www.pcmag.com /news/passkeys-advocate-the-end-goal-is-youre-getting-rid-of-passwords

Les clés d’accès sont là et il suffit de convaincre les gens de les utiliser

Un responsable de la FIDO Alliance reconnaît que les gens peuvent encore hésiter face au concept de mot de passe, mais insiste sur le fait que l'authentification par mot de passe est « fondamentalement erronée ».

Rob Pegoraro :

Les clés d'accès promettent de réduire la routine de connexion à un simple clic ou pression suivi d'une confirmation biométrique rapide de votre présence en personne, mais l'adoption de ce concept par l'industrie peut sembler bloquée à un stade latent.

Lors d'une conférence d'une journée sur l'identité et l'authentification à Washington la semaine dernière, le chef d'un groupe professionnel derrière la norme sur les clés d'accès a reconnu que des obstacles subsistent pour cette authentification post-mot de passe, mais a souligné à quel point les choses se sont réchauffées pour les clés d'accès en général.

"De mon point de vue, 2023 a été l'année du mot de passe", a déclaré Andrew Shikiar, directeur exécutif et directeur du marketing de l' Alliance FIDO , lors d'un discours l'après-midi.
Il a cité un total de 8 milliards de comptes d'utilisateurs qui autorisent désormais l'accès par mot de passe, avec plus de 96 % des navigateurs actifs et plus de 98 % des appareils mobiles prenant en charge l'authentification par mot de passe.

Shikiar a admis que les gens peuvent encore hésiter face au concept – « personne n'a utilisé de mot de passe » – mais a qualifié l'authentification par mot de passe de « fondamentalement erronée » car elle permet des défaillances humaines telles que la réutilisation de mots de passe sur plusieurs sites et le fait de se laisser tromper par des escroqueries par phishing .

Shikiar a prédit qu'en 2024, le nombre de comptes activés par mot de passe « atteindra les 20 milliards », ajoutant « je pense que nous dépasserons ce chiffre ».

Une conversation avec lui par la suite a cependant mis en évidence certains blocages persistants malgré des mesures réelles montrant comment les mots de passe ont rationalisé l'expérience client pour les entreprises qui les ont adoptés .

Prenons un exemple cité par Shiakar dans son discours : le déploiement par Air New Zealand l'année dernière de la prise en charge des clés d'accès, ce que son site appelle « notre option préférée » pour la sécurité des comptes.
Il a déclaré que la compagnie aérienne avait constaté un taux d'adhésion de 30 % au cours des premières 24 heures, après quoi ses taux d'abandon de connexion avaient chuté de 50 %.
(Google a signalé des améliorations d'efficacité similaires grâce à l'adoption du mot de passe.)

Cependant, les compagnies aériennes américaines n'ont pas encore montré le moindre signe de détection des mots de passe sur leur radar : leur prise en charge de l'authentification multifacteur a à peine dépassé les questions de sécurité .

Shikiar a suggéré que la taille relativement petite d'Air New Zealand l'avait aidée à adopter les mots de passe plus rapidement : « Ils peuvent se déplacer rapidement parce que c'est une compagnie aérienne plus petite. »

Mais il a reconnu que l'industrie du voyage devrait utiliser les passe-partout.
Cela n'est pas tant dû à la valeur des transactions, mais à la fréquence à laquelle les compagnies aériennes et les hôtels exigent non seulement un nom d'utilisateur et un mot de passe, mais également un nom de famille, ce qui, comme l'a noté Shiakar, brise les gestionnaires de mots de passe qui n'attendent que les deux premiers champs.

Par exemple, Hyatt exige les trois champs pour sa connexion régulière.
Mais l'activation de sa nouvelle option de clé d'accès réduit mon processus de connexion au déverrouillage de 1Password et à un clic une fois pour utiliser la clé d'accès cryptée enregistrée dans ce gestionnaire de mots de passe.

