HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 4. szám 157–168.
DOI: 10.32567/hm.2021.4.12

Nimsz Vivien[1]

A társkereső applikációk biztonsági kockázatai

The Security Risks of Dating Applications

Az ember társas lény, a digitális világ pedig újabbnál újabb megoldásokat kínál arra, hogy a felhasználók internetes felületen találják meg az ideális társat. Az információs társadalomban az online párkeresés jelenségéről és lehetőségéről mindenki tud, azonban a felhasználók közül csak kevesen beszélnek róla nyíltan, gátlások nélkül. Milyen veszélyekkel járhat a túlzott társkeresőalkalmazás-használat és a kevésbé biztonságtudatos attitűd? Lehetnek-e hatással a tárkereső alkalmazásokon közétett személyes adatok a leendő hivatásos állomány tagjainak karrierútjaira? Kutatásom során főként ezekre a kérdésekre kerestem a választ, amelynek során a Nemzeti Közszolgálati Egyetem tisztjelölt és civil hallgatóinak hozzáállását vizsgáltam, többek között információbiztonsági szempontból. A tanulmánnyal fel szeretném hívni a leendő közszférában dolgozó, társkereső alkalmazásokat igénybe vevő felhasználók figyelmét az adatbiztonság jelentőségére, a biztonságos attitűd fontosságára, és arra, hogy karrierjük előtt igazán érdemes körültekintően és megfontoltan dönteni a saját magukról publikált adatokkal kapcsolatban, különös tekintettel az esetleges visszaélések alapját képező különleges adatokra.

Kulcsszavak: információbiztonság, adatvédelem, social engineering, tudatosítás, társkereső alkalmazások

Humans are social beings. The digital world always provides newer solutions to find the ideal partner. In the information society everyone knows about the phenomenon and possibility of online dating, but few users talk about it openly, without inhibitions. What are the dangers of overuse and a less safety-conscious attitude? How can published personal data affect the career path? In order to find the answers to these questions, I examined the attitudes among the students of the University of Public Services. With this study, I would like to draw attention to the importance of data security and a secure attitude among the users who work or are going to work in the public sector.

[1] Nemzeti Közszolgálati Egyetem, hallgató, e-mail: nimszvivi@gmail.com

Keywords: **information security, data protection, social engineering, awareness, dating applications**

1. Bevezetés

Az információs társadalom és a digitális világ olyan gyökeres változásokat hozott az emberek mindennapi szokásaiban, amelyek hatást gyakorolnak többek közt az emberi kapcsolatokra, a viselkedési normákra és az ismerkedési szokásokra egyaránt. Általánosságban elmondható, hogy a digitális eszközök befolyása egyenesen arányos a digitális infrastruktúra fejlettségével. A közösségi oldalak folyamatos elterjedésével egy időben a felhasználók temérdek mennyiségű adathalmazt kezdtek megosztani a világhálón, mit sem sejtve a lehetséges kockázatokról, fenyegetettségekről. Az általános adatvédelmi rendelet[2] (*General Data Protection Regulation,* GDPR) új fejezethez lendítette az internetes kultúrát mind felhasználói, mind szolgáltatói aspektusból, azonban ettől függetlenül megállapíthatjuk, hogy a felhasználók többsége kevésbé érzékeny az adat- és információbiztonságára, így a növekvő internethasználat következtében rengeteg információt lehet összegyűjteni a kevésbé biztonságtudatos személyekről, legyen szó preferenciáikról, kapcsolati hálójukról, aktuális tartózkodási helyükről.[3] Ezen adatok, metaadatok idegen kézbe kerülése számottevő hátrányokat, károkat okozhat mind magánéletünk, mind karrierünk szempontjából. Továbbá fontos megemlíteni azt is, hogy gyakran párosul az állampolgárok alacsony felhasználói tudatossága mellé egyfajta kíváncsiságérzet, amely arra ösztönzi a jóhiszemű felhasználókat, hogy a mulatságos, ámde értelmetlen és kattintásvadász linkeket megnyissák. Ez a tevékenység egyúttal egyenes utat jelenthet ahhoz, hogy valaki social engineering támadás áldozatává váljon. A *social engineering* a kibertámadásoknak egy olyan típusa, amely során a támadók a humán tényezőn keresztül férnek hozzá a védett informatikai rendszerekhez, védekezni mégis rendkívül nehéz ellene, hiszen ehhez a legkevésbé változtatható tényezőt, az emberi személyiséget kellene megváltoztatni.[4]

