Kétfaktoros hitelesítés

Authenticator alkalmazások működése

A modern kori információs világban elengedhetetlen a felhasználói fiókok fokozott védelme az egyre gyakoribb online támadások kivédése érdekében. Az online fiókok nagy része jelenleg is egy védelmi faktort használ, ami a felhasználó által megadott jelszó, azonban a jelszavak gyengesége és a szofisztikált támadási módok miatt további biztonsági faktorok bevezetése indokolt. A kétfaktoros hitelesítés (2FA) lényege, hogy egy második védelmi tényezőt alkalmazunk a fiók védelme érdekében, melyre jelenleg több alternatív megoldás is van.

A Vhelpi-nél ez a megoldás a TOTP hitelesítő, más néven Authenticator alkalmazások használata. Ennek lényege, hogy az alkalmazás szerver generál egy titkos kulcsot, melyet egy QR kódba ágyazva megoszt a felhasználóval, aki beszkennelheti egy speciális Authenticator alkalmazással, így innentől a kulcs a telefonon is elérhető lesz. Ez a speciális alkalmazás képes a titkos kulcs segítségével 30 másodpercig érvényes, 6 számjegy hosszú hitelesítő kódokat generálni, melyet a felhasználónak meg kell adnia belépéskor az e-mail címe és a jelszava mellé. A hitelesítő kódot a szerver tudja ellenőrizni, hiszen a generáláshoz használt titkos kulcs a szerveren is megtalálható.

A kétfaktoros hitelesítés beállításának megkezdése előtt egy Authenticator alkalmazás telepítése szükséges. Ugyan több ilyen ingyenes applikációs is elérhető, mi azonban a Google Authenticator és a Microsoft Authenticator alkalmazást javasoljuk. Ezek letöltési linkjei itt találhatók:

- Google Authenticator (Android)
- Microsoft Authenticator (Android)
- Google Authenticator (iOS)
- Microsoft Authenticator (iOS)

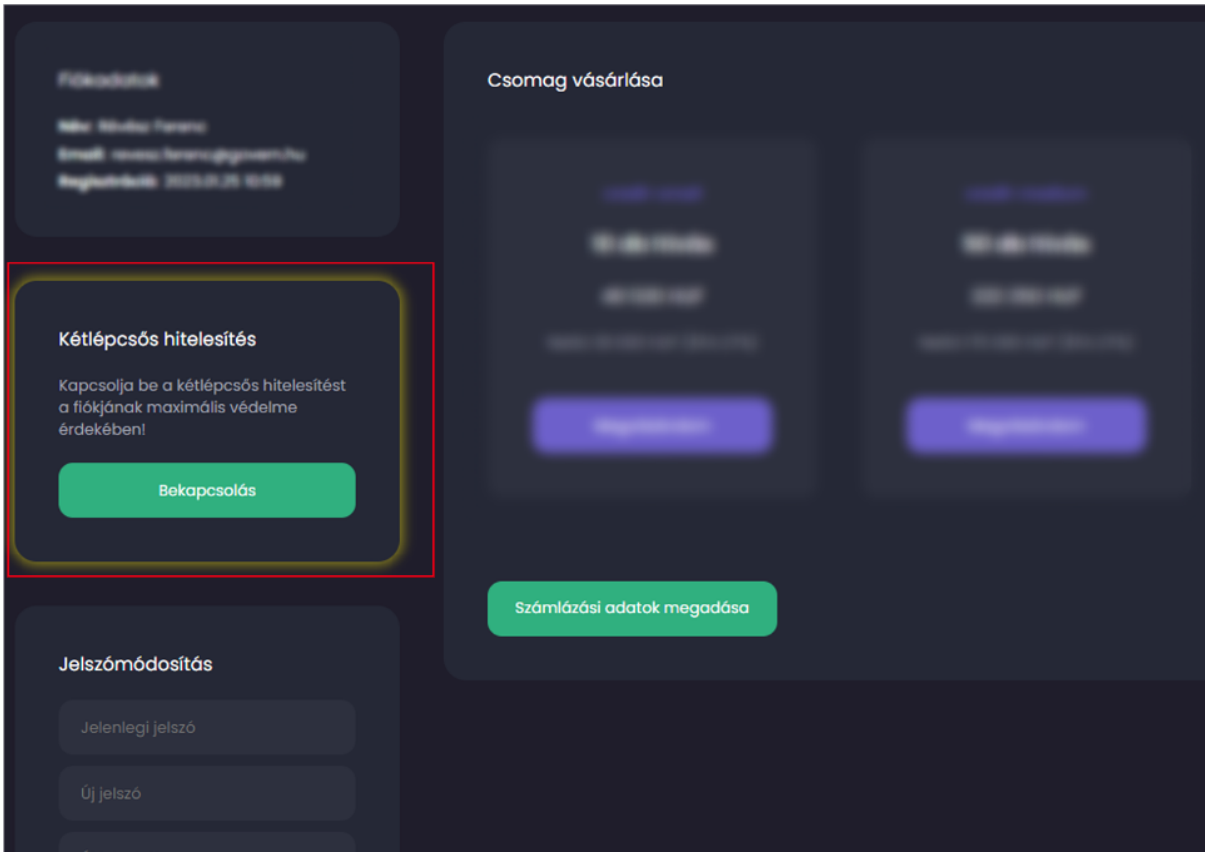
Fontos: A kézikönyv csak a Google Authenticator használatát tárgyalja.

