



# FELHASZNÁLÓI SEGÉDLET

Microsoft365 elektronikus levelezési fiók védelem kéttényezős (2FA<sup>1</sup>)  
belépéssel

Microsoft Authenticator mobil applikáció és M365 levelezési fiók illesztése  
Android és iOS mobil telefon operációs rendszere alatt



---

<sup>1</sup> **2FA** – Two Factor Authentication. Egy fiókhoz vagy rendszerhez való hozzáférés előtt két különböző/eltérő hitelesítési forma megadása. 1. réteg, amit tud (jelszó) 2. réteg, amivel rendelkezik, amit birtokol (authenticator kód, SMS)

# Tájékoztató

Előzmény: KC/376/2023. Kancellári munkavállalói tájékoztató (1. sz. melléklet), a Microsoft 365 szolgáltatáshoz kapcsolódó kétfaktoros azonosítás bevezetéséről.

Lépésfeladat eszközeinek jelölés magyarázata.

A 2FA telepítés mobil telefonkészülékén és az asztali/hordozható eszközén, együttesen történik.

A telepítési folyamat lépéseinek számozása mögött, piktogrammal került feltüntetésre, hogy időszerűen melyik eszközén kell dolgoznia.

Mobil telefonkészülék:



Kijelző/monitor/képernyő:



Számítógépen, hordozható eszközön végzett feladatok.

„Kattintson”



„Koppintson”





## 1. Lépés

Asztali (Pc) vagy hordozható eszközén (Notebook, Laptop) indítsa el internet böngészőjét (Google Chrome, Mozilla Firefox, Microsoft Edge) majd a címsorba (címmezőbe) írja be a <https://office.com> web címet és nyomjon Entert.

A felületen kattintson a „Bejelentkezés” gombra.

A megjelenő ablakban adja meg Egyetemi levelezési fiókjának címét (1), majd ezt követően kattintson a „Tovább” gombra (2) vagy válassza ki e-mail fiókjának címét és kattintson a „Tovább” gombra, vagy mentett bejelentkezési adatok esetén **(Nem jelent személyi biztonságot, nem ajánlott!)**, folytassa a 2. Lépéstől.



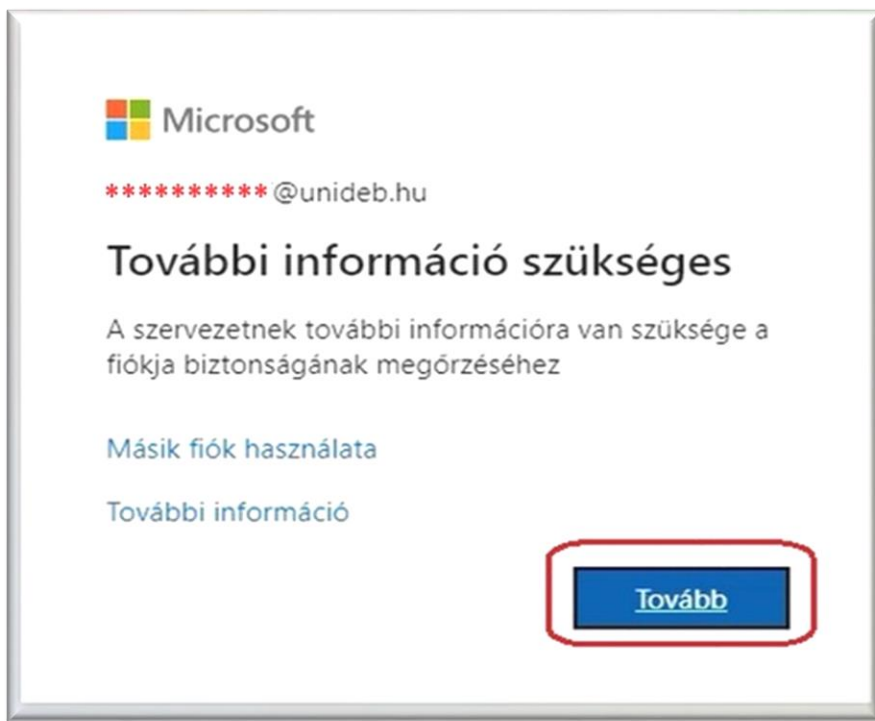
## 2. Lépés

Gépelje be Egyetemi EduID felhasználói adatait, Felhasználói nevét, jelszavát, majd ezt követően kattintson a „Bejelentkezés” gombra vagy mentett belépési adatok esetén (!) kattintson a „Bejelentkezés” gombra.



