ÚJ ÉV,
ÚJ FOGADALMAK

Legyen 2022 a tudatos internethasználat éve!
2022. január 3-án indul a "Biztonság közérthetően" sorozatunk.

Hétfőnként egy-egy kiberbiztonsági tippet mutatunk be részletesen, mindenki számára érthetően.

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN
Országos Rendőr-főkapitányság

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 készülekre 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!

1. Miért fontos a jó jelszóválasztás?

A jelszavak jelentik az első, sőt, ha nincs kétfaktoros hitelesítés, akkor az egyetlen védelmi vonalat a felhasználói fiókjainkhoz és az ott tárolt adatainkhoz. Alapvető, hogy minden felhasználói fiókhoz (e-mail, közösségi oldal, netbank, online tárhely, szolgáltatás, stb.) egyedi, hosszú és bonyolult jelszót állítsunk be, mivel egy ilyen jelszó kitalálása vagy feltörése gyakorlatilag lehetetlen, illetve ha valamelyik jelszavunk esetleg nyilvánosságra is kerül, más fiókjainknál nem tudnak majd visszaélni vele.

2. Kiszivárgott valamilyen személyes adatom?

Időről időre érdemes leellenőrizni, hogy kiszivárgott-e valamilyen személyes adatunk. Ehhez nyújt segítséget a https://haveibeenpwned.com/ oldal. Itt a regisztrációkhoz használt e-mail cím(ek) vagy telefonszámok megadásával ellenőrizhetjük, hogy kiszivárgott-e valamilyen személyes adatunk. Ha történt adatszivárgás, akkor az oldal tájékoztat arról is, hogy melyik szolgáltatás érintett és milyen típusú adatunk (e-mail, felhasználói név, jelszó (egyszerű szövegben vagy titkosítva) érintett. Az oldal nincs a konkrét adatok, - így természetesen a jelszó birtokában sem, ezért azokat megjeleníteni sem tudja.

3. Miért érdemes jelszókezelőt használni?

Egy felhasználó akár több tucat különböző felhasználói fiókkal/regisztrációval is rendelkezhet, így mindegyikhez egyedi, hosszú és bonyolult jelszót megjegyezni gyakorlatilag lehetetlen. Ebben segít egy jelszókezelő, amely eltárolja a felhasználói fiókhoz tartozó e-mail címet/felhasználói nevet és jelszót.

4. Hogyan működik a jelszókezelő?

A jelszókezelő lehet online szolgáltatás, amely egy weblapon keresztül érhető el, önállóan telepíthető alkalmazás a számítógépen, böngészőhöz tartozó kiegészítő, mobiltelefonos alkalmazás, illetve ezek kombinációja is. A legtöbb jelszókezelő képes a tárolt adatokat a különböző eszközeink között, pl. asztali böngésző kiegészítője (plug-inje) és a mobiltelefonos alkalmazás között szinkronizálni, de vannak olyan jelszókezelők is, amelyek csak egy eszközön tárolják az adatokat.
Léteznek ingyenes és fizetős jelszókezelők is. Az adatokat az alkalmazások titkosítva, mint egy széfben tárolják. A széf kinyitásához, vagyis a titkosítás feloldásához egy mesterjelszót kell megadni. Így gyakorlatilag elegendő egy jelszó, a mesterjelszó megjegyzése.

5. Regisztráció

Érdemes a kiválasztott szolgáltatás böngészős kiegészítőjét és a mobiltelefonos alkalmazását telepíteni, majd valamelyiken keresztül elvégezni a regisztrációt. Ehhez minden esetben meg kell adni egy megfelelő hosszúságú és bonyolultságú, máshol nem használt jelszót és általában az e-mail címünket. A regisztrációt követően bejelentkezhetünk a szolgáltatásba a böngésző kiegészítőben és a mobiltelefonos alkalmazásban is. A bejelentkezés után érdemes bekapcsolni a kétlépcső hitelesítést is, ha elérhető ez a funkció.

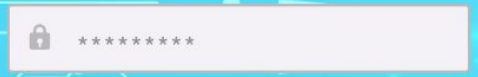


6. A jelszókezelő használata

A jelszókezelő nem csak a bejelentkezéshez szükséges adatokat (felhasználói név/e-mail, jelszó, szolgáltatás neve) tudja tárolni, de a böngészőben történő bejelentkezéskor automatikusan ki tudja tölteni a megfelelő adatokat. A jelszógenerátor segítségével könnyen létrehozhatunk egyedi jelszavakat, megadva azt is, hogy a jelszó milyen hosszú legyen, tartalmazzon-e nagybetűt, kisbetűt, számokat vagy speciális karaktereket. A különböző jelszókezelők további szolgáltatásokat is nyújthatnak.

Mi az a router?