Kutatásom középpontjában az Y és a Z generáció mindennapi szokásai közé befurakodó tárkereső alkalmazások állnak. De mit is nevezhetünk tárkereső alkalmazásoknak? A szakirodalom nem rendelkezik egységesen kialakított fogalomrendszerrel, így a meghatározást több publikáció álláspontja alapján ismertetem. Társkereső alkalmazásnak nevezzük azokat az applikációkat, amelyekre a felhasználók főképp – de nem kizárólag – párkeresés céljából regisztrálnak. A tárkereső alkalmazások általában sajátos algoritmussal rendelkeznek, amelyek segítségével a felhasználók által megosztott adatok és információk alapján ajánlanak fel potenciális partnereket.[5] Ezt

[2] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről.

[3] Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36.

[4] Bányász Péter: Social Engineering and Social Media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77.

[5] Francesca Comunello – Lorenza Parisi – Francesca Ieracitano: Negotiating Gender Scripts in Mobile Dating Apps: Between Affordances, Usage Norms and Practices. *Information, Communication & Society,* 24. (2021), 8. 1140–1156.

a fajta algoritmust gondolta tovább a *Fekete tükör* (ismertebb angol nevén: *Black Mirror*) elnevezésű televíziósorozat is a 4. évad 4. részében. Az epizód során a rendszer beállítottság és érdeklődési kör alapján választotta ki a legmegfelelőbb párosításokat, de a felek még képen sem látták egymást az első találkozóig. A sorozatban prezentált rendszer több ponton is elrugaszkodik a valóságtól, szinte már a valódi társkereső alkalmazások paródiájaként bukkant fel, azonban a készítők által bemutatott algoritmus emlékeztet a való életben alkalmazott algoritmusokra.

Napjainkban a tárkereső alkalmazások elsődleges célja, hogy első körben virtuális köteléket, azt követően pedig az offline térben is megvalósuló kontaktot alkossanak két fél között az online térben létrejövő írásbeli kommunikáció segítségével.[6] Ezek az applikációk szenzitív adatok sokaságát várják el tőlünk a használatért cserébe. Az átlagfelhasználó logikusan gondolhatja azt, hogy minél többet oszt meg saját profilján magáról, annál hatékonyabban vetheti bele magát a párkeresésbe, azonban az online tér tartogathat némi meglepetést az óvatlan felhasználók számára. Első hangzásra nem tűnhet olyan kockázatosnak személyes adatokat megosztani magunkról az internetes platformokon, vagy akár az online beszélgetéseinkben, azonban számos veszéllyel járhat. Olykor az emberek nem is gondolják, mennyire könnyen válhatnak adatlopás vagy egyéb más támadás áldozatává, továbbá, ha esetlegesen konkrét személy befolyásolása lenne a támadók fő célpontja, mi más jelenthetne optimális megoldást, mint a társadalom által gyakran tabutémaként kezelt társkereső alkalmazások nyújtotta nyílt forrású információgyűjtés, amellyel nagymértékben nő a felhasználói profillal rendelkezők körében a profilozás és zsarolás kockázata is.

