

Szász Antónia – Kiss Gábor: Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra

Hivatkozás/reference:

Szász Antónia – Kiss Gábor: „Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra”,

Információs Társadalom,

XVIII. évf. (2018) 3–4. szám, 82–104. old.

<https://dx.doi.org/10.22503/infiars.XVIII.2018.3-4.4>

Információs Társadalom

Pokol Béla:
Az emberi lét rétegei és a robotetika kérdései

Eszenyiné Borbély Mária:
A magyar települési könyvtárakban dolgozó könyvtárosok digitális kompetenciájának állapota – egy országos reprezentatív vizsgálat eredményei

Vári László:
Szabadság határokkal, avagy európai útmutató a szólásszabadság jogszervi gyakorlásához

Képes Gábor:
A számítógéppontokról a digitális esélyegyenlőségig: 50 éves a Neumann János Számítógép-tudományi Társaság

2018. XVIII. évfolyam 3–4. szám

A tanulmányban ismertetett kutatás fő célja az informatikai biztonsági kurzus hatásának vizsgálata a hallgatók szokásaira, attitűdjére és mindennapi információbiztonsági tudatosságára, valamint az alkalmazott oktatási módszerek elemzése és fejlesztése. Az oktatás során a hallgatók egy csoportja videofelvételeket nézett, amelyek jelszavak visszafejtettségét mutatták be megfelelő programok használatával. A másik csoportban ki is próbálhatták ezeket a programokat, tesztelhették akár saját jelszavaik feltörhetőségét is. A kurzust megelőzően és azt követően felvett online kérdőíves felmérés a hallgatók személyes életében is megjelenő hatást az egyéni jelszó- és eszközhasználat vizsgálatával igyekezett feltárni. A válaszokban tükröződő gyakorlatok biztonságos, illetve biztonsági kockázatnak kitett voltak alapján kerültek pontozásra. Az elemzés eredményei azt mutatták, hogy a programhasználat kiegészített, a hallgatói aktivitást facilitáló módszernek szignifikánsan nagyobb hatása volt a hallgatók információbiztonsági attitűdjére, gyakorlatára és tudatosságára, mint a videóval támogatott oktatási módszernek.

Kulcsszavak: e-inklúzió, információbiztonság, oktatási módszerek, attitűdváltozás, tudatosság

Password retrieval programs in education and their effects on information security awareness

The main purpose of the research is to examine the impact of the information security course on students' habits, attitudes, and everyday security awareness, furthermore to analyse and develop methods used in education. In this study two groups were compared. In the first group, students watched video recordings exemplifying password decryption by using appropriate programs. In the second group, students could try out these programs testing the retrievability of their own passwords. Before and after the course an online questionnaire survey was carried out. The impact appearing in students' personal lives was revealed by examining their individual password and device usage. Answers were scored according to their safety, or security risk. It has been demonstrated that the educational method supported by decrypter programs that facilitate student activity had a significantly greater impact on the students' information security attitudes, practices, and awareness than those method applying only video demonstrations.

Keywords: e-inclusion, information security, educational methods, attitude change, awareness

A folyóiratban közzétett művek a *Creative Commons Nevezd meg! - Ne add el! - Így add tovább! 4.0 Nemzetközi Licenc* feltételeinek megfelelően használhatók.

Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra

Bevezetés

Az informatikai képzések hatékonyságát és a hallgatók informatikai, illetve információbiztonsággal kapcsolatos kompetenciáit több felsőoktatási intézményben, számos képzési területen és szakon vizsgáljuk egy több éves, nemzetközi együttműködésben megvalósuló kutatási projekt keretében. A jelen tanulmányban bemutatott kutatás a projektbe illeszkedik. Fő célja az informatikai biztonsági kurzus hatásának vizsgálata a hallgatók jelszóhasználati szokásaira, attitűdjére és mindennapi biztonsági tudatosságára, valamint ezzel szoros összefüggésben az alkalmazott oktatási módszerek elemzése és fejlesztése.

Problémafelvetés – A kutatás háttere

Az Európai Bizottság európai digitális menetrendjének és a digitális kompetenciák keretrendszerének kulcsfogalma az inklúzió (Ferrari et al. 2013, Vuorikari et al. 2016, Carretero et al. 2017). Szemléleti befogadást és elfogadást jelent, amely az informatikai képzésben is kiemelt jelentőségű. Nyilvánvaló szerepe van a kompetenciák megszerzésében és alkalmazásában is, amely a tanulási eredményekre fókuszáló képzési rendszer fő célja. A szakmai kompetenciák összetevői – 1. tudás, 2. képesség, 3. attitűd, 4. autonómia és felelősség – közül a hagyományos műszaki felsőoktatás az első kettő ellenőrzésére koncentrált, míg a másik kettő formálódásáról alig volt visszajelzés, jóllehet az információbiztonság immanens részeiről van szó.

Megoldást keresve a fenti problémára jelen kutatás megtervezésekor a hallgatók szemléletének, attitűdjének, szokásainak vizsgálatát helyeztük középpontba. Minthogy a tanulás eredményességének felmérése során a dolgozatok és a vizsgák a tárgyi ismereteket és a szakmai alkalmazást kéri számon, ám az attitűdváltozásról kevés képet adnak, a hallgatók személyes életében is megjelenő hatást az egyéni jelszó- és eszközhasználat vizsgálatával igyekeztünk feltárni.

Az információbiztonságnak természetesen ennél jóval több szintje és összetevője van. Ám a felelős és tudatos jelszó- és eszközhasználatnak kiemelt jelentősége van mind az egyéni, mind a szervezeti adat- és rendszervédelem szempontjából, továbbá a képzés során kialakított kompetenciák (ideértve a vonatkozó ismereteket, tudatosságot és hozzáállást) meghatározóak a későbbi munkahelyi, információbiztonsági magatartás, a kapcsolódó szabályzatok és protokollok megismerése, megértése és követése szempontjából is.¹

¹ Az információbiztonsági tudatosság összetevőit és állapotát vizsgáló hazai kutatások közül például említhető Nemeslaki és Sasvári (2014), illetve Illéssy, Nemeslaki és Som (2014), amelyek a magyar üzleti és közzsférában tanulmányozták a témát. Benkő (2017) pedig az adattudatosság szintjeiről, útjairól, fejlesztésének szükségességéről, eddigi kezdeményezéseiről és tapasztalatairól ad széleskörű áttekintést.

Didaktikai kérdések

Különböző multimédiás és informatikai eszközöket évek óta használunk az oktatásban szemléltetésre, tudásátadásra, kompetenciafejlesztésre, ám ezek – korábbi kutatási eredményeink alapján – nem váltották ki azt a mértékű (illetve esetenként azt az irányú) változást, amelyet szerettünk volna elérni az információbiztonsági tudatosság terén. Ezért úgy gondoltuk, hogy érdemes a hallgatók interaktivitását előmozdító, tevékenység-központú oktatásinformatikai eszközöket bevonni az oktatásba, és górcső alá venni. Arra törekszünk, hogy a tanítás/tanulás céljához, feladatához, illetve adott fázisához megtaláljuk a megfelelő, a hallgatók számára is érdekesnek ígérkező, kompetenciáikat még jobban fejlesztő oktatásinformatikai eszközöket, technológiákat, és ezzel úgynevezett integrált tanulási környezetet alakítsunk ki (Ollé 2015, Lévai és Papp-Danka 2015).²

Kitekintés

Az információbiztonság oktatási módszereivel és eszközeivel az utóbbi években egyre többen foglalkoznak, attól a céltól vezérelve, hogy a képzések eredményességét növeljék. A publikációk egy része a képzések tartalmára vagy módszertani és eszközkészletének bővítésére tesz javaslatot, illetve új oktatási eszközök vagy képzési programok bevezetését ismerteti. Többségük az ezekkel elért hatásokat empirikus kutatás keretében nem vizsgálja; vagy hatékonyságukat az elsajátított ismeretek tesztelésén keresztül értékeli, illetve a képzéssel való elégedettséget méri fel. Bízunk benne, hogy az új kezdeményezések többrétű hatásvizsgálatáról is olvashatunk a jövőben.³ Az írások azon részénél, amelyek az információbiztonság több összetevőjét igyekeznek felmérni, inkább állapotfelvételekkel lehet találkozni (például az információbiztonsági tudatosság, a kapcsolódó ismeretek, gyakorlatok, attitűdök keresztmetszeti vizsgálatával), mint a képzések által elért változások mérésével.

Mindazonáltal, már az 1980-as évektől megfogalmazódott az információbiztonsági ismeretek, gyakorlat és tudatosság felmérése mellett az ezek fejlesztését célzó képzések hatásairól való visszajelzések, illetve a kapcsolódó mérések és értékelések szükségessége. Például Yngström és Björck (1999) korábbi tapasztalataikat összegezve mutatta be az első Információbiztonság-oktatási Világkonferencián a fentiek jelentőségét, illetve lehetőségeit (egyéni és szervezeti oldalról). Az egyetemi-akadémiai szféra, a szervezeti képzések és az információbiztonság gyakorlati szakemberei egyaránt hangsúlyozták ennek fontosságát. Napjainkban is hivatkozzák például Kruger és Kearney (2006) mérési-értékelési prototípusát, valamint Davis (2008) ajánlását arról, milyen módszerekkel lehet hatékonyan mérni az információbiztonsági tudatosságot fejlesztő képzések hatását az ismeretek, az attitűd és a viselkedés dimenzióiban.⁴ Világszerte egyre több (bár arányaiban még viszonylag kevés)

² Az oktatásinformatikai módszerek alkalmazásáról lásd még (Ollé et al. 2013).

³ Ígéretesnek tűnik a 2016-ban indult *Journal of Cybersecurity Education, Research and Practice* című folyóirat, amely a kiberbiztonság oktatásával kapcsolatos kutatásokról és jó gyakorlatokról is közöl írásokat.

⁴ Davis (2008) szerint az ismereteket értékelő tesztekkel, az attitűdöt és a viselkedést kérdőíves felmérések, interjúk és fókuszcsoportok segítségével, illetve a viselkedés mérőeszközeivel lehet hatékonyan mérni. Kruger és Kearney (2006) olyan felméréseket javasol, amelyek a viselkedés mellett a véleményekről és preferenciákról is adnak visszajelzést (amit hasznosnak tart kiegészíteni fizikai tesztelések adataival, illetve rendszeradatokkal).

kutatás foglalkozik az információbiztonsági képzések hatásának mérésével e dimenziókban.⁵ Ezek többnyire egy adott képzési program vagy egy újonnan bevezetett módszer hatását veszik górcső alá, nem végzik el több módszer komparatív analízisét (a hatékony oktatási módszerek kiválasztása és fejlesztése érdekében).

Saját kutatási projektünk keretében az informatikai biztonsági kurzus hatását többféle módszer alkalmazása mellett vizsgáljuk, fontos célként megjelölve az oktatás során használt eszközök és módszerek elemzését is. Jelen tanulmányban két módszert hasonlítottunk össze.

