



### MUNKAVÁLLALÓI TÁJÉKOZTATÓ

*Kétfaktoros azonosítás bevezetése az unideb.hu postafiókokhoz kapcsolódóan*

A Debreceni Egyetem valamennyi dolgozója részére

#### Tisztelt Munkatársak!

Az informatikai biztonság, alkalmazásbiztonság erősítése érdekében szükségessé vált a kétfaktoros felhasználói azonosítás fokozatos bevezetése az unideb.hu Microsoft 365 levelező szolgáltatásban.

A Debreceni Egyetem felhasználói, munkavállalói nagy tömegű személyes-, egészségügyi különleges-, gazdálkodási-, kutatási adathoz, információhoz férnek/férhetnek hozzá, amelyek az Egyetem számára nem csak anyagi, de jelentős mértékű eszmei értéket is képviselnek. Az adatok, információk hatékony és erős védelme elsősorban az azt kezelő felhasználókon keresztül történhet meg, valamint a rendszerekbe történő belépés biztonságának növelésével.

A kizárólag egyszerű jelszavakon alapuló technikák, mára már nem tudják szükségszerűen biztosítani a kívánt biztonsági szintet. A jelszavak megkövetelt formai bonyolításával, periodikus cseréjével egy pontig növelhető a jelszavak biztonsága, támadásokkal szembeni ellenállása, viszont az azonosítás során egy másik, a memorizált jelszótól független, új faktor bevezetése nagyságrendekkel megnöveli az azonosítás biztonságát.

A többszörös hitelesítés (multi faktoros azonosítás – MFA vagy kétfaktoros azonosítás 2FA) engedélyezésével gondoskodhatunk arról, hogy először az egyetemi dolgozók által leggyakrabban használt szolgáltatás, az elektronikus levelezés biztonsági szintje jelentősen emelkedjen. Így azon túl, hogy a hitelesítés erősebbé válik, várhatóan az egyetemi e-mail címek kompromittálódása megszűnik.

Az egyetemen használt Microsoft 365 szolgáltatás támogatja a kétfaktoros hitelesítést, mivel a legtöbb felhasználó használ email szolgáltatást, ezért itt a legcélravezetőbb elkezdni az IT biztonság fokozását, valamint a szabályozásoknak történő megfelelést.

A bevezetés ütemezetten szervezeti egységenként fog megtörténni, tervezetten 2023. júniusától 2023. decemberéig. Első körben a mostani bevezetés csak intézményen kívüli hálózatokból teszi kötelezővé ezt a fajta hitelesítést.

Az ütemezéseknek megfelelően az érintett szervezeti egységek előzetesen értesítve lesznek a szolgáltatás részükre történő alkalmazásáról. A hitelesítési beállítás elvégzéséhez kapcsolódóan a felhasználói segédlet is kiküldésre fog kerülni. Technikai segítséget a beállítások elvégzéséhez szükség esetén az Informatikai Szolgáltató Központ a 66333-as telefonszámon, vagy az Informatikai Biztonsági Központ a 62820-as telefonszámon fog biztosítani.

A biztonság erősítése közös érdekünk, kérem támogató hozzáállásukat!

Debrecen, 2023. május 26.

Üdvözlettel:

  
Dr. Bács Zoltán  
Kancellár