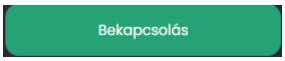
Fontos: Figyeljen arra, hogy a hitelesítő kódjait ne ossza meg senkivel, illetve fokozottan figyeljen a telefonja épségére és a telepített Authenticator alkalmazás megtartására, ugyanis ezek hiányában elveszítheti fiókjához való hozzáférést.

Fontos: Elhagyott vagy elromlott készülék esetén hitelesítő kódok híján már csak helyreállító kóddal (későbbi fejezet) léphetünk be a fiókunkba. Ilyenkor kapcsoljuk ki átmenetileg a kétfaktoros hitelesítést, majd rögtön aktiváljuk újra, de már az új mobiltelefonunkat használva.

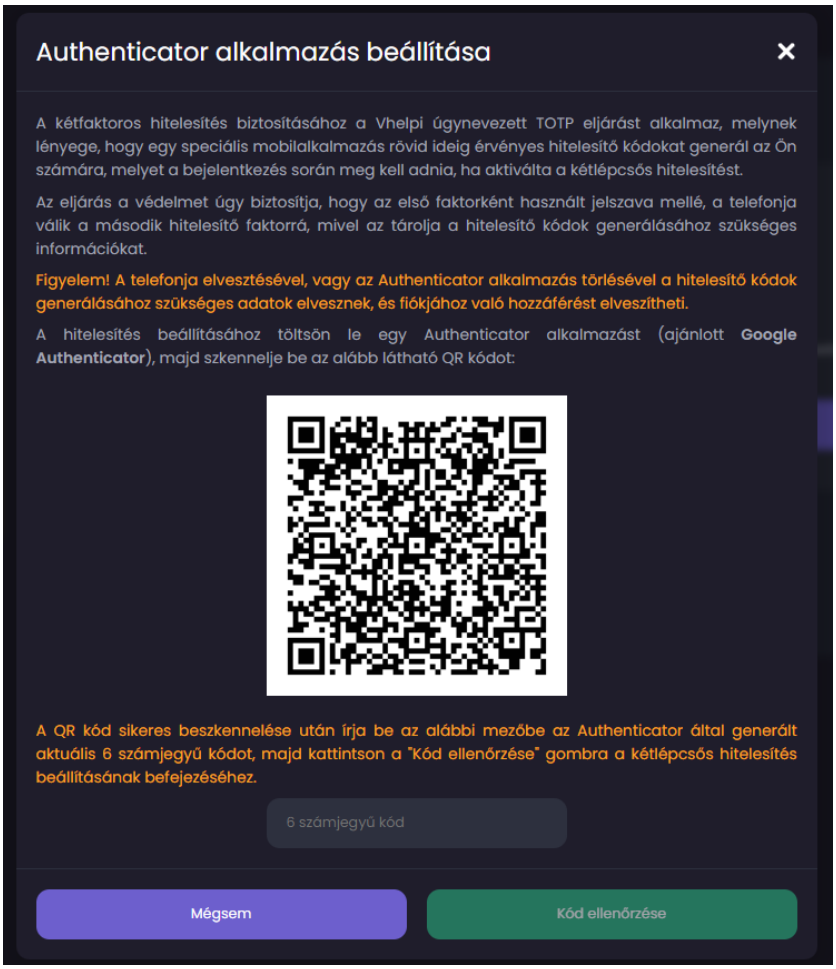
Funkció beállítási folyamata

Az alkalmazás letöltése után a kétfaktoros hitelesítési folyamat beállítás folytatható a Vhelpi Profil felületén, mely a jobb felső sarokban található lenyíló menüből érhető el.

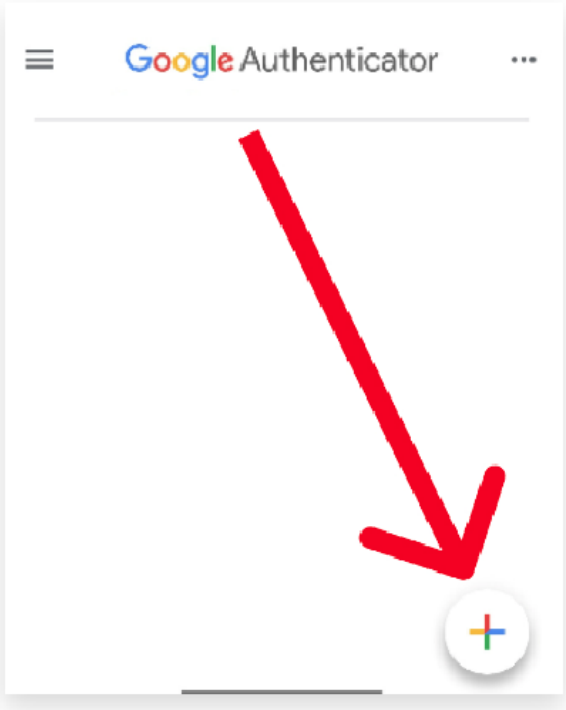


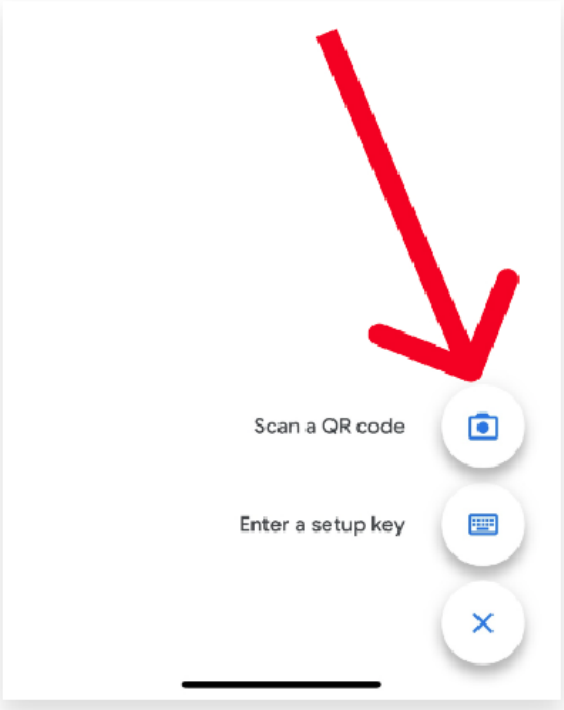
A 

gombra kattintva megjelenik egy QR kód, melyet a korábban letöltött Authenticator applikációval beolvashatunk.

