



Klucze dostępu: kolejny krok w stronę przyszłości bez haseł

Gwałtowne nasilenie się cyberataków sponsorowanych przez państwa i aktywności przestępczej online sprawia, że jeszcze więcej uwagi poświęcamy bezpieczeństwu ludzi, firm i urzędów. W tym celu dzielimy się wiedzą, tworzymy nowe rozwiązania i stale rozwijamy systemy cyberbezpieczeństwa, abyśmy wszyscy żyli w bezpieczniejszym świecie.

Hasła są dziś kluczowym elementem dbania o bezpieczeństwo online, ale coraz częściej są zagrożone, na przykład przez phishing. Google od dawna dostrzega ten trend i zaleca stosowanie rozwiązań do weryfikacji tożsamości, takich jak uwierzytelnianie dwuskładnikowe. Najpierw był menedżer haseł Google, potem klucze bezpieczeństwa, a teraz – klucze dostępu.

Wyzwanie

Od ponad 60 lat nasze komputery i zasoby cyfrowe są zabezpieczane hasłami. Obecnie jednak nie chronią one danych użytkowników i firm w wystarczającym stopniu. Ataki phishingowe są coraz bardziej rozbudowane i zaawansowane. Wykorzystują często słabe punkty w hasłach. Przykłady:

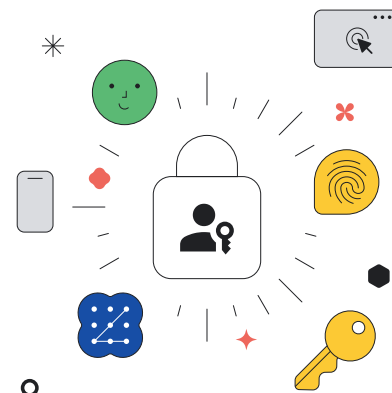
- ✓ Ponad **60% przypadków wycieku danych** w 2021 roku było skutkiem kradzieży danych lub phishingu¹.
- ✓ Wycieki danych wskutek phishingu w samym 2022 roku kosztowały **średnio 4,91 mln dolarów** na organizację².
- ✓ W 2022 roku liczba ataków phishingowych wzrosła o **61%** w ciągu sześciu miesięcy odnotowano ich aż 255 mln³.

Uwierzytelnianie dwuskładnikowe pomaga, ale jednocześnie stanowi dodatkowe utrudnienie dla użytkownika i wciąż nie chroni skutecznie przed atakami phishingowymi ani ukierunkowanymi, takimi jak wymiana karty SIM w celu kradzieży kodu z SMS-a.

Rozwiązanie

Z pomocą FIDO Alliance wprowadziliśmy obsługę kluczy dostępu. Stanowią one prostszą i bezpieczniejszą alternatywę dla haseł. Dzięki temu miliardy ludzi na całym świecie zyskują dostęp do rozwiązania odpornego na techniki phishingowe. Klucze dostępu pozwalają zastąpić hasła wygodniejszym i bezpieczniejszym sposobem logowania z użyciem odcisku palca, skanowania twarzy lub blokady ekranowej.

Na początku 2023 roku udostępniliśmy to rozwiązanie użytkownikom prywatnych kont Google, a także 9 mln klientów Google Workspace oraz użytkownikom stron i aplikacji zewnętrznych dostępnych w przeglądarce Chrome i systemie Android.



Najprostszy i najszybszy sposób logowania

Klucze dostępu są **4-krotnie prostsze** od haseł, bo nie trzeba ich ani pamiętać, ani wpisywać. Wystarczy przyłożyć palec, zeskanować twarz lub odblokować ekran, aby zalogować się na dowolnym urządzeniu i dowolnej platformie⁴.