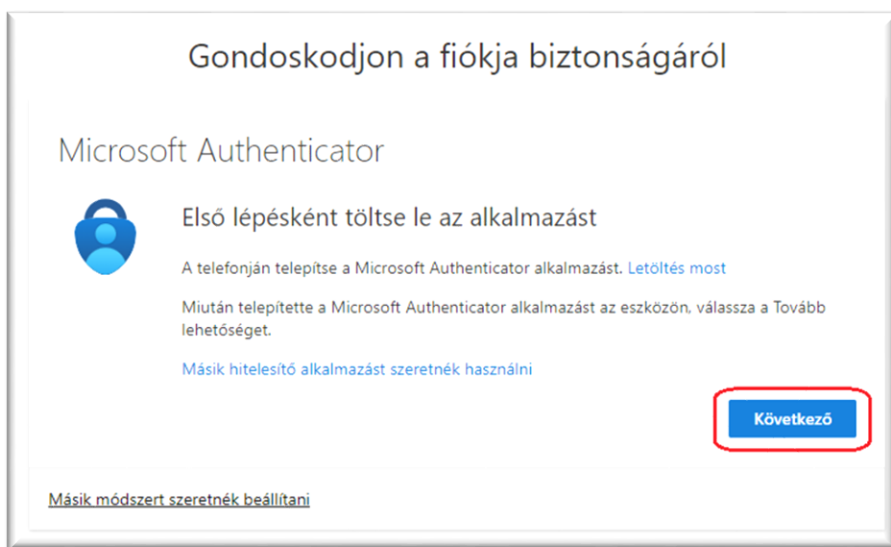
### 3. Lépés

Kattintson a „Tovább” gombra (Semmi mást nem kell kiválasztania!).



### 4. Lépés

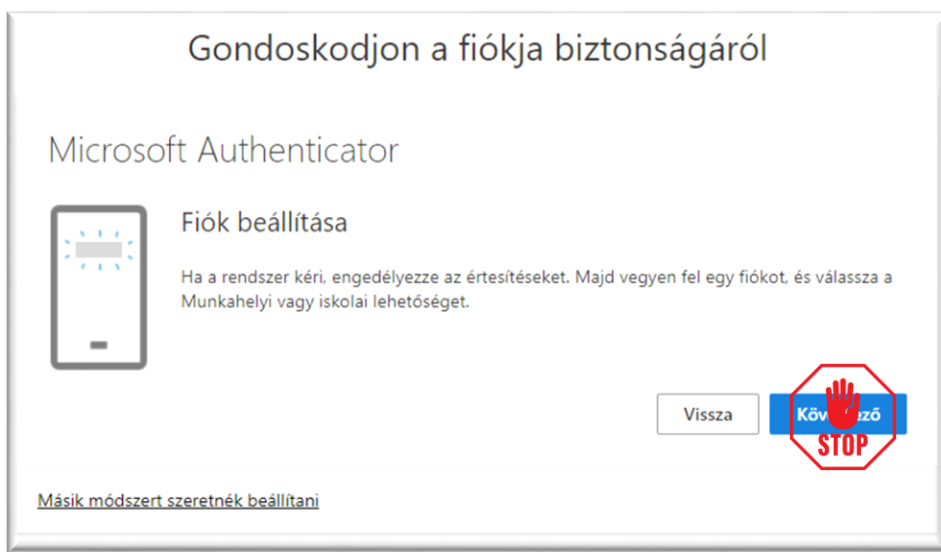
Kattintson a „Következő” gombra (Semmi mást nem kell kiválasztania!).





## 5. Lépés

NE kattintson a „Következő” gombra.



**Most ne kattintson a „Következő” gombra, ezt majd a 11. lépésben kell megtennie.**



**Oka:** A következő oldal egy QR kódot tartalmazna, amit Önnek telefonkészülékével be kell olvasnia. A szolgáltató időkorlátot alkalmaz a képernyőjén/kijelzőjén megjelenített QR kód beolvasásához, ami letelhet addig, amíg a mobil applikációt (Microsoft Authenticator) telefonjára telepíti, majd azt használatba veszi.



**VEGYE ELŐ MOBIL TELEFONKÉSZÜLÉKÉT!**



## 6. Lépés

A. Amennyiben mobil készülékén **már van telepítve**, és egyéb kötelem miatt (mint például a NEPTUN) használatban is van **az Authenticator**.

