Versione digitale e accessibile qui

Google

Passkey: il futuro senza password è sempre più vicino

Con il drammatico aumento degli attacchi informatici sponsorizzati dagli stati e da utenti malintenzionati online, siamo impegnati più che mai a proteggere le persone, le organizzazioni e i governi condividendo le nostre competenze, mettendo la società nelle condizioni di affrontare i rischi e lavorando continuamente per far progredire lo stato dell'arte della cybersicurezza al fine di costruire un mondo più sicuro per tutti.

Oggi le password sono essenziali per la sicurezza online, ma minacce quali il phishing continuano ad aumentare. Google ha da tempo preso coscienza del problema, incoraggiando gli utenti a utilizzare strumenti di autenticazione come la verifica in due passaggi (2SV), il Gestore delle password di Google, i token di sicurezza e adesso le passkey.

La sfida

Le password vengono utilizzate sui computer da oltre 60 anni, ma oggi non sono più sufficienti per tenere al sicuro i dati degli utenti e delle organizzazioni. Gli attacchi di phishing continuano ad aumentare in quantità e sofisticatezza, approfittando delle falle di sicurezza delle password. Per esempio:

- Oltre il **60% della violazione dei dati** del 2021 ha comportato il furto di credenziali o attacchi di phishing.[1]
- La violazione dei dati causata dal phishing è costata alle organizzazioni **in media 4,91 milioni di dollari** nel 2022.[2]
- Gli attacchi di phishing sono aumentati del **61%** nel 2022, raggiungendo i 255 milioni nell'arco di sei mesi.[3]

La verifica in due passaggi/l'autenticazione a due fattori (2SV/2FA) è utile, ma potrebbe mettere a dura prova l'utente con ulteriori attriti e comunque non protegge del tutto dagli attacchi di phishing e da attacchi mirati come il "Sim swapping" per la verifica tramite SMS.

La soluzione

Collaborando con FIDO Alliance, abbiamo reso possibile il supporto delle passkey, un'alternativa più semplice e sicura alle password, portando una tecnologia resistente al phishing a miliardi di persone in tutto il mondo. Con le passkey, è possibile evitare di inserire la password per un'esperienza di accesso più facile e sicura, utilizzando l'impronta digitale, il riconoscimento facciale o il blocco schermo.

A partire dai primi mesi del 2023, le passkey sono diventate disponibili per gli account personali Google, per gli utenti di più di 9 milioni di clienti di Google Workspace, nonché per i siti e app di terze parti su Chrome e Android.

Il modo più semplice e veloce di accedere

Le passkey sono **quattro volte più semplici** da usare, dal momento che non è necessario ricordarle o digitarle. Basta usare l'impronta digitale, la scansione del volto o il blocco schermo per accedere a tutti i dispositivi e le piattaforme.[4]

Sicurezza all'avanguardia

Le passkey offrono la protezione più efficace contro minacce quali il phishing. Dal momento che vengono conservate fisicamente sul tuo dispositivo, non possono essere indovinate o riutilizzate, aiutandoti così a proteggere le tue informazioni dagli attacchi.

La tua privacy, solo nelle tue mani

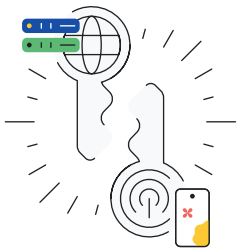
La tua passkey rimane privata sul tuo dispositivo personale e non viene mai condivisa con Google o con altri partner di terze parti. Ti basta usare l'impronta digitale, il riconoscimento facciale o il blocco schermo per verificare che sei tu ad accedere alla tua chiave d'accesso privata.

Safer with Google

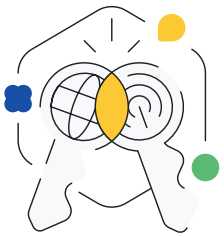
Versione digitale e accessibile qui

Google

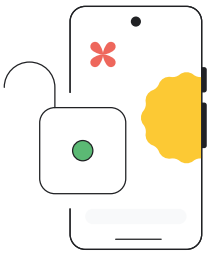
Come funziona



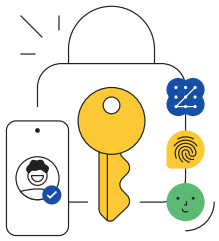
Una passkey è composta da due parti: una chiave di accesso pubblica sul server per il sito web a cui stai accedendo, e una chiave privata corrispondente sui tuoi dispositivi.



Quando effettui l'accesso, il sito web controlla se la chiave d'accesso pubblica corrisponde a quella privata.



Per farlo, ti viene chiesto semplicemente di sbloccare il tuo dispositivo.



Accederai al tuo account, mentre la tua chiave d'accesso privata e i tuoi dati biometrici rimarranno al sicuro sul tuo dispositivo e non verranno mai condivisi con nessuno.

Per un ecosistema più sicuro

Portare le passkey ad aziende e governi

Le passkey introducono vantaggi significativi in termini di sicurezza e usabilità per gli utenti e siamo entusiasti di essere il primo grande provider pubblico di servizi cloud a fornire questa tecnologia ai nostri clienti, dalle piccole imprese alle grandi aziende, fino alle scuole e i governi.

Le nostre partnership per un accesso sicuro e senza password su tutto Internet

Collaboriamo con altri brand per attivare le passkey su tutte le piattaforme Chrome e Android, fornendo una tipologia di accesso più semplice e sicura per gli utenti. Molti partner in settori come l'e-commerce, la fintech, i viaggi e altri hanno deciso di unirsi a noi in questo viaggio verso un futuro senza password. Tra questi 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal e Yahoo! Japan.

Il nostro viaggio verso un futuro senza password

Le passkey ci avvicinano sempre di più al futuro senza password che abbiamo progettato per oltre dieci anni.

2008 — Abbiamo introdotto Gestore delle password di Google per accedere in modo più semplice e sicuro.

2011 — Abbiamo offerto la verifica in due passaggi (2SV) per gli account Google.

2012 — Abbiamo fornito token di sicurezza resistenti al phishing ai dipendenti Google.

2013 — Ci siamo uniti a FIDO Alliance per guidare gli standard aperti per un mondo senza password.

2014 — Abbiamo reso i token di sicurezza resistenti al phishing disponibili per tutti.

2017 — Abbiamo introdotto il Programma di protezione avanzata (APP) per utenti ad alto rischio.

2019 — Abbiamo esteso il nostro supporto FIDO su Android per riautenticazioni senza password su tutti i siti web.

2023 — Abbiamo attivato le passkey per account Google, clienti Workspace e partner di terze parti su Chrome e Android.

Mentre le password continueranno a far parte delle nostre vite in questa fase di passaggio verso le passkey, noi continuiamo a impegnarci per aiutare le persone e chi fa parte del settore a compiere questo passo verso un modo di accedere più semplice e sicuro con Google.

Fonti: 1 - Verizon Data Breach Investigation report 2022 | 2 - IBM Cost of Data Breach report 2023
3 - CNBC's Cyber Report | 4 - Google Security Blog, maggio 2023

Safer with Google

Scopri in che modo Google protegge tutti gli utenti quando sono online su g.co/safety