

Cybersécurité : Google met les mots de passe et TLS au menu de fin d'année

Des mots de passe piratés, réutilisés ou insuffisamment sécurisés ? Il y a Password Checkup pour vous avertir.

Cette promesse, c'est celle de l'outil Password Checkup.

Google l'[avait lancé](#) en début d'année sous la forme d'une [extension Chrome](#).

Le groupe américain vient de franchir une étape supplémentaire [en l'intégrant](#) dans son [gestionnaire de mots de passe](#).

Check-up Mots de passe

Vérifiez vos mots de passe enregistrés pour renforcer la sécurité de votre compte.



[Vérifier les mots de passe](#)

Password Checkup s'appuie sur une base de plusieurs milliards de paires identifiant / mot de passe connues comme ayant filtré.

Plusieurs engagements sont pris en matière de sécurité. Entre autres :

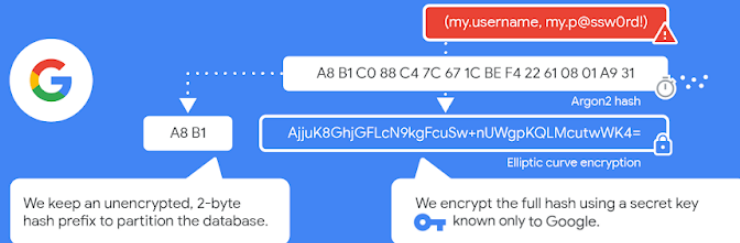
- ne jamais signaler d'informations permettant d'identifier un utilisateur ;
- éviter tout détournement de l'outil, que ce soit côté client ou côté serveur ;
- minimiser l'empreinte face aux protocoles cryptographiques qui remplissent un rôle comparable ([PIR](#), [PSI](#), [OT](#)...).

Under the hood:

How Password Checkup helps keep your accounts safe

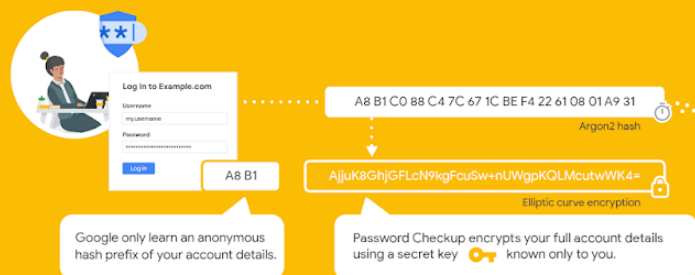
01

Whenever Google discovers a username and password exposed by a data breach, we store a strongly hashed and encrypted copy of the data.



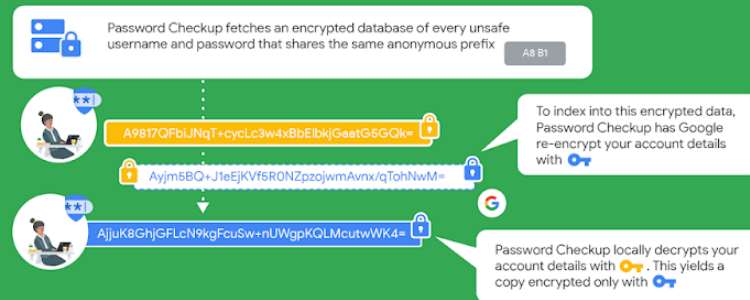
02

When you log in to a site you use around the web, Password Checkup will send a strongly hashed and encrypted copy of your username to Google. This ensures that Google never learns your account details.



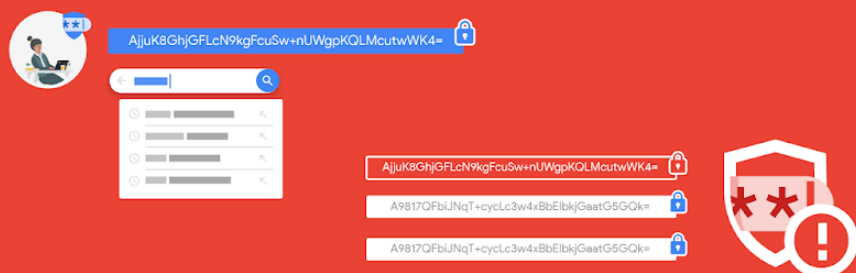
03

We use **private set intersection** with **blinding** to search through every unsafe username and password without revealing your account details, or anyone else's, during the process.



04

The final check for whether your username or password was in a data breach is entirely local. If your account details were exposed, you should change your password immediately.



Google

Au dernier pointage, l'extension compte un peu moins d'un million d'utilisateurs. Google dit avoir analysé, en septembre, 21 millions de logins... et détecté 316 000 mots de passe compromis.