1. Nyissa meg mobil készülékén az Authenticatort (amennyiben kéri az Authenticator zárolásának a feloldását, tegye meg a készülékének védelme szerinti móddal (ujjlenyomat, arc-, írisz felismerés, PIN kód, minta)
2. Koppintson a készülék kijelzőjének jobb felső felületen látható „+” jelre
3. Koppintson a „Munkahelyi vagy iskolai fiók” opcióra
4. Koppintson a „QR kód beolvasása” pontra
5. **Folytassa** a telepítést a „Felhasználói leírás” **11. lépésétől (13. oldal)**

B. Amennyiben mobil készülékén **még nincs telepítve Authenticator**.

Töltse le mobil készülékére, telefonjának operációs rendszerére vonatkozó módszer valamelyike szerint) a **Microsoft Authenticator** applikációt.



A Microsoft Authenticator *ingyenesen letölthető és használható* mobil applikáció.

**Kérjük az applikációk letöltési felületén e szöveg előtt látható ikont keresse!**



Letöltése iOS-es eszközre (Apple)

### 1. Feladat



Telefonján nyissa meg a **AppStore** alkalmazást.

### 2. Feladat



A keresés mezőbe írja be a Microsoft Authenticator szöveget

### 3. Feladat

Koppintson a jobb alsó sarokban található  jelre.

### 4. Feladat

Koppintson a Microsoft Authenticator applikáció „**Telepítés**” gombjára



Letöltése Android-os eszközre (Samsung, LG, Motorola, Alcatel,..)

### 1. Feladat



Telefonján nyissa meg a **PlayÁruház** alkalmazást.

### 2. Feladat



A keresés mezőbe írja be a Microsoft Authenticator szöveget

### 3. Feladat

Koppintson a jobb alsó sarokban található  jelre.

### 4. Feladat

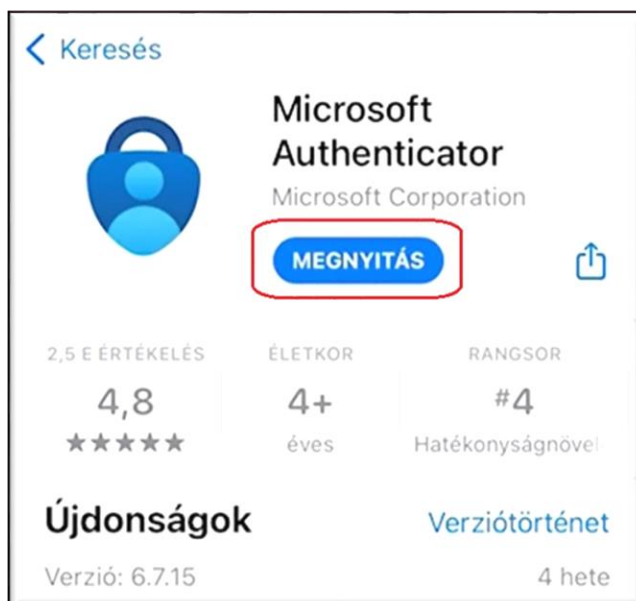
Koppintson a Microsoft Authenticator applikáció „**Telepítés**” gombjára



**Felhívjuk figyelmét, hogy az újabb Huawei telefonkészülékek HarmonyOS operációs rendszere nem támogatja a Microsoft Authenticator applikáció használatát.**

E készülékek esetén az SMS módszer szerinti védelmet kell telepítenie, az „0365\_2FA\_SMS\_beállítás.pdf” dokumentum leírását követve.

A letöltési és telepítési folyamat befejezése után **indítsa el** az applikációt a megjelenő „**Megnyitás**” gombra koppintva.





## 7. Lépés

Koppintson az „Elfogadás” gombra.



## 8. Lépés

Minden egyéb bejelölést mellőzve, koppintson a „Folytatás” gombra.







## 9. Lépés

Koppintson a „Munkahelyi vagy iskolai fiók hozzáadása” gombra.



A következő, 10. lépés feladatsora eltér ANDROID és iOS mobil operációs rendszerek tekintetében.

A készülékek típusát az alábbi ikonokkal jelezzük.

