chrome enterprise

Limitez les risques de violation de données et de vol d'identité de votre entreprise avec l'extension Alerte mot de passe du navigateur Chrome

Introduction

Quid de la sécurité de votre organisation et de vos données lorsque vos collaborateurs réutilisent massivement leur mot de passe d'entreprise sur d'autres sites ?

Lors d'une enquête Google/Harris Poll menée en 2019 auprès de 3 000 adultes, 65 % des personnes interrogées ont répondu réutiliser leurs mots de passe dans plusieurs comptes (mais pas tous) ou réutiliser le même mot de passe *pour tous leurs comptes*.

La réutilisation des mots de passe reste monnaie courante

52 % Réutilisation du même mot de passe pour plusieurs comptes (mais pas tous)

35 % Utilisation d'un mot de passe différent pour tous les comptes

13 % Réutilisation du même mot de passe pour tous les comptes

chrome enterprise

Il suffit à un pirate informatique de récupérer *un seul mot de passe professionnel d'un de vos collaborateurs* pour pouvoir accéder aux appareils de cette personne, ainsi qu'au réseau et aux données de votre organisation. Les méthodes qu'il emploie à cette fin sont nombreuses. Les trois plus courantes sont les attaques par force brute, l'ingénierie sociale et l'hameçonnage.

Et si le navigateur Chrome empêchait en amont l'utilisateur de réutiliser ses mots de passe professionnels ?
La protection de votre organisation et de vos collaborateurs s'en trouverait renforcée et vous gagneriez en tranquillité d'esprit.

Règle Alerte mot de passe du navigateur Chrome

La règle Alerte mot de passe du navigateur Chrome aide les entreprises à lutter contre le vol d'identité et la violation de leurs données et de celles des employés. Pour ce faire, elle détecte dès qu'un employé saisit ses identifiants professionnels sur un autre site Web.

En protégeant *à la fois* les identifiants Google et non Google, la règle Alerte mot de passe renforce encore la sécurité des comptes et des données de l'entreprise. L'équipe informatique peut la gérer sur tous les principaux systèmes d'exploitation, dont Chrome OS, Windows[1], Mac[2] et Linux.

Protection de la confidentialité

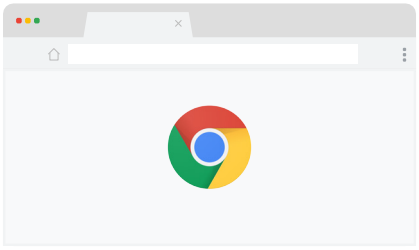
Google attache une grande importance à la protection de la confidentialité des utilisateurs. Nous ne stockons qu'une empreinte non réversible du mot de passe sur le disque. Personne ne peut voir les identifiants de vos utilisateurs. **Les données d'identification ne quittent jamais la machine locale. Elles ne sont en aucun cas envoyées à Google ni partagées avec des tiers.** Vous pouvez donc activer la règle Alerte mot de passe en étant assuré que la sécurité et la confidentialité de vos utilisateurs seront bien préservées.

[1] Microsoft®, Windows® et Internet Explorer® sont des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.
[2] Mac et macOS sont des marques d'Apple Inc. enregistrées aux États-Unis et dans d'autres pays.

chrome enterprise

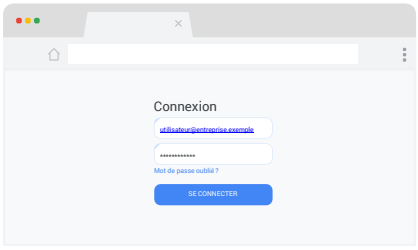
Fonctionnement de la règle Alerte mot de passe

Examinons d'abord la règle Alerte mot de passe du point de vue de l'utilisateur final. Son activation par l'équipe informatique n'a pas d'incidence sur l'expérience de l'utilisateur.

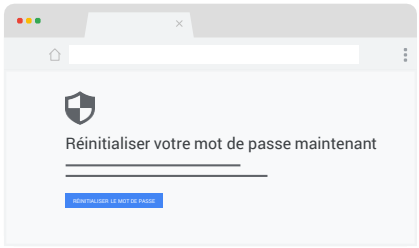


1. L'utilisateur ouvre le navigateur Chrome. . .

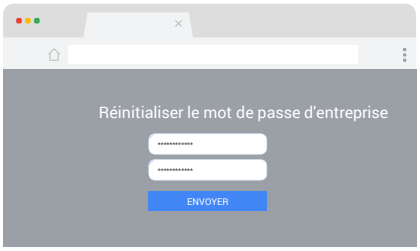
2. . . . se connecte au réseau de l'entreprise via votre connexion d'entreprise habituelle. . .



3. . . . et accède à un site où il utilise le même mot de passe (même avec un nom d'utilisateur différent).



4. Alerte mot de passe avertit l'utilisateur qu'il utilise le même mot de passe. L'utilisateur peut alors choisir. . .



5. . . . d'accéder à la page de réinitialisation du mot de passe.

Lorsqu'un utilisateur réutilise ses identifiants professionnels sur un site Web n'appartenant pas à son organisation, un avertissement s'affiche. Il est ensuite redirigé vers la page permettant de modifier le mot de passe.

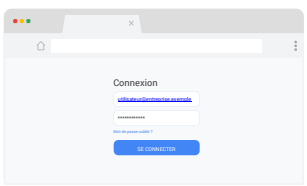
Voici ce qui se passe dans le backend, lorsque la règle Alerte mot de passe est activée :

1. L'utilisateur se connecte au réseau de l'entreprise via votre connexion d'entreprise habituelle.

2. (Non visible par l'utilisateur) Sans que l'utilisateur ne voie d'invite, Alerte mot de passe capture et stocke le mot de passe sous forme de hachage sur la machine locale.

3. Le travail de l'utilisateur n'est pas impacté.

1



3

Deux modes de fonctionnement existent pour Alerte mot de passe.

Le **mode Surveillance passive** consigne les réutilisations de mot de passe dans le système de fichiers local ou dans le journal des événements Windows sans afficher d'avertissements à l'utilisateur final. Vous êtes ainsi informé que des collaborateurs de votre entreprise réutilisent leur mot de passe.

Le **mode Détection active** affiche un avertissement à l'utilisateur dès qu'il réutilise ses identifiants professionnels sur des sites Web n'appartenant pas à l'entreprise ou sur des sites d'hameçonnage. Ces événements peuvent également être consignés dans le système de fichiers local ou dans le journal des événements Windows.

chrome enterprise

Activer Alerte mot de passe

La règle Alerte mot de passe est incluse dans les modèles Enterprise de Google. Vous pouvez l'activer dans la console de la gestion cloud du navigateur Chrome, indépendamment du système d'exploitation utilisé, ainsi que par le biais d'une stratégie de groupe dans les environnements Microsoft.

Premiers pas avec la règle Alerte mot de passe du navigateur Chrome

Que vous soyez client G Suite ou non, avec ou sans fournisseur SSO, configurer la règle Alerte mot de passe est très simple. Vous pouvez l'activer sur n'importe quel navigateur Chrome Enterprise géré par une stratégie GPO ou cloud. Découvrez comment gérer votre navigateur Chrome Enterprise dans le cloud ou via une stratégie de groupe. Consultez le livre blanc technique sur la règle Alerte mot de passe du navigateur Chrome pour savoir en détail comment configurer chacune des options.

Conclusion

La règle Alerte mot de passe du navigateur Chrome renforce la sécurité des données de votre entreprise en affichant un avertissement aux utilisateurs qui tentent de réutiliser leurs identifiants professionnels sur des sites Web d'hameçonnage ou non approuvés. Dans le monde hyperconnecté actuel, où les attaques par hameçonnage et autres sont devenues monnaie courante et dévastatrices, la règle Alerte mot de passe est un outil incontournable pour la sécurité de votre entreprise.

Si vous souhaitez en savoir plus sur l'option Alerte mot de passe du navigateur Chrome, **voici quelques ressources qui pourraient vous intéresser** :

Regardez la vidéo sur Alerte mot de passe.

Approfondissez l'Alerte mot de passe du navigateur Chrome.

Si vous êtes client Google Workspace, lisez les questions fréquentes sur la protection contre l'hameçonnage avec Alerte mot de passe dans l'aide pour les administrateurs.

Découvrez comment protéger vos utilisateurs contre les attaques d'hameçonnage.

Accédez aux options de téléchargement du navigateur Chrome pour votre entreprise.

Informez-vous sur la formule d'assistance Enterprise pour le navigateur Chrome.

Parcourez la liste des règles disponibles pour le navigateur Chrome.

Lisez les dernières notes de version sur le navigateur Chrome pour les entreprises.

Restez informé des dernières mises à jour du navigateur Chrome sur le blog des versions de Chrome.

Lisez le blog Google officiel sur la sécurité.

Consultez le Centre d'aide du navigateur Chrome pour les entreprises et le forum d'aide du navigateur Chrome.

Accédez à l'outil public de suivi des bugs pour le navigateur Chrome.