A router az otthoni hálózat és az internet összekapcsolását és az adatforgalmat irányító eszköz. Sok esetben az internetszolgáltató biztosítja a felhasználóknak a routert, ehhez csatlakoznak vezetékkel vagy vezeték nélkül (WIFI-n) keresztül az eszközeink. Használhatunk saját routert is, ilyenkor ezt a szolgáltató eszközéhez kell csatlakoztatni, és az internetszolgáltató eszköze csak átjáróként funkcionál. Ebben az esetben a saját routerünk általában több funkcióval rendelkezik.



Miért kell megváltoztatni a router gyári jelszavát?

A router adminisztrációs felületére történő belépéshez jelszóra van szükség. Ez minden eszköz esetében gyárilag megegyezik, általában „admin”. A jelszó birtokában illetéktelenek is hozzáférhetnek a routerhez, módosíthatják a beállításait és elérhetik az otthoni hálózatot, valamint a rajta található eszközöket is. A routerünk az otthoni hálózatunk bejárati ajtaja, a jelszó pedig a kulcs hozzá. Csak akkor ér valamit, ha egyedi és csak mi ismerjük azt.

Hogyan változtassuk meg a router gyári jelszavát?

Mind szolgáltatói, mind a saját router adminisztrációs felületét a böngészőben lehet elérni, a router IP címének megadásával. Ez gyártóként változik, de általában 192.168.0.1. vagy 192.168.1.1, és a router alján lévő címkén vagy a csomagolásán szerepel. Az IP címet a böngészőbe bírva megjelenik bejelentkezési felület, ahol meg kell adni az adminisztrátori jelszót, és egyes típusoknál a felhasználói nevet. A gyári jelszó és a felhasználói név is „admin”, de ez is megtalálható a router alján lévő címkén és felhasználói útmutatóban.

A felhasználói routereknél a bekapcsolást követő első beállításkor általában kéri ennek megváltoztatását. Minden esetben egyedi, máshol nem használt jelszót adjunk meg, amit jegyezzünk fel egy papírra, és tegyünk biztonságos helyre.

Akkor is változtassuk meg saját routerünk jelszavát – és ha lehet, a bejelentkezéshez szükséges felhasználói nevet is –, ha ezt a beállításkor nem ajánlotta fel. Hasonlóan járjunk el a szolgáltatói router esetében is. A szolgáltató által végzett frissítéskor az alapértelmezett adatokra visszaállíthatja ezeket a beállításokat).

A felhasználói nevet általában az Adminisztráció vagy Rendszer menüpontban lehet megváltoztatni. Ehhez meg kell adni a régi jelszót, majd általában kétszer az újat.

Mi az a firmware?

A firmware az elektronikai eszköz (pl. router) működését irányító szoftver. A firmware vezérli magát a routert, határozza meg, hogy milyen funkciókkal, beállítási lehetőségekkel rendelkezik. A firmware-k hardverspecifikusak, így mindig a megfelelő típusú és verziójú routerhez készített firmwaret szabad csak telepíteni.

Miért kell a firmwaret frissíteni?

A gyártók kisebb-nagyobb gyakorisággal szoktak frissíteni a routereik firmware-jét. Ezek a frissítések tartalmazhatnak új funkciókat, javíthatják a teljesítményt vagy sérülékenységeket és egyéb hibákat javíthatnak. A sérülékenységek sebezhetővé teszik a routert, lehetőséget biztosítanak, hogy illetéktelen személyek is belépjenek rajta keresztül az otthoni hálózatunkba és az ott lévő eszközökbe. A frissítések javítják az ismertté vált sérülékenységeket és növelik a hálózatunk biztonságát.



Hogyan kell telepíteni a router firmware-jét?

A firmware-t tartalmazó fájlt a router gyártója készíti és teszi közzé honlapján az eszköz aloldalán, általában a Támogatás nevű menüpontban. A fájlt le kell tölteni a számítógépre, majd a router adminisztrációs felületén keresztül kell telepíteni. Ezt a böngészőben lehet elérni, a router IP címének megadásával, ami gyártókként változik, de általában 192.168.0.1. vagy 192.168.1.1, és a router alján lévő címkén vagy a csomagolásán szerepel. Az IP címet a böngészőbe beírva megjelenik a bejelentkezési felület, ahol meg kell adni az adminisztrátori jelszót, és egyes típusoknál a felhasználói nevet. Keressük meg az Adminisztráció vagy Rendszer menüben a Firmware frissítése funkciót. Itt ki kell választani a letöltött fájlt, majd a feltöltés/frissítés gombra kattintva a router telepíti az új firmware-t. A telepítés során a router újraindul. Csak az adott típusú és verziójú routerhez készült firmware-t telepítse, különben a router működőképtelenné válhat. A telepítés lehetőleg vezetékes kapcsolattal csatlakozó számítógépről végezze el. A pontos típust és verziószámot megtalálja a router alján lévő címkén és a csomagolásán is.