DOI: https://doi.org/10.12700/btsz.2025.7.3.15

CYBERSECURITY PROFILES AMONG GENERATION Z AND ALPHA

KIBERBIZTONSÁGI PROFILOK A Z ÉS ALFA GENERÁCIÓ KÖRÉBEN

MÓDNÉ TAKÁCS Judit[1] – POGÁTSNIK Monika[2]

Abstract

Due to the increased online presence of Gen Z and Alpha, their cybersecurity awareness is a critical social issue. The aim of this research was to assess the cybersecurity awareness of Gen Z and Alpha, identify influencing factors, and uncover user profiles. The study employed a quantitative survey methodology with a sample of 3275 young individuals from Fejér County, Hungary. Data were analyzed using descriptive and inferential statistics, alongside K-means cluster analysis. Results indicated no significant difference in overall awareness levels between the generations. Average daily internet usage was found to be negatively correlated with awareness. Cluster analysis identified five distinct profiles: "Proactive Protectors," "Average Users," "Technologically Confident," "Passively Cautious," and "Vulnerable Novices." Higher parental educational attainment was significantly associated with membership in more aware profiles. Cybersecurity awareness exhibits complex patterns. The identified profiles allow for the development of targeted prevention strategies to address the specific risks of each group.

Keywords

cybersecurity awareness, user profiles, Generation Z, Generation Alpha

Absztrakt

A Z és Alfa generációk fokozott online jelenléte miatt kiberbiztonsági tudatosságuk kritikus társadalmi kérdés. A kutatás célja a Z és Alfa generációk kiberbiztonsági tudatosságának felmérése, a befolyásoló tényezők azonosítása és felhasználói profilok feltárása volt. Kvantitatív kérdőíves vizsgálatban 3275 Fejér vármegyei fiatal vett részt. Az adatokat leíró és következtető statisztikai módszerekkel és K-means klaszteranalízissel elemeztük. Az eredmények alapján generációk között nem volt szignifikáns különbség az átlagos tudatossági szintben. Az átlagos napi internethasználat negatívan korrelált a tudatossággal. A klaszteranalízis öt profilt tárt fel: Proaktív védelmezők, Átlagfelhasználók, Technológiai magabiztosak, Passzív óvatosak és Sebezhető kezdők. A magasabb szülői iskolázottság tudatosabb profilokkal járt együtt. A kiberbiztonsági tudatosság komplex mintázatokat mutat. A feltárt profilok lehetővé teszik célzott prevenciós stratégiák kidolgozását az egyes csoportok specifikus kockázatainak kezelésére.

Kulcsszavak

kiberbiztonsági tudatosság, felhasználói profilok, Z generáció, Alfa generáció

[1] modne.t.judit@amk.uni-obuda.hu | ORCID: 0000-0001-8463-4032 | assistant lecturer, Obuda University Alba Regia Faculty | PhD student, Obuda University Doctoral School for Safety and Security Sciences | tanársegéd, Óbudai Egyetem Alba Regia Kar | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] pogatsik.monika@amk.uni-obuda.hu | ORCID: 0000-0002-2698-7291 | associate professor, Obuda University Alba Regia Faculty | egyetemi docens, Óbudai Egyetem Alba Regia Kar

BEVEZETÉS

A kiberbiztonság kritikus szerepet tölt be a 21. században, ahol a globális kiberbiztonsági szakemberhiány súlyosan érinti a vállalkozásokat, ipari szektort, ahol a hiányos, nem megfelelő védelmi rendszerek lassabb reagálást és gyengébb megelőzést eredményeznek [1]. Az információbiztonság területén a technikai tudás mellett egyre fontosabbá válnak releváns puha készségek (problémamegoldás, kritikus gondolkodás és együttműködési készségek), amelyek nélkülözhetetlenek a növekvő komplexitású kiberbiztonsági kihívások kezeléséhez[2]. A jövő munkavállalóinak oktatási folyamatában kritikus fontosságú a digitális kompetenciák fejlesztése, amely magában foglalja a biztonsági attitűdök formálását és a puha készségek erősítését a digitális munkakörnyezet elvárásainak megfelelően[3]. Bár a fiatalabb generációk technológiailag jártasak, gyakran hiányzik belőlük a kiberbiztonsági tudatosság és a preventív viselkedési stratégiák alkalmazása[4]. Az Alfa generáció technológiai fejlettsége nem párosul megfelelő érzelmi érettséggel, és tapasztalatlanságuk, könnyű manipulálhatóságuk akadályozza a kiberbiztonsági kockázatok helyes értékelését. A Z és Alfa generáció korai internethasználata eltérő tanulási stílusokat és viselkedési mintákat alakít ki [5], valamint eltérő online kockázatvállalási attitűdöket és biztonsági tudatosságot eredményez. Az Alfa generáció specifikus információbiztonsági tudatosságára vonatkozó empirikus adatok hiánya indokolja generációspecifikus vizsgálatukat a kiberbiztonsági kutatásokban.

A kutatás célja a Z és Alfa generációk jellegzetes kiberbiztonsági profiljainak azonosítása, valamint ezen profilok demográfiai és viselkedési hátterének feltárása.
A kutatás három fő kérdésre keresi a választ:

- K1: Milyen alapvető különbségek azonosíthatók a Z és Alfa generációk internethasználati és biztonsági szokásaiban?
- K2: Mely demográfiai és pszicho-szociális tényezők magyarázzák leginkább az egyes generációk tudatossági szintjét?
- K3: Milyen csoportok és profilok alakíthatók ki a kiberbiztonsági tudatossági dimenziók és befolyásoló tényezők alapján?

IRODALMI ÁTTEKINTÉS

Ez a fejezet röviden bemutatja a kiberbiztonsági tudatosság fogalmát és dimenzióit, áttekinti a Z és Alfa generáció digitális kompetenciáival kapcsolatos magyarországi kutatásokat, valamint elemzi a generációs különbségeket az online térhasználatban és a kapcsolódó kockázati tényezőket.