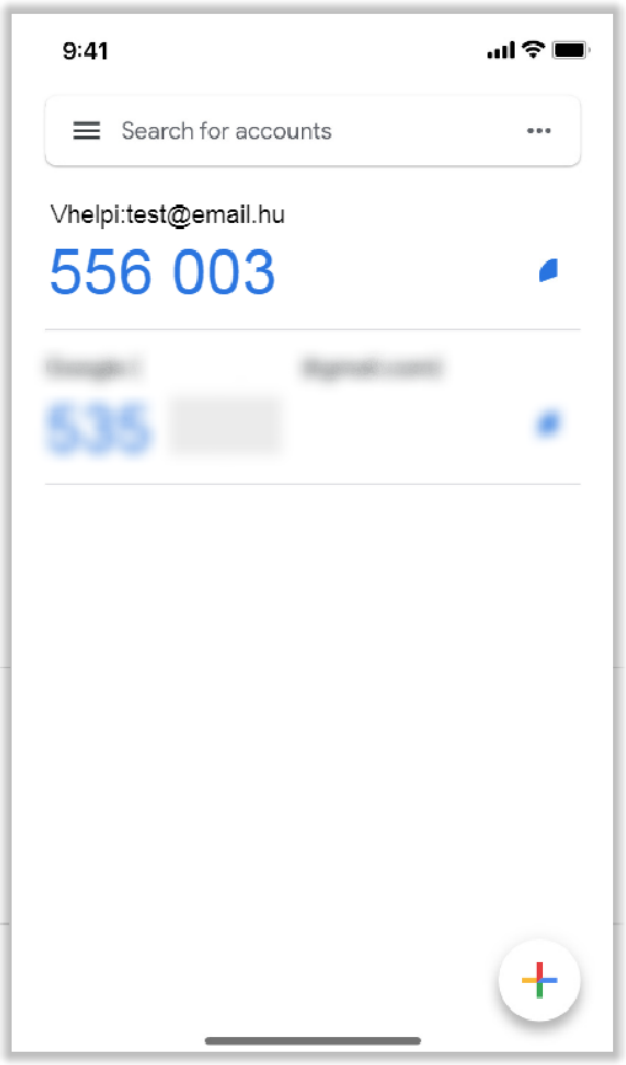


A Google Authenticator alkalmazásban a jobb alsó sarokban található színes "+" gombra, majd a megjelenő "QR-kód beolvasása" (angolul "Scan a QR code") gombra kattintva megnyílik a telefon kamerája, amivel beolvasható a Vhelpi felületén megjelentő QR-kód.

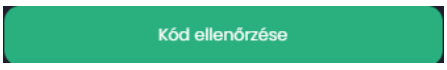




Amint az alkalmazás sikeresen beolvasta a Vhelpi által megjelenített QR-kódot, a főképernyőn megjelenik a fiók neve (Vhelpi) és a felhasználó e-mail címe, illetve egy 30 másodpercenként változó, 6 számjegyű kód.

