

Egyetemi hallgatók jelszókezelési gyakorlata

Összefoglalás: Az oktatási szektor világszerte egyre gyakrabban válik kibertámadások célpontjává, melyet nemzetközi kutatási eredmények is alátámasztanak. A digitális oktatási-, tanulást támogató és tanulmányi adminisztrációs informatikai rendszerek elterjedésével az oktatási intézmények egyre több személyes, vagy érzékeny adatot kezelnek elektronikusan, illetve támaszkodnak ezeknek a rendszereknek a szolgáltatásaira a tanítás-tanulási folyamat során. Az adatok biztonságának, továbbá az oktatási rendszerek rendelkezésre állásának fenntartásához nélkülözhetetlen a tanárok és diákok megfelelő szintű kiberbiztonsági tudatossága, ezen belül is a biztonságos jelszókezelés. A nem megfelelő jelszóhasználati gyakorlatok növelhetik az adatokhoz való illetéktelen hozzáférések kockázatát, vagy kiesést okozhatnak a tanítás-tanulási folyamatban. A tanulmányban szereplő kutatás 2023-ban, illetve 2024-ben készült, magyar egyetemi hallgatók körében. A vizsgálat több hiányosságot tár fel a jelszókezelés terén, amely rávilágít arra, hogy szükség van célzott oktatási és tudatosságnövelő programokra, amelyek segítenek a hallgatók kiberbiztonsági tudatosságának és felkészültségének javításában.

Kulcsszavak: Online biztonság, információbiztonság, jelszókezelés, kiberbiztonsági tudatosság.

Abstract: The education sector is increasingly becoming a target of cyberattacks globally, as supported by international research findings. With the proliferation of digital educational, learning support, and academic administration systems, educational institutions manage more personal and sensitive data electronically. These systems are relied upon extensively during the teaching and learning process. Ensuring data security and maintaining educational systems' availability requires an adequate level of cybersecurity awareness among teachers and students, particularly in secure password management. Poor password practices can heighten the risk of unauthorized

* Pécsi Tudományegyetem, „Ok-
tatás és Társadalom” Nevelés-
tudományi Doktori Iskola
Email: laszlo@bottyán.com

[31] Kost, E. (2024, January 18): *The State of University Cybersecurity: 3 Major Problems in 2023 | UpGuard*. *Www.upguard.com*. <https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges>

[2] Check Point Research. (2023): *Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most*. *Check Point Blog*. <https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/>

[3] Verizon (2022): *DBIR Data Breach Investigations Report*. <https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf>

data access or even cause disruptions to the teaching-learning process. The study detailed in this paper, conducted in 2023 and 2024 among Hungarian university students, reveals several deficiencies in password management. These findings highlight the necessity of targeted educational and awareness-raising programs to improve students' cybersecurity knowledge and preparedness.

Keywords: Online security, information security, password management, cybersecurity awareness.

Bevezetés

A téma aktualitását jól tükrözi, hogy egyre több nemzetközi szakmai szervezet tesz közzé jelentést az aktuális kiberfenyegetettségekről, kibertámadásokról és ezek hatásairól az oktatási szektort érintően. A független kiberbiztonsági osztályzásokkal, és kockázatkezeléssel foglalkozó amerikai UpGuard 1500 egyetem és 5000 egyetemi beszállító kiberbiztonsági kockázatelemzését végezte el. Megállapításuk szerint a kiberbűnözés egyre nagyobb problémát jelent a felsőoktatásban, 2020 és 2021 között 75%-kal nőtt az oktatási szektort célzó kibertámadások száma. [1] Az amerikai-izraeli multinacionális IT-biztonsági szolgáltató, a Check Point felmérése szerint az oktatási intézmények átlagosan heti 2507 kibertámadást tapasztaltak világszerte 2023 első negyedében, ami 15%-kal több, mint 2022-ben. [2] A világ egyik legnagyobb telekommunikációs vállalata, az amerikai székhelyű Verizon 2022-es adatbiztonsági jelentése szerint az oktatási szektorban drámai növekedést mutat a zsarolóvírus-támadások száma, amely az adatbiztonsági incidensek több, mint 30%-áért felelős. Jelentésükben azt is megemlítik, hogy a szektornak sokkal hatékonyabban kellene védekeznie a személyazonosság-lopás, illetve hitelesítő adatok megszerzésére irányuló támadások ellen. [3]

