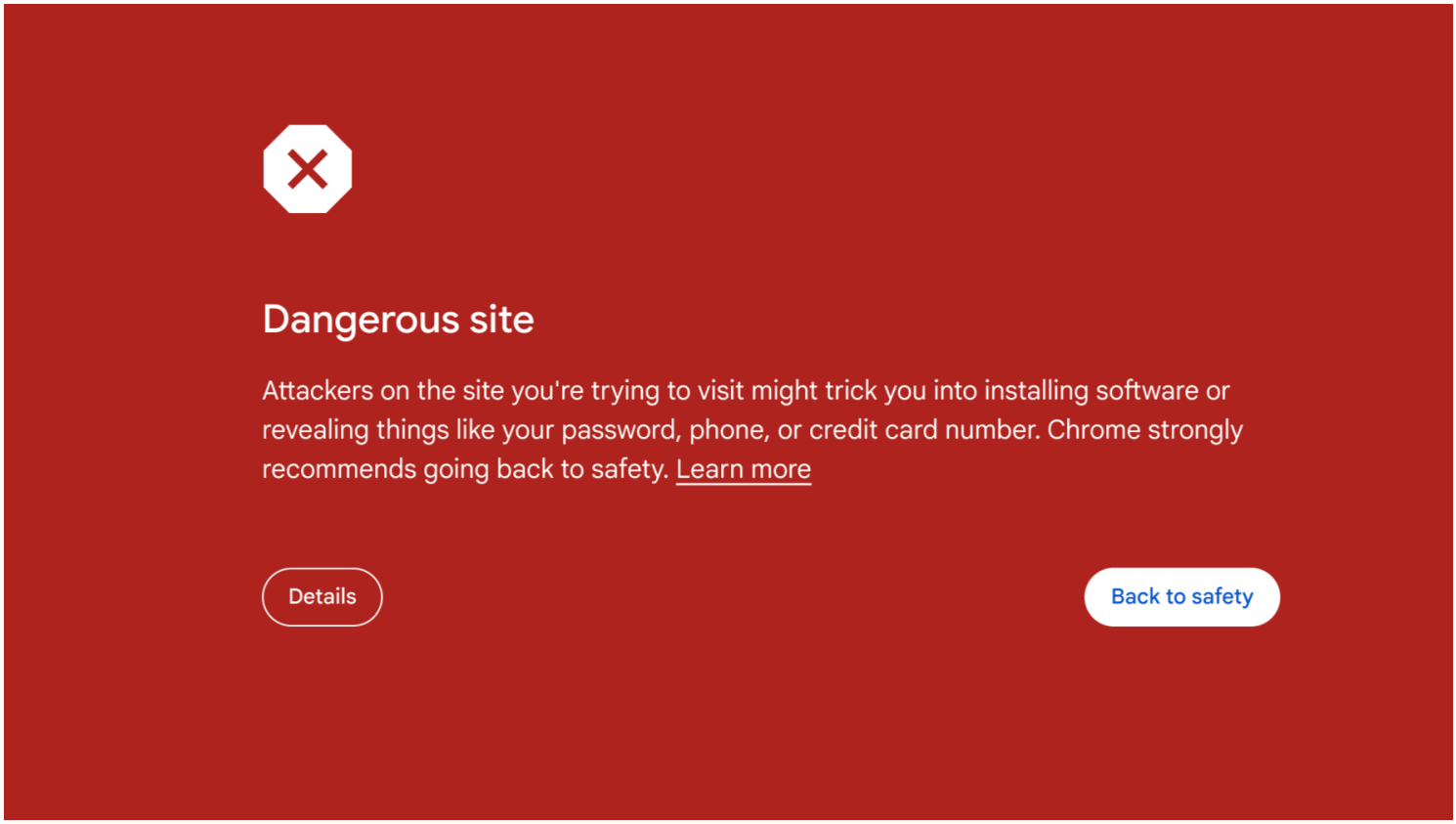
www.pcmag.com /news/chrome-privacy-update-blocks-25-more-phishing-attempts-google-says

La mise à jour de confidentialité de Chrome bloque 25 % de tentatives d'hameçonnage supplémentaires, selon Google

Le navigateur avertit désormais en temps réel les utilisateurs qui visitent une URL non sécurisée

Emily Dreibelbis :



Google a mis à jour la façon dont Chrome signale les sites potentiellement dangereux, ce qui, selon lui, bloquera 25 % de tentatives de phishing en plus sans compromettre la vie privée des utilisateurs.

Il est disponible dès maintenant dans le mode de protection standard de la navigation sécurisée sur ordinateur et iOS, et arrivera sur Android plus tard ce mois-ci.
Vérifiez si vous l'avez activé en accédant à **Paramètres** > **Confidentialité et sécurité** > **Sécurité**.
Ensuite, sélectionnez le niveau de « Navigation sécurisée » : protection renforcée, Protection standard ou Aucune protection.

Dans le passé, la protection standard était inférieure à la moyenne, dit Google.
Lorsqu'un utilisateur accède à une page Web, Google vérifie sur le backend si elle figure sur une liste de sites susceptibles d'être dangereux.
Le problème est que la liste était mise à jour toutes les 30 à 60 minutes et stockée localement sur l'appareil.
De nos jours, la plupart des sites dangereux existent moins de 10 minutes, et il y en a beaucoup trop pour être stockés sur la plupart des appareils.

« À mesure que les attaquants deviennent de plus en plus sophistiqués, nous avons constaté le besoin de protections capables de s'adapter aussi rapidement que les menaces contre lesquelles elles se défendent », explique Google.

Une protection renforcée offrait une plus grande couverture, mais obligeait l'utilisateur à donner plus de données, selon The Verge.
Mais avec la nouvelle approche de Google, la protection Standard offre désormais la même sécurité sans compromettre la vie privée.

Voici comment cela fonctionne : lorsque Chrome accède à une page Web, Google vérifie si l'URL est déjà connue pour être sûre.
Si ce n'est pas le cas, il lance le processus de vérification en temps réel.

Tout d'abord, il crypte ou « obscurcit » l'URL.
Ensuite, le système le convertit en hachages complets de 32 octets, qui deviennent rapidement une version tronquée sur 4 octets.
Les hachages cryptés sont ensuite envoyés à un serveur de confidentialité indépendant, exploité par le fournisseur de cloud Fastly.

Supprime rapidement tous les identifiants personnels des hachages, tels que l'adresse IP, et les transfère au serveur de navigation sécurisée via une connexion TLS.
Là, il va dans un pool anonyme de demandes d'autres utilisateurs de Chrome, ce qui rend plus difficile l'identification des activités d'une personne.

Recommandé par nos rédacteurs

Enfin, le serveur de navigation sécurisée déchiffre les préfixes, vérifie s'ils font partie de la liste des URL non sécurisées et émet un avertissement en cas de correspondance.
Cela pourrait signifier que les utilisateurs voient des avertissements plus fréquemment, ce qui pourrait être gênant, mais il semble qu'ils seront mieux protégés.

« Si vous voulez encore plus de protection, vous pouvez toujours activer le mode de protection renforcée de la navigation sécurisée, qui utilise l'IA pour bloquer les attaques, fournit des analyses approfondies des fichiers et offre une protection supplémentaire contre les extensions Chrome malveillantes », explique Google.

Enfin, Google a également mis à jour la fonctionnalité de vérification des mots de passe sur iOS.
Il signalera désormais les mots de passe faibles et réutilisés en plus des mots de passe compromis.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240316
"C'est ensemble qu'on avance"