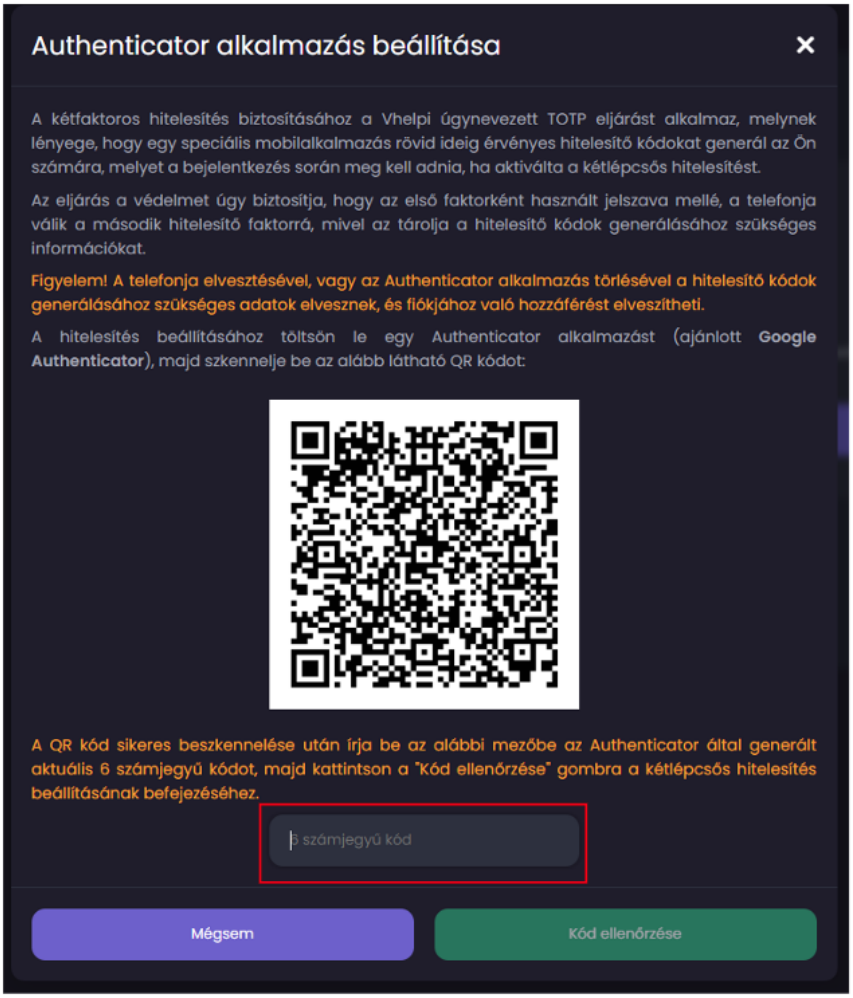


Ahhoz, hogy ellenőrizni tudjuk, hogy telefonja sikeresen beolvasta a hitelesítő kód generálásához szükséges információkat, kérjük írja be a telefonján aktuálisan megjelenő 6 számjegyű kódot a Vhelpi felületén látható mezőbe a QR kód alatt, majd kattintson a

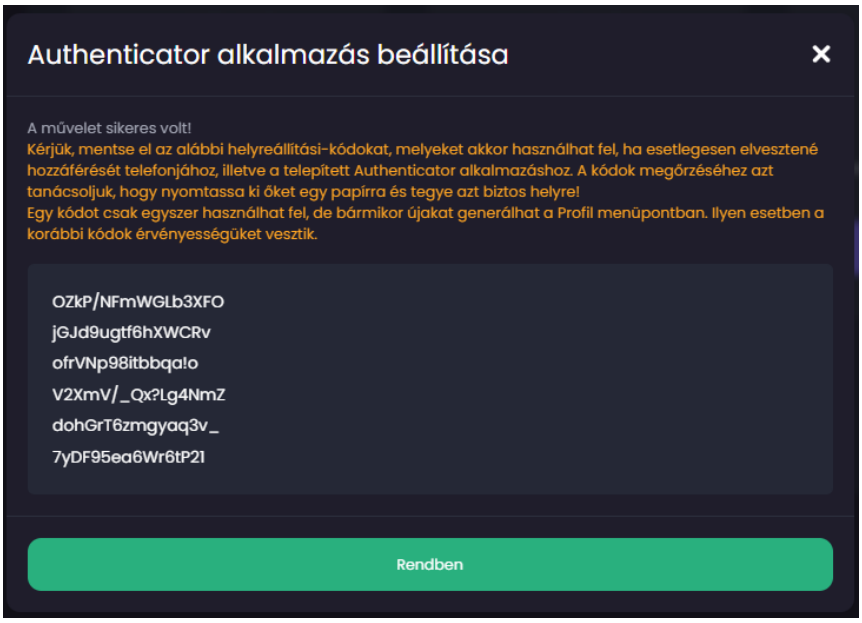


gombra.

Fontos: A hitelesítő kódot mindig szóközök nélkül írja be, ahol a rendszer kéri, attól függetlenül, hogy az Authenticator alkalmazásokba szóközzel tagolva vannak a kódok a jobb olvashatóság miatt.



Ha a kód visszaellenőrzése sikeres volt, a következő felületen 6 darab helyreállítási-kód látható. Mindegyik kód egyszer használható a hitelesítő kódok helyett, ha esetlegesen a felhasználó nem férne hozzá telefonjához (átmenetileg vagy esetleg véglegesen). Ezeket a kódokat célszerű biztos helyre elmenteni, akár kinyomtatni egy papírra és biztos helyre rakni.