Szakirodalmi háttér

Az információbiztonság fogalmának tárgyalásakor a szakirodalom legtöbbször az információs rendszerek, illetve a bennük tárolt adatok bizalmasságát (confidentiality), sértetlenségét (integrity) és a rendelkezésre állását (availability) említi. Ilyen vonatkozásban az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény a következőképpen definiálja az információs rendszerek biztonságát: „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos”. [4] Jelen tanulmány, az egyetemi hallgatók internetes fiók- és jelszókezelési szokásai szempontjából az említett három biztonsági követelmény közül leginkább a bizalmasság fontos. A bizalmasság fogalmát az ISO/IEC 27001 információbiztonsági szabvány úgy definiálja, hogy csak a megfelelő személyek férhetnek hozzá a szervezet birtokában lévő információkhoz. ([5] Az adatokhoz való jogosulatlan hozzáférést alapesetben az akadályozza meg, ha valamilyen azonosítási és hitelesítési módszert használunk, például azonosító és jelszó. [6]

Szerencsére egyre gyarapodó nemzetközi szakirodalmat lehet felfedezni a felsőoktatásban tanulók jelszókezelési szokásaival, illetve kiberbiztonsági tudatosságával kapcsolatban. Gabra és munkatársai nigériai egyetemisták körében végzett kutatásában a jelszókezeléssel kapcsolatos kérdésre 367-ből 204-en válaszoltak úgy, hogy nem használnak nehezen kitalálható jelszavakat. Az eredmény jól mutatja a biztonságos jelszókezeléssel kapcsolatos ismeretek hiányát. [7] Alqahtani Szaud-Arábiában végzett kutatása rávilágított, hogy a jelszókezelés szignifikánsan befolyásolja a megkérdezett egyetemi hallgatók kiberbiztonsági tudatosságát. [8] Moallem a kaliforniai Szilícium völgyben végzett felmérést főiskolai hallgatók körében, az Egyesült Államokban. A felmérés eredményei azt mutatják, hogy a megkérdezettek között alacsony például a kétfaktoros hitelesítés vagy a komplex jelszavak használata. Az oktatási intézményeknek pedig nincs aktív tudatosságnövelő programja arra, hogy ezeken a területeken a hallgatók tudatossági szintjét növeljék. [9]

[4] Magyarország Kormánya. (2013): 2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról. *MAGYAR KÖZLÖNY*, (69.), pp. 50241–50255.

[5] ISO (2022): ISO/IEC 27001 standard – information security management systems. ISO. <https://www.iso.org/standard/27001>

[6] Erdősi P. M.–Solymos Á. (2019): *IT biztonság közérthetően*. Budapest: Neumann János Számítógép-tudományi Társaság.

[7] Gabra, A.–Sirat, M.–Hajar, S.–Dauda, I. (2020): Cyber security awareness among university students: A case study. *Science Proceedings Series*, 2., (1.), pp. 82–86. <https://readersinsight.net/SPS/article/view/1320>

[8] Alqahtani, M. A. (2022): Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12., (5.). <https://doi.org/10.3390/app12052589>

[9] Moallem, A. (2019): Cyber Security Awareness Among College Students. In: Ahram, Tareq Z.–D. Nicholson (Eds.): *Advances in Human Factors in Cybersecurity*, pp. 79–87. Springer International Publishing. https://doi.org/10.1007/978-3-319-94782-2_8

[9] Moallem, A. (2019): Cyber Security Awareness Among College Students. In: Ahram, Tareq Z.–D. Nicholson (Eds.): *Advances in Human Factors in Cybersecurity*, pp. 79–87. Springer International Publishing. https://doi.org/10.1007/978-3-319-94782-2_8

[10] Tamil, E.–Othman, A.–Idris, M.–Zakaria, O. (2007): Password Practices: A Study on Attitudes towards Password Usage among Undergraduate Students in Klang Valley. *Journal for the Advancement of Science & Art*, 3., pp. 37–42.