Az OSINT[7] történetében új fejezetet nyitott a közösségi és társkereső oldalak megjelenése, hiszen meglehetősen átalakították, kiegészítették a hagyományos médiumokból történő hírszerzést.[8] De hogyan történhet meg a nyílt forrású információszerzés alkalmazása az egyik legnépszerűbb társkereső alkalmazáson, a Tinderen? Az applikáció alapvetően csak a felhasználók keresztnevét mutatja, de ha nem vagyunk elég körültekintőek, hamar kinyomozhatókká vállhatuk más platformokon egyaránt. Ennek egyik példája lehet az Instagram, amelyet szintén Tinderes profilunkhoz csatolhatunk. Az Instagramos profilok gyakran a felhasználó valós nevét tartalmazzák, ily módon akaratlanul is valós nevünkkel szerepelhetünk, ha figyelmetlenek vagyunk. Az oktatási intézmény, munkahely megadásával adatvédelmi szempontból nagymértében növeljük sebezhetőségünket, de az azonos profilkép használata is könnyítést jelenthet egy esetleges virtuális „kukkolónak".

A helyzetmeghatározásra támaszkodó applikációk nagy gyakorisággal jelennek meg mindannyiunk okostelefonján, de manapság már egyre több weboldal is engedélyt kér helyzetünk használatához. A helyzetmeghatározást használó felületek valóban kényelmesebbé, gyorsabbá tudják tenni internetes böngészésünk folyamatát, gondoljunk csak az étel-házhozszállítással foglalkozó platformokra, amelyek listázzák számunkra a legközelebbi éttermeket, de akár az e-közszolgáltatásokat nyújtó

[6] Randy Jay C. Solis – Ka Yee J. Wong: To Meet or Not to Meet? Measuring Motivations and Risks as Predictors of Outcomes in the Use of Mobile Dating Applications in China. *Chinese Journal of Communication,* 12. (2019), 2. 204–223.

[7] *Open source intelligence,* azaz nyílt forrású információszerzés.

[8] Bányász (2015): i. m.

mobilapplikációkat is idesorolhatjuk. A helyzetmeghatározáson kívül elterjedt metódusnak számít az a megoldás, amelynek során az applikációk Bluetooth használatával cserélnek kódot, kommunikálnak egy esetleges másik készülékkel. Ilyen módszerrel működik például a koronavírus-járvány során fejlesztett VírusRadar applikáció, amely a hatóságokat segítette kontaktkutatás alkalmával.[9] Ezek a megoldások, technológiák kényelmet tudnak biztosítani mindennapi életünkben, azonban a komfortot, nem mindig múlja felül a biztonságérzetünk.

A társkereső alkalmazások gyakorta egyfajta relevancián alapulnak. Korábban a már emlegetett közös érdeklődési kör jelentette az alapkövet – amelyet a regisztrációnál egyfajta kérdőívvel mértek –, azonban manapság releváns információnak számít a felek lokációja is. Három olasz kutató, Adriano Di Luzio, Alessandro Mei, Julinda Stefa – nem túl etikus módon – vette a bátorságot és letesztelte, hogy mekkora mértékű gondot jelent a Happn nevezetű társkereső alkalmazásról adatokhoz jutni illegális módon. A Happn szintén helyzetmeghatározásra alapozó applikáció, amelynek célja, hogy a felhasználók tudomást szerezzenek arról, hogyha egymás közelében tartózkodnak. A kutatók úgynevezett közbeékelődéses támadást *(man-in-the-middle attack)* produkáltak, amelynek során két fél közé (jelen esetben a felhasználó és a Happn alkalmazás) betolakodik egy harmadik fél is. Az ilyen és ehhez hasonló támadások során az alkalmazások és a weblapok azt hiszik, hogy a valós végponttal, azaz a felhasználóval kommunikálnak, a felhasználó pedig szintén azt hiszi, hogy csupán az alkalmazás számára szolgáltat adatokat. A kutatóknak sikerült ily módon, Róma területén több mint 10 000 ember adatait begyűjteni. A tanulmány végén hangsúlyozták, hogy harmadik félnek nem adták ki ezeket a személyes adatokat, illetve azokat a kutatás végéig egy titkosított adatbázisban tárolták, majd a kutatás végén mindet megsemmisítették.[10]

