DEBRECENI EGYETEM

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

Iktatószám: KC/ 292 /2023.
Tételszám: 01.24.
Ügyintéző: Tóth Attila 62820

TÁJÉKOZTATÓ

a Debreceni Egyetem tanulmányi rendszerét érintő informatikai támadásról

A Debreceni Egyetem valamennyi dolgozója részére

Tisztelt Munkatársak!

A Debreceni Egyetemet is elérte a hazai felsőoktatási intézmények tanulmányi rendszerét érintő informatikai támadássorozat. Egy hacker egy megszerzett oktatói azonosítóval bejutott a Neptun rendszerbe, ahonnan politikai üzenetet küldött ki több hallgatónak. Az ország más egyetemeit érintő informatikai támadásból tanulva prevenciós intézkedéseket vezettünk be, és ennek köszönhetően az üzenet csak minimális számú hallgatóhoz jutott el belső üzenetként. A Neptun rendszeren belül letiltásra került minden üzenet és e-mail küldési funkció, amely további intézkedésig érvényben marad. A Neptun belső üzenetküldő szolgáltatása helyett az egyetem oktatási egységei az e-learning (Moodle) rendszeren keresztül tarthatják a kapcsolatot hallgatóikkal.

Az elektronikus tanulmányi rendszer rendeltetésszerűen működik tovább, alapvető funkcióit ellátja (pl. vizsgajelentkezés, teljesítmények bejegyzése stb.).

Mindezek mellett szükséges a Neptun elérését is biztosító hálózati azonosítóhoz (LDAP) kapcsolódó **jelszó kötelező megváltoztatása.** Ezt a https://eduid-manager.unideb.hu/hu oldalon tudják megtenni, a bal oldalon található **„EduID Bejelentkezés"** majd a **„Saját eduID jelszó módosítása"** linken keresztül. Amennyiben kérdés merül fel, kérjük jelezzék a *helpdesk@it.unideb.hu* email címen, ill. az 06-52-512-900/66333 melléken.

A Debreceni Egyetem a helyzetre reagálva tovább szigorítja információbiztonsági protokolljait, és mindent megtesz annak érdekében, hogy polgárainak adatai és szellemi termékei biztonságban legyenek. Ez a jövőben magasabb szintre emelt, a felhasználókat is érintő biztonsági lépéseket eredményez.

Első lépésként a használatban lévő O365 levelezési rendszerben bevezetésre kerül a kétfaktoros azonosítás, továbbá a fontosabb szakrendszerek (pl.: Neptun) esetében megköveteljük a kétfaktoros azonosításhoz szükséges fejlesztések elvégzését annak bevezethetőségéhez.
Továbbá felhívjuk minden munkavállaló figyelmét, hogy a jövőben még erősebb biztonságtudatossági magatartást tanúsítson és postafiókjának kezelése során tartsa be az alábbi irányelveket:

- **Figyeljenek,** hogy a „levél külső feladótól származik"-e!
- Soha **ne kattintsanak** e-mailben érkező bejelentkezési, vagy személyes, illetve érzékeny adat megadását kérő üzenetekben szereplő **hivatkozásokra, adataikat soha ne adják meg**!
- Amennyiben adathalászatra utaló eseményt tapasztalnak, vagy a **munkahelyi e-mail fiókjukba gyanúsnak** ítélt **levél** érkezik, **jelöljék meg SPAM üzenetként,** valamint **értesítsék az Informatikai Szolgáltató Központ, és az Informatikai Biztonsági Központ munkatársait a helpdesk@it.unideb.hu és az ibk.helpdesk@unideb.hu email címen!**

A fentiek betartásával megelőzhető, hogy a belépési azonosító és jelszó ellopásával illetéktelenek által későbbi támodássorozat eszközölhető legyen!

A következő hónapokban az informatikai biztonságtudatossági oktatások is kiemelt szerepet kapnak és folyamatosak lesznek!

Debrecen, 2023. május 03.

Üdvözlettel:

Prof. Dr. Bács Zoltán
kancellár

DEBRECENI EGYETEM Kancellár 1. 4028 Debrecen, Kassai út 26.