Et même si l'industrie technologique a été beaucoup plus rapide à prendre en charge les clés d'accès, en partie grâce à la décision de Google de les activer pour tous les utilisateurs grand public en mai dernier , de curieuses lacunes dans la prise en charge persistent.

Par exemple, alors que Meta a annoncé la prise en charge du mot de passe WhatsApp (au début uniquement pour Android) en octobre, il n'a pas encore fait de même pour Facebook lui-même.
Et X, anciennement Twitter, n'a déployé la prise en charge des clés d'accès (dans son cas, iOS uniquement) que la semaine dernière , malgré des années de rachats de comptes très médiatisés .

C'est un monde en ligne étrange dans lequel un compte Nintendo peut bénéficier d'une meilleure sécurité que l'une de vos principales identités sur les réseaux sociaux.

Dans d'autres cas, la prise en charge du mot de passe d'une entreprise ou d'une organisation peut être facile à manquer, car elle n'utilise pas ce mot pour la décrire ou enterre toute l'option.
Le portail login.gov du gouvernement fédéral, par exemple, propose une option « Ajouter un déverrouillage par reconnaissance faciale ou tactile » , alors que je n'ai pu trouver l'option de clé d'accès que sur un compte professionnel PayPal, car l'extension de navigateur de 1Password m'y a dirigé directement.

(L'application Live Transcribe de Google , que j'ai utilisée au cours de cette interview, a fourni une démonstration involontaire de la mauvaise visibilité des mots de passe lorsqu'elle transcrivait systématiquement le mot « clé de passe » comme autre chose, par exemple « panier », « skis passés », « pâtés » , " et " coller ")

Shikiar a également partagé quelques leçons apprises sur l'utilisation des clés d'accès, en particulier sur le moment où les entreprises peuvent le mieux présenter une clé d'accès à un client.
Réponse courte : lorsqu'ils doivent modifier un paramètre de sécurité pour une raison ou une autre et qu'ils ont déjà accédé aux paramètres de ce compte.

Recommandé par nos rédacteurs

"Personne n'aime passer par les paramètres de sécurité", a-t-il déclaré.
"Mais si vous êtes là, c'est le bon moment pour les attraper."

Et cela est particulièrement vrai si le client doit réinitialiser un mot de passe, car l'ajout d'un mot de passe peut garantir que le client n'aura plus à se soucier des mots de passe.

Shikiar a reconnu ses inquiétudes quant à ce qui pourrait arriver si un utilisateur de mot de passe perd l'appareil mobile qu'il utilise pour authentifier une connexion par mot de passe sur un autre ordinateur.
Dans ce scénario de mot de passe courant, le téléphone indique au navigateur d'un ordinateur de bureau ou portable via une connexion Bluetooth cryptée que le bon utilisateur est réellement garé devant le clavier.

Mais il a ajouté que, étant donné que toutes les principales implémentations de clés d'accès offrent déjà une synchronisation cryptée de bout en bout des clés d'accès, la perte d'un appareil n'est pas un désastre tant que vous conservez l'accès au service de synchronisation des clés d'accès, qu'il s'agisse du trousseau iCloud d'Apple ou autre. gestionnaires de mots de passe tiers comme 1Password, Bitwarden et Dashlane .

"Tout ce que vous avez à faire est de récupérer votre compte principal auprès de ce fournisseur", a déclaré Shikiar.

Les entreprises qui déploient des mots de passe, quant à elles, peuvent exercer une surveillance plus minutieuse sur les personnes qui se connectent encore avec des mots de passe.
Et une fois qu'un nombre suffisant d'utilisateurs activent les clés d'accès, un utilisateur revenant d'une connexion par clé d'accès à un mot de passe peut lui-même représenter un signe avant-coureur d'une compromission de compte.

« Il est important d'avoir des chiffres plus élevés », a-t-il déclaré.

"Parce que, vous savez, l'objectif final est de vous débarrasser des mots de passe."

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240206
"C'est ensemble qu'on avance"