2018-ban egy izraeli információbiztonsággal foglalkozó cég által fény derült arra, hogy a Tinder-felhasználók minimális adat megosztásával is könnyen válhatnak megfigyelés, zsarolás áldozatává, ez pedig betudható annak a ténynek, hogy a Tinderen tárolt fotókat nem titkosított csatornán továbbítják. De hogyan is lehet ezt a biztonsági rést kihasználni? Aki közös wifihálózatra van csatlakozva a megfigyelni kívánt emberrel, nemcsak láthatja a képeket, hanem azt is megtudhatja az adatforgalom követésével, hogy kiket húzott jobbra, illetve kiket balra, és mikor van az illetőnek találata. (Az alkalmazáson belüli szimpátiát a jobbra pöccintéssel lehet kifejezni, ha pedig nem szeretnénk az adott felhasználóval kapcsolatba kerülni, balra kell húzni a profilt.) Ezzel a módszerrel kideríthető, hogy a megfigyelt személynek kik tetszenek, ezáltal pedig egyenes út vezethet egy esetleges érzelmi zsaroláshoz.[11] A szervezet demonstrálásképp megalkotott egy szoftvert, amely működés közben ezt a biztonsági rést vette alapul, és bemutatta azt a Tinder fejlesztőinek.[12]

[9] Attila Német – Sándor Magyar: An Investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible National Security application (PART1). *National Security Review Issue,* (2020), 2. 52–64.

[10] Adriano Luzio – Alessandro Mei – Julinda Stefa: Uncovering Hidden Social Relationships through Location-based Services: The Happn case study. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2018. 802–807.

[11] Tóth Balázs: Titkosítás nélkül pörögnek a képek a Tinderen. *Index.hu,* 2018. január 24.

[12] Andy Greenberg: Tinder's Lack of Encryption Lets Strangers Spy on Your Swipes. *Wired,* 2019. január 23.

Nem véletlen a mondás, miszerint információbiztonság szempontjából az ember a leggyengébb láncszem. Befolyásolhatóság, kíváncsiság, manipulálhatóság erőteljes emberi jellemzők. Ezek az emberi tulajdonságok mind-mind hozzájárulnak a social engingeering alapú támadások sikerességéhez. A social engineering során a bűnözök az információbiztonságot nem, vagy csak kevésbé ismerő, vakon együttműködő személyektől szereznek információt. Ezek az értesülések később gyakran akár védett rendszerekhez történő hozzáférés kulcsaként szolgálnak, vagy csak egyszerűen megkönnyítik a jogtalan hozzáférést.[13] A social engingeeringen belül megkülönböztethetünk két válfajt: a humán alapú támadásokat és az informatikai alapú támadásokat.[14] A humán alapú támadások kapcsán szóba jöhet például számos olyan példa, amelynek során az emberek érzelmeire próbál a támadó hatni. Így történt ez már a 2000-es évek elején is, amikor Anna Kurnyikova orosz teniszsztár állítólagos szerelmes levele terjedt el világszerte. A levél szövegében pikáns képeket ígértek a sportolóról, ám ez természetesen nem volt elérhető az ígért linken.[15] Ez a fajta „szerelmeslevél" ugyan maradandó károkat nem okozott azoknak, akik megnyitották, azonban kiváló módon szemlélteti, hogy olykor milyen olcsó trükkökkel lehet rávenni a mit sem sejtő felhasználót a kattintásra. Ezek alapján nem nehéz levonni a következtetést, hogy aki 2021-ben az érzelmeket kihasználva szeretne adatokhoz és információkhoz jutni, nagy eséllyel fordul a társkereső alkalmazásokhoz.

