5. FELHASZNÁLÓI FIÓKOK BIZTONSÁGA

A felhasználói fiókok (pl. közösségi oldal, levelezési fiókok) védelme a tárolt adatok, információk, fényképek, videók miatt különösen fontos. Ha illetéktelen személy lép be a felhasználói fiókba, az ott tárolt információkat ugyanúgy láthatja, még ha azokat nem is osztotta meg a profil tulajdonosa. A megszerzett információkkal visszaélhetnek, nagy nyilvánosság részére közzé tehetik vagy akár zsarolhatják is vele az áldozatot.

A felhasználói fiókok védelmének célja, hogy csak a jogosult tudjon belépni és hozzáférni a fiókban tárolt adatokhoz.

ELEMEI:

- megfelelő **JELSZÓ** és a jelszó védelme,
- **KÉTFAKTOROS HITELESÍTÉS**,
- **MUNKAMENET LEZÁRÁSA** – kilépés a fiókból.

A megfelelő jelszóról részletesebben a JELSZAVAK kiadványban olvashat.

BIZTONSÁGI TANÁCSOK

- Mindig válasszon megfelelő jelszót!
- Ha lehet, kapcsolja be a kétfaktoros hitelesítést!
- Nem kizárólagosan használt számítógépen lépjen ki a felhasználói fiókból! A böngésző bezárása nem mindig elég!
- Okostelefonján, tabletjén állítson be képernyőzárat!
- Jelszavát mindig tartsa titokban, ne adja meg senkinek!

KÉTFAKTOROS HITELESÍTÉS

A kétfaktoros hitelesítés azt jelenti, hogy a hagyományos **FELHASZNÁLÓI NÉV – JELSZÓ PÁROS** mellett a rendszer még egy **MÁSIK MÓDON** is hitelesíti a felhasználót. A hitelesítés módja lehet:

- **BIOMETRIKUS HITELESÍTÉS**: arc, ujjlenyomat, retina,
- **TUDÁS ALAPÚ HITELESÍTÉS**: jelszó, válasz, PIN kód, minta,
- **BIRTOKLÁS ALAPÚ HITELESÍTÉS**: token, kártya.

A felhasználó név – jelszó páros tudás alapú hitelesítésnek minősül.

Ha a második hitelesítés módja megegyezik az elsődleges hitelesítés módjával, jelen esetben az is tudásalapú, akkor kétlépcsős hitelesítés történik, ha a második módja eltér az elsődlegesétől, (pl. biometrikus vagy birtoklás alapú hitelesítés), akkor beszélünk kétfaktoros hitelesítésről.

A kétfaktoros hitelesítés nagyobb biztonságot nyújt a felhasználói fiókokra. Jellemzően új, korábban nem használt eszközön történő belépéskor használandó. Az általunk rendszeresen használt eszközökön **KIKAPCSOLHATÓ**, meggyorsítva ezzel a belépés folyamatát.

KIBERBIZTONSÁGI TIPPEK

A kétfaktoros hitelesítés általában a felhasználó okostelefonjának segítségével történik, legbiztonságosabb, ha valamilyen alkalmazáson keresztül. Ez lehet a szolgáltatás **SAJÁT ALKALMAZÁSA** (Facebook, Google vagy az adott bank applikációja). Ebben az esetben az alkalmazásban lehet jóváhagyni a másik eszközön (pl. számítógépen) történő bejelentkezést.
Léteznek **AUTENTIKÁCIÓS ALKALMAZÁSOK**, amelyekben egy **QR KÓD** segítségével lehet rögzíteni az adott oldalt, és bejelentkezéskor az adott oldalhoz rendelt – rendszeres időközönként változó – kódot kell megadni a másik eszközön.
Az oldal küldhet egyszeri alkalomra szóló hitelestő kódot **SMS-BEN VAGY E-MAILBEN**. Ezek kevésbé biztonságosak, mint az előző megoldások.

A különböző szolgáltatók kétfaktoros hitelesítést hívják **KÉTFAKTOROS VAGY KÉTLÉPCSŐS AZONOSÍTÁSNAK** is. Az eltérő elnevezés ellenére ugyanarról a technikai megoldásról van szó.

MUNKAMENET LEZÁRÁSA

A nem kizárólag általunk használt számítógépen (iskolában, munkahelyen, ismerősnél, nyilvános helyen) mindig **JELENTKEZZÜNK KI** a felhasználói fiókból, a böngésző **BEZÁRÁSA NEM ELEGENDŐ**, mivel az oldal újbóli megnyitása esetén belép az utóljára használt felhasználói fiókba. Egy ilyen számítógépeken a felhasználói nevünket és jelszavunkat se jegyeztessük meg a böngészővel! Célszerű a böngésző **PRIVÁT/ INKOGNITÓ MÓDJÁNAK** használata. Ebben az esetben a böngésző nem menti a böngészési előzményeket, a cookie-kat, a webhelyadatokat és az űrlapokon megadott adatokat.
A privát/inkognitó mód bekapcsolása:

- Internet Explorer: CTRL+SHIFT+P
- Mozzila Firefox: CTRL+SHIFT+P
- Chrome: CTRL+SHIFT+N

TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN

www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

www.facebook.com/internettudatosan

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN
Országos Rendőr-főkapitányság