[11] Issa, A.-J. S.–Suliman, J. R.–Askar, E.–Benhamed, D.–Kamiz, Z.–OunAlah, S. (2024): How students deal with password security: Case study of nalu university students. *European Scientific Journal, ESJ*, 28., (505.). <https://eujournal.org/index.php/esj/article/view/18045>

[12] Fredericks, D. T.–Futcher, L. A.–Thomson, K. (2016): Comparing Student Password Knowledge and Behaviour: A Case Study. In: Proceedings of the Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016). *Lulu.com*.

[13] Awad, M.–AlQudah, Z.–Idwan, S.–Jallad, A. H. (2020): Evaluating Password Behavior at a Small University. *Journal of Computer Science*, 15., (1–9.). <https://doi.org/10.3844/jcsp.2019.1.9>

[14] Senthilkumar, K.–Easwaramoorthy, S. (2017): A survey on cyber security awareness among college students in tamil nadu. *IOP Conference Series: Materials Science and Engineering*, 263., (4.). <https://doi.org/10.1088/1757-899X/263/4/042043>

Tamil és munkatársai Malajziában 4 egyetemen végeztek kutatást egyetemi hallgatók jelszókezelési szokásairól. Arra jutottak, hogy a megkérdezett hallgatók jelentős hányadánál nem mondható biztonságosnak a jelszókezelési gyakorlat. [10] Riley az Egyesült Államokban végzett kutatást főiskolai hallgatók körében jelszókezelési gyakorlatukról. Arra jutott, hogy a hallgatók nem figyelnek sem a jelszavak összetettségére, sem arra, hogy mennyi időközönként változtatják meg azokat, illetve személyes kötődésű szavakat-számokat használnak. Saida és Jemaz Líbiában végzett kutatásának vizsgálati eredmények azt mutatták, hogy a vizsgált egyetem hallgatóinak mindösszesen a fele ismeri az intézményi jelszópolitikát. [11] Fredericks és munkatársai egy dél-afrikai egyetemen végzett felmérés eredményeit publikálták, melyben egyetemi hallgatók jelszókezeléssel kapcsolatos tudását és viselkedését mérték. A felmérés eredményei és megállapításai azt mutatták, hogy a válaszadók megfelelő tudással rendelkeznek a biztonságos jelszókezelés terén, azonban nem mindig alkalmazzák ismereteiket a gyakorlatban. [12] Awad és munkatársai az Egyesült Arab Emírségekben végzett kutatása alapján megállapították, hogy a megkérdezett egyetemi hallgatók nincsenek tisztában a biztonsági követelményekkel, és jelszavaik túlnyomó többsége napokon vagy rövidebb időn belül feltörhető. [13] Moallem Kaliforniában, az Egyesült Államokban végzett kutatása egyetemi hallgatók kiberbiztonsági tudását mérte. Az eredmények azt mutatták, hogy a megkérdezettek ugyanolyan nehézségű jelszót, vagy bizonyos esetekben ugyanazt a jelszót használják több fiókhoz is. [9] Senthilkumar és Easwaramoorthy Indában végzett kutatásában kiemeli a biztonságos jelszókezelés eltérő szintjeit a vizsgált városok egyetemi hallgatói között. [14] Kutatótársaimmal 2023-ban, Magyarországon, egyetemi hallgatók körében végzett kutatásunk szintén megállapította, hogy a válaszolók gyakran használják ugyanazt a jelszót több internetes fiókhoz, és ritkábban változtatják meg azokat.