Módszerek

Oktatási módszerek és eszközök

Jóllehet napjainkban sok hír jelenik meg a médiában rendszerfeltörésről, adateltulajdonításról, adatszivárogtatásról, jelszavakhoz való illetéktelen hozzáférésekről, adatokkal való visszaélésekről és károkozásról, filmek, könyvek szólnak tehetséges hackerekről, személyes, vállalati és kormányzati rendszerekbe való behatolásról, mégis azt tapasztaltuk, hogy a hallgatók a saját életükben nem érzik e veszély realitását. Vagy ha igen, jelszóhasználati szokásaik kevésbé biztonságosak; sok esetben a kényelmi szempontok érvényesülnek a biztonsági szempontokkal szemben.⁶ Ezért fontosnak tartjuk, hogy közel vigyük hozzájuk és minél szemléletesebben mutassuk be a biztonsági kockázatok mibenlétét, az információ- és rendszervédelem jelentőségét, és tudatosítsuk bennük az emberi oldal, az egyéni jelszókezelés meghatározó voltát (Keszthelyi 2013, Keszthelyi és Kaděna 2016). Ennek részeként a kurzus keretében multimédiás támogatással a jelszófeltörés technikai megoldásait és menetét is megismertetjük velük.

Az interneten sokféle programot lehet találni a jelszóval védett fájlok, tömörített állományok megnyitásához, valamint a vezeték nélküli hálózatokhoz való csatlakozáshoz, azáltal, hogy a titkosítva tárolt jelszavak eredetijét visszafejtik. E programok létjogosultságát a fejlesztők azzal magyarázzák, hogy maga a felhasználó feleltheti el a korábban védelmi céllal megadott jelszavát, és szeretne a saját anyagaihoz újra hozzáférni. Azonban ezek a programok felhasználhatók idegen fájlok, hálózatok eléréséhez is, így támadásnak kitéve azokat. A programok közül azokkal lehet gyorsabban eredményt elérni, amelyek a számítógépben lévő videokártya által nyújtott plusz számítási kapacitást is ki tudják használni, kiterjesztve a jelszófeltörési feladatot erre a párhuzamos feldolgozásra alkalmas hard-

⁵ Ilyen például Stephanou (2008) az információbiztonsági tudatosság fejlesztését célzó képzések felhasználói viselkedésre gyakorolt hatásának vizsgálatáról írt dolgozata. Vagy Konak (2018) tanulmánya, amely egy középiskolás diákok számára kidolgozott, tapasztalati tanuláson alapuló, kollaboratív, virtuális, számítógépes labor használatával kiegészített, egyhetes kiberbiztonsági képzési program hatásait az ismeretbővülés mellett az egyéni hatékonyság szempontjából is vizsgálja. Veseli (2011), illetve Prah, Otchere és Opan (2016) éppen Davis (2008), illetve Kruger és Kearney (2006) módszertani javaslatait követve vizsgálják információbiztonsági tudatosság programok hatásosságát az ismeretekre, az attitűdre és a viselkedésre vonatkozóan: Veseli (1) a jelszóvédelem és jelszókezelés; (2) az érzékeny információk kezelése, (3) a social engineering, (4) a fizikai / irodai védelem, valamint (5) az incidenskezelés területén; Prah és munkatársai pedig (1) az előírások követése; (2) a jelszavak titkossága, biztonságos kezelése; (3) az e-mail- és internethasználat; (4) a mobil eszközök; (5) a biztonsági incidensek jelentése; továbbá (6) az akciók és következmények témakörökben.

⁶ Ez egybevág Schneier (2015: 201), illetve Szabó és Révész (2017: 50) megállapításával.

velemre is. A jelszóvédelem alapját az adja, milyen hosszú és összetettségű a jelszó, mivel ettől függ, hogy milyen gyorsan lehet sikeres a jelszó visszafejtése. Az említett programokkal jól lehet szemléltetni a gyenge és erős jelszavak visszafejtése közötti időbeli különbséget, ezzel rámutatva a hosszabb, összetettebb jelszavak használatának előnyeire.

A jelszófeltörés sikerességét nagyban meghatározza a támadó felkészültsége, alkalmazott módszerei és eszközei, előzetes ismeretei is (például a felhasználóról, az eredeti vagy a kódolva tárolt jelszavakról, illetve ezek részeiről). Az órákon az előzetes információszerzés veszélyeiről, módszereiről és lehetőségeiről is sok szó esett, és a megszerzhető információk terén igyekeztünk bemutatni a felhasználók komoly szerepét és felelősségét.⁷ A jelszóvisszafejtő programokkal ugyan nem jelszavas védelemmel ellátott rendszerekbe való behatolásról lehetett tapasztalatot szerezni, nagy hangsúlyt fektettünk arra, hogy felhívjuk a figyelmet és összefüggéseiben segítsünk megérteni, hogy a jelszó- és rendszervédelem szempontjából milyen fontos a használt rendszerek, szolgáltatások hozzáférés-védelmi megoldásai és beállításai (például a jelszavak megadására, változtatásának gyakoriságára vonatkozó előírások, a sikertelen belépési próbálkozások számának limitálása, a szokatlan tevékenységek monitorozása) mellett a jelszavak egyéni kezelésének, tárolásának mikéntje is. (Példának okáért, ha a felhasználó a böngészőben menti el a jelszavát, és a támadó hozzáfér a böngészőhöz, akkor hozzájuthat az eltárolt jelszóhoz is.)⁸

A jelszóvisszafejtő programok által alkalmazott módszerek az eredeti jelszavak közvetlen megtalálását vagy a megszerzett, egyirányú (*hash*) függvényen elkódolt változatuk visszafejtését célozzák, oly módon, hogy összehasonlítják a szoftver által generált karaktersorozatok titkosított változatával. A *szótártámadás*, például, adott szótárak szavait próbálja ki.⁹ A *szótámadás* a szavak különböző variánsait is megvizsgálja (ismert jelszórészlet alapján vagy szótárak szavainak felhasználásával). A *brute force* („nyers erő”) a teljes kipróbálás módszere, minden karaktert behelyettesít a megadott készletből. *Maszkolással* a jelszavak felépítése és karakterkészlete állítható be (sok felhasználó például nagybetűvel kezdi a jelszavát, majd a kisbetűk után a jelszó végére írja a számokat, speciális karaktereket). *Kombinációs támadás* több szóból álló jelszavak visszafejtésére alkalmazható, amelynek során különböző szótárak is megadhatók. *Hibrid támadás* esetén a *leet* ábécé szerint átalakított jelszavak is próbálhatók (amelyekben például *E* betű helyett 3-as, *a* betű helyett @ szimbólum szerepel).

A hallgatóknak olyan videofelvételeket vetítettünk, amelyeken jelszavak visszafejtését rögzítettük különböző jelszófeltörő programok használatával. A felvételek érzéketlenül mutatták be a programok működését és módszereit, illetve a jelszófeltörés gyorsaságát. Ahol a folyamat hosszabb ideig tartott, ott a felvételek vágott verzióit mutattuk be.

⁷ Bevett módszer például, hogy a támadók a közösségi oldalakon, a felhasználói profilokról igyekeznek információt szerezni a felhasználókról. Ugyanis a tapasztalatok szerint a jelszavakban gyakorta megjelenik a saját, illetve egy családtagja vagy kedvence neve, beceneve, születési ideje stb. Ezen adatok megadása, hozzáférhetőségük korlátozása a felhasználó felelőssége. A rendszervédelem oldaláról pedig, ha a felhasználó nem gondoskodik megfelelő vírusvédelemről, akkor a támadók kémprogram segítségével is könnyedén hozzájuthatnak a jelszavakhoz.

⁸ Beszéltünk arról is, hogy ha egy rendszerben adott a kétlépcsős vagy biometrikus azonosítás lehetősége, érdemes használni, ám tudatosítani kell, hogy a mobil eszközök, amelyre például a belépéshez szükséges megerősítő kód érkezik, szintén feltörhetők (s így a támadó számára a megerősítő kód is ismertté válhat).

⁹ A programok az elsők között tesztelik a népszerű, a felhasználók által leggyakrabban használt jelszavakat. Az utóbbi évek ranglistáit a kurzus során is áttekintettük.

A kurzus kezdete előtt a hallgatók a felsőoktatási intézmény által felkínált – az évfolyamlétszám és a teremkapacitás alapján meghatározott számú – három csoportba jelentkezhetek a Neptun tanulmányi rendszerben. A hallgatók maguk választottak csoportot, és illesztették be az órarendjükbe. (A csoportok összetételét a kutatók nem befolyásolták.) A három csoportból kettőben a jelszófeltörésekről készült videofelvételeket tekintették meg, a harmadikban ki is próbálhatták ezeket a programokat, megnézhették akár saját jelszavaik visszafejtési idejét, annak könnyen feltörhetőségét is.

A kutatás során a videós szemléltetést alkalmazó, illetve a programhasználattal kísé-
gészített oktatási módszer hatását vizsgáltuk és hasonlítottuk össze.

Adatfelvételi és elemzési módszerek

A kurzust megelőzően (a tanév elején) és fél évvel a kurzust követően (a tanév végén) online kérdőíves felmérést végeztünk az Óbudai Egyetem biztonságtechnikai mérnök szakos, másodéves, nappali tagozatos hallgatói körében, kétharmados kitöltési arány mellett. Rákérdeztünk arra, hogy a fontosnak tartott szolgáltatásaikhoz mennyire használnak különböző jelszavakat, milyen gyakran változtatják ezeket, milyen hosszúak (hány karakterből állnak) a jelszavaik, milyen karakterfajtaikat használnak, miként tárolják a jelszavaikat, belépnek-e idegen wifihálózatra (mobil hotspotra). A válaszokban tükröződő gyakorlatokat biztonságos, illetve biztonsági kockázatnak kitett voltuk alapján pontoztuk (a biztonságosabb gyakorlat kapott magasabb pontszámot); ezzel eredeti, nominális változóinkat ordinális mérési szintű változókká transzformáltuk, így alkalmasak voltak arra, hogy rangszámításon alapuló statisztikai módszerekkel elemezzük őket. A változók átkódolását az 1. táblázat foglalja össze.