A social engingeering mint támadási forma megjelent már a társkereső alkalmazások vonatkozásában a hadműveleti területeken is. A Hamasz palesztin szervezet megbízásából tevékenykedő hackereknek az Izraeli Védelmi Erőknél (IDF) szolgáló katonák százait sikerült megvezetni dekoratív hölgyek képeivel, ennek eredményeképp az izraeli katonák egy alkalmazást töltöttek le eszközeikre, amelynek segítségével a palesztinok hozzáfértek a teljes mobiltelefon-készülékhez és a tartózkodási helyhez.[16] Ebben a példában a hadszíntéren használták ki az ellenfél kevésbé biztonságtudatos attitűdjét. Az Egyesült Államokban egy csalási hullám keretein belül több száz gyanútlan civil felhasználót sikerült átvernie azoknak a bűnözőknek, akik katonáknak adták ki magukat. A támadók főképp szenzitív üzenetekkel, az érzelmekre hatva jutottak el trükkösen odáig, hogy a felhasználók pénzt utaljanak nekik.[17]

2. Módszerek

A fentiekben bemutatott támadási formák, sérülékenységek rendkívül jól prezentálják, hogy a társkereső alkalmazások biztonsági kockázataival igenis szükséges foglalkozni. Mindezekre tekintettel kutatásomban a társkereső applikációk felhasználóinak motivációját, szokásait, hozzáállását vizsgáltam többek közt információbiztonsági szempontból,

[13] Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37.

[14] Bányász–Bóta–Csaba (2019): i. m.

[15] Kurnyikova, a féregvírus. *Index.hu,* 2001. február 13.

[16] Molnár Csaba: Dekoratív hölgyek képével verték át a Hamász hekkerei az izraeli katonákat. *Index.hu,* 2020. február 17.

[17] Barb Chiles: Military Romance Scams: Are You a Target? *Military.com,* (é. n.).

a Nemzeti Közszolgálati Egyetem (NKE) hallgatóinak körében. Vizsgálódásom során két hipotézist fogalmaztam meg, amelyek a következők:

H1: Az NKE hallgatói jellemzően unalomból és szórakozásból regisztráltak társkereső alkalmazásokra, nem a párkeresés volt a fő cél.

H2: A NKE hallgatói nagyobb százalékban vallják magukat biztonságtudatosnak adatvédelmi szempontból, mint sem.

Munkám egyik központi elemét az általam készített kérdőív jelentette, amelyet csak és kizárólag a NKE hallgatói tölthettek ki. Felmérésem azért korlátozódott az NKE hallgatóinak körére, mert feltételezem, hogy a kitöltők egyetemi tanulmányaik elvégzését követően az állami szférában fognak munkát vállalni, akár a hivatásos állomány tagjaként, akár a civil állomány részeként, így amennyiben ezek a hallgatók nem részesülnek olyan, az adat- és információbiztonsági tudatossággal kapcsolatos oktatásban, amelynek segítségével felismerhetik a fenyegetéseket, magas fokú kockázatot jelentenek az őket foglalkoztató szervezet számára.[18]

A kérdéssor három részből állt, a kitöltők a demográfiai adatok megadásával kezdhették a válaszadást, itt főképp az életkort, a legmagasabb végzettséget, és azt vizsgáltam, hogy melyik kar hallgatója az adott illető. Ezt követően a társkereső alkalmazásokon felbukkanó jellemző viselkedési formákra, attitűdökre vonatkozó kérdések következtek, majd végül a harmadik részben adat- és információbiztonsági tudatossággal kapcsolatos kérdésekkel zárult a kérdőív.

Kérdőívem második részéhez és az interjúm során egyaránt Rhiannon B. Kallis *Understanding the Motivations for Using Tinder* című kutatásában szereplő felmérést ismételtem meg.[19] Empirikus vizsgálatában főképp nyitott kérdésekkel dolgozott, de zárt kérdések is felbukkantak. A kapcsolatot e-mailben vettem fel a szerzővel, amelynek során kifejtettem kutatásom célkitűzéseit, kérésemre még aznap választ kaptam. A harmadik részhez Kathryn Parsons és szerzőtársai 2017-ben végzett kutatásához kapcsolódó kérdőívét használtam fel, amelyet teljes egészében publikáltak a cikkben.[20] Ebben az írásban Tudás–Képesség–Viselkedés modell segítségével mérték fel a kitöltők kompetenciáit. Ez alapján a „Tudáshoz" soroljuk az ismeret jellegű elemeket (elvek, elméletek, tények ismeretét). A „Képesség" a „Tudás" alkalmazásának képességét jelöli, amelynek során az egyén megoldja a felmerülő problémákat. A „Viselkedés" a tényleges viselkedésformákat jelenti. A tudásra vonatkozó kérdések esetében a „tudom", „ismerem", „megértem", „azonosítom", „felismerem" jellegű állításokat, a képességre vonatkozó kérdések esetében a „képes vagyok felismerni", „képes vagyok figyelembe venni" stb. jellegű állításokat, míg a viselkedésre vonatkozó kérdések esetében „tudatosan használom", „törekszem" stb. típusú állításokat fogalmaztam meg.[21]

