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.

#FelhasználóiFiók #Jelszó #KétfaktorosAzonosítás #MunkamenetLezárása #PrivátMód

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 azonosítás**
- **Munkamenet lezárása** – kilépés a fiókból
- A megfelelő jelszóról részletesebben a JELSZAVAK ÉS JELMONDATOK kiadványban olvashat.

KÉTFAKTOROS AZONOSÍTÁS

A kétfaktoros azonosítás azt jelenti, hogy a hagyományos **felhasználói név – jelszó páros** mellett a rendszer még egy **másik módon** is azonosítja a felhasználót. Az azonosítás módja lehet:

- **Biometrikus azonosítás:** arc, ujjlenyomat, retina
- **Tudás alapú azonosítás:** jelszó, válasz, PIN kód, minta.
- **Birtoklás alapú azonosítás:** token, kártya.

A felhasználó név – jelszó páros tudás alapú azonosításnak minősül. Ha a második azonosítás módja megegyezik az első azonosítás módjával, jelen esetben az is tudásalapú, akkor **kétlépcsős** azonosítás történik, ha a második módja eltér az elsőétől, (pl. biometrikus vagy birtoklás alapú azonosítás) akkor beszélünk **kétfaktoros** azonosításról.

A kétfaktoros azonosítás 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.

BIZTONSÁGI TANÁCSOK

- Mindig válasszon megfelelő jelszót!
- Ha lehet, kapcsolja be a kétfaktoros azonosítást!
- 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!

A kétfaktoros azonosítás általában a felhasználó okostelefonjának segítségével történik, legbiztonságosabb, ha valamilyen alkalmazás segítségével.

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 rögzíteni lehet az adott oldalt, és bejelentkezéskor az adott oldalhoz rendelt – rendszeres időközönként változó – kódot kell megadni a másik eszközön.

Az oldal küldhet egyszeri alkalomra szóló hitelesítő kódot **SMS-BEN VAGY E-MAILBEN.** Ezek kevésbé biztonságosak, mint az előző megoldások.

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 újból megnyitása esetén belép az utoljára 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.

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