Pont	Jelszavak különbözősége
1	azonosak
2	van egy közös, állandó részük
3	teljesen különbözőek

Pont	Jelszóváltoztatás gyakorisága
1	nem cseréli
2	ha fölmerül a gyanú, hogy valaki megtudhatta
3	évente vagy ritkábban
4	3–6 havonta
5	1–2 havonta

Pont	Jelszavak karakterszáma
1	< 8
2	8–10
3	11–13
4	14–16
5	> 16

Pont	Karakterfajta a jelszavakban
1	csak kisbetű
2	nagy- és kisbetű vegyesen
3	nagy- és kisbetű és számok vegyesen
4	nagy- és kisbetű, szám, speciális karakter

Pont	Jelszavak tárolása ¹⁰
1	megjegyezteti egy részét a böngészővel
2	mindet felírja
3	van, amelyiket felírja
4	mindet megjegyzi
5	jelszómenedzser programot használ

Pont	Idegen wifire / mobil hotspotra belépés
1	bármikor
2	olykor, de azért többnyire védett hálózatra
3	egyéltalán nem

1. táblázat: A változók átkódolása

¹⁰ Itt jegyezzük meg, hogy a Jelszótárolás változónál háromféle kódolást alkalmaztunk. Végkövetkeztéseink mindhárom esetben ugyanazok voltak. A tanulmányban azt a kódolást mutatjuk be, amely a jelszómenedzser program használatát a legmagasabb pontszámmal értékeli, ugyanis a „minden

A változás- és eltérésvizsgálatokat leíró statisztikákkal, a szignifikanciaszintet nemparaméteres próbákkal végeztük (Lehmann 2006, Siegel 2016). A jelszóhasználatot mérő változók közötti összefüggések vizsgálatára struktúrákereső statisztikai módszereket alkalmaztunk. Az eredményeket a hallgatók saját jelszóhasználati szokásaira vonatkozó magyarázatának kvalitatív elemzésével egészítettük ki. Így a változásokat a biztonság mellett a tudatosság dimenziójában is értékelhettük.

Hipotéziseinket 5%-os szignifikanciaszinten teszteltük. Az eredményeknél az empirikus szignifikanciaszintet tüntetjük fel (sig. rövidítéssel), amely a nullhipotézis fennállásának valószínűsége a mintából számolt próbastatisztika alapján.

A minta bemutatása

Az elemzés során *1. csoport*nak nevezzük a videós, *2. csoport*nak a programhasználatot kiegészített oktatásban részt vevő hallgatók körét. A 70 fős évfolyamból 48 fő az 1-es, 22 fő a 2-es csoportba tartozott. Azok kerültek a mintába, akik a kurzus előtt és után is kitöltötték a kérdőívet. Az alminták összetételét és a kitöltési arányokat a 2. táblázat foglalja össze.

Csoportok (módszerek)	Létszám (fő)	%	Minta (fő)	%	Kitöltési arány
1. (video)	48	68,6%	27	58,7%	56,3%
2. (video+program)	22	31,4%	19	41,3%	86,4%
Összesen	70	100,0%	46	100,0%	65,7%

2. táblázat: Az alminták bemutatása

A két csoport összetétele a vizsgált háttérváltozók (nem, életkor, lakóhely, szülők iskolai végzettsége, internetezéssel töltött idő, humán/reál beállítottság, valamint ECDL vizsgával rendelkezés) szerint nem mutatott szignifikáns eltérést 5%-os szignifikanciaszinten a homogenitásvizsgálat eredménye alapján, az életkor változót kivéve.¹¹

Az átlagéletkor az 1. csoportban 20,4 év volt (2,2 év szórással), a 2. csoportban 20,7 év (1,3 év szórással). Az eltérés nem szignifikáns a Mann–Whitney-próba eredménye alapján (sig.=0,103). A válaszadók életkora 19–26 év közötti. Többségük 19–21 év közötti (az

jelszavát megjegyzi” opció gyakran társult a szolgáltatásokhoz használt egyetlen vagy néhány rövid, egyszerű jelszó megjegyzésével (vagyis nem biztonságos jelszóhasználat), és így kevésbé mutat tudatos magatartást, míg a jelszómenedzser program használata már nemcsak biztonságos, hanem tudatos magatartás is, amelynek vizsgálata egyik fő célkitűzésünk.

¹¹ A két csoport háttérváltozók szerinti összetételét Fisher-féle egzakt próbával hasonlítottuk össze a kis mintaelemszám és az alacsony várható cellagyakoriságok (részben ebből adódó) nagy aránya miatt. A homogenitásvizsgálat eredményei: Nem (sig.=0,270); Lakóhely (sig.=0,640); Apa iskolai végzettsége (sig.=0,073); Anya iskolai végzettsége (sig.=0,059); Internetezéssel töltött idő tanítási napokon a kurzus előtt (sig.=0,191) és után (sig.=0,089); Internetezéssel töltött idő szabadnapokon a kurzus előtt (sig.=0,075) és után (sig.=0,253); Humán/reál beállítottság a kurzus előtt (sig.=0,424) és után (sig.=0,213); ECDL vizsga megléte a kurzus előtt (sig.=0,235) és után (sig.=0,363). Az Életkor változónál (életkoronkénti összehasonlítás esetén) a Fisher-próba szignifikáns eltérést mutatott (sig.=0,003); fiatalabb és idősebb életkori kategóriák kialakítása esetén azonban az eltérés már nem volt szignifikáns (sig.=0,719, illetve sig.=0,682; az életkor változó átkódolásától függően).

1. csoportban 85,18%, a 2. csoportban 73,68% az arányuk). A 23 év felettiek az 1. csoportban voltak (27-ből 5 fő, 18,52%); a 22–23 évesek a 2. csoportban (19-ből 5 fő, 26,32%).

A férfiak és nők aránya az évfolyamon és a mintában egyaránt 80%, illetve 20% volt. Az alapsokaságban 70 főből 56 férfi (80,0%) és 14 nő (20,0%) volt, a mintában 37 férfi (80,4%) és 9 nő (19,6%). 9-ből 7 hallgatónő az 1. csoportba, 2 pedig a 2. csoportba került, tehát a két csoport nemek szerinti összetétele között volt eltérés, de nem szignifikáns.

Eredmények

1. Eltérés- és változásvizsgálatok

1.1. A két csoport közötti összehasonlítások

A Mann–Whitney-próba *a kurzus előtt* nem mutatott szignifikáns eltérést a két csoport jelszó- és eszközhasználati szokásai között. *A kurzus után* már szignifikáns különbségek mutatkoztak: az 5 jelszózváltozóból 4-nél szignifikánsan jobb eredményei voltak a vegyes módszerrel oktatott 2-es csoportnak, és szignifikánsan javult a mobil hotspotra való belépéssel kapcsolatos gyakorlatuk is (3. táblázat).

sig. értékek	Jelszó-különbözőség	Jelszó-változtatás	Jelszó-hosszúság	Karakter-fajták	Jelszótárolás	Mobil hotspot
<i>Előtte</i>	0,706	0,142	0,820	0,447	0,168	0,556
<i>Utána</i>	0,035	0,002	0,002	0,000	0,990	0,038

3. táblázat: A két csoport közötti összehasonlítás a kurzus előtt és után:
a Mann–Whitney-próba eredményei

1.2. Változásvizsgálatok

A kurzus előtti és utáni adatok összehasonlítására Wilcoxon-féle párosított mintás próbát alkalmaztunk. Egyoldali ellenhipotézisünk szerint a kurzus után javultak a jelszóhasználati szokások. Az *1. csoportban* nem mutatkozott szignifikáns javulás. A jelszózváltoztatás gyakorisága javult leginkább (itt a sig. érték közel is van 0,05-höz), illetve néhány hallgatónál tapasztaltunk pozitív változást egy-egy változónál. A *2. csoportban* a jelszótároláson kívül minden változónál szignifikáns volt a javulás (4. táblázat).

sig. értékek	Jelszó-különbözőség	Jelszó-változtatás	Jelszó-hosszúság	Karakter-fajták	Jelszótárolás	Mobil hotspot
1. csoport	0,500	0,053	0,391	0,353	0,111	0,240
2. csoport	0,034	0,000	0,001	0,002	0,308	0,010

4. táblázat: Változásvizsgálat: a Wilcoxon-próba eredményei
(egyoldali empirikus szignifikancia-értékek)

Míthogy a csoportok között kiindulásnál, a tanév elején, nem volt szignifikáns különbség, feltételezhető, hogy a tanév végére tapasztalt javulásban az oktatási módszernek volt szerepe.

1.3. Leíró statisztikák

Az alábbiakban áttekintjük a csoportokon belül történő változásokat és a csoportokat együttesen leíró jellemzőket a kurzus előtti, illetve utáni adatok elemzése alapján. Már az 5. és 6. táblázatban közzétett helyzetmutatók is jól tükrözik a változás irányát és mértékét.

1. csoport	Jelszó-különbözőség		Jelszó-változtatás		Jelszó-hosszúság		Karakter-fajta		Jelszótárolás		Mobil hotspot	
skála:	(1–3)		(1–5)		(1–5)		(1–4)		(1–5)		(1–3)	
	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>
átlag	2,07	2,07	2,44	2,81	2,70	2,74	3,11	3,15	3,48	3,26	2,00	2,07
medián	2,00	2,00	2,00	3,00	2,00	2,00	3,00	3,00	4,00	4,00	2,00	2,00
minimum	1	1	1	2	2	2	2	3	1	1	1	1
maximum	3	3	4	5	5	5	4	4	5	5	3	3

5. táblázat: Leíró statisztikák: helyzetmutatók (1. csoport)

2. csoport	Jelszó-különbözőség		Jelszó-változtatás		Jelszó-hosszúság		Karakter-fajta		Jelszótárolás		Mobil hotspot	
skála:	(1–3)		(1–5)		(1–5)		(1–4)		(1–5)		(1–3)	
	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>	<i>Előtte</i>	<i>Utána</i>
átlag	2,16	2,53	2,84	3,68	2,68	3,63	3,21	3,68	3,11	3,32	1,89	2,37
medián	2,00	3,00	2,00	4,00	2,00	3,00	3,00	4,00	4,00	4,00	2,00	2,00
minimum	1	2	2	3	1	2	3	3	1	1	1	1
maximum	3	3	4	5	5	5	4	4	4	5	3	3

6. táblázat: Leíró statisztikák: helyzetmutatók (2. csoport)

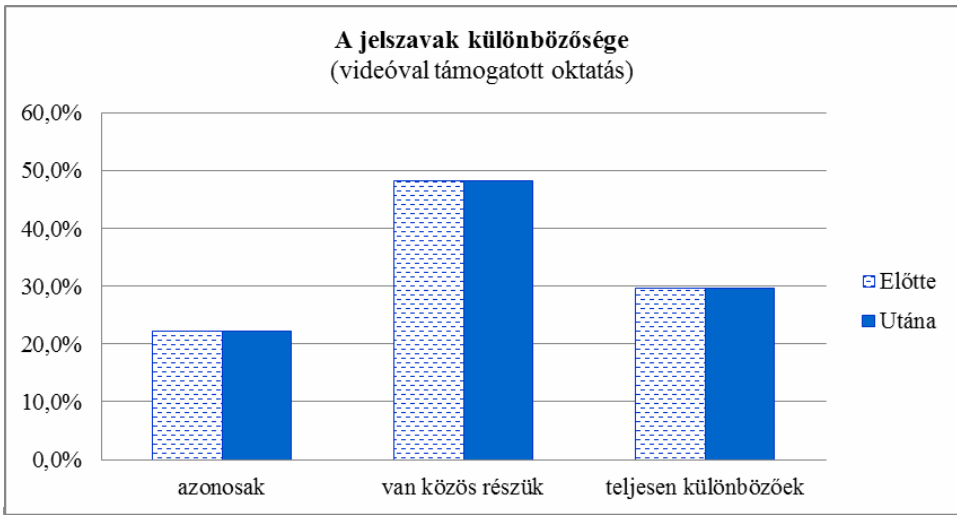
Látható, hogy a 2. csoportban nagyobb mértékben növekedtek az átlagpontszámok, négy változónál nőtt a medián, továbbá a minimum, illetve maximum érték is.