A kiberbiztonsági tudatosság fogalma és dimenziói

A szakirodalomban a kibertérnek számos meghatározása olvasható. A kibertér (*cyberspace*) kifejezés eredete a görög „*kyber*” szóból származik, amelynek jelentése hajózni vagy navigálni[6]. Maga a fogalom nehezen definiálható, hiszen ez egy összetett és folyamatosan változó digitális ökoszisztéma, amelyben az emberek és eszközök a hálózatokon keresztül kommunikálnak és működnek. A fogalmat Magyarország Nemzeti Kiberbiztonsági Stratégiája (2013) is definiálja[7], mely szerint a kibertér globális, összekapcsolt elektronikus rendszerek hálózata, ahol adatok és információk áramlanak, a társadalmi és

gazdasági folyamatainkat érintően. Magyarország kibertere ennek a globális hálózatnak az a része, ami hazánkban található vagy minket érint.

A kiberbiztonság (*cybersecurity*) a számítógépes rendszerek, hálózatok, programok és adatok védelmét jelenti a digitális támadások, illetéktelen hozzáférések, károkozások és lopások ellen. A célja a digitális eszközök, rendszerek és a rajtuk tárolt információk bizalmasságának (*confidentiality*), sértetlenségének (*integrity*) és rendelkezésre állásának (*availability*) biztosítása (*CIA elv*).[8]

A kiberbiztonsági tudatosság (*cybersecurity awareness*) egyrészt a kibertér és annak veszélyeivel kapcsolatos tudást, az ismeretek szerzésének, megértésének és feldolgozásának képességét, valamint annak gyakorlati megvalósításának igényét jelenti[9]. A kiberbiztonsági tudatosság képzésének, fejlesztésének célja az egyének felelős magatartásának biztosítása a kiberbiztonság terén, így fontos megérteni, a tudatosság, az egyéni jellemzők és az oktatás összefüggéseit a magatartásra gyakorlat hatásának szempontjából[10].

Generációs különbségek az online tér használatában, kockázati tényezők

A digitális kompetenciák és a kiberbiztonsági tudatosság nemcsak egyéni, hanem generációs szinten is jelentősen eltérnek. A fiatalabb generációk digitális bennszülöttként szocializálódtak, így számukra az online tér természetes közegként funkcionál. Ezzel szemben az idősebb generációk számára a digitális környezet inkább tanult, tudatosan elsajátított világ, amelyhez gyakran kritikusabb attitűddel közelítenek[11].

Ez a különbség azonban nem csupán az eszközhasználat gyakoriságában, hanem a digitális viselkedés minőségében is megmutatkozik. Ribble [12] modellje szerint a digitális állampolgárság nem redukálható technikai készségekre, hanem magában foglalja az etikus viselkedést, a jogi tudatosságot és a biztonsági attitűdöket is. A fiatalabb generációk technikai jártassága gyakran nem párosul megfelelő kiberbiztonsági tudatossággal: a jelszavak védelme, az adatkezelés, a közösségi média beállításainak tudatos használata vagy a forráskritika alkalmazása sok esetben hiányos. Ribble hangsúlyozza, hogy a digitális írástudás fejlesztése során nem elegendő a technológiai eszközök használatának oktatása, hanem szükséges a digitális viselkedés normáinak és kockázatainak tudatosítása is.

A digitális szocializáció eltérő mintázatai szintén hozzájárulnak a generációs különbségekhez. Smith, Hewitt és Skrbiš[13] kutatása alapján a fiatalabb generációk számára az online tér nemcsak információforrás, hanem identitásformáló közeg is, amelyben a közösségi elismerés és a vizuális tartalmak dominanciája gyakran háttérbe szorítja a biztonsági szempontokat. Ez a fajta szocializációs dinamika hozzájárulhat ahhoz, hogy a fiatalabb felhasználók kevésbé érzékenyek a digitális kockázatokra, például az adathalászatra, a személyes adatok kiszolgáltatására vagy a manipulált tartalmak felismerésére.

Boghosian[14] ezzel összhangban rámutat arra, hogy a digitális írástudás és a kiberbiztonsági tudatosság nem csupán technikai, hanem demokratikus kompetenciák is. A szerző szerint a digitális higiénia, azaz az online viselkedés tudatossága, a forráskritika, a jelszókezelés és a digitális lábnyom kontrollja alapvető feltétele a demokratikus részvételnek. A generációs különbségek nemcsak a technológiahasználat módjában, hanem az információkhoz való viszonyulásban is megmutatkoznak: a fiatalabb generációk gyakran kevésbé képesek felismerni a dezinformációt, és hajlamosabbak az adatvédelmi kockázatok alábecsülésére.

A generációk eltérő erősségei komplementer kapcsolatban állnak: a fiatalabbak technikai és szociális kompetenciái, valamint az idősebbek szabálytudatossága és kockázatkerülése együttesen előnyös lehet. A fejlesztési stratégiáknak a technikai készségek mellett a generációk közötti tudásmegosztásra is kell fókuszálniuk egy olyan digitális kultúra kialakítására, amelyben a kompetencia és tudatosság egyensúlyban van.

A KUTATÁS MÓDSZERTANA

A Fejér vármegyei Z és Alfa generáció kiberbiztonsági tudatosságának felmérésére kvantitatív módszertant alkalmaztunk. A deduktív logikán alapuló, leíró és hipotézis-tesztelő vizsgálat adatgyűjtési eszköze egy korábban adaptált és validált kiberbiztonsági tudatosság kérdőív volt.

Mintavétel és adatgyűjtés folyamata

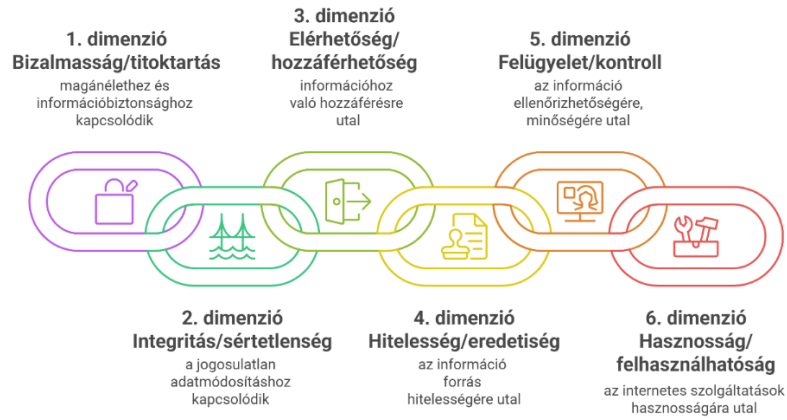
A résztvevők célzott kényelmi mintavétellel kerültek kiválasztásra. Az adatgyűjtés 2022 szeptembere és 2023 májusa között történt online és papíralapú kérdőívekkel. A kérdőíveket Fejér vármegye összes oktatási intézményéhez eljuttattuk, ahol pedagógusok és vezetők segítségével érték el a célcsoportot. A válaszadási arány intézményenként jelentősen változott (45 iskola, 1-444 válaszadó/iskola), ami korlátozhatja az általánosíthatóságot.