ANDROID

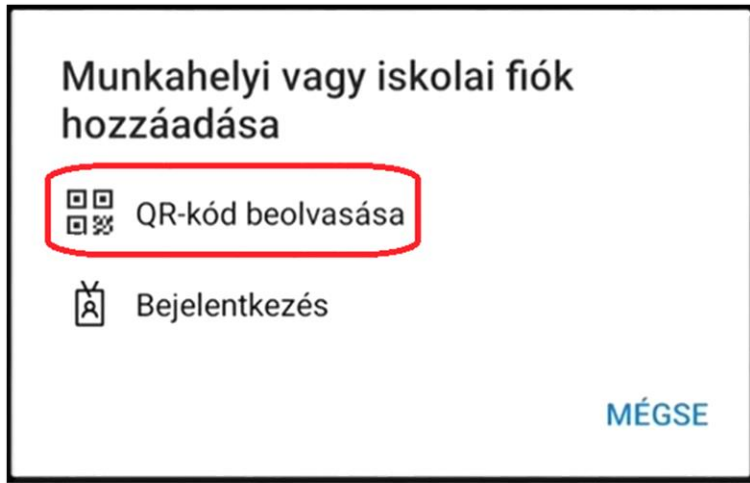
iOS



10. Lépés



Koppintson a „QR-kód beolvasása” gombra.

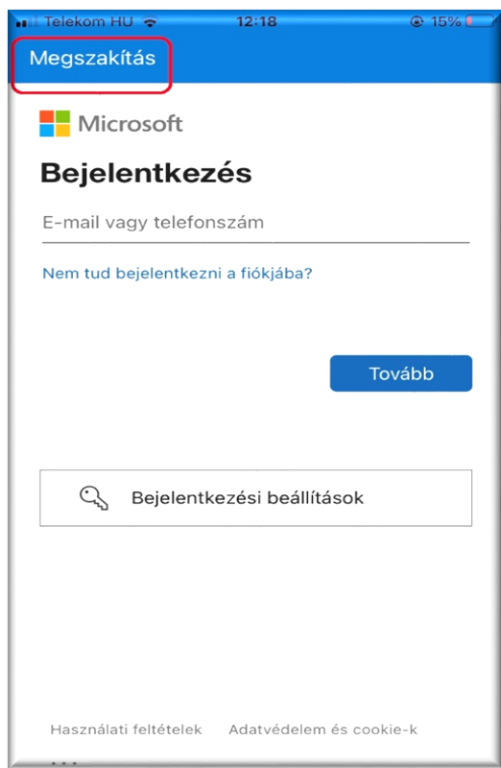


Lapozzon a 13. oldalra és folytassa a telepítési folyamatot a 11. lépéssel!

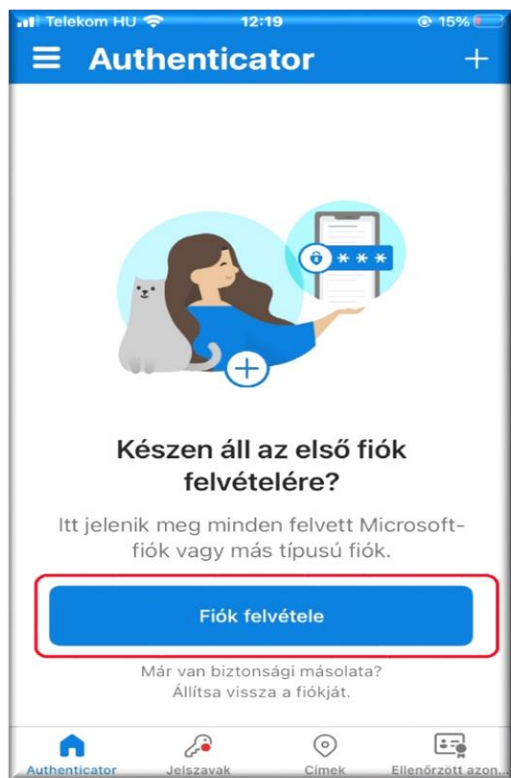
## 10, Lépés



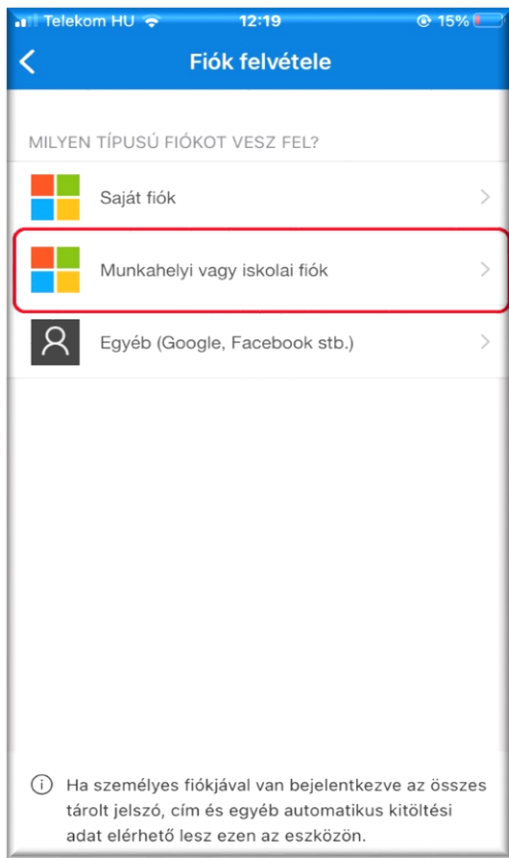
Koppintson a bal felső sarokban látható „Megszakítás” gombra