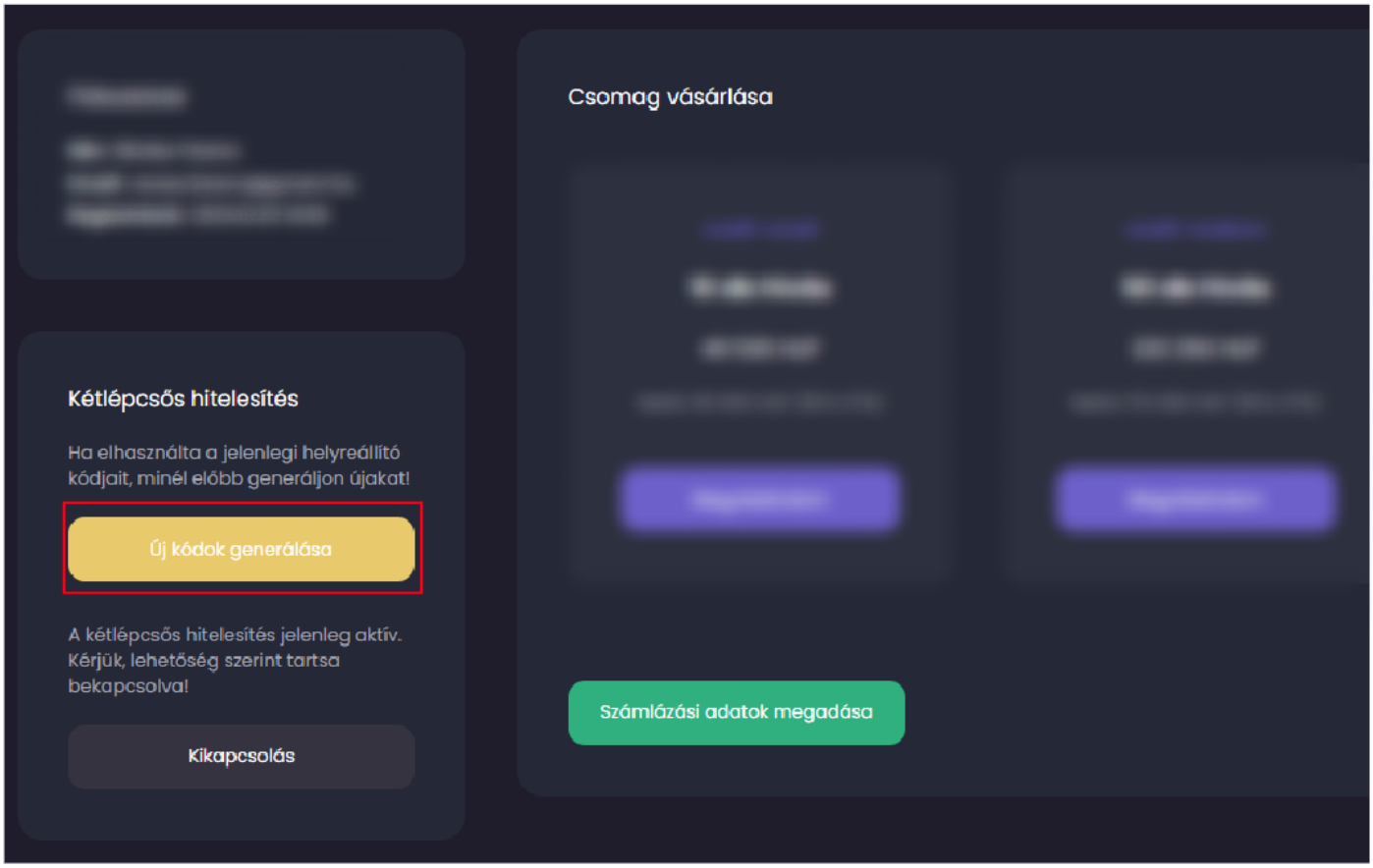


Fontos: Minden helyreállító-kód csak egy bejelentkezéshez használható, utána érvénytelenné válik, ezért ha már több kód is fel lett használva, érdemes generálni új 6 darab kódot. (következő fejezet)

Fontos: Mobilkészülék csere esetén az Authenticator applikációk biztosítanak eszközök közötti fiók szinkronizációt.