[18] Bányász Péter: *A közösségi média lehetőségei és kihívásai a védelmi szférában.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2018.

[19] Rhiannon B. Kallis: Understanding the Motivations for Using Tinder. *Qualitative Research Reports in Communication,* 21. (2020), 1. 66–73.

[20] Kathryn Parsons et al.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers & Security,* 66. (2017), 40–51.

[21] Bányász (2019): i. m.

A kérdőíven felül fókuszcsoportos interjúkat végeztem, amellyel célzottan vizsgáltam hallgatótársaim motivációját a regisztrációhoz, attitűdjét az alkalmazás használata közben, és azt, hogy milyen adatokat osztanak meg az applikáció hatékony, sikeres használata érdekében. A fókuszcsoportos interjúk során minden karról meghallgattam három nő és három férfi hallgatótársamat, ezt követően pedig kontrollcsoportként vizsgáltam más felsőoktatási intézmények hallgatóinak hozzáállását is.

Kutatási eredményeim szöveges, statisztikai kiértékeléséhez Sajtos László *SPSS Kutatási és adatelemzési kézikönyv*ét hívtam segítségül. A válaszok értékelése során kereszttábla-elemzést alkalmaztam, amely széles körben elterjedt módszernek számít. Két vagy több változó közötti összefüggést vizsgál, illetve ezek kombinált gyakoriságát, eloszlását mutatja. Az elemzés során azt vizsgáljuk meg, hogy két nominális vagy ordinális változó kapcsolatban áll-e egymással, máshogy magyarázva a kereszttábla-elemzés nem más, mint két gyakoriságelemzés együttes vizsgálata két nem metrikus változó esetében. A kereszttáblával kapcsolatos statisztikák közül talán leggyakrabban használt a Pearson-féle khi-négyzet, amely a két változó összefüggésének szignifikanciáját méri. A mutatószám alapján megállapítható, hogy van-e statisztikai összefüggés a két változó között.[22] A khi-négyzet próba feltétele, hogy az elvárt gyakoriság minden egyes cellában minimum 5 kell legyen. A khi-négyzet próbán kívül elemzésem során figyelembe vettem még a Cramer's V együtthatót, amely egy asszociációs együttható és két nominális változó közötti kapcsolat szorosságát mutatja meg. Az érték 0 és 1 közötti intervallumban van, minél közelebb áll az 1-hez, annál erősebb statisztikai kapcsolatról beszélhetünk.[23]

3. Eredmények

A kérdőívemet összesen 198-an töltötték ki (n = 198), azonban fontos megemlíteni, hogy nem minden kérdésnél lehetett a válaszadást kiértékelni, ezért az egyes kérdések elemzésénél adattisztogatást végeztem (erről bővebben a továbbiakban fogok szólni). A kérdőív teljesen anonim formában volt elérhető. A válaszadók között 121 nő és 77 férfi volt. A kitöltők 86,4%-ának érettségi a legmagasabb végzettsége, 11,6%-nak alapszakos diploma, 1,5%-ának mesterszakos diploma és 0,5%-nak doktori fokozat. A legtöbb kitöltésszámról a karok megoszlásában az Államtudományi és Nemzetközi Tanulmányok Kar (ÁNTK) esetében beszélhetünk, számszerűsítve 69,2%. Az összes kitöltésszám (n = 198) 18,7%-át jelenti a Hadtudományi és Honvédtisztképző Kar tisztjelölt és civil hallgatóinak kitöltése, 11,6%-át a Rendészettudományi Kar hallgatói, 0,5%-át pedig a Víztudományi Karról érkezett 1 db kitöltés.

