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.