A következő ábraszorozat a változás arányát érzékelteti: azt mutatja meg, a válaszadók milyen százalékban válaszoltak az egyes kérdésekre, és ez hogyan változott a kurzus után. Az összesített eredményeket az egyénienkénti változások elemzésével egészítettük ki.

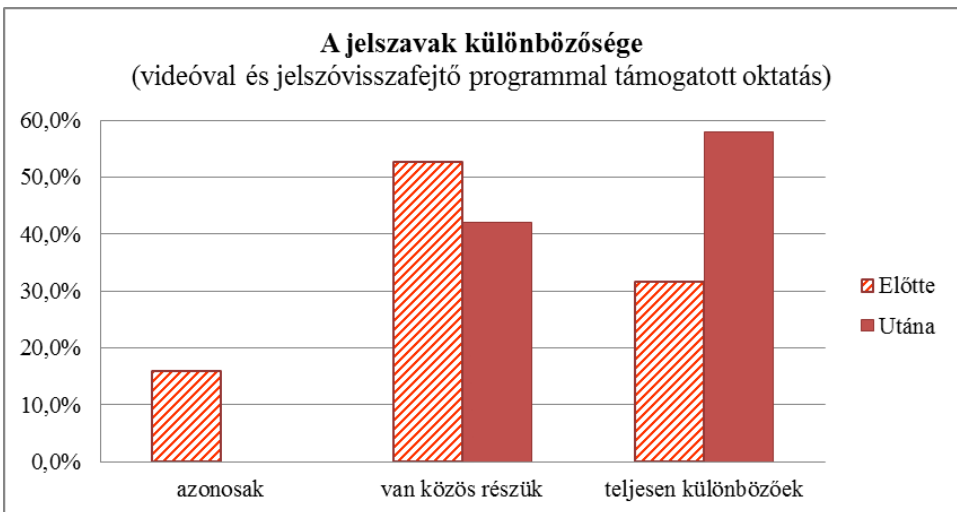
Jelszó-különbözőség (eltérő jelszavak használata)

1. csoport: Összesítve nincs változás a gyakorisági eloszlásban (1. ábra). Egyéni változások: a 27 válaszadóból 4 fő biztonságosabb, 4 fő kockázatosabb jelszóhasználatra váltott, 19 fő (70,4%) nem változtatott. A válaszadók felének jelszaiban van közös rész. 21 fő (77,8%) részben vagy teljesen különböző jelszavakat használ; 6 fő (22,2%) azonosakat.

2. csoport: A tanév elején 3 fő azonos jelszót használt minden szolgáltatáshoz, a tanév végére már senki. A kurzus előtt a válaszadók fele (52,6%) részben azonos, 31,6%-a teljesen különböző jelszavakat használt (2. ábra). A kurzus után 57,9% teljesen különböző jelszavakat használ, a többiek részben azonosakat. Egyéni változások: 19 főből 8 fő (42,1%) biztonságosabb, 3 fő kockázatosabb jelszóhasználatra váltott, 8 főnél (42,1%) nincs változás.



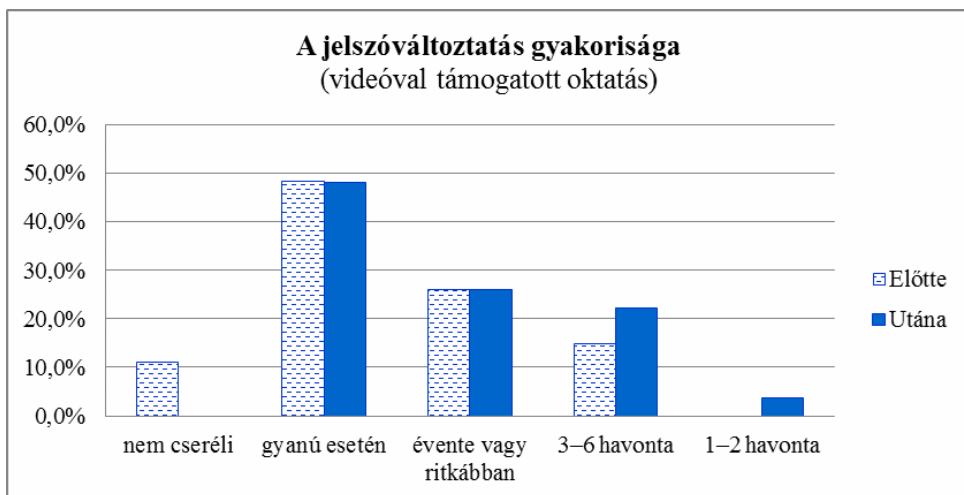
1. ábra: A jelszavak különbözőségének változása (1. csoport)



2. ábra: A jelszavak különbözőségének változása (2. csoport)

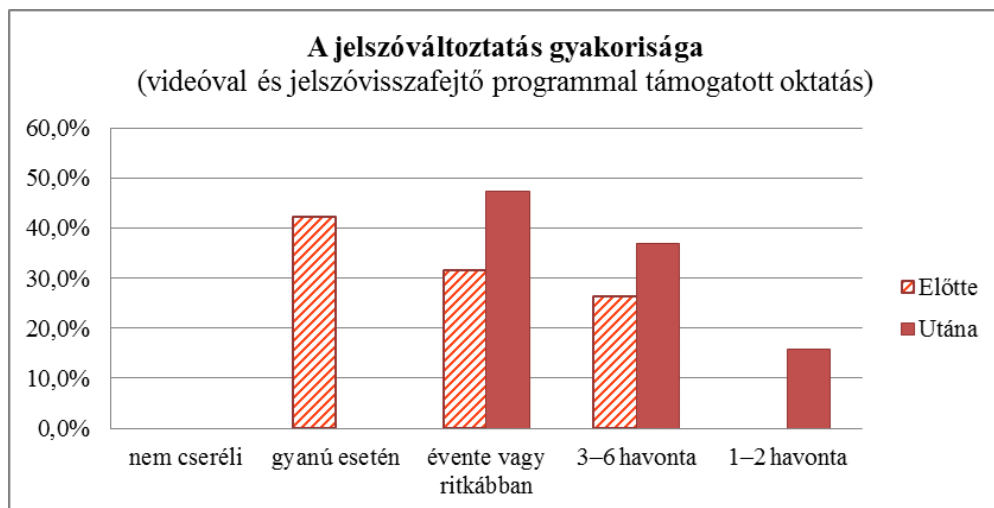
A jelszóváltoztatás gyakorisága

1. csoport: A kurzus után nagyobb arányban vannak a gyakoribb jelszóváltoztatók, és nincs olyan, aki sosem cseréli (3. ábra). A hallgatók ötöde sűrűbben változtatja a jelszavait. Egyéni változások: 27-ből 11 fő (40,7%) biztonságosabban cseréli jelszavait, közülük 5 főnél van nagyobb javulás (a többiek gyanú esetén, illetve évente vagy ritkábban cserélik); 13 főnél (48,1%) nincs változás.



3. ábra: A jelszócsere gyakoriságának változása (1. csoport)

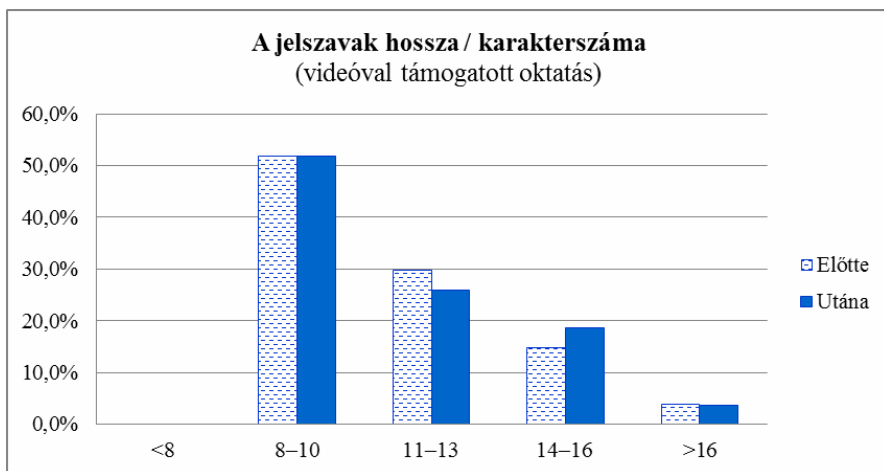
2. csoport: A kurzus után többen vannak a gyakoribb jelszóváltogatók (4. ábra). Nincs olyan, aki sosem cseréli. Egyéni változások: 19-ből 14 főnél (73,7%) javulás történt, 5 főnél (26,3%) nincs változás. 8 fő (42,1%) gyanú esetén cserélte; ők a kurzus után „évente vagy ritkábban” választ adtak. A bizonyos rendszerességgel változtató 11 fő közül 6 fő (54,5%) a kurzus után gyakrabban kezdte változtatni a jelszavait.



4. ábra: A jelszócsere gyakoriságának változása (2. csoport)

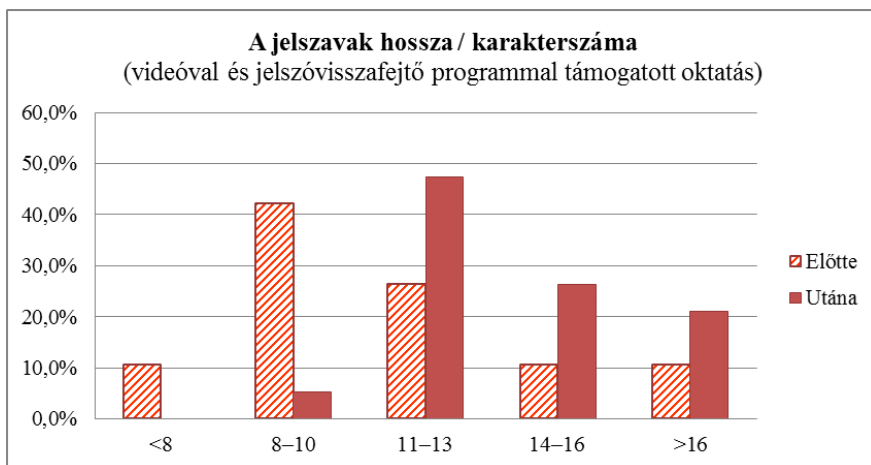
A jelszavak hossza (karakter száma)

1. csoport: Alig van változás (1 fővel kevesebb a 11–13, 1 fővel több a 14–16 karakteres jelszavakat használó). A válaszadók fele 8–10 karakteres jelszavakat használ (5. ábra). Egyéni változások: 27-ből 17 főnél (63,0%) nincs változás, 4 fő pár karakterrel rövidebb, 6 fő pár karakterrel hosszabb jelszavakat használ.