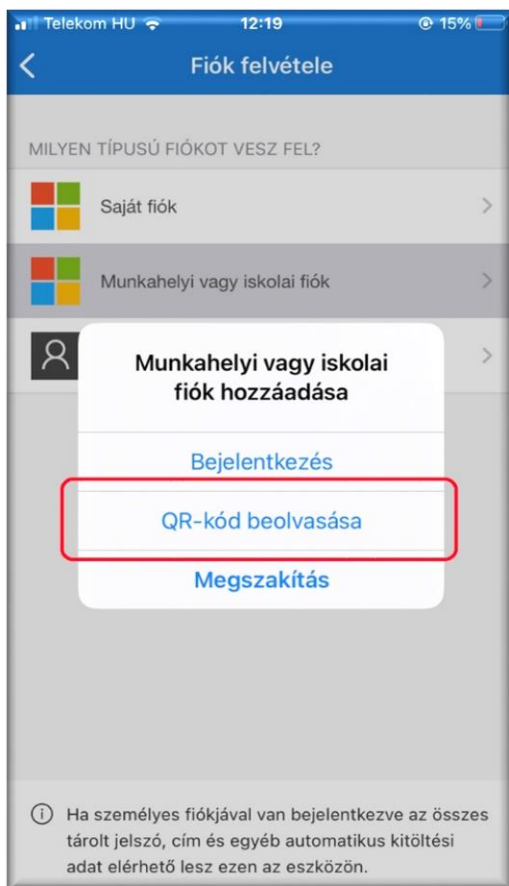
Koppintson a „Fiók felvétele” gombra



Koppintson a „Munkahelyi vagy iskolai fiók” gombra



Koppintson a „QR-kód beolvasása” gombra






## 11. Lépés

Most kattintson a monitorján/kijelzőjén a „Következő” gombra.

### Gondoskodjon a fiókja biztonságáról

#### Microsoft Authenticator



##### Fiók beállítása

Ha a rendszer kéri, engedélyezze az értesítéseket. Majd vegyen fel egy fiókot, és válassza a Munkahelyi vagy iskolai lehetőséget.

[Másik módszert szeretnék beállítani](#)

Kattintását követően, az alábbi képernyőkép jelenik meg a QR kóddal.


### Gondoskodjon a fiókja biztonságáról

#### Microsoft Authenticator

##### A QR-kód beolvasása

A Microsoft Authenticator alkalmazással olvassa be a QR-kódot. A művelet összekapcsolja a Microsoft Authenticator alkalmazást a fiókjával.

Miután beolvasta a QR-kódot, válassza a Tovább lehetőséget.

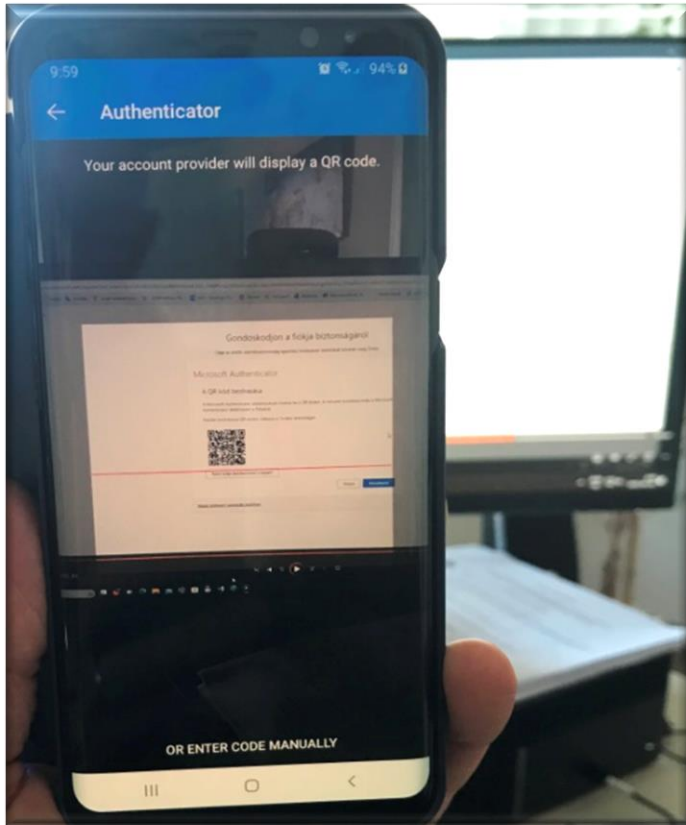


[Másik módszert szeretnék beállítani](#)