A H1 hipotézisem szerint a társkereső alkalmazások felhasználói jellemzően unalomból és szórakozásból regisztrálnak, nem a párkeresés a fő cél. A hipotézis vizsgálata közben kérdőívem kilencedik kérdését elemeztem IBM SPSS Statistics

[22] Sajtos László – Mitev Ariel: *SPSS kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.
[23] Khi-négyzet próba jelentése és alkalmazása az SPSS-ben: https://spssabc.hu/ketvaltozos-elemzes/khi-negyzet-proba

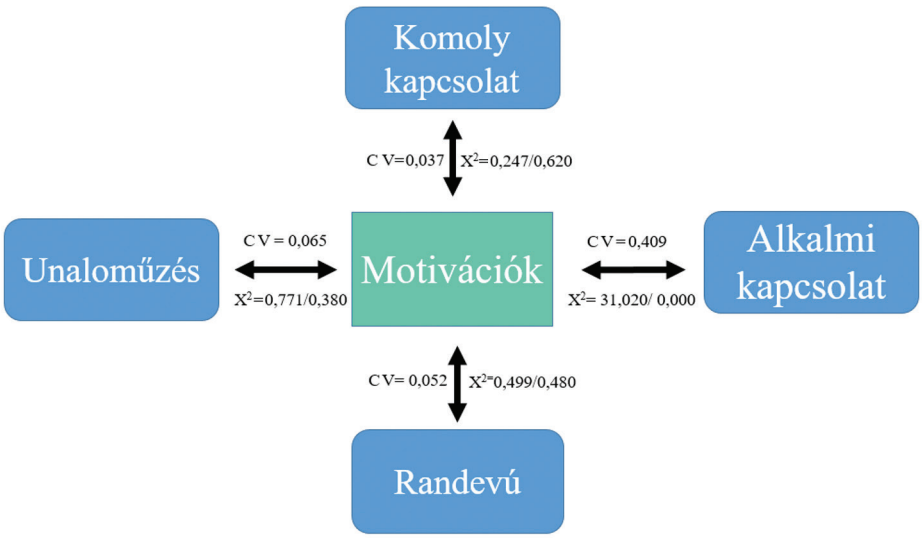
24 nevezetű programmal, amely így szól: Mi motiválta arra, hogy regisztráljon társkereső alkalmazásra?

A válaszok kiértékelése során a fentebb említett kereszttábla-elemzést alkalmaztam, szám szerint négyet, mivel négy különféle lehetséges opciót lehetett választani a válaszadás során, a kitöltők több motivációt is bejelölhettek válaszként. Ötödik opcióként megjelent az „egyéb" rovat, amelyben rendszerint komolytalan válaszok érkeztek, így végül ezt az opciót nem értékeltem ki. A motivációk esetében a nemmel összefüggésben vizsgáltam a kapott adatokat. Az összes, 198 kitöltés helyett 185 (n = 185) válaszadást tudtam értékelni. Az első vizsgálatom arra vonatkozott, van-e összefüggés a nemek és a között, hogy komoly kapcsolat szerzése érdekében regisztrált-e a platformra a kitöltő. A khi-négyzet teszt (x^2 = 0,247; df = 1) kétoldali szignifikanciaszintje 0,620, tehát nincs statisztikailag szignifikáns kapcsolat a két változó között, mivel a kétoldali szignifikanciaszint nem nagyobb mint 0,05. Ezt követően Cramer's V (C V) mutató segítségével is vizsgálódtam. Ahogy már említettem, C V mutató esetén a nullához való közelség függetlenséget, míg az egyhez való közelség erős kapcsolatot jelent a két változó között. Ebben a példában a következőképp alakult: A C V mutató értéke 0,037, ezáltal kijelenthetem, hogy a meglehetősen gyenge a két változó közötti kapcsolat.