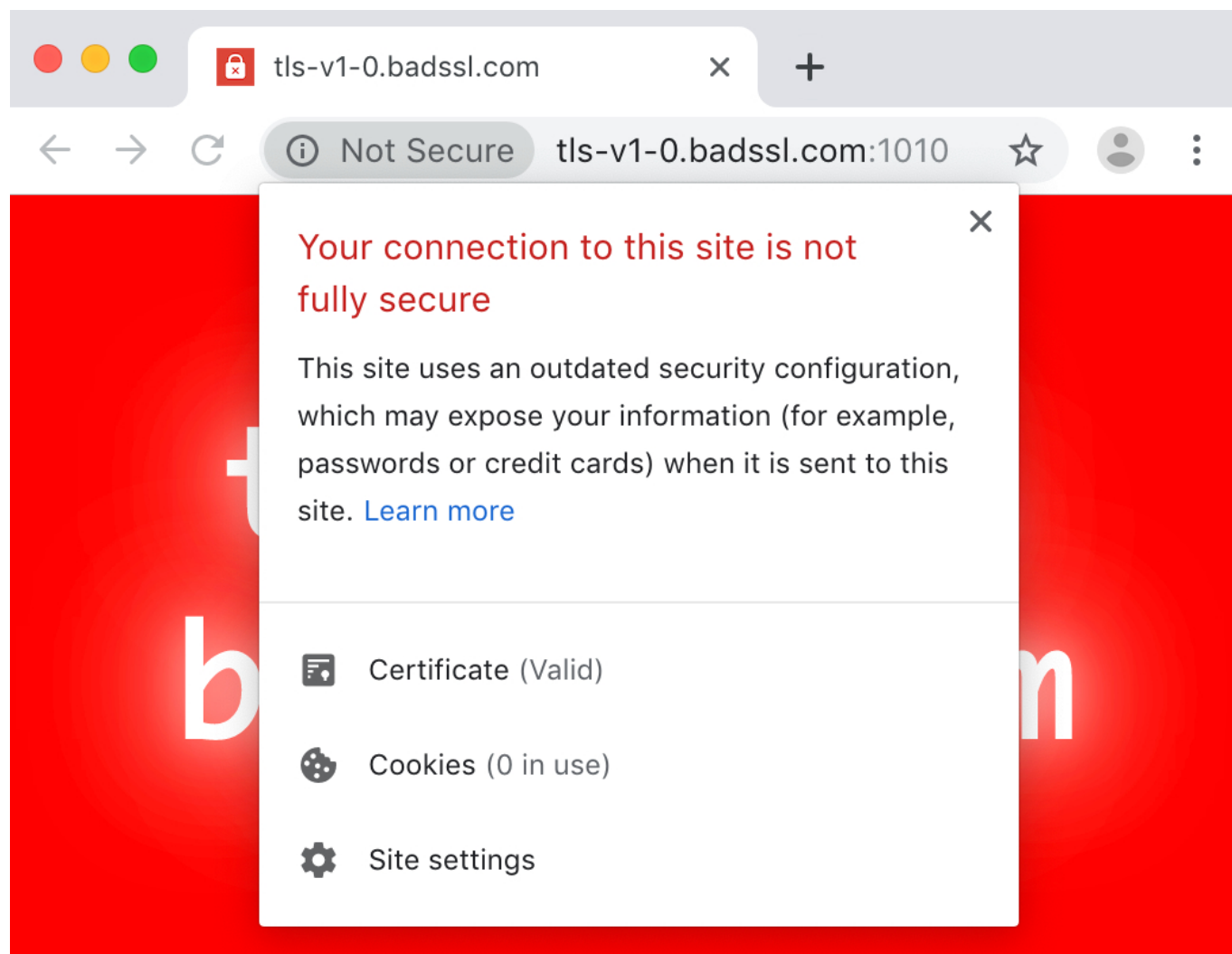
En plus de son intégration au gestionnaire de mots de passe, l'outil est accessible sur les terminaux Android, *via* l'application Google. Son arrivée dans Chrome est prévue d'ici à la fin de l'année

(expérimentation en cours [sur le canal Canary](#)).

TLS : les anciens poussés vers la sortie

Des précisions [sont fournies](#) en parallèle quant à la fin de la prise de charge de TLS 1.0 et 1.1. Deux versions considérées comme obsolètes, car reposant sur des algorithmes de chiffrement mis en défaut (MD5 et SHA-1).

Une première phase est prévue pour janvier 2020 avec la sortie de Chrome 79. Un indicateur « non sécurisé » apparaîtra dans la barre d'adresse.



Le blocage interviendra à partir du mois de mars, avec Chrome 81, sous la forme d'un interstitiel.



Your connection is not fully secure

This site uses an outdated security configuration, which may expose your information (for example, passwords, messages, or credit cards) when it is sent to this site. [Learn more](#)

NET::ERR_SSL_OBSOLETE_VERSION

Advanced

Back to safety

Google invite à la transition vers TLS 1.2 (spécifications publiées en 2008) ou toute version ultérieure. Il souligne qu'elle est déjà bien avancée : moins de 1 % des connexions sur chrome passent sur TLS 1.0 ou 1.1.

Les anciennes versions du protocole pourront être conservées jusqu'en janvier 2021 sur les déploiements de Chrome en entreprise.