.
Même si vous pensez que Facebook est l'application sociale la moins sécurisée , il n'est ni réalisable ni idéal pour la plupart des gens de supprimer l'intégralité de leur présence en ligne pour empêcher le piratage de compte.
Hunt a déclaré que cette idée n'était pas non plus nécessaire avec un petit ajustement de l'état d'esprit.
Si vous ne divulguez pas de données sensibles en premier lieu, vous n'avez pas à craindre de les perdre.

«Maintenant, je publie presque exclusivement publiquement sur Facebook.
Cela s'explique en partie par le fait que si vous publiez en privé, vous êtes à un contrôle de sécurité pour que ces informations soient publiques ».
Troy a expliqué : « Donc, si vous partez du principe que les choses que vous publiez sur ces plateformes sont exposées au public et que vous adaptez votre comportement en conséquence, le risque diminue vraiment. »

Refusez d'indiquer votre date de naissance lorsque vous achetez quelque chose en ligne. Ne publiez pas de photos publiques de vos enfants en ligne.
N'oubliez pas qu'Internet est éternel et que toute information que vous divulguez risque d'être découverte.

Améliorez votre routine de confidentialité en ligne

Les mots de passe faibles constituent souvent la majeure partie des enregistrements de violations de données et, même si personne ne les aime, ils sont utilisés pour sécuriser les comptes en ligne de la plupart des gens.
Prenez l'habitude d' utiliser un gestionnaire de mots de passe , d'enregistrer les mots de passe sur vos appareils et d'activer l'authentification multifacteur sur vos comptes pour améliorer vos chances d'éviter les retombées d'une future violation de données.



Capture d'écran, pour visionner la vidéo, cliquer le lien suivant:

How to Protect Yourself From Data Breaches: Plan Ahead | PCMag

Un gestionnaire de mots de passe vous oblige souvent à créer un mot de passe principal fort , mais de nombreux gestionnaires de mots de passe permettent désormais aux utilisateurs de se connecter à l'aide de méthodes d'authentification sans mot de passe telles que l'analyse du visage ou des empreintes digitales.

Si vous craignez de créer un mot de passe principal devinable, le gestionnaire de mots de passe fera plus que simplement rechercher une longueur minimale et l'utilisation de différents caractères.
L'application évaluera les mots de passe faciles à retenir comme étant faibles, vous obligeant à créer un mot de passe principal susceptible de protéger vos informations.

Organisez votre vie en ligne pour prévenir le vol d'identité

Pour éviter d'être victime de crimes d'identité engendrés par des violations de données, c'est une bonne idée de lire périodiquement vos relevés de carte de crédit et de garder un œil sur votre rapport de crédit.
Connaître votre situation financière peut vous aider à détecter toute activité frauduleuse liée aux délits d'identité avant qu'elle ne devienne incontrôlable.

Il est également judicieux de mettre à jour les paramètres de confidentialité de vos comptes, applications et appareils et d'investir dans une suite de sécurité puissante . Consultez notre guide sur ce qu'il faut faire lorsque vous avez été piraté, et réfléchissez également aux nombreuses façons de disparaître complètement en ligne .

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240128
"C'est ensemble qu'on avance"