A részvétel önkéntes és anonim volt, etikai irányelveknek megfelelően. A résztvevők tájékozott beleegyezést adtak, az Alfa generáció tagjainál szülői hozzájárulással. A célcsoport a Z generáció (1995-2009) és az Alfa generáció (2010-2025, 5. évfolyamtól) tagjaiból állt. Az X és Y generáció tagjai, valamint a hiányos kitöltések kizárásra kerültek a 3473 fős mintából. Az adattisztítás során 198 kiugró értéket távolítottunk el. A végleges minta (N = 3275) 74,4%-a Z generáció (N = 2438), 25,6%-a Alfa generáció (N = 837). A résztvevők 53,3%-a fiú (N = 1746), 46,7%-a lány N = 1529). Oktatási szintek szerint: általános iskola 37% (N = 1215), középiskola 53% (N = 1726), felsőoktatás 10% (N = 334).

A minta Fejér vármegyei reprezentativitását χ^2-próbákkal vizsgáltuk a KSH 2022-es referenciaadataival [15,16] összevetve. Nem találtunk szignifikáns eltérést a nemek arányában az általános iskolában ($\chi^2(1, N = 1215) = 1.40$, $p = .237$), a középiskolában ($\chi^2(1, N = 1726) = 1.25$, $p = .263$), és a 10-29 éves korcsoportban ($\chi^2(1, N = 3275) = 1.90$, $p = .168$). A generációs ($\chi^2(1, N = 3275) = 3.80$, $p = .051$), és a generációkon belüli nemi megoszlások is reprezentatívak voltak (Alfa: $\chi^2(1, N = 837) = 0.17$, $p = .680$, Z: $\chi^2(1, N = 2438) = 3.44$, $p = .064$). A felsőoktatásban azonban férfi dominancia mutatkozott ($\chi^2(1, N = 334) = 126.05$, $p < .001$), így ez az alcsoport nem reprezentatív. A kényelmi mintavétel miatt – a demográfiai illeszkedés ellenére is – az eredmények általánosíthatósága korlátozott.

Kutatási eszköz és mérődimenziók

A végleges kérdőív az adaptált Kiberbiztonsági tudatosság kérdőív (CS-C-H)[17] tételeit, valamint demográfiai kérdéseket tartalmazott. A 25 kérdésből, 5 alskálából álló Cybersecurity Scale-t (CS-C) Arpaci és mtsai alkották meg 2021-ben[18]. A CS-C-H kérdőív a felhasználók kiberbiztonsági gyakorlatát és felfogását méri, valamint megfelelő validitással és megbízhatósággal rendelkezik[19]. A teljes skála Cronbach-alfa értéke .836, és a hat alskála belső konzisztenciája ($.621 < \alpha < .795$). A kérdőív hat dimenzión keresztül (1. ábra) vizsgálja a felhasználók kiberbiztonsággal kapcsolatos gyakorlatát, tudását és tudatosságát.



1. Ábra: A Kiberbiztonsági tudatosság kérdőívhez tartozó dimenziók [forrás: saját szerkesztés]

Adatfeldolgozás és elemzés

A kvantitatív adatok kódolására, tisztítására és feldolgozására az SPSS 27, Excel és Python 3.11.13 szoftverkörnyezetek kerültek alkalmazásra. Az adatelemzés leíró statisztikákat (átlag, szórás), Pearson-korrelációt, lineáris regressziót, megbízhatósági vizsgálatot (Cronbach's α) tartalmazott. A közvetítő hatások mediációs útelemzéssel kerültek vizsgálatra. A csoportok közötti különbségek vizsgálatára a változók típusától függően különböző teszteket alkalmaztunk: két független csoport esetén független mintás t-próbát, nem normális eloszlás esetén Mann-Whitney U tesztet, több csoport összehasonlítására ANOVA, illetve nem parametrikus esetben Kruskal-Wallis H tesztet. Kategorikus változók esetén χ^2-próbát használtunk. Homogén alcsoportok azonosítására K-means klaszterelemzést végeztünk. A statisztikai szignifikancia szintje $p < 0,05$.[20]

KUTATÁSI EREDMÉNYEK

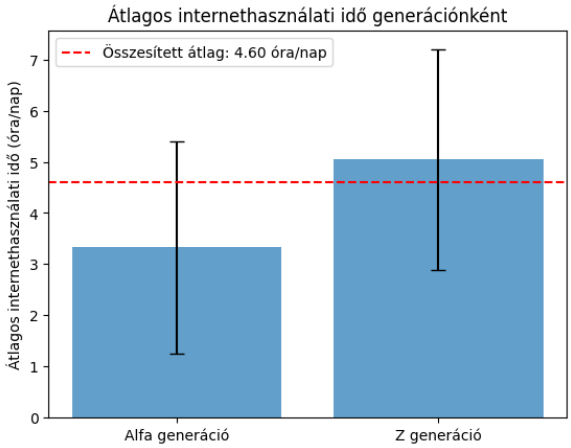
Ez a fejezet a kvantitatív elemzések eredményeit mutatja be. Először a leíró statisztikákat és korrelációkat ismertetjük, majd az alcsoportok közötti különbségeket vizsgáljuk. Ezt követően a kiberbiztonsági tudatosságot befolyásoló tényezők regressziós modelljeit, végül a biztonságtudatosság, attitűdök és viselkedésmintázatok alapján képzett klasztereket mutatjuk be.