Egy másik szintén hazai, a Dunaújvárosi Egyetem hallgatói körében végzett kutatás azt állapította meg, hogy a legtöbb válaszoló továbbra sem követi a biztonságos jelszómenedzsmenttel kapcsolatos követelményeket a gyakorlatban. A témában további szerteágazó kutatások folynak és számos tényezőt vizsgálnak. [15, 16]

A kutatás háttere

A 2023. októberében végzett online kérdőíves felmérés célja a kiberbiztonsági tudatosság mérése volt, egyetemi hallgatók körében. A kérdőív összesen 30 állítást tartalmazott, melyből 4 kérdés került a vizsgálat tárgyába, amely a jelszóhasználattal kapcsolatos. Az adatfelvétel három magyarországi egyetemen történt, mely mintából a releváns eredmények összevetése érdekében csak egy fővárosi egyetem hallgatóinak válaszai kerültek a vizsgálat tárgyába. A válaszokat 5 fokozatú Likert-skálán lehetett megadni. A minta nagysága így $N=57$ volt, melyből 30 nő és 27 férfi.

A 2024. októberében végzett online kérdőíves felmérés célja a zsarolóvírusok elleni védekezés mérése volt, egyetemi hallgatók körében. A kérdőív összesen 14 állítást tartalmazott, melyből 3 kérdés került a vizsgálat tárgyába, amely a jelszóhasználattal kapcsolatos. A 2023-as kutatással való összevethetőség érdekében az adatok ugyanazon a fővárosi egyetemen tanuló hallgatók körében kerültek felvételre.

A válaszokat 3 fokozatú Likert-skálán lehetett megadni. A minta nagysága így $N=21$ volt, melyből 18 férfi és 3 nő, így a válaszoló férfiak a második kutatásban felülreprezentáltak. Az adatfelvételre Google Forms segítségével került sor, az adatelemzésre pedig az IBM SPSS Statistics v25 verziójával.

Kutatási eredmények

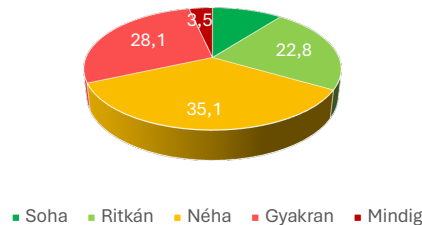
Az említett két kutatásból jelen tanulmányban két témakör kerül bemutatásra, az egyik az azonos jelszavak használata, a másik pedig a jelszókomplexitás.

2023-ban a „Figyelek arra, hogy az összes internetes jelszavam azonos legyen” állításra 57 válaszolóból 2 fő (3,5%) válaszolt úgy, hogy mindig, 16 fő (28,1%) válaszolt úgy, hogy gyakran, 20 fő (35,1%) válaszolt úgy, hogy néha, 13 fő (22,8%) válaszolt úgy, hogy ritkán, és 6 fő (10,5%) válaszolt úgy, hogy soha. (1. ábra, 1. táblázat)

[15] Nagy, B.–Joós, A.–Bognár, L. (2018): An improvement for a mathematical model for distributed vulnerability assessment. *Acta Universitatis Sapientiae, Mathematica*, 10., (2.), pp. 203–217. <https://doi.org/10.2478/ausm-2018-0017>

[16] Nagy, B.–Joós, A.–Bognár, L. (2020): Assessing the effect size of users' consciousness for computer networks vulnerability. *Acta Universitatis Sapientiae, Mathematica*, 12., (1.), pp. 14–29. <https://doi.org/10.2478/ausm-20200002>

1. ábra. Válaszok százalékos megoszlása a „Figyelek arra, hogy az összes internetes jelszavam azonos legyen” állításra

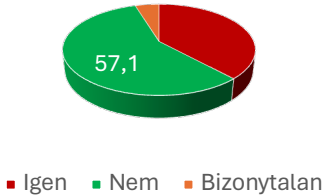


1. táblázat. Válaszok megoszlása a „Figyelek arra, hogy az összes internetes jelszavam azonos legyen” állításra

	Frequency	Percent	Valid Percent	Cumulative Percent
Soha	6	10.5	10.5	10.5
Ritkán	13	22.8	22.8	33.3
Néha	20	35.1	35.1	68.4
Gyakran	16	28.1	28.1	96.5
Mindig	2	3.5	3.5	100.0
Total	57	100.0	100.0	

2024-ben a „Több internetes fiókhoz használom ugyanazt a jelszót, mert így biztosan nem felejttem el” állításra 21 válaszolóból 8 fő (38,1%) válaszolt igennel, 12 fő (57,1%) nemmel és 1 fő (4,8%) bizonytalan. (2. ábra, 2. táblázat)

2. ábra. Válaszok százalékos megoszlása a „Több internetes fiókhoz használok ugyanazt a jelszót, mert így biztosan nem felejttem el” állításra

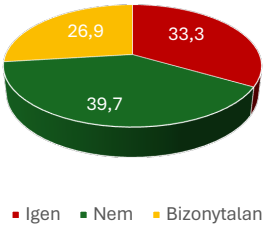


2. táblázat. Válaszok megoszlása a „Több internetes fiókhoz használok ugyanazt a jelszót, mert így biztosan nem felejttem el” állításra

	Frequency	Percent	Valid Percent	Cumulative Percent
Igen	8	38.1	38.1	38.1
Nem	12	57.1	57.1	95.2
Bizonytalan	1	4.8	4.8	100.0
Total	21	100.0	100.0	

Mivel az állítások ugyanazt a kiberbiztonsági területet célozzák meg, tehát azt hivatottak kideríteni, hogy a válaszolók ugyanazt a jelszót használják-e több internetes fiókhoz is, a két adathalmaz összevonásra került. Az 5 fokozatú Likert-skálán a „Mindig” és a „Gyakran” válaszok a 3 fokozatú Likert-skálán az „Igen” válasszal; a „Ritkán” és „Soha” válaszok a 3 fokozatú Likert-skálán a „Nem” válasszal; a „Néha” pedig a „Bizonytalan” válasszal kerültek összefűzésre. Ebben a megközelítésben a két adatfelvétel együttes, összefűzött eredménye az alábbi lett. A 78 válaszolóból 26 fő (33,3%) válaszolt igennel, 31 fő (39,7%) nemmel és 21 fő (26,9%) bizonytalan. (3. ábra, 3. táblázat)

3. ábra. A 2023-as és 2024-es kutatás összefűzött adatai alapján a válaszok százalékos megoszlása a több internetes fiókhoz használt megegyező jelszó témakörében

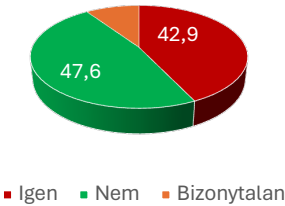


3. táblázat. A 2023-as és 2024-es kutatás összefűzött adatai alapján a válaszok megoszlása a több internetes fiókhoz használt megegyező jelszó témakörében

	Frequency	Percent	Valid Percent	Cumulative Percent
Igen	26	33.3	33.3	33.3
Nem	31	39.7	39.7	73.1
Bizonytalan	21	26.9	26.9	
Total	78	100.0	100.0	100.0

2024-ben a „Rövidebb jelszavak nagybetűkkel és speciális karakterekkel biztonságosabbak, mint a hosszú jelszavak e karakterek keveréke nélkül” állításra 21 válaszolóból 9 fő (42,9%) válaszolt igennel, 10 fő (47,6%) válaszolt nemmel, és 2 fő (9,5%) bizonytalan. (4. ábra, 4. táblázat)

