1. Mi az a kétfaktoros hitelesítés?

A hagyományos felhasználói név és jelszó páros mellett a felhasználói fiókba (pl. Facebook, Gmail, Instagram, netbank, online tárhely, stb.) történő belépéshez még egy másik módon is hitelesíteni kell a felhasználót, vagyis nem elég a jelszó ismerete.

2. Miért fontos a kétfaktoros hitelesítés használata?

A felhasználói név/jelszó páros manapság már nem nyújt elég erős védelmet a felhasználói fiókoknak. A jelszavak kiszivároghatnak, kitalálhatóak, feltör-hetőek és birtokukban az arra nem jogosult személyek is beléphetnek a felhasználói fiókba. A kétfaktoros hitelesítés alkalmazásával ezt tudjuk megelőzni.

3. Hogyan történik a kétfaktoros hitelesítés?

A második hitelesítési lépcső jellemzően egy egyszerhasználatos kód (One Time Password) megadásával történik. Ez a kód érkezhet egy korábban magadott e-mail címre, illetve mobiltelefonszámra SMS-ben.

Másik lehetőség, hogy egy mobiltelefonos alkalmazásban generált, az adott felhasználói fiókhoz tartozó 6 számjegyű kódot kell megadni. Ez a kód 30 másodperceként változik, és mindig csak az aktuálissal lehet belépni a felhasználói fiókba. Ez megoldás biztonságosabb, mint az e-mailes vagy SMS-es kódküldés.

Netbankba vagy a Google fiókba történő belépést a bank, illetve a Google saját mobiltelefonos alkalmazásbában lehet jóváhagyni. Erre egy felugró üzenetben figyelmeztet az alkalmazás. A netbankok esetében általában alapértelmezetten be van állítva a kétfaktoros hitelesítés. Itt is érdemes azonban a hitelesítés módjaként a bank saját mobiltelefonos alkalmazását választani a SMS vagy email helyett.

5. Kétfaktoros hitelesítő (Two-factor authentication - 2FA) alkalmazás beszerzése és használata

A 2FA alkalmazást androidos telefonra Google Play Áruházból vagy iOS készülékre az App Store-ból tudunk letölteni. Ingyenes megoldásként ajánljuk a 2FA Authenticator alkalmazás használatát. Az alkalmazásban tárolt adatok PIN kóddal, illetve ujjlenyomattal védhetőek és beállítható, hogy a Google Drivera vagy iCloudba készítsen biztonsági mentést róluk. Így a mobiltelefon elvesztése vagy meghibásodása esetén is visszaállíthatók egy új készüléken. Új QR kód beolvasása + gombra kattintva történik.

6. Hogyan lehet bekapcsolni?

A kétfaktoros hitelesítést érdemes minden esetben a számítógép böngészőjében bekapcsolni. A beállításhoz szükség lesz egy androidos mobiltelefonra vagy iPhonera.

Facebook
Lépj be a Facebook fiókodba!

A kétfaktoros hitelesítést az alábbi menüben lehet bekapcsolni:

Fiók – Beállítások és adatvédelem – Beállítások – Biztonság és bejelentkezés – Kétfaktoros hitelesítés használata – Módosítás – Hitelesítő alkalmazás használata

1. A rendszer kéri a fiók használatának megerősítését.
2. Beállítás külső hitelesítő alkalmazáson keresztül
3. QR kód beolvasása az alkalmazással (pl. 2FA Auth)
4. Kattints a Folytatás gombra
5. Megerősítő kód beírása
6. Visszaigazolás

Google
Lépj be a Gmailbe!

Kattints a jobb felső sarokban profilképre – Google fiók kezelése – Biztonság – Bejelentkezés a Google-ba – Kétlépcsős azonosítás – Bejelentkezés telefon segítségével

1. Kattints a Beállítás gombra!
2. Jelszó újbóli megadása.
3. Telefon kiválasztása és kattintson a Tovább gombra!
4. Próba következik. Kattintson a Tovább gombra!
5. Véglegesítés! Kattintson a Bekapcsolás gombra!