Leíró statisztika és korreláció

A vizsgálati minta 3275 főt tartalmaz, ebből 837 fő (25,6%) az Alfa generációhoz (10-14 év), 2438 fő (74,4%) a Z generációhoz (15-29 év) tartozik. A nemek eloszlása: 1746 férfi (53,3%) és 1529 nő (46,7%). Lakóhely szerint a városi lakosok a legnagyobb csoportot alkotják ($N = 1220$, 37,3%), ezt követik a kistelepülési lakóhelyűek ($N = 1178$, 36%) és a megyeszékhelyi lakosok ($N = 819$, 25%). A budapesti válaszadók aránya alacsony ($N = 58$, 1,8%). A szülők legmagasabb iskolai végzettsége alapján a felsőfokú végzettségűek dominálnak ($N = 1515$, 46%), ezt követi az érettségizettek aránya ($N = 1212$, 37%), a szakmunkás végzettségűek ($N = 447$, 14%) és az általános iskolai végzettségűek $N = 101$, 3,1%).

A résztvevők átlagosan 4,6 órát ($SD = 2,27$) töltöttek naponta internetezéssel. A Z generáció szignifikánsan több időt töltött online, mint az Alfa generáció ($U = 579609,000$,

$p < ,001$; $r_s = .338$, $p < ,01$) (2. ábra). Az Alfa generáció átlagosan 3,33 ± 2,08, a Z generáció 5,05 ± 2,16 órát internetezett naponta. Az Alfa generációban az iskolatípus szignifikánsan befolyásolta az internethasználat idejét ($\chi^2(1, N = 837) = 8{,}81$, $p = ,003$), a 6-8 osztályos gimnáziumi tanulók több időt töltöttek online. A nem, lakóhely és szülői iskolai végzettség nem mutatott szignifikáns kapcsolatot az internethasználat mértékével.



2. Ábra: Átlagos napi internethasználati idő generációnként [forrás: saját szerkesztés]

A Z generációnál a napi internethasználattal több demográfiai változó is szignifikáns, bár gyenge kapcsolatot mutatott. A nők többet interneteztek, mint a férfiak ($U = 695566{,}00$, $p = ,011$). Szignifikáns különbségek mutatkoztak az iskolatípus ($\chi^2(2, N = 2438) = 56{,}19$, $p < ,001$), szakirány ($\chi^2(2, N = 2438) = 60{,}80$, $p < ,001$), tudományterület ($\chi^2(5, N = 2438) = 72{,}43$, $p < ,001$) és a szülői iskolázottság ($\chi^2(3, N = 2438) = 15{,}07$, $p = ,002$) szerint, míg a lakóhely nem volt releváns. A felsőoktatásban résztvevő hallgatók töltötték a legtöbb időt online ($M = 5{,}27$, $SD = 2{,}02$). Tudományterületenként a Z generáción belül, az informatika és gazdaságtudomány diákjai interneteztek legtöbbet (5,44 ± 2,14 óra). A Z generáción belül az általános iskolai végzettségű szülők gyermekei (5,37 ± 2,43 óra) töltik a legtöbb, a felsőfokú végzettségűek gyermekei a legkevesebb időt online (4,85 ± 2,14 óra).

A kiberbiztonsági tudatosság kérdőív elemzése alapján a válaszadók általánosan magas szintű tudatosságról számoltak be, a teljes pontszám átlaga magas volt ($M = 96{,}57$, $SD = 14{,}70$) a maximálisan elérhető 125 ponthoz képest. A legerősebb területeknek a hitelesség (20,96 ± 4,09), a felügyelet (20,72 ± 3,97) és a bizalmasság (16,86 ± 3,30) alskálák bizonyultak. Az egyedi tételek elemzése azt mutatja, hogy a válaszadók óvatosak a jelszavak megosztásával, az adataik láthatóságának korlátozásával és az ismeretlen forrásból származó e-mailekkel szemben ($4{,}35 < M < 4{,}51$).

Ezzel szemben a legalacsonyabb átlagpontszámot a sértetlenség alskálánál figyeltük meg (12,60 ± 3,86). Ez az eredmény ellentmondásos attitűdökre utal: míg a válaszadók egyértelműen elutasították azt az állítást, hogy az adatmegosztás kockázatmentes ($M = 2{,}37$), ami pozitív, addig mérsékelt bizalmukat fejezték ki a kibertérben való adattárolással kapcsolatban, hogy az adataik biztonságban vannak ($M = 3{,}19$) és nem veszhetnek

el (M = 3,69), ami potenciális sebezhetőségre utal. Hasonlóképpen, a proaktív védelmi eszközök használatát mérő hozzáférhetőség alskála (14,15 ± 4,35) és a hasznosság alskála (11,28 ± 2,73) pontszámai is alacsonyak voltak. Különösen a rendszeres vírusellenőrzésre (M = 3,35) és a letöltött fájlok vizsgálatára (M = 3,48) vonatkozó tételek kaptak alacsonyabb értékelést, ami arra utal, hogy a passzív óvatosság (pl. bizalmatlanság) erősebb, mint az aktív, rutinszerű védelmi cselekvések.

A magasabb internethasználat gyenge, de szignifikáns negatív kapcsolatot mutat a kiberbiztonsági óvatossággal. Ez különösen az elérhetőségek megosztásánál (r_s = -,152, p < ,001), az ismeretlen e-mailek megbízhatóságánál (r_s = -,104, p < ,001), és a vírusellenőrzésnél (r_s = -,104, p < ,001) nyilvánvaló. Az összesített pontszámmal is negatív a korreláció (r_s = -,080, p < ,001), jelezve, hogy több online idő alacsonyabb kiberbiztonsági tudatossággal jár.

Az Alfa generációnál ez a kapcsolat a legerősebb. Az internethasználat növekedése erősebb negatív korrelációt mutat a személyes adatok védelmével (r_s = -,233, p < ,001), jelszóerősséggel (r_s = -,126, p < ,001) és ismeretlen források kerülésével (r_s = -,108, p = ,002). Egyedül ennél a generációnál mutatott pozitív kapcsolatot a kibertéri adattárolás biztonságába vetett téves hit (r_s = ,089, p = ,010). Az összesített pontszámmal való negatív korreláció itt a legerősebb (r_s = -,104, p = ,003). A Z generációnál gyengébb korrelációk mutatkoztak. Szignifikáns negatív kapcsolat volt az internethasználat és a személyes adatok védelme (r_s = -,102, p < ,001), bankkártyaadatok kezelése (r_s = -,066, p < ,001) és vírusvédelem (r_s = -,088, p < ,001) között. Az összesített pontszámmal való kapcsolat szintén negatív, de gyengébb (r_s = -,072, p < ,001).

Összehasonlító elemzések

Az egyutas varianciaanalízis szignifikáns különbségeket mutatott a napi átlagos internethasználati csoportok között a teljes kiberbiztonsági tudatosságban, $F(4, 3270)$ = 5,23, p < ,001. A Tukey HSD post-hoc teszt szerint a napi 7+ órát internetező csoport szignifikánsan alacsonyabb tudatossági pontszámmal rendelkezett (M = 93,92) a kevesebbet használó csoportokhoz képest (M = 96,28–97,54). A hasznosság alskálán fordított mintázat jelentkezett (p < ,001): a napi 0-1 órát internetezők mutatták a legalacsonyabb pontszámot (M = 10,52), szignifikánsan elmaradva a többi csoporttól, mivel a kevésbé aktív internethasználók ritkábban használják a kibertér szolgáltatásait információkezelésre, problémamegoldásra és közösségi média alkalmazásokra.

A nemi különbségek vizsgálata a független mintás t-próba eredményei a kiberbiztonsági tudatosság szintjével kapcsolatban nem mutatott szignifikáns különbséget a férfiak és nők között, de az alskálákat vizsgálva a nők szignifikánsan magasabb pontszámot értek el a bizalmasság (M = 17,07; $t(3273)$ = -3,46, p < ,001) és a hitelesség (M = 21,28; $t(3271,48)$ = -4,21, p < ,001) alskálákon. Ezzel szemben a férfiak a proaktív védelmet mérő hozzáférhetőség alskálán értek el szignifikánsan magasabb pontszámot (M = 14,39; $t(3273)$ = 3,39, p < ,001).

Az egyutas ANOVA szignifikáns különbségeket mutatott a szülők iskolai végzettsége alapján képzett csoportok között a teljes kiberbiztonsági tudatosságban, $F(3, 3271)$ = 4,97, p = ,002. A post-hoc Tukey HSD teszt igazolta ezt a pozitív kapcsolatot, ahol az általános iskolai végzettségű szülőkkel rendelkező válaszadók szignifikánsan alacso-

nyabb kiberbiztonsági tudatosság pontszámot értek el (M = 93,02) a magasabb iskolai végzettséggel rendelkező szülők gyermekeihez képest. A hitelesség alskálán is a magasabb szülői végzettség fokozottabb óvatosságot eredményez az ismeretlen e-mailek, biztonsági tanúsítvány nélküli weboldalak és adathalász támadások kezelésében. A hozzáférhetőség dimenzióban szintén pozitív összefüggés mutatkozott, tehát a diplomás szülők gyermekei gyakrabban alkalmaznak proaktív védelmi intézkedéseket (vírusirtó programok, tűzfal). A bizalmasság alskálán is a diplomás szülőkkel rendelkezők mutatták a legmagasabb pontszámot (M = 17,09), amely szignifikánsan meghaladta a többi csoport értékeit. Ez fokozott óvatosságot jelez a személyes adatok megosztásában és a privátszféra védelmével kapcsolatban.

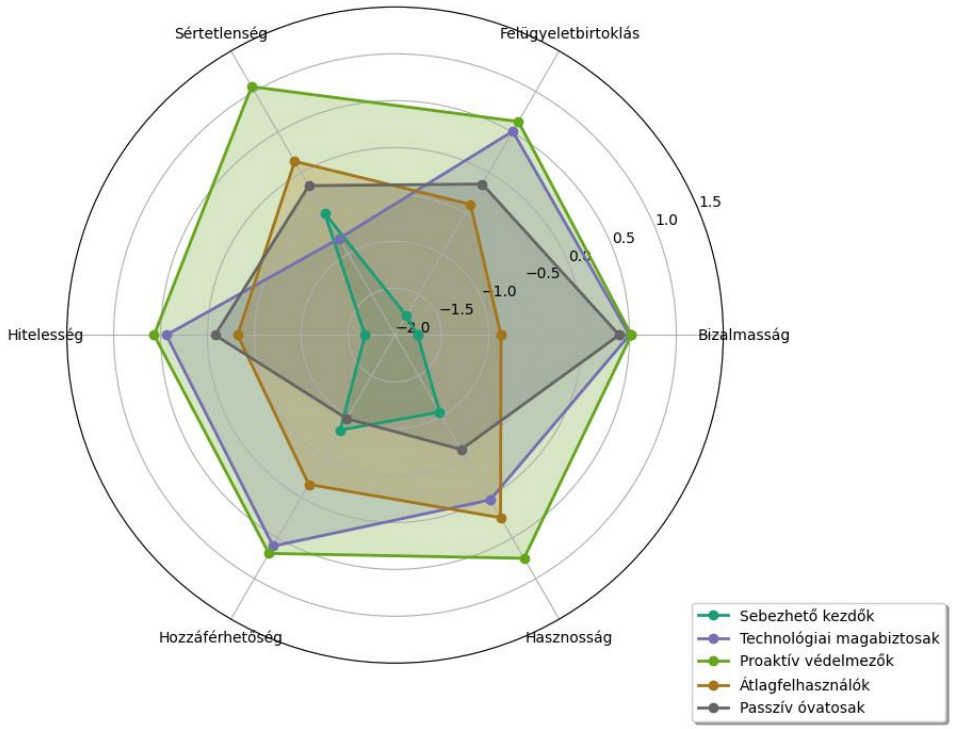
Regressziós eredmények, összefüggések

A kiberbiztonsági tudatosság szint jóslására lineáris regressziós modellt alkalmaztunk, független változókként a generációt, nemet, napi internethasználatot és szülői iskolázottságot bevonva. A modell szignifikáns volt, $F(4, 3270)$ = 5,69, p < ,001, azonban alacsony magyarázó erővel (R^2 = ,007) rendelkezett. Egyedül a napi átlagos internethasználat bizonyult szignifikáns negatív prediktornak (β = -,076, p < ,001), jelezve, hogy a több online töltött idő alacsonyabb kiberbiztonsági tudatossággal jár együtt.

A személyes adatok és privátszféra védelmét mérő bizalmasság alskála lineáris regressziós modellje szignifikáns volt, $F(3, 3271)$ = 23.62, p < ,001, R^2 = ,021, ahol a női nem magasabb (β = ,065, p < ,001), míg a fokozott internethasználat alacsonyabb adatvédelmi tudatosságot jelzett előre (β = -,127, p < ,001). Az online források és kommunikáció megbízhatóságának értékelését mérő hitelesség alskála lineáris regressziós modellje szignifikáns volt, $F(3, 3271)$ = 9.72, p < ,001, R^2 = ,009, ahol a női nem magasabb (β = ,076, p < ,001), míg a fokozott internethasználat alacsonyabb kritikai gondolkodást jelzett előre az ismeretlen e-mailek, bizonytalan weboldalak és potenciális fenyegetések kezelésében (β = -,050, p = ,004). A proaktív technikai védelmi eszközök (vírusirtó, tűzfal) használatát mérő hozzáférhetőség alskála lineáris regressziós modellje szignifikáns volt, $F(3,3271)$ = 12,81, p < ,001, R^2 = ,012, ahol a férfi nem (β = -,056, p < ,001) és a kevesebb internethasználat (β = -,087, p < ,001) magasabb technikai biztonsági tudatosságot jelzett előre. A kibertér szolgáltatásainak (közösségi média, felhőalkalmazások) aktív használatát mérő hasznosság alskála lineáris regressziós modellje szignifikáns volt, $F(3, 3271)$ = 8,38, p < ,001, R^2 = ,008, ahol egyedül a fokozott internethasználat jelzett előre magasabb digitális eszközhasználatot (β = ,083, p < ,001).

Kiberbiztonsági felhasználói profilok

Annak érdekében, hogy a különböző pontszámtartományú alskálák egyenlő súllyal vegyenek részt a klaszterek kialakításában, a hat alskála nyers pontszámait Z-értékekké standardizáltuk (átlag = 0, szórás = 1). A klaszterezési eljárást ezeken a standardizált változókon hajtottuk végre, ami biztosította, hogy az algoritmus tisztán a tudatossági dimenziók közötti relatív mintázatok alapján képezze a csoportokat. A K-means klaszterelemzés a hat kiberbiztonsági alskála alapján öt, tartalmilag elkülönülő felhasználói profilt tárt fel (N = 360–837). Az iterációs folyamat 52 lépésben stabil konvergenciát ért el, jelezve a klaszterek megbízhatóságát. Az azonosított csoportokat a 3. ábra szemlélteti a standardizált Z értékekkel.



3. Ábra: Kiberbiztonsági klaszterek Z-értékei kiberbiztonsági alskálákon [forrás: saját szerkesztés]

1. Proaktív védelmezők (N = 825)
Ez a csoport a legmagasabb és legkiegyensúlyozottabb kiberbiztonsági tudatossággal rendelkezik. Szinte minden dimenzióban átlag feletti, pozitív Z-értékeket értek el. Az ő profiljuk egy proaktív, felkészült és minden dimenzióban tudatos, óvatos felhasználói típust ír le.

2. Átlagfelhasználók (N = 591)
Középszintű tudatossággal jellemezhetők, a legtöbb pontszámuk enyhén átlag alatti (negatív Z-értékek). Ők a tipikus „nemtörődöm" felhasználók, akik a legtöbb területen alulmaradnak az átlaghoz képest.

3. Technológiai magabiztosak (N = 837)
Tagjaik átlag feletti tudatossággal rendelkeznek a legtöbb technikai és óvatossági dimenzióban, mint a felügyelet (jelszókezelés Z = ,51) és a hozzáférhetőség (proaktív védekezés Z = ,60). Ezzel szemben ők rendelkeznek a legalacsonyabb pontszámmal a sértetlenség alskálán (Z = -,81). Ez a profil egy olyan felhasználói típust ír le, amelyik bár ért a technikai védelemhez, naivan azt hiszi, az adatai alapvetően biztonságban vannak, alábecsülik a valós kockázatokat.

4. Passzív óvatosak (N = 662)
Tagjai átlag feletti óvatosságot mutatnak a bizalmasság terén (Z = ,39), tehát vigyáznak a személyes adataikra. Ezzel éles ellentétben ők rendelkeznek a legalacsonyabb pontszámmal a hozzáférhetőség alskálán (Z = -,97). Egy olyan felhasználói típust ír le, amelyik

mentálisan óvatos és gyanakvó, de a gyakorlatban nem teszi meg a szükséges technikai lépéseket (pl. vírusirtó használata) a védelem érdekében.

5. Sebezhető Kezdők (*N* = 360)

Különösen alacsony tudatosságot mutatnak a felügyelet (Z = -1,76), bizalmasság (Z = -1,76) és hitelesség (Z = -1,76) dimenzióban. A legkisebb és legveszélyeztetettebb csoport, általánosan felkészületlen, reaktív felhasználói típust, a legnagyobb kockázatot képviselik.

A χ^2-próbák több demográfiai változó és klasztertagság között szignifikáns kapcsolatokat tártak fel. A szülői iskolázottság mutatta a legerősebb összefüggést ($\chi^2(12, N = 3275) = 31.26$, $p = .002$, *Cramer's V* = .056). Az általános iskolai végzettségű szülők gyermekei felülreprezentáltak a „*Sebezhető kezdők*" csoportjában (standardizált reziduális = 2,5), míg a diplomás szülők gyermekei alulreprezentáltak voltak ebben a csoportban (standardizált reziduális = -2,5). A napi internethasználat szintén szignifikáns kapcsolatot mutatott ($\chi^2(16, N = 3275) = 50,82$, $p < .001$, Cramer's V = ,062). A 7+ órát internetezők felülreprezentáltak a „*Sebezhető kezdők*" (standardizált reziduális = 3,0) és „*Átlagfelhasználók"* (standardizált reziduális = 2,4) csoportjaiban.. A tudományterület és a klasztertagság között is szignifikáns összefüggés volt kimutatható ($\chi^2(20, N = 3275) = 42,94$, $p = .002$, Cramer's V = ,057). Az informatika szakos hallgatók felülreprezentáltak a „*Technológiai magabiztosak*" profiljában (standardizált reziduális = 2,0), míg az általános tantervű képzésben résztvevők a „*Sebezhető kezdők*" csoportjában mutattak magasabb arányt (standardizált reziduális = 2,0). A generáció gyenge kapcsolatot ($\chi^2(4, N = 3275) = 10,50$, $p = .033$, Cramer's V = ,057), míg a *'nem'* nem mutatott szignifikáns összefüggés ($\chi^2(4, N = 3275) = 9,40$, $p = ,052$).

KÖVETKEZTETÉSEK

Az eredmények generációs különbségeket tártak fel az átlagos napi internethasználatot érintően. A Z generáció tagjai (*M* = 5,05, *SD* = 2,16) szignifikánsan több időt töltenek online, mint a fiatalabb, Alfa generációba tartozók (M = 3,33, SD = 2,08), ami az életkori sajátosságokkal és az eltérő életszakaszokkal magyarázható. Az Alfa generáción belül az internethasználatot elsősorban az oktatási kontextus befolyásolja, ahol a magasabb követelményű, 6-8 osztályos gimnáziumokba járó diákok online aktivitása magasabb, amit valószínű az iskolai feladatok eltérő jellege, illetve a nagyobb szabadsággal járó középfokú oktatási intézmény befolyásoló hatása okozhat. Ebben a korcsoportban a demográfiai háttér (nem, lakóhely, szülők végzettsége) még nem képez szignifikáns különbséget, ami egy viszonylag homogén használati mintázatra utal. Ezzel szemben a Z generációnál egy sokkal összetettebb kép rajzolódik ki, ahol a digitális szokásokat számos szocio-demográfiai tényező árnyalja. A nemi különbségek mellett az iskolázottság szintje és iránya is kulcsfontosságúvá válik; szint szerint a felsőoktatásban, szakirány szerint az informatika és gazdaságtudományi területeken tanulók használják legintenzívebben az internetet. Különösen figyelemre méltó az a fordított kapcsolat, miszerint az alacsonyabb iskolai végzettségű szülők gyermekei töltik a legtöbb időt online, jelezve, hogy a szocio-ökonómiai háttér eltérő módon befolyásolhatja a digitális szokásokat a fiatal felnőttkorban.

A válaszadók magas kiberbiztonsági tudatosságról számoltak be (*M* = 96,57, *SD* = 14,70), különösen a jelszókezelés, adatvédelem és e-mail források ellenőrzése terén.

Tudatában vannak az adatmegosztás kockázatainak és nem bíznak a kibertérben tárolt adatok sértetlenségében, ami konzisztens óvatos attitűdöt tükröz. A proaktív védelmi intézkedések (vírusellenőrzés, fájlvizsgálat) azonban alacsonyabb értékeket mutattak, jelezve a passzív védekezési stratégiák dominanciáját. Ez összhangban van azzal, hogy a fiatalok önbizalma gyakran meghaladja tényleges tudásukat: bár úgy vélik, jobban eligazodnak az online térben, mint szüleik, ez a magabiztosság nem mindig párosul a kiberbiztonsági kockázatok megfelelő felismerésével [12,21,22].

Az eredmények alapján az internethasználat intenzitása és a kiberbiztonsági tudatosság kapcsolatban áll. A legaktívabb felhasználók (7+ óra/nap) alacsonyabb biztonsági tudatossággal rendelkeztek. Ez összhangban van korábbi kutatásokkal, amelyek szerint a túlzott internethasználat csökkentheti a kritikus gondolkodást online környezetben [23,24]. A nők magasabb bizalmasság- és hitelességtudatossággal rendelkeztek, míg a férfiak proaktívabb technikai védekezést alkalmaztak. A szülői iskolázottság pozitív hatása a kiberbiztonsági tudatosságra megerősíti a családi szocializáció jelentőségét a digitális kompetenciák fejlesztésében[25]. A magasabban iskolázott szülők valószínűleg tudatosabb digitális nevelést nyújtanak, ami a gyermekek fokozott kiberbiztonsági tudatosságában tükröződik.

A regressziós elemzések legfontosabb megállapítása, hogy a fokozott internethasználat alacsonyabb kiberbiztonsági tudatossággal járt együtt, kivéve a hasznosság dimenzióban, ahol ez a kapcsolat pozitív. A nők magasabb adatvédelmi és kritikai tudatossággal, a férfiak pedig jobb technikai védekezéssel rendelkeztek.

A klaszterelemzés öt elkülönülő kiberbiztonsági profilt tárt fel, amelyek meghaladják az egydimenziós tudatossági modelleket. A főbb megállapítás, hogy a tudatosság ellentmondásos mintázatokat mutat: a „*Technológiai magabiztosak*” gyakorlati tudásuk ellenére alábecsülik a kockázatokat, míg a „*Passzív óvatosak*” óvatosságuk dacára nem alkalmaznak megfelelő technikai védelmet. A szociokulturális háttér bizonyult a legerősebb prediktív tényezőnek: a magasabb iskolázottságú szülők gyermekei tudatosabb profilokhoz tartoztak, hangsúlyozva a családi szocializáció szerepét. Az internethasználat intenzitása paradox kapcsolatot mutatott: a legaktívabb felhasználók (7+ óra/nap) a legkevésbé tudatos csoportokban koncentrálódtak.

Az eredmények alátámasztják, hogy az univerzális prevenciós stratégiák helyett profil-specifikus, célzott beavatkozásokra van szükség az egyes csoportok egyedi sebezhetőségeinek kezelésére.

ÖSSZEFOGLALÁS

A kutatás a Fejér vármegyei Z és Alfa generációk kiberbiztonsági tudatosságát vizsgálta, a generációs különbségekre, a befolyásoló tényezőkre és a jellegzetes felhasználói profilokra fókuszálva.

Bár a Z generáció szignifikánsan több időt tölt online, a két generáció átlagos kiberbiztonsági tudatossági szintje között nincs szignifikáns különbség. A különbségek a tudatosság jellegében mutatkoznak meg, az egyes aldimenziókban eltérő erősségekkel és gyengeségekkel(K1). Az elemzés kimutatta, hogy a demográfiai változók önmagukban gyenge bejósló erővel bírnak. A legerősebb és legkövetkezetesebb tényezőnek a napi átlagos internethasználat, mely szerint az intenzívebb online jelenlét következetesen alacsonyabb tudatossággal járt együtt. Emellett a szülői iskolai végzettség emelkedett ki kulcsfontosságú szociokulturális faktorként, ahol a magasabb végzettség szignifikánsan magasabb

tudatosságot jelzett előre (K2). A klaszteranalízis sikeresen azonosított öt, egymástól jól elkülönülő felhasználói profilt. Ezek a profilok – a „Proaktív védelmezők”-től a „Sebezhető kezdők”-ig, valamint a köztes csoportokig, mint a „Technológiai magabiztosak”, az „Átlag-felhasználók, és a „Passzív óvatosak” – bizonyítják, hogy a kiberbiztonsági tudatosság nem egy lineáris skála, hanem különböző attitűdök és viselkedésminták komplex mintázata. Ezen profilokhoz való tartozást szignifikánsan befolyásolta a szülői végzettség, a választott tudományterület és az internethasználati szokások, ami célzott, profil-specifikus oktatási és prevenciós stratégiák kidolgozásának szükségességét támasztja alá (K3).

A kapott eredmények különösen fontosak a digitális kompetenciák fejlesztése és az oktatási stratégiák szempontjából, hangsúlyozva a proaktív intézkedésekre, a helyes döntéshozatalra és a kritikus gondolkodásra nevelés fontosságát a kiberbiztonság területén.

FELHASZNÁLT IRODALOM[3]

[1] D. Z. Tommaso, „Future Research on the Cyber Security Skills Shortage”, *Cyber Security Education: Principles and Policies*, 2020.

[2] Nemzeti Kibervédelmi Intézet: 2025-ös kiberfenyegetések új dimenziói. [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/hirek/2025-os-kiberfenyegetesek-uj-dimenzioi/ (utolsó megtekintés 2025.04.02)

[3] T. J. Módné, M. Pogátsnik, „A systematic review of human aspects in Industry 4.0 and 5.0: Cybersecurity awareness and soft skills”, *27th IEEE International Conference on Intelligent Engineering Systems (INES 2023)*, 2023, pp. 33–40, https://doi.org/10.1109/ines59282.2023.10297768

[4] J. Zarębska et al., „Research on students' perception of information technology security – a new era of threats”, *Zeszyty Naukowe, Politechnika Śląska*, 2023.

[5] F. T. Cimene, „Generation Alpha Students' Behavior as Digital Natives and their Learning Engagement”, *Psychology and Education: A Multidisciplinary Journal*, 2024, pp. 258–273, doi: 10.5281/zenodo.14007254.

[6] R. Mészáros, „A kibertér társadalomföldrajzi megközelítése”, *Magyar Tudomány*, 2001.

[7] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiá-járól; 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, 1. melléklet, 1. §, 2013.

[8] Y.C. Kar, M.F. Zolkipli, „Review on Confidentiality, Integrity and Availability in Information Security”, *Journal of ICT in Education*, vol 8(2), 2021, pp. 34–42, https://doi.org/10.37134/jictie.vol8.2.4.2021

[9] S. Chaudhary et al, „Developing metrics to assess the effectiveness of cybersecurity awareness program”, *J Cybersecur*, köt. 8, sz. 1, 2022, doi: 10.1093/cybsec/tyac006.

[10] I. Corradini, „Developing Cybersecurity Awareness”, *Studies in Systems, Decision and Control,* köt. 284. 2020. doi: 10.1007/978-3-030-43999-6_6.

[11] E. J. Helsper, R. Eynon, “Digital natives: where is the evidence?,” *British Edu-cational Research Journal*, vol. 36, no. 3, 2010, pp. 503–520.

[12] M. Ribble, „Digital Citizenship in Schools: Nine Elements All Students Should Know”, *International Society for Technology in Education*, 2015.

[3] példák hivatkozásokra | REFERENCES examples of references

[13] J. Smith et al, "Digital socialization: young people's changing value orientations towards internet use between adolescence and early adulthood," *Information, Communication & Society*, vol. 18, no. 9, 2015, pp. 1022–1038.
[14] H. Boghosian, „Cyber Citizens: Saving Democracy with Digital Literacy", *Boston, MA: Beacon Press*, 2025.
[15] KSH, "Népszámlálási adatbázis – Központi Statisztikai Hivatal", [Online] Elérhető: https://nepszamlalas2022.ksh.hu/adatbazis/ (utolsó megtekintés 2025.06.02)
[16] KSH, "22.1.2.1. A lakónépesség nem, vármegye és régió szerint, január 1.", [Online] Elérhető: https://www.ksh.hu/stadat_files/nep/hu/nep0034.html (utolsó megtekintés 2026.06.02)
[17] J. Módné Takács és M. Pogátsnik, „A Comprehensive Study on Cybersecurity Awareness: Adaptation and Validation of a Questionnaire in Hungarian Higher Technical Education", *Acta Polytechnica Hungarica*, köt. 21, sz. 10, 2024, pp. 533–552, doi: 10.12700/APH.21.10.2024.10.32.
[18] I. Arpaci és K. Sevinc, „Development of the cybersecurity scale (CS-S): Evidence of validity and reliability", *Information Development*, köt. 38, sz. 2, 2022, pp. 218–226, doi: 10.1177/0266666921997512.
[19] J. Wim et al., „Marketing research with SPSS", *FT Publishing International*, 2010.
[20] L. Sajtos és A. Mitev, „SPSS Kutatási és adatelemzési kézikönyv", *Alinea Kiadó*, Budapest, 2007. ISBN:978 963 9659 08 7
[21] N. Calvin, „The Cyber Talent Gap and Cybersecurity Professionalizing", *International Journal of Hyperconnectivity and the Internet of Things*, vol 2(1), 2018, pp. 42–51.
[22] C. Berényi, Á. Csiszárik-Kocsir, "A digitális szocializáció hatása a középiskolás fiatalok eszközhasználatára," *Vállalkozásfejlesztés a XXI. században*, vol. 2023/2, 2023, pp. 241–254.
[23] B. Meggyesfalvi, "Kockázati tényezők a digitális térben – A gyerekek internet- és közösségi média használata és az online áldozattá válás," *Belügyi Szemle*, vol. 71, no. 12, 2023, pp. 2163–2178. https://doi.org/10.38146/BSZ.2023.12.3
[24] D. Szabó, E. Dani, "Smartphones and social media as status symbol of Gen Z," *Folia Toruniensia*, vol. 22, 2021.
[25] B. B. Budai, "Digitális készségfejlesztés," *Akadémiai Kiadó*, 2021. [Online] Letölthető: https://akademiai.hu/ptudx00468-digitalis-keszsegfejlesztes.html (utolsó megtekintés 2025.04.02)