Sorban a következő választási lehetőségként a „randevúk miatt regisztráltam" menüpontot adtam meg, az elemzés menete azonos volt. A khi-négyzet teszt (x^2 = 0,499; df = 1) kétoldali szignifikanciaszintje ebben az esetben 0,480, tehát statisztikailag szignifikáns kapcsolatról megint nem tudunk beszélni. A C V mutató értéke 0,052, tehát szintén gyenge kapcsolatot tudtam megállapítani.

A harmadik vizsgálatom bizonyult statisztikai szempontból a legizgalmasabbnak, amelynek során azt elemeztem, hogy a válaszadók neme és az „érzelemmentes alkalmi kapcsolat kialakítása céljából regisztráltam" opciót választók között van-e összefüggés. A khi-négyzet teszt (x^2 = 31,020; df = 1) kétoldali szignifikanciaszintje ebben az esetben 0,00, tehát statisztikailag szignifikáns kapcsolatról tudunk beszélni, vagyis a válaszadók neme befolyásolta azt, hogy érzelemmentes alkalmi kapcsolat motiválta a regisztrációra vagy sem. C V mutató értéke 0,49, tehát közepes kapcsolatot tudunk megállapítani a két változó között.

Végül, de nem utolsósorban analizáltam az „unaloműzésképpen regisztráltam" elnevezésű választási lehetőséget is a nemek vonatkoztatásában. A Khi-négyzet teszt (x^2 = 0,771; df = 1) kétoldali szignifikanciaszintje ebben az esetben 0,380, tehát ebben az esetben sem tudunk statisztikailag szignifikáns kapcsolatról beszélni, vagyis a válaszadók neme nem befolyásolta azt, hogy az unaloműzés motiválta a regisztrációra, vagy sem. C V mutató értéke 0,065, tehát gyenge kapcsolatot tudunk megállapítani a két változó között. A négy vizsgált motivációt összesítve az 1. számú ábrán mutatom be. Összegezve elmondható, hogy statisztikailag szignifikáns kapcsolatról tudunk beszélni az érzelemmentes alkalmi kapcsolat kialakításából eredendő motivációk és a nemek között, ezáltal igazoltam a H1 hipotézisemet.



1. ábra

Mi motiválta arra, hogy társkereső alkalmazásra regisztráljon?

Forrás: a szerző szerkesztése

Ezt követően a H2 hipotézisemre vonatkozóan végeztem vizsgálatot. H2 hipotézisem így hangzik: Az NKE hallgatói nagyobb százalékban vallják magukat biztonságtudatosnak adatvédelmi szempontból, mint sem. A korábbiakban már említett Tudás–Képesség–Viselkedés modell segítségével tettem fel kérdést H2 hipotézisemre tekintettel, amely így hangzott: Biztonságtudatosnak gondolja-e magát adatvédelmi szempontból? A válaszadók (n = 198) 75,8%-a gondolja magát adatvédelmi szempontból biztonságtudatosnak, míg 24,2%-a nem, ezzel H2 hipotézisemet alátámasztottam, továbbá vizsgáltam még a változók közti statisztikai kapcsolatokat, a nemmel összevetve. A Khi-négyzet tesztet itt is elvégeztem, amelynek eredménye statisztikailag szignifikáns kapcsolatról nem tudott beszámolni. (x^2 = 0,013; df = 1) kétoldali szignifikanciaszintje ebben az esetben 0,910, vagyis a válaszadók neme nem befolyásolta azt, hogy adatvédelmi szempontból biztonságtudatosnak vallották magukat a kitöltők, vagy sem. A C V mutató értéke 0,008 tehát nagyon gyenge kapcsolatot tudunk megállapítani a két változó között.

Érdekességképp megkérdeztem hallgatókat, hogy hallgattak-e az egyetemen adat- és/vagy kiberbiztonsági tudatossággal kapcsolatos kurzust (n = 198)? A válaszadók 57,6%-a nyilatkozta azt, hogy hallgatott korábban ezzