# Kétfaktoros azonosításra vált a Google

***A cég a jelszavak világnapján jelentette be, hogy hamarosan automatikus beállítássá válik a felhasználóknál a lényegesen nagyobb biztonságot jelentő kétfaktoros azonosítás.***

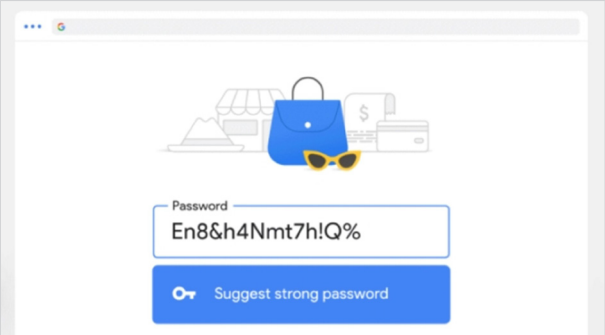
A jelszavak világnapjára időzítve a Google egy sor biztonsággal kapcsolatos fejlesztéséről, törekvéséről számolt be. Ezek közül az egyik felhasználók milliárdjait érinti, mivel a keresőóriás bejelentette, hogy alapértelmezetté teszi a fiókoknál a kétfaktoros azonosítást.

A vállalat területért felelős elnöke által jegyzett blogbejegyzés a jelszavakkal kapcsolatban gyakran emlegetett problémák felemlegetésével indul. Például a felhasználók gyakran ugyanazt a karaktersort használják több szolgáltatásnál is, ami értelemszerűen az összes ilyen belépési pontot sebezhetővé teszi, ha a személyes adatok bárhonnan kiszivárognak, ellopják azokat. Hogy a koronavírusról szóló tavalyi évben sem lett kisebb probléma az internetes biztonság (sőt!), arról árulkodik az is, hogy a cég statisztikája szerint 2020-ban rendszerükben megnégyszereződött a „mennyire erős a jelszavam” keresések száma.

**Egy cél, két faktor**

A Google hosszabb távon mindenképpen szeretné átadni a múltnak a sok szempontból problémás jelszavakra épülő azonosítást, de addig amíg ez valósággá válik, meg kívánja erősíteni a felhasználói fiókok védelmét. Mivel a leggyengébb láncszem általában maga az ember, a most bejelentett „erőszakos” módosítás logikusnak tűnik.

Utóbbi lényege, hogy a jelszavak mellett egy másik azonosítási formát is igényelnek majd belépéskor




a Google szolgáltatásai. A kétfaktoros azonosítás általánosan bevetett formája az, hogy egyszer használatos kódot küldenek a felhasználó telefonjára, postaládájába, így azt az adott bejelentkezési felületen megadva pedig igazolható a személyazonosság.

A Google azonban igyekszik ezt a folyamatot úgy egyszerűsíteni, hogy közben a biztonsági szempontok se sérüljenek. Ennek módja ez a fentebb látható beléptető rendszer, amely további számok és kódok bepötyögése, másolása helyett megelégszik azzal, hogy a felhasználó „leokézza” a belépési kísérletről tájékoztató felületet.

Mindez a cég saját biztonsági rendszerére épül, amely alapból megtalálható a Chrome böngészőben és az androidos eszközökben, de az iPhone-tulajdonosok sem maradnak ki a védelemből, köszönhetően a Smart Lock alkalmazásnak.

A telefonunkhoz kötött extra azonosítási lépéssel valószínűleg az elkövetkező hetekben, hónapokban, mivel a Google a funkciót minden egyes felhasználónál alapértelmezetté fogja tenni (már amennyiben a fiók beállításai ezt lehetővé teszik). Természetesen akit ez jobban zavar, mint amennyire aggódik a személyes adatai kompromittálódása miatt, az dönthet úgy, hogy kikapcsolja a kétfaktoros azonosítást.

Forrás: https://bitport.hu/ketfaktoros-azonositasra-valt-a-google

Válogatta: Fonyó Istvánné