Ochrona konta nowej generacji

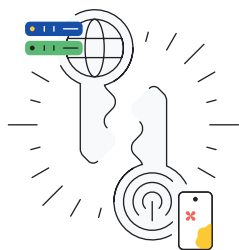
Klucze dostępu to najskuteczniejsza dostępna metoda zabezpieczenia kont przed phishingiem. Ponieważ są przechowywane na Twoim lokalnym urządzeniu, nie da się ich zgadnąć ani powielić, dzięki czemu Twoje dane są bezpieczne przed hakerami.

Prawdziwa prywatność

Klucz dostępu jest przechowywany bezpiecznie na Twoim prywatnym urządzeniu i nigdy nie jest udostępniany Google ani innym firmom czy organizacjom. Po prostu zeskanuj odcisk palca lub twarz albo odblokuj ekran, aby zweryfikować, że to Ty chcesz skorzystać z klucza.



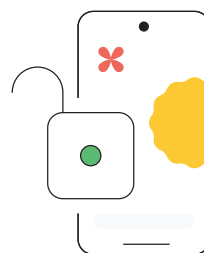
Od kuchni



Klucz dostępu składa się z dwóch części: klucza publicznego na serwerze witryny, w której się logujesz, oraz klucza prywatnego na urządzeniu.



Gdy logujesz się na konto, witryna sprawdza, czy klucz publiczny odpowiada kluczowi prywatnemu.



W tym celu musisz jedynie odblokować swoje urządzenie.



To wszystko – strona loguje Cię na konto, ale Twój klucz prywatny i dane biometryczne nie nigdy opuszczają urządzenia i nie są nikomu udostępniane.

Budowa bezpieczniejszego ekosystemu

Klucze dostępu dla firm i instytucji rządowych

Klucze dostępu przynoszą użytkownikom liczne korzyści, jeśli chodzi o bezpieczeństwo i funkcjonalność. Dlatego też niezmiernie cieszymy się, że jesteśmy pierwszym dostawcą chmury publicznej oferującym tę technologię naszym klientom – tak małym firmom, jak i korporacjom, szkołom i instytucjom rządowym.

Wspólne dążenie do bezpiecznego logowania bez haseł

Ściśle współpracujemy z różnymi markami, aby umożliwić logowanie się kluczem dostępu w przeglądarce Chrome i urządzeniach z Androidem, tak aby było to jak najłatwiejsze dla użytkowników. W tę podróż wyruszyło już wiele firm z różnych sektorów, takich jak e-commerce, technologie finansowe czy podróże, m.in. 1Password, Adobe, Dashlane, DocuSign, Kayak, Mercari, PayPal i Yahoo! Japan.

Podróż do świata bez haseł

Klucze dostępu to kolejny krok w stronę przyszłości bez haseł, do której dążymy od ponad dekady.

| 2008 | 2011 | 2012 | 2013 | 2014 | 2017 | 2019 | 2023 |
|---|---|---|--|---|---|--|--|
| premiera Menedżera haseł Google, który ułatwia bezpieczne logowanie się na konto. | uruchomienie weryfikacji dwuskładnikowej dla kont Google. | wprowadzenie odpornego na ataki phishingowe klucza bezpieczeństwa dla pracowników Google. | dołączenie do FIDO Alliance w celu tworzenia otwartych standardów na potrzeby logowania bez haseł. | rozszerzenie dostępu do kluczy bezpieczeństwa odpornych na phishing dla wszystkich. | wprowadzenie Programu ochrony zaawansowanej dla osób na eksponowanych stanowiskach. | rozszerzenie obsługi standardu FIDO na Androidzie na potrzeby uwierzytelniania na wielu stronach bez używania hasła. | włączenie kluczy dostępu na kontach Google, Workspace oraz u partnerów zewnętrznych na platformach Chrome i Android. |

Na drodze do powszechnego stosowania kluczy dostępu hasła wciąż pozostaną nieodłączną częścią naszego życia. Będziemy jednak nieustannie pomagać ludziom oraz firmom z branży w robieniu kolejnego kroku w stronę świata, w którym logowanie się na konta jest szybsze i bezpieczniejsze.