Веб-доступні версії тут

Google

Ключі доступу: на крок ближче до майбутнього без пароля

З різким зростанням кількості спонсорованих державами кібератак і зловмисників в Інтернеті ми більше, ніж будь-коли, зосереджені на захисті людей, компаній і урядів, ділячись нашим досвідом, розширюючи можливості суспільства та постійно працюючи над вдосконаленням кібербезпеки, щоб допомогти створити безпечніший світ для всіх.

Сьогодні паролі важливі для безпеки в Інтернеті, але такі загрози, як фішинг, продовжують зростати. Google давно усвідомлює ці проблеми та заохочує використовувати інструменти автентифікації, як-от двоетапна перевірка (2SV), Менеджер паролів Google, ключі безпеки, а тепер і ключі доступу.

Проблема

Паролі використовувалися з комп'ютерами понад 60 років, але для захисту даних користувачів і організацій сьогодні їх уже недостатньо. Фішингові атаки продовжують зростати у своєму масштабі та складності, використовуючи слабкі місця безпеки в паролях. Наприклад:

- Понад **60% випадків витоку даних** у 2021 році були пов'язані з викраденими обліковими даними або фішингом.[1]
- Витоки даних, спричинені фішингом, коштували організаціям **у середньому 4,91 мільйона доларів США** в 2022 році.[2]
- Кількість фішингових атак виросла на **61%** у 2022 році, досягнувши 255 мільйонів за шість місяців.[3]

2-етапна перевірка/2-факторна автентифікація (2SV/2FA) допомагає, але вона може створювати додаткові навантаження на користувача та все ще не повністю захищає від фішингових і цілеспрямованих атак, як-от підміна SIM-карти для проходження перевірки через SMS.

Рішення

У партнерстві з FIDO Alliance ми ввімкнули підтримку ключів доступу — простішої та безпечнішої альтернативи паролям, яка надає стійку до фішингу технологію мільярдам людей у всьому світі. За допомогою ключів доступу ви можете не вводити пароль, а скористатись можливістю простішого та безпечнішого входу за допомогою відбитка пальця, сканування обличчя або блокування екрана.

З початку 2023 року ключі доступу стали доступні для особистих облікових записів Google і для користувачів більш ніж 9 мільйонів клієнтів Google Workspace, а також сторонніх веб-сайтів та додатків у Chrome та Android.

Найпростіший і найшвидший спосіб входу

Ключі доступу **в 4 рази простіше** використовувати, оскільки їх не потрібно запам'ятовувати чи вводити. Ви просто використовуєте відбиток пальця, сканування обличчя або блокування екрана для входу на всіх своїх пристроях і платформах.[4]

Безпека облікового запису нового покоління

Ключі доступу забезпечують найнадійніший захист від таких загроз, як фішинг. А оскільки вони зберігаються на вашому локальному пристрої, їх неможливо вгадати або повторно використати, що допомагає захистити вашу інформацію від зловмисників.

Конфіденційність, якою вона має бути

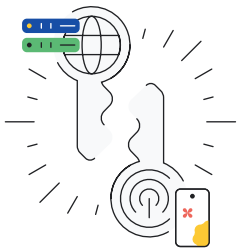
Ваш ключ доступу залишається конфіденційним на вашому особистому пристрої та ніколи не передається Google чи іншим стороннім партнерам. Ви просто використовуєте відбиток пальця, сканування обличчя або блокування екрана, щоб підтвердити, що саме ви отримуєте доступ до свого закритого ключа.

Safer with Google

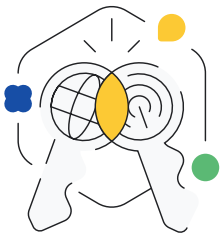
Google

Веб-доступні версії тут

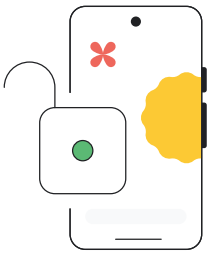
За лаштунками



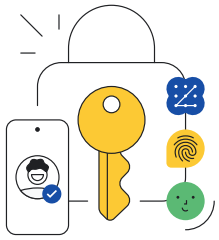
Ключ доступу складається з двох частин: відкритого ключа на сервері веб-сайту, на якому ви виконуєте вхід, та відповідного закритого ключа на ваших пристроях.



Коли ви входите, веб-сайт перевіряє, чи ваш відкритий ключ збігається з вашим закритим ключем.



Щоб переконатися, що це так, вас просто попросять розблокувати пристрій.



Ви ввійдете у свій обліковий запис, а ваш закритий ключ і ваші біометричні дані залишаться в безпеці на вашому пристрої, і вони ніколи не будуть передані.

Створення безпечнішої екосистеми

Надання ключів доступу компаніям і державним установам

Ключі доступу надають користувачам значні переваги в безпеці та зручності використання, і ми раді бути першим великим постачальником публічних хмарних технологій, який надає цю технологію нашим клієнтам — від малих і великих підприємств до шкіл і державних установ.

Партнерство для безпечнішого входу в Інтернет без пароля

Ми співпрацюємо з брендами, щоб використовувати ключі доступу на платформах Chrome і Android, забезпечуючи простіший і безпечніший вхід для їхніх користувачів. Численні партнери в таких галузях, як електронна комерція, фінансові технології, подорожі тощо, уже приєдналися до нашої безпарольної ініціативи, зокрема 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal і Yahoo! Japan.

Наша безпарольна подорож

Ключі доступу наближають нас до безпарольного майбутнього, яке ми планували вже більше десяти років.

2008 — Запущено Менеджер паролів Google для простішого та безпечнішого входу.

2011 — Увімкнено двоетапну перевірку (2SV) для облікових записів Google.

2012 — Представлено стійкий до фішингу ключ безпеки для співробітників Google.

2013 — Приєднання до FIDO Alliance, щоб просувати відкриті стандарти для світу без паролів.

2014 — Ключі безпеки, стійкі до фішингу, доступні всім.

2017 — Представлено програму розширеного захисту (Advanced Protection Program, APP) для користувачів із високим рівнем ризику.

2019 — Розширено нашу підтримку FIDO в Android для повторної авторизації без пароля на веб-сайтах.

2023 — Увімкнено ключі доступу для облікових записів Google, клієнтів Workspace і сторонніх партнерів у Chrome і Android.

Хоча паролі й надалі залишатимуться частиною нашого життя, коли ми переходимо на ключі доступу, ми прагнемо допомогти людям та іншим у галузі перейти на новий рівень, щоб зробити вхід у Google простішим і безпечнішим.

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

Safer with Google

Дізнайтеся, як Google забезпечує безпеку всіх в Інтернеті, на веб-сайті g.co/safety