5. ábra: A jelszóhosszúság változása (1. csoport)

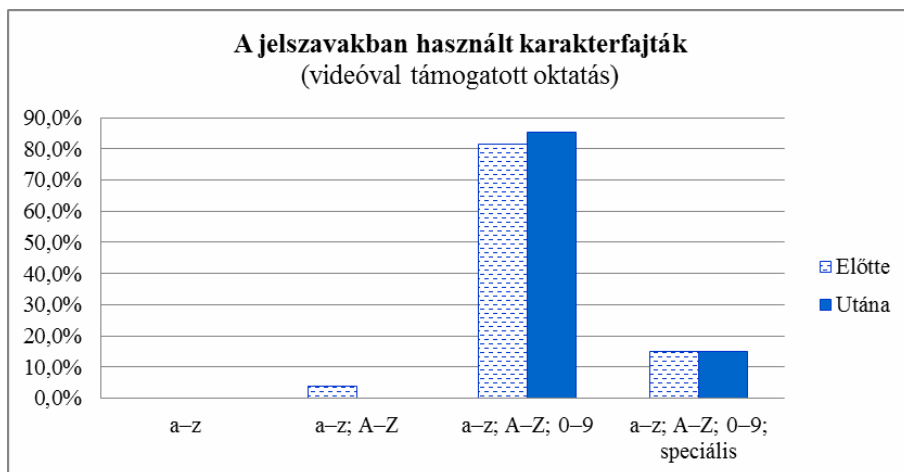
2. csoport: A kurzust követően többen használnak hosszabb jelszavakat (6. ábra). A kurzus előtt a válaszadók fele nagyon rövid jelszavakat használt. A kurzus után 8 karakternél rövidebbet már senki; 8–10 karaktereset 1 fő. 11–13 karaktereset a válaszadók fele, ennél hosszabbat a másik fele. Egyéni változások: 19-ből 13 fő (68,4%) hosszabb jelszavakat kezdett használni, 1 fő pár karakterrel rövidebbet, 5 főnél nincs változás (2 fő továbbra is nagyon hosszú jelszavakat használ).



6. ábra: A jelszóhosszúság változása (2. csoport)

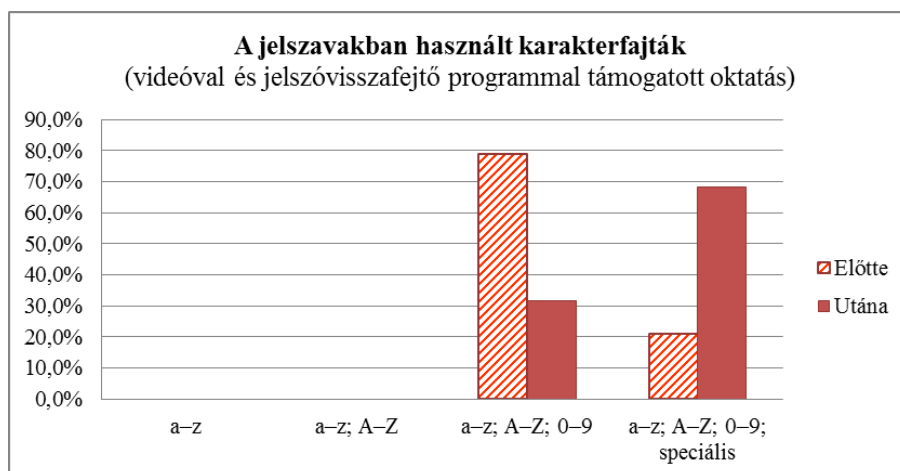
Karakterfajták (a jelszavak összetettsége)

1. csoport: A karakterfajták változatossága alig mutat változást (7. ábra). (1 fővel többen használnak számokat is.) Egyéni változások: a többségnél, 27-ből 23 főnél (85,2%) nincs változás, 2 főnél javulás, 2 főnél visszalépés történt.



7. ábra: A karakterfajták változatosságának alakulása (1. csoport)

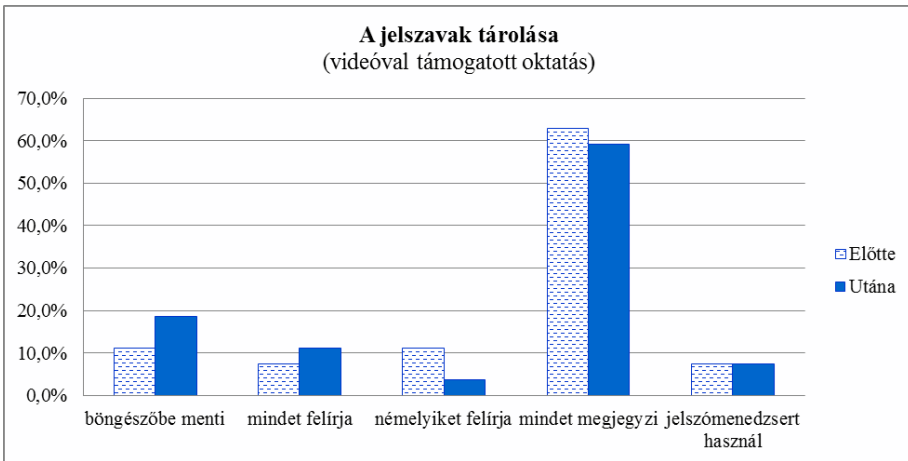
2. csoport: Szemmel látható a javulás (8. ábra). A kurzus előtt a válaszadók ötöde (21,1%) használt speciális karaktereket is a jelszávaiban a kis- és nagybetűkön, számokon kívül, a tanév végére már kétharmaduk (68,4%). (A kurzus előtt 4 fő, utána további 9 fő.)



8. ábra: A karakterfajták változatosságának alakulása (2. csoport)

Jelszavak tárolása

1. csoport: Egy-egy személynél történt kis javulás vagy visszalépés, de összességében nincs szignifikáns változás (9. ábra). A többség megjegyzi a jelszavait. Többen kezdtek megjegyeztetni a jelszavaikat a böngészővel. Egyéni változások: 27-ből 22 főnél (81,5%) nincs változás (közülük 2 fő jelszómenedzser programot használ továbbra is, 15 fő megjegyzi a jelszavát), 2 főnél javulás, 3 főnél visszalépés történt.



9. ábra: A jelszavak tárolásának alakulása (1. csoport)

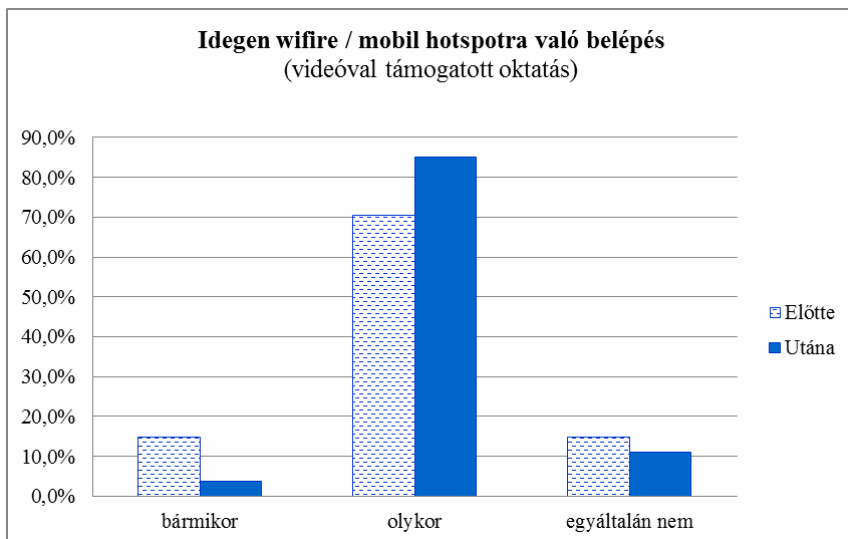
2. csoport: Néhány hallgatónál van kis javulás vagy visszalépés, de összességében nincs szignifikáns változás (10. ábra). Nincs olyan, aki minden jelszavát felírta a kurzus előtt vagy után. Többen jegyzik meg a jelszavukat. Egyéni változások: 19-ből 10 főnél (a hallgatók felénél) nincs változás, 6 főnél (31,6%) javulás, 3 főnél visszalépés történt.



10. ábra: A jelszavak tárolásának alakulása (2. csoport)

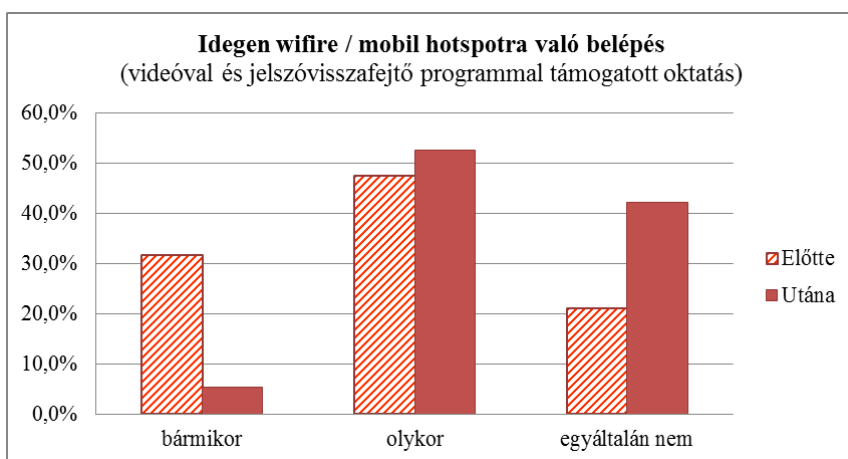
Belépés idegen wifire / mobil hotspotra

1. csoport: A válaszadók nagy többsége olykor belép idegen, nyitott wifire (11. ábra). A tanév végére megnőtt a számuk is. (A kurzus előtt a válaszadók 70,4%-a használt mobil hotspotot, a kurzus után 85,2%-uk.)



11. ábra: Az idegen wifire való belépés változása (1. csoport)

2. csoport: A válaszadók fele olykor belép idegen wifire (12. ábra). 6-ról 1 főre csökkent azok száma, akik bármikor belépnek idegen wifire, és megnőtt azok száma, akik egyáltalán nem lépnek be. Egyéni változások: 19-ből 10 főnél (52,6%) javulás, 2 főnél visszalépés történt, 7 főnél (36,8%) nincs változás (2 fő a legjobb gyakorlatot tartotta meg).