## 12. Lépés

Olvassa be a kijelzőjén látható QR-kódot, telefonja világosabb letapogató ablakának, a kijelző QR-kódot tartalmazó felülete felé közelítéssel.



## 13. Lépés

Sikeres beolvasást követően az applikáció kéri engedélyét a telefonjára történő rögzítéshez.

Kérem, koppintson az „Engedélyezem” gombra.

Felhasználói fiókja ezzel felvételre került telefonján a Microsoft Authenticator applikációba, ami az alábbi képet mutatja.



**! FIGYELEM!**

A Microsoft Authenticator hozzáférése (használata) során kéri/kérheti telefonjának biztonsági feloldás használatát.

Ez, a telefonjának idegen hozzáférés védelem érdekében beállított biztonsági módszere, ami lehet biometrikus (irisz-, arc felismerés, ujjlenyomat), PIN kód, jelszó, minta (3x3 pontos alakzat között húzott vonal).

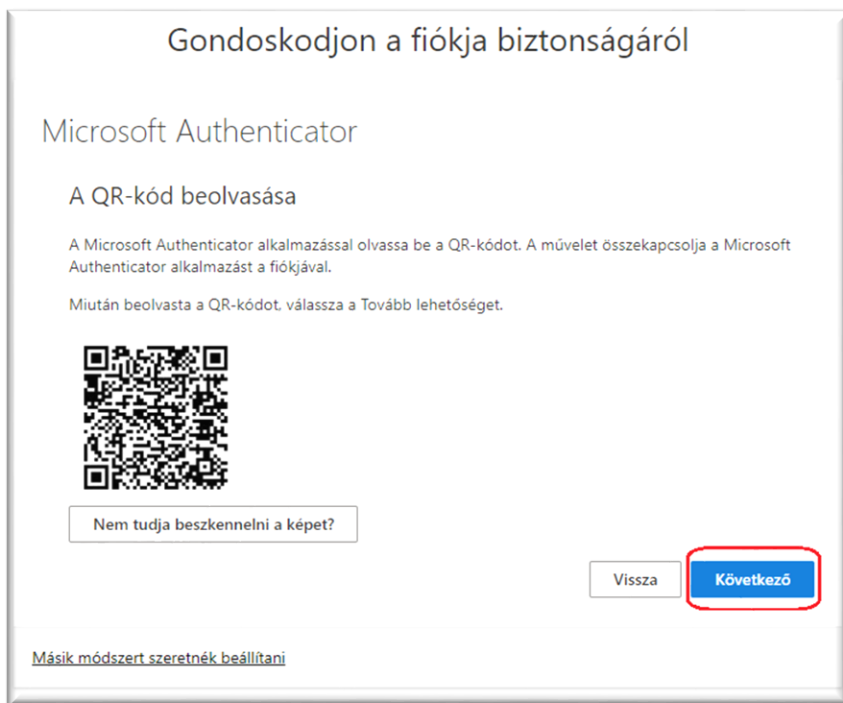


**Tegye le mobil telefonkészülékét és tekintsen a monitorra.**



#### 14. Lépés

Kijelzőjén kattintson a „Következő” gombra.



&



#### 15. Lépés

Kijelzőjén az alábbi kép jelenik meg, ami tartalmazza a kéttényezős hitelesítés ellenőrző számjegyét.







Ezt a számjegyet írja be (1.) a **telefonján** megjelenő Microsoft Authenticator beviteli mezőjébe („Adja meg a számot itt” felületre kattintást követően), majd kattintson a kékre színeződött „IGEN” gombra (2.).



Ön próbál bejelentkezni?

Debreceni Egyetem  
\*\*\*\*\*@unideb.hu

A bejelentkezéshez adja meg a megjelenített számot.

1.   
37

2.

NEM, NEM ÉN VAGYOK

NEM LÁTOM A SZÁMOT



Ön próbál bejelentkezni?

Debreceni Egyetem  
\*\*\*\*\*@unideb.hu

A bejelentkezéshez adja meg a megjelenített számot.