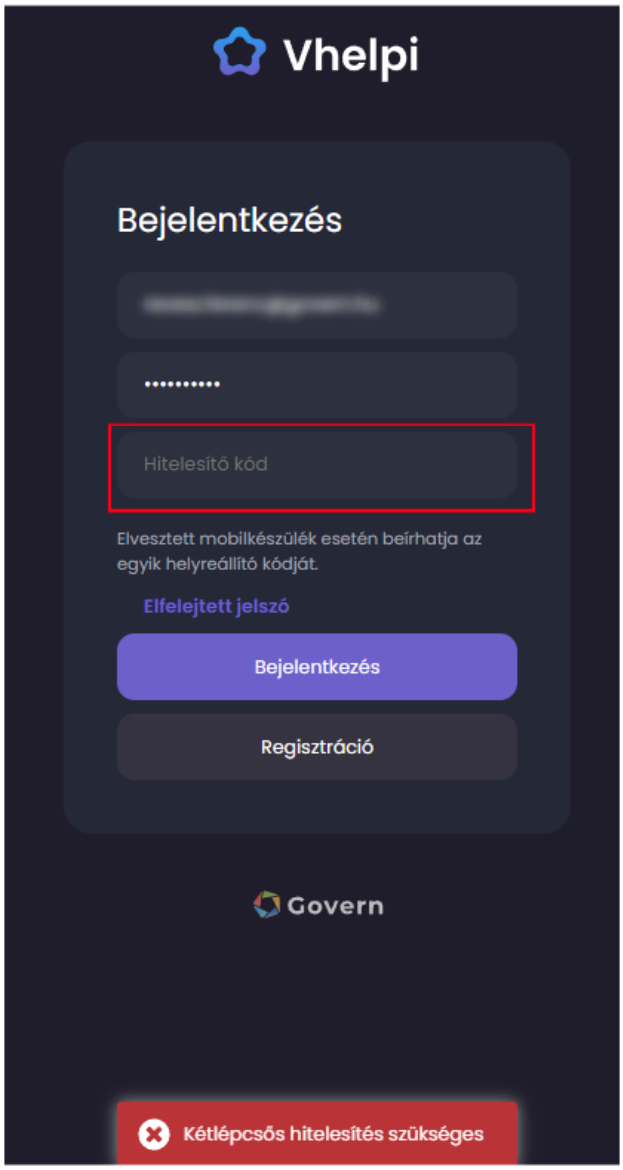
Helyreállító kódok újragenerálása

A kétfaktoros hitelesítés beállítás során a Vhelpi 6 darab helyreállító kódot generált, mely mindegyike csak egyetlen belépés erejéig alkalmazható. Ugyan kicsi az esélye, hogy egy felhasználó 6 alkalommal vesztené el mobiltelefonjához való hozzáférést, és egy-egy helyreállító kódot kellene elhasználnia, mégis figyelembe vettük ezt a lehetőséget is. A Profil oldalon lehetőség van 6 darab új helyreállítási kódot generálni, de fontos megemlíteni, hogy ilyen esetben a korábbi helyreállító kódok érvénytelenné válnak.



Bejelentkezés menete kétfaktoros hitelesítéssel

Kétfaktoros hitelesítés esetében a bejelentkezés menete hasonlóan működik, mint alapesetben: a felhasználó megadja e-mail címét és jelszavát, majd a Bejelentkezés gombra kattintva megpróbál bejelentkezni. Ha a belépési adatok helyesek, és a fiókban aktív a kétfaktoros hitelesítés, megjelenik egy 3. mező a felületen, melybe meg kell adni az Authenticator alkalmazásból kiolvasott, aktuálisan érvényes 6 számjegyű hitelesítő kódot. A felhasználó kényelme érdekében nem csak az aktuális 30 másodperces időintervallumban érvényes hitelesítő kódot fogadja el a rendszer, hanem időablak szerűen az előző és a következő időintervallumhoz tartozó kódokat is. Ebből kifolyólag nem jelent problémát, ha egy kód begépelése közben az Authenticator applikáció megváltoztatja a kódot, mivel azt a kód is elfogadja a rendszer, amit a felhasználó eredetileg is elkezdett beírni.



Abban az esetben, ha a bejelentkezés idején a felhasználó telefonja nincs kéznél, esetleg elvesztette hozzáférését a telefonhoz és az Authenticator applikációhoz, a 6 számjegyű hitelesítő kód helyett megadható egy korábban generált helyreállító kód is, mely a használat után érvénytelenné válik.

Változat #3
Révész Ferenc hozta létre 3 június 2024 10:06:15
Révész Ferenc frissítette 3 június 2024 14:01:44