12. ábra: Az idegen wifire való belépés változása (2. csoport)

2. Pontszámkülönbségek analízise

A kurzus eredményessége, illetve az alkalmazott oktatási módszerek hatásának értékelése szempontjából nem közömbös, hogy egyetlen vagy egyszerre több területen is jelentkezett-e javulás (vagy romlás). Ezért, miután a vizsgált változókra egyenként áttekintettük a változás irányát és mértékét, érdemes megvizsgálni, a hallgatók hány változónál mutattak egyidejűleg javulást, visszalépést vagy stagnálást. Erre a pontszámkülönbségek analízise alapján megadhatjuk a választ. A pontszám növekedésén kívül az is pozitívum, ha valaki a legjobb gyakorlatát tartja meg, ezért rögzítettük, amikor a hallgatók a kiadható maximális pontszámot tartották meg. A 7–10. táblázatok a vizsgált változók összesített statisztikáit mutatják.

Javulás (magasabb pontszámot ért el)				
<i>Változó</i>	1. csoport		2. csoport	
db	fő	%	fő	%
0	8	29,63	1	5,26
1	11	40,74	2	10,53
2	6	22,22	5	26,32
3	2	7,41	4	21,05
4	0	0,00	3	15,79
5	0	0,00	4	21,05
Összesen	27	100,00	19	100,00

7. táblázat: Egyidejű javulás

A legjobb gyakorlat megtartása (a maximális pontszámot tartotta meg)				
<i>Változó</i>	1. csoport		2. csoport	
db	fő	%	fő	%
0	19	70,37	10	52,63
1	6	22,22	7	36,84
2	2	7,41	1	5,26
3	0	0,00	0	0,00
4	0	0,00	1	5,26
Összesen	27	100,00	19	100,00

8. táblázat: A legjobb gyakorlat megtartása

Nincs változás, bár javulhatott volna (nem változott a pontszáma)				
<i>Változó</i>	1. csoport		2. csoport	
db	fő	%	fő	%
0	0	0,00	4	21,05
1	0	0,00	4	21,05
2	6	22,22	2	10,53
3	5	18,52	7	36,84
4	8	29,63	1	5,26
5	5	18,52	1	5,26
6	3	11,11	0	0,00
Összesen	27	100,00	19	100,00

9. táblázat: Egyidejű stagnálás

Visszalépés / romlás (alacsonyabb pontszámot ért el)				
Változó	1. csoport		2. csoport	
db	fő	%	fő	%
0	13	48,15	12	63,16
1	9	33,33	7	36,84
2	5	18,52	0	0,00
Összesen	27	100,00	19	100,00

10. táblázat: Egyidejű visszalépés / romlás

1. csoport: A videós csoport felénél visszalépés történt egy vagy két jelszóváltozónál, a többség több változónál sem mutatott változást, pedig javulhatott volna.

2. csoport: A videóval és jelszóviSSZafejtő programmal is támogatott csoportban nagyobb arányban történt javulás egyszerre több jelszóváltozónál. A válaszadók 63,2%-ánál egyetlen változónál sem volt visszalépés, 7 főnél (36,8%) pedig csak egyetlen jelszóváltozónál. 21%-uk (ez a mintában 4 fő) egyetlen változónál sem stagnált úgy, hogy javulhatott volna: ők 5-6 változónál javulást mutattak vagy a legjobb gyakorlatot tartották meg.

3. Háttérváltozók szerinti összehasonlítások

A jelszóváltozókat és a mobil hotspot használatot demográfiai és egyéb háttérváltozók szerinti összehasonlításban is vizsgáltuk nemparaméteres (Mann–Whitney- és Kruskal–Wallis-) próbák segítségével.

A nem, a lakóhely (falu, kisváros, nagyváros), az életkor, illetve az életkori kategória, a szülők iskolai végzettsége, az internetezéssel töltött idő tanítási, illetve szabadnapokon, továbbá a humán/reál beállítottság egyik csoportban sem differenciálta a jelszó- és a wifi-használatot, a kategóriás változók csoportjai közötti összehasonlítások nem mutattak szignifikáns különbséget sem a kurzus előtt, sem utána – két kivétellel, a jelszótárolás változónál. A kategóriákon belüli alacsony létszámok miatt ezekből nem lehet messzemenő következtetést levonni, ezért csak megemlítjük.

A jelszótárolás változónál a *kurzus előtt* a tanítási napokon internetezéssel töltött idő szerinti összehasonlítás mutatott szignifikáns eltérést az 1. csoportban (sig.=0,024); a *kurzus után* a szabadnapokon internetezéssel töltött idő szerinti a 2. csoportban (sig.=0,020); ugyanis a 2–5 órát internetezőik körében nagyobb arányban voltak olyanok, akik nem tárolták biztonságosan a jelszavaikat (elmentették a böngészőbe vagy felírták egy részüket).

A *kurzus utáni* méréseknél az ECDL vizsgával rendelkezők és nem rendelkezők között szignifikáns különbség mutatkozott a jelszóhosszúság tekintetében a 2. csoportban (sig.=0,029): az ECDL vizsgával rendelkezők közül mindenki hosszú jelszavakat használt.¹²

4. Kapcsolatvizsgálatok

A jelszóváltozók és a mobil hotspot használatot mérő változó közötti együttjárást a nemparaméteres Spearman-féle ρ (ró) rangkorrelációs együtthatóval mértük.

¹² Az 1. csoportban a kurzus előtt 27 válaszadóból 12 főnek (44,4%), utána 13 főnek (48,1%) volt ECDL vizsgája; a 2. csoportban a kurzus előtt 19 válaszadóból 5 főnek (26,3%), utána pedig 6 főnek (31,6%).

4.1. A kurzus előtti és utáni változó párok együjtjárása

A korrelációs számítás eredményét a 11. táblázatban foglaltuk össze.

Vátozó:	Jelszóeltérés		Jelszócsere		Jelszóhossz	
Csoport:	1.	2.	1.	2.	1.	2.
$\rho =$	0,699	0,117	0,357	0,666	0,657	0,535
sig.=	0,000	0,634	0,067	0,002	0,000	0,018
Vátozó:	Karakterfajták		Jelszótárolás		Mobil hotspot	
Csoport:	1.	2.	1.	2.	1.	2.
$\rho =$	0,168	0,351	0,775	0,084	0,354	0,337
sig.=	0,401	0,141	0,000	0,732	0,070	0,158

11. táblázat: Kurzus előtt és után mért változók közötti együjtjárás

Ez alapján azt találtuk, hogy minél biztonságosabb volt a kurzus előtti jelszóhasználat, annál biztonságosabbnak mutatkozott a kurzus után.

1. csoport: A jelszóeltérés (jelszó-különbözőség), a jelszóhosszúság és a jelszótárolás változók esetén a kapcsolat közepesnél erősebb, 1%-os szinten is szignifikáns.

2. csoport: A jelszócsere, vagyis a jelszóváltoztatás gyakorisága és a jelszóhosszúság változók között a kapcsolat közepesnél erősebb, a jelszócsere 1%-os szinten is szignifikáns.

Azoknál a változóknál, amelyeknél a korrelációs kapcsolat gyengének mutatkozott, ezt úgy értelmezhetjük, hogy a korábbi jelszóhasználati szokások nem voltak meghatározóak a későbbiekre; fentebb láttuk, hogy a 2. csoportnál több változónál történt szignifikáns javulás.

4.2. A különböző változók közötti együjtjárás a kurzus előtt, illetve után

A korrelációs mátrix helyett az alábbiakban csak a szignifikáns kapcsolatokat közöljük.

1. csoport:

A kurzus előtt a jelszavak különbözősége és karakterszáma között közepesnél kicsit gyengébb, negatív irányú, szignifikáns rangkorrelációs kapcsolat volt ($\rho = -0,400$; sig.=0,039); vagyis minél hosszabbak voltak valakinek a jelszavai, annál kevésbé használt eltérő jelszavakat a különböző szolgáltatásaihoz. A jelszavak különbözősége és a mobil hotspotra való belépést mérő változó között közepesnél gyengébb, pozitív, 5%-os szinten még éppen szignifikáns együjtjárás mutatkozott ($\rho = 0,388$; sig.=0,046); vagyis akik eltérő jelszavakat használtak, azok között nagyobb arányban voltak azok, akik óvatosabban csatlakoztak idegen mobil hotspotra, és fordítva.

A kurzus után a jelszavak különbözősége és a jelszóváltoztatás gyakorisága között szignifikáns, pozitív, közepesnél kicsit gyengébb rangkorrelációs kapcsolat volt ($\rho = 0,400$; sig.=0,039); vagyis minél inkább különböző jelszavakat használt valaki, annál inkább jellemző lett rá, hogy gyakrabban kezdte változtatni a jelszavait.

2. csoport:

A kurzus előtt a jelszavak különbözősége és a jelszótárolás között viszonylag erős, negatív irányú, szignifikáns korrelációs kapcsolat mutatkozott ($\rho = -0,722$; sig.=0,000); vagyis

minél inkább eltérő jelszavakat használt valaki, annál kevésbé tárolta biztonságosan a jelszavait (például felírta egy részüket).

A *kurzus után* nem volt szignifikáns kapcsolat a változópaárok között. Az előbbi két változó közötti korrelációs kapcsolat sokkal gyengébb lett ($\rho = -0,123$; $\text{sig.} = 0,616$).

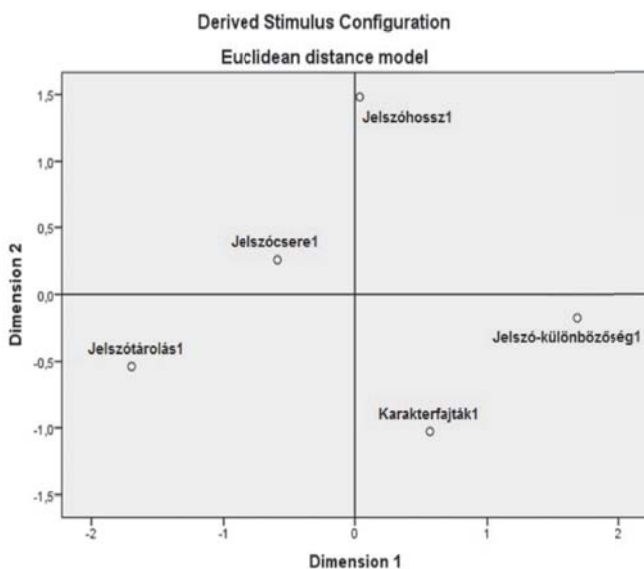
5. Többdimenziós skálázás

A jelszóhasználati szokások összefüggéseire szerettünk volna nagyobb figyelmet fordítani, ezért a mögöttük lévő struktúrák feltárására a többdimenziós skálázás módszerét (*multidimensional scaling*, röviden MDS) (Kruskal és Wish 1978) alkalmaztuk standardizált, ordinális mérési szintű jelszóváltozókkal, euklideszi értelemben vett távolságdefinícióval. E módszerrel a változók közötti összefüggéseket alacsonyabb dimenziójú térben vizsgáltuk.

A jelszóhasználati szokásokat mérő változókat nem ugyanazon skálán pontoztuk,¹³ ezért annak érdekében, hogy jobban összemérhetők legyenek, standardizáltuk azokat (oly módon, hogy a pontértékeket elosztottuk a kiadható maximális pontszámmal).

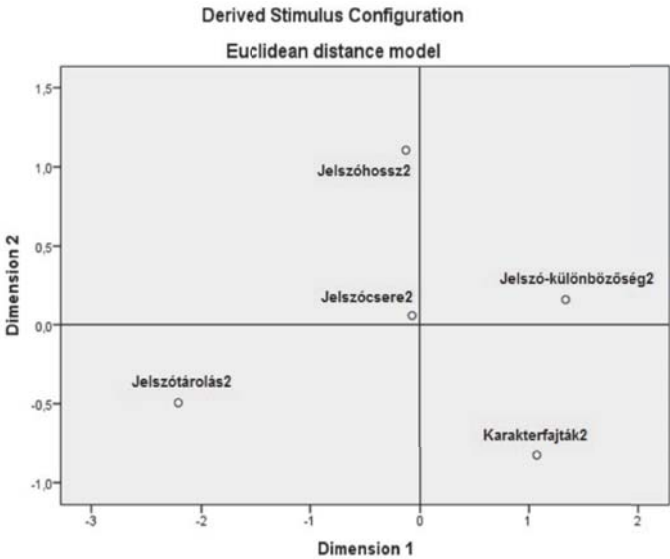
A 2. csoportnál a jelszóhasználati szokásokat mérő standardizált változók elrendezése már kétdimenziós leképezésben is nagyon jó illeszkedést mutat a kurzus előtt ($\text{Stress} = 0,00384$; $\text{RSQ} = 0,99982$) és után is ($\text{Stress} = 0,00498$; $\text{RSQ} = 0,99983$). A Stress-értékek 0,05-nél jóval kisebbek, vagyis az eredeti és a redukált térbeli távolságok megfelelnek egymásnak, a dimenziócsökkentés a lényeges információkat megőrizte mindkét esetben. Az RSQ értékek 1-hez nagyon közeliek, ami az eredeti és a redukált struktúrák nagyon jó illeszkedését mutatja.

A kurzus előtti kétdimenziós elrendezést a 13. ábra, a kurzus utáni a 14. ábra mutatja. A kurzus előtti mérések változóit 1-es, a kurzus utániakat 2-es indexszel jelöltük.



13. ábra: Kétdimenziós struktúra a kurzus előtt (2. csoport)

¹³ Példának okáért, 2 pontos növekedés a Jelszó-különbözőséget mérő változónál a legrosszabb gyakorlatról a legjobbra való váltást jelenti (minden szolgáltatáshoz (1) azonos, illetve (3) teljesen eltérő jelszavakat használ), míg például a Jelszóhosszúság változónál csupán annyit, hogy néhány karakterrel hosszabbak lettek a jelszavai.



14. ábra: Kétdimenziós struktúra a kurzus után (2. csoport)

A vízszintes tengely a jelszóhasználat biztonságos/nem biztonságos voltát mutatja: a nagyobb koordinátaérték biztonságosabb jelszóhasználatot mutat, a kisebb koordinátaérték kisebb biztonságot, nagyobb kitettséget.

A függőleges tengely a tudatosság szerint dimenzionál: a nagyobb pontérték tudatosabb (információbiztonság-tudatosabb) jelszóhasználatot mutat.

A tengelyre eső pontok az átlagos értéket mutatják.

Az eredmények értelmezése: A jelszóváltozók együttesen szignifikáns javulást mutatnak: az összesített standardizált jelszópontszámok vizsgálata alapján (a Wilcoxon-próba eredménye: sig.=0,000). Nőtt az átlag mindkét dimenzióban. Ha egy változónál átlagos mértékű a javulás, e változónak nem változik az adott dimenzióban a tengelyhez képesti helyzete (a koordináta-pontszáma). Ha az átlagosnál nagyobb mértékben javul, akkor nő, ha kisebb mértékben, akkor csökken a koordináta-pontszáma.

A jobb áttekinthetőség kedvéért közöljük a változók (stimulusok) helyzetének koordinátáit a 12. táblázatban.

Stimulusok koordinátái	Kurzus előtt (1)		Kurzus után (2)	
	Dimenzió		Dimenzió	
Stimulus neve:	D1	D2	D1	D2
Jelszó-különbözőség	1,6789	-0,175	1,3314	0,1578
Jelszócsere	-0,5854	0,2586	-0,0681	0,0574
Jelszóhossz	0,0361	1,482	-0,1246	1,1053
Karakterfajták	0,5666	-1,028	1,0711	-0,8268
Jelszótárolás	-1,6963	-0,538	-2,2097	-0,4937

12. táblázat: A jelszóváltozók (stimulusok) koordinátái (2. csoport)
(1. dimenzió: biztonság / 2. dimenzió: tudatosság)

a) *Jelszó-különbözőség*: A biztonság ennél a változónál átlag feletti és a legmagasabb szintű volt a kurzus előtt és után is (a többség részben vagy teljesen különböző jelszavakat használt), értéke kicsit csökkent (ugyanis több változónál javult a biztonsági szint, s így az átlag is). A tudatossági szint átlag alattiról kissé (az új) átlag feletti lett.

b) *Jelszócsere – a jelszóváltoztatás gyakorisága*: A biztonság a kurzus előtt és után átlag alatti, de javult, közeledett az átlaghoz. A jelszóváltoztatás tudatos magatartást kíván. Az átlagnál tudatosabb tartományban volt a kurzus előtt és után is; értéke kicsit csökkent.

c) *Jelszóhosszság*: Biztonsági szempontból átlagosnak mondható. Javulást mutat, de a többi változóhoz képest az átlagosnál kisebb mértékben, ezért kissé átlag alatti lett az értéke. (A többség 14 karakternél rövidebb jelszavakat használ.) A leginkább tudatos magatartást mutatta a kurzus előtt és után is. Ezt alátámasztják a hallgatók szöveges válaszai, amelyekből kiderül, hogy tudatosan és növekvő számban használnak hosszabb jelszavakat.

d) *Karakterfajta*: Biztonsági szempontból átlag feletti volt és a kurzus után tovább javult. A tudatosság dimenzióban átlag alatt volt és maradt, de javulást mutatott. Ennek az lehet az oka, hogy a hallgatók sokféle karaktertípust használnak a jelszavaikban, ezért nehéz differenciálni, a tudatosságot számszerűen kimutatni. Ugyanakkor több hallgató megemlítette szöveges válaszában, hogy azért nem változtatja gyakrabban a jelszavait, mert (hosszú és) bonyolult jelszót használ, sokféle karakterrel.

e) *Jelszótárolás*: Biztonsági és tudatossági szempontból átlag alatti volt és maradt. A tudatosság kismértékű javulást, a biztonság ennél nagyobb visszalépést mutat. – Sokan megjegyzik a jelszavaikat, ami nem feltétlenül tudatos magatartás. 19-ből 10 főnél (a hallgatók felénél) nincs változás, 6 főnél javulás, 3 főnél visszalépés történt. Nem magas (19-ből 4 fő), de a tanév végére sem csökkent azok száma, akik megjegyeztetik a jelszavaikat a böngészővel, ami kényelmes, de nem tudatos – és kevésbé biztonságos – magatartás.

Az 1. csoport esetén nem voltak szignifikánsak a változások, ezért jelen tanulmányban az MDS ábrákat és elemzésüket nem közöljük. (Megemlítjük, hogy itt is jó illeszkedésű kétdimenziós redukált struktúrákat kaptunk. A kurzus előtt: Stress = 0,02418; RSQ = 0,99559; a kurzus után: Stress = 0,00298; RSQ = 0,99988.)

6. *Kvalitatív elemzések*

Nagyon tanulságosak a hallgatók nyitott kérdésekre adott válaszai. Itt csak egy-két példát tudunk említeni. Rákérdeztünk például arra, hogy a hallgató miért cseréli vagy nem cseréli a (fontosnak értékelt szolgáltatásokhoz használt) jelszavait. Kiderült, hogy sokan biztonságosnak tartják a jelszavaikat, pusztán egy, esetleg két ismerv miatt: mert hosszúak és/vagy bonyolultak, és e miatt a biztonságérzet miatt nem érzik szükségét, hogy (egyáltalán vagy gyakrabban) cseréljék. Mások lustaságra hivatkoztak, vagy arra, hogy már „benne van az ujjukban”, villámgyorsan begépelik, fejből. Vagyis esetükben a kényelmi szempontok diadalmaskodtak a biztonsági szempontok felett.

A kurzus előtt az 1. csoport 27 fős mintájából 12 fő (44,4%), a kurzus után 20 fő (74,0%) említett válaszában biztonsági szempontot (például ügyel a biztonságra, vagy biztonságosnak tartja a jelszavát). Tudnak róla, ám jelszóhasználati szokásaik nem mutattak szignifikáns javulást a kurzus végére. A 2. csoport 19 fős mintájából 18-an említettek biztonsági szempontot a kurzus előtt, 15 fő (78,9%) a kurzus után – a többiek lustaságra hivatkoztak; volt, aki le is írta, hogy tudja, hogy gyakrabban kellene cserélnie a jelszavát, de túl lusta hozzá. Tehát nem elég tudni, hanem megfelelő felelősséggel és attitűddel is kell viseltetni az iránt, hogy biztonságosan használják a jelszavaikat, védjék az adataikat.

Diszkusszió és konklúzió

Jóllehet a jelen tanulmányban bemutatott elemzést egy adott szakon, kis mintaelemszám mellett végeztük, következtetéseink ezért korlátozott érvényűek, ám a kutatás több tanulsággal szolgált mind didaktikai szempontból, mind a további kutatások és fejlesztések tervezését illetően.

A vizsgált hallgatói csoportok mindegyikében multimédiás eszközöket alkalmaztunk az oktatás során, változatos módon mutattuk be a jelszavak sérülékenységet, hívtuk fel a figyelmet az egyéni jelszókezelés és ebben az információbiztonsági tudatosság fontosságára. Elemzéseink alapján a programhasználattal kiegészített, és ezzel a hallgatók aktivitását támogató, az interaktív tevékenykedést facilitáló módszernek nagyobb hatása volt a hallgatók információbiztonsági attitűdjére, gyakorlatára és tudatosságára, mint a csak videóval támogatott oktatási módszernek. Ugyanakkor a kutatás rávilágított azokra a pontokra is, amelyekre az oktatás során érdemes nagyobb figyelmet fordítani, ahol (mint például a jelszavak tárolását illetően) még nem tapasztaltunk jelentős javulást (a kurzus során szó volt a jelszavak biztonságos tárolásáról, de a jelszótörő programok kipróbálása ezt nem érintette).

Az eredmények diszkussziója arra enged következtetni, hogy a két csoport közötti különbség, vagyis az alkalmazott oktatási módszerek eltérő hatékonyságának hátterében az áll, hogy ezekkel mennyire lehet bevonni a hallgatókat a tanulási folyamatba, mennyire vesznek részt ebben aktív szereplőként vagy inkább befogadóként.

A jelszóvisszafejtő programok oktatásban való alkalmazására jellemzőek az oktatási virtuális valóság főbb ismérvei: (1) „... szimulációs környezetet hoz létre, amelyben a tanuló megfigyelő, résztvevő és alkotó szerepet tölthet be”; (2) „komplex körülményeket és közeget teremt az elmerülés és átélés lehetőségéhez...”; (3) nehezen megközelíthető, illetve (4) védett, biztonságos tapasztalásokra ad lehetőséget (Aczél 2017: 10–11). A programhasználat az ember-számítógép interakció során olyan szimulált teret, egyfajta virtuális valóságot hoz létre, amely a hallgatók tapasztalati, szituatív, megfigyelő és egyben tevékenységalapú tanulását támogatja (Aczél 2017: 12–13): az egyéni, élményszerű megtapasztalás, a cselekvés, a kipróbálás, a tudástesztelés és átélés lehetőségét egy újszerű, virtuális közegben, ahol a tevékenységből eredő következmények szemmel láthatóak, anélkül, hogy a fizikai világban valós károkat okoznának.

A kutatás során a hatékonyságvizsgálat rámutatott a virtuális valóság oktatási alkalmazásának egyik további, lényegi vonására is. Eredetileg a fogalom az „*immersive virtual reality*”, azaz a beágyazott virtuális valóságra vonatkozott, tehát arra, hogy a felhasználó belemerül ebbe a mesterséges világba. A képzés hatékonysága szempontjából a lényeg tehát nem az, hogy a felhasználót egy számítógéppel generált háromdimenziós világ veszi körül, hanem a személyessé tett hallgatói aktivitás.

Az órákon szemléltetőeszközüket használt jelszóvisszafejtő programokat személyi számítógépen lehetett kipróbálni, de lépést tartva a technika fejlődésével és a hallgatók eszközhasználati szokásainak változásával, célul tűztük ki új multimédiás programok fejlesztését mobil eszközökön való felhasználásra.

E tanulmány kereteit túlfeszítette volna, de a jövőben a különböző (műszaki, informatikai, gazdasági, pedagógiai) képzési területeken, több hazai és határon túli intézményben futó kutatási projektünk tapasztalatait is szeretnénk összegezni és közzétenni. Természetesen az egyes képzési területeken és szakokon más az információbiztonsággal foglalkozó (vagy e területre is kitekintő) kurzus célja, mélysége, különböző részletességgel tér ki a technológiai aspektusokra, eltérőek a hallgatók előzetes ismeretei, és más az infor-

matikai előképzettségük is, illetve, van, ahol nemcsak felhasználóként, hanem szakemberként is foglalkozniuk kell információbiztonsággal; mindazonáltal a több területről származó kutatási eredmények fontos tanulságokkal szolgálhatnak. Bízunk benne, hogy több hasonló kutatás indul és kerül publikálásra, amelyekkel lesz lehetőségünk összevetni saját kutatásunkat és eredményeinket, és a jövőben további partnerek bevonásával közös, standardizált kutatást tudunk végezni, kitágítva a kutatás horizontját az információbiztonság egyéb területeire is.

Irodalom

- Aczél Petra, „Virtuális valóság az oktatásban – Ment-e a VR által az oktatás elébb?”, *Információs Társadalom*, XVII. évf. (2017) 4. szám, 7–24. old. <http://doi.org/10.22503/infars.XVII.2017.4.1>
- Benkő Livia, „Az adattudatosság szintjei és útjai”, *Információs Társadalom*, XVII. évf. (2017) 4. szám, 54–73. old. <http://doi.org/10.22503/infars.XVII.2017.4.4>
- Carretero, Stephanie, Riina Vuorikari and Yves Punie, *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*, Publications Office of the European Union, Luxembourg, 2017. <https://doi.org/10.2760/38842>
- Davis, Paula, „Measuring the Effectiveness of Information Security Awareness Training”, White Paper, *SAI Global*, 2008. <https://www.saiglobal.com>
- Ferrari, Anusca (author), Yves Punie (ed.) and Barbara N. Brečko (ed.), *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe*, Publications Office of the European Union, Luxembourg, 2013. <https://doi.org/10.2788/52966>
- Illéssy Miklós, Nemeslaki András és Som Zoltán, „Elektronikus információbiztonság tudatosság a magyar közgazdatisban”, *Információs Társadalom*, XIV. évf. (2014) 1. szám, 52–73. old. http://www.infonia.hu/digitalis_folyoirat/2014/2014_1/i_tarsadalom_2014_1_illessy_nemeslaki_som.pdf
- Keszthelyi, András, „About passwords”, *Acta Polytechnica Hungarica*, Vol. 10. (2013) No. 6., pp. 99–118. https://www.uni-obuda.hu/journal/Keszthelyi_44.pdf
- Keszthelyi, András és Esmeralda Kaděna, „Misunderstanding how Passwords Work”, in Pál Michelberger (ed.), *Management, Enterprise and Benchmarking in the 21st Century, III.*, Óbuda University, Keleti Faculty of Business and Management, Budapest, 2016, pp. 83–92. https://kgk.uni-obuda.hu/sites/default/files/06_KEA.pdf
- Konak, Abdullah, „Experiential Learning Builds Cybersecurity Self-Efficacy in K-12 Students”, *Journal of Cybersecurity Education, Research and Practice*, Vol. 3. (2018) No. 1., Article 6., 16 p. <https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss1/6>
- Kruger, Hennie A. and Wayne D. Kearney, “A prototype for assessing information security awareness”, *Computers & Security*, Vol. 25. (2006) No. 4., pp. 289–296. <http://doi.org/10.1016/j.cose.2006.02.008>
- Kruskal, Joseph B. and Myron Wish, *Multidimensional Scaling*, Sage Publications, London, 1978.
- Lehmann, Erich L., *Nonparametrics: Statistical Methods Based on Ranks*, Revised edition, Springer-Verlag, New York, 2006.
- Lévai Dóra és Papp-Danka Adrienn (szerk.), *Interaktív oktatásinformatika*, ELTE Eötvös Kiadó – Eszterházy Károly Főiskola, Eger, 2015. <http://www.eltereader.hu/interaktiv-oktatasinformatika/>
- Nemeslaki András és Sasvári Péter László, „Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában”, *Infokommunikáció és jog*, XI. évf. (2014) 4. szám (60. lapszám), 169–177. old. <http://real.mtak.hu/22237/>, https://infojog.hu/wp-content/uploads/pdf/201460_NemeslakiAndras_SasvariPeter.pdf
- Ollé János, „Interaktivitás és tevékenység-központúság az oktatásinformatikában”, in Lévai Dóra és Papp-Danka Adrienn (szerk.), *Interaktív oktatásinformatika*, ELTE Eötvös Kiadó – Eszterházy Károly Főiskola, Eger, 2015, 9–16. old. <http://www.eltereader.hu/interaktiv-oktatasinformatika/>

- Ollé János, Papp-Danka Adrienn, Lévai Dóra, Tóth-Mózer Szilvia és Virányi Anita, *Oktatásinformatikai módszerek. Tanítás és tanulás az információs társadalomban*, ELTE Eötvös Kiadó, Budapest, 2013. <http://www.eltereader.hu/kiadvanyok/oktatasinformatikai-modszerek/>
- Prah, Abigail N. W., Angela Aba Otchere and Kojo Ennin Opan, "The Perceived Effectiveness of Information Security Awareness", *Information and Knowledge Management*, Vol.6. (2016) No.7., pp. 62–73. <https://www.iiste.org/Journals/index.php/IKM/article/view/31730>
- Schneier, Bruce, "Fear and convenience", in Marc Rotenberg, Julia Horwitz and Jeramie Scott (eds.), *Privacy in the Modern Age: The Search for Solutions*, The New Press, New York, 2015, pp. 200–203.
- Siegel, Sidney, *Nonparametric Statistics for the Behavioral Sciences*, McGraw-Hill, New York, 1956.
- Stephanou, Anthony, *The Impact of Information Security Awareness Training on Information Security Behaviour*, Thesis, Faculty of Commerce, Law and Management, University of the Witwatersrand, Johannesburg, 2008. <http://hdl.handle.net/10539/7421>
- Szabó Endre Győző és Révész Balázs, „Adataink biztonságban – adatainkban a biztonság?”, *Információs Társadalom*, XVII. évf. (2017) 1. szám, 45–54. old. <http://doi.org/10.22503/infars.XVII.2017.1.3>
- Veseli, Ilirjana, *Measuring the Effectiveness of Information Security Awareness Program*, Thesis, Department of Computer Science and Media Technology, Gjøvik University College, Norway, 2011. <http://hdl.handle.net/11250/143980>
- Vuorikari, Riina, Yves Punie, Stephanie Carretero and Godelieve Van Den Brande, *DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model*, Publications Office of the European Union, Luxembourg, 2016. <https://doi.org/10.2791/11517>
- Yngström, Louise and Fredrik Björck, "The Value and Assessment of Information Security Education and Training", in Louise Yngström and Simone Fischer-Hübner (eds.), *Proceedings of the IFIP TC11 WG11.8 First World Conference on Information Security Education (WISE1)*, International Federation for Information Processing, Stockholm, 1999, pp. 271–292. <https://people.dsv.su.se/~bjorck/files/infosec-education.pdf>

Szász Antónia, PhD. Egyetemi tanulmányait az ELTE matematika és kulturális antropológia szakán végezte. Doktori fokozatát a szociológiai tudományok területén szerezte meg a Budapesti Corvinus Egyetemen. Tagja a Magyar Kulturális Antropológiai Társaságnak (2006-tól elnökségi tag), a Magyar Szociológiai Társaságnak, a Magyar ILIAS Közösség Egyesületnek és a „Ratkó István Matematika interdiszciplináris alkalmazásai” tudományos műhelynek. Szívesen foglalkozik az oktatás módszertani kérdéseivel, e-learninggel, adatelemzéssel, szimbólumkutatással és az információs társadalom különböző aspektusaival. Az elmúlt években érdeklődésének homlokterébe került az információbiztonság és a kiberbűnözés társadalmi kontextusa.

Kiss Gábor, PhD. 1970-ben született Budapesten. 1992-ben az Bánki Donát Gépipari Műszaki Főiskolán szerzett diplomát szervező-informatika, 1996-ban a Kossuth Lajos Tudományegyetemen informatikatanár szakon. 2013-ban számítástudományból doktorált a Debreceni Egyetemen. 1992 óta oktat az Óbudai Egyetem, illetve jogelőd intézményeiben, 2014 óta mentor a FernUniversität in Hagen-en. Informatikadidaktika területén 2003-ban a Frei Universität Berlin, 2006-ban az Universität Paderborn intézményekben is végzett kutatást. A Gesellschaft für Informatik e.V., az NJSZT, az International Association for Cyber Science and Engineering, a European Educational Research Association tagja. 2012 óta az Oktatási Hivatal külső szakértője. Kutatási területei: informatikaoktatás, mobileszközök a gyógyászatban, autonóm járművek információbiztonsági kérdései.