1.

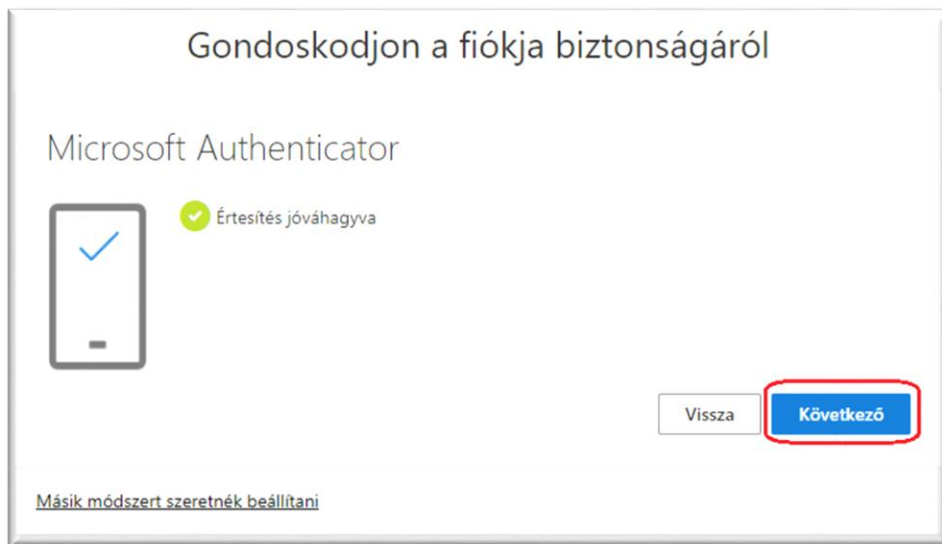
Nem, nem én vagyok.

2.



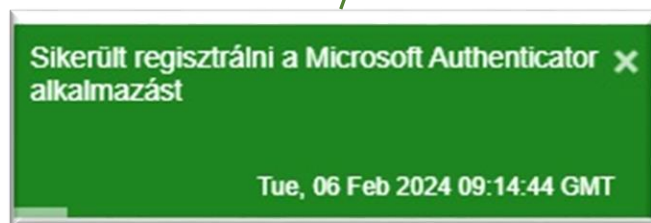
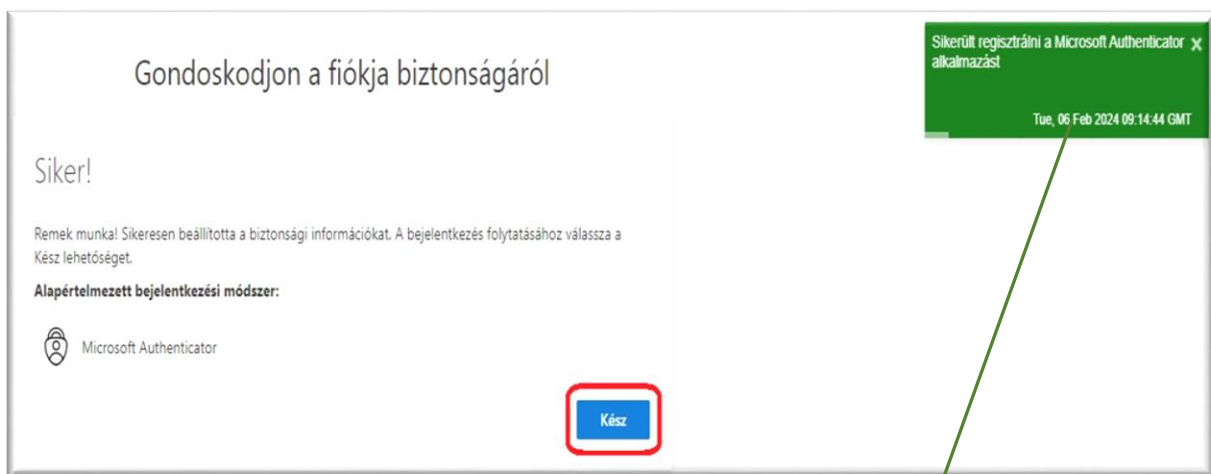
## 16. Lépés

Kijelzőjén kattintson a „Következő” gombra (Semmi mást nem kell kiválasztania!).

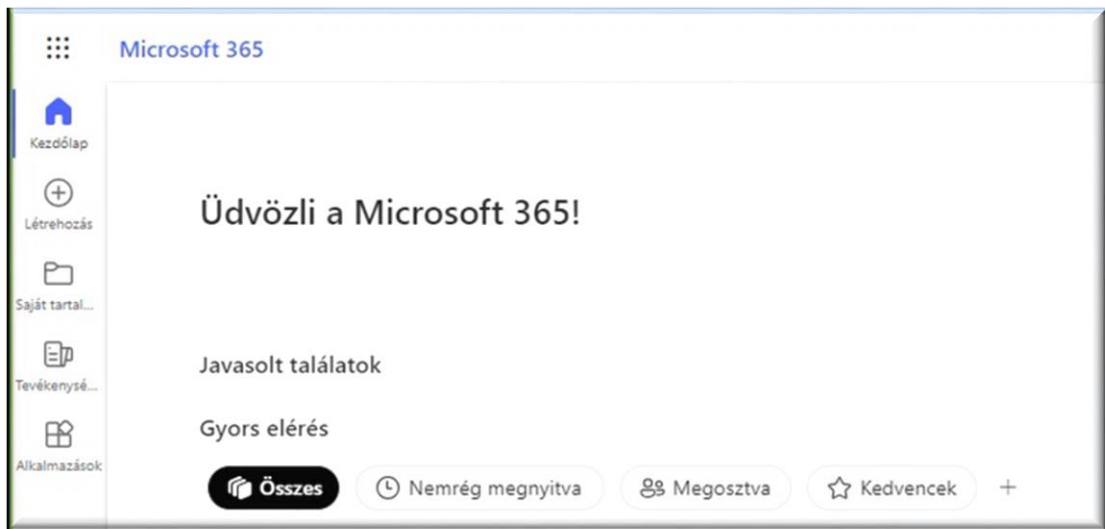


## 17. Lépés

Kijelzőjén kattintson a „Kész” gombra



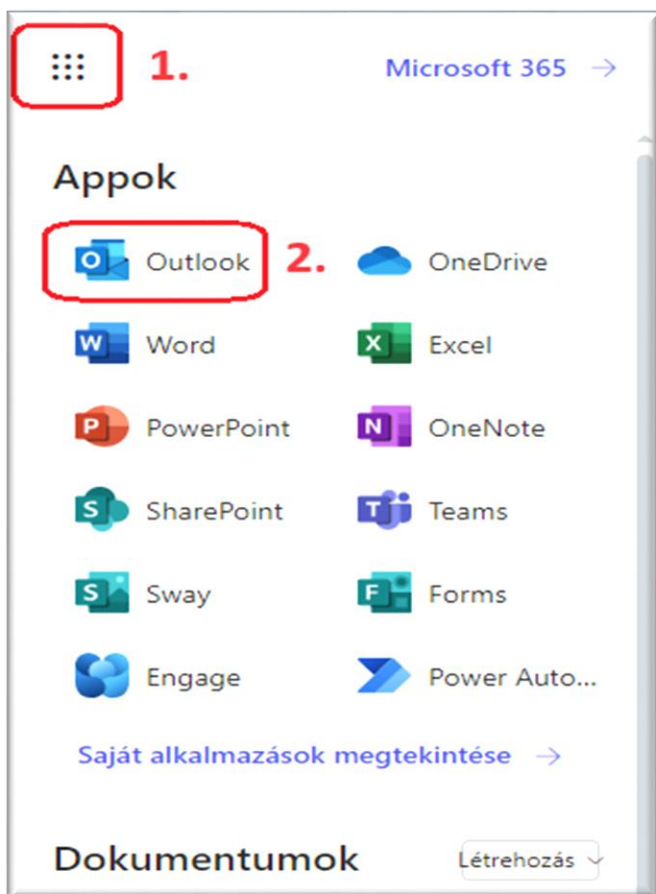
A hitelesítés sikeresen megtörtént, a belépés engedélyezett az Office felületre.



## 18. Lépés

A levelező felület megnyitása.

Kattintson a képernyő bal felső sarkában található kockamezőre/pontmezőre/hamburger menüre (1.), majd a kattintson az „Outlook” ikonra (2.).





**DEBRECENI  
EGYETEM**

**KANCELLÁR**

☎: H-4028 Debrecen, Kassai út 26.;  
H-4002 Debrecen, Pf.: 400.  
☎: (52) 512-729, Fax: (52) 512-730  
✉: kancelliar@fin.unideb.hu

Iktatószám: KC/ ~~376~~ /2023.  
Tételszám: 01.24  
Ügyintéző: Tóth Attila 62820

**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 többtényezős 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 elkezdeni 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