4. ábra. Válaszok százalékos megoszlása a „Rövidebb jelszavak nagybetűkkel és speciális karakterekkel biztonságosabbak, mint a hosszú jelszavak e karakterek keveréke nélkül” állításra



4. táblázat. Válaszok megoszlása a „Rövidebb jelszavak nagybetűkkel és speciális karakterekkel biztonságosabbak, mint a hosszú jelszavak e karakterek keveréke nélkül” állításra

	Frequency	Percent	Valid Percent	Cumulative Percent
Igen	9	42.9	42.9	42.9
Nem	10	47.6	47.6	90.5
Bizonytalan	2	9.5	9.5	
Total	21	100.0	100.0	100.0

Szintézis, összefoglalás

A két kutatás összefűzött adatai alapján a válaszolók egyharmada ugyanazt a jelszót adja meg több internetes fiókhoz is. Azonos jelszavak használata több internetes fiókhoz növeli a kockázatot az ún. credential stuffing támadás ellen. A támadók automatizált eszközökkel és módszerekkel már kiszivárgott hitelesítő információkat használnak fel különböző webszolgáltatásokba, internetes fiókokba történő belépéshez. Ennek során a fiókban tárolt személyes adatokat tudnak ellopni, vagy más rosszindulatú tevékenységet indítani. [17]

A válaszolók több, mint fele nincs tisztában a biztonságos jelszavakkal szemben támasztott aktuális követelményekkel. Az amerikai National Institute of Standards and Technology (NIST) legfrissebb, 2024-es SP 800-63-4 számú irányelve szerint a biztonságos jelszavak előállításához a jelszóhossz fontosabb szempont a komplexitásnál, amennyiben erős jelszót szeretnénk létrehozni. (NIST) A nem biztonságos jelszó növeli a kockázatát az ún. brute-force, vagyis teljes kipróbálás módszerén alapuló támadások ellen. A jelszó megfejtésére irányuló támadás során a támadók szisztematikusan kipróbálnak minden lehetséges karakter kombinációt, a megfelelő kombináció kiderítésére. [18]

Az eredmények tükrében a fejlesztési javaslatok is kirajzolódni látszanak. A biztonságos jelszókezelés, a biztonságos jelszavak előállítása és az adathalászat elleni védekezés indokolt témája lenne egy célzott egyetemi kiberbiztonsági tudatosságnövelő programnak.

[17] ESET (2024a): *Credential stuffing* | ESET Glossary. Eset.com. https://help.eset.com/glossary/hu-HU/credential_stuffing.html

[18] ESET (2024b): *Brute-force támadás elleni védelem* | ESET Endpoint Security | ESET Online súgó. Eset.com. https://help.eset.com/ees/9/hu-HU/idh_config_epfw_brute_force_attack_protection.html

A tudatosságnövelő programok segítenek mind a tárgyi tudás fejlesztésében, például a biztonságos jelszavak előállításához szükséges tárgyi tudás megszerzésében; mind pedig a biztonságos jó gyakorlatok kialakításában, a biztonságos jelszómenedzsmenthez.

A téma aktualitása és az eredmények tükrében számtalan további kutatás indokolt, amely az oktatási szektor, és a tanítási-tanulási folyamatban résztvevők kiberbiztonsági tudatosságát méri. A fiók- és jelszókezelési szokások mellett a kiberbiztonsági tudatosság számos területén érdemes vizsgálni, például a pszichológiai manipuláció, közösségimédia-használat, internet- és e-mail-biztonság, zsarolóvírusok stb. Ezek a kutatások egyrészt hozzájárulnak az intézmények, illetve a tanítás-tanulási folyamatban résztvevők hatékony védekezési képességeihez a kibertérben; másrészt célzott javaslatokkal támogatja a hallgatók digitális írástudásának fejlesztését; végül hozzájárul a társadalom magasabb szintű kiberbiztonsági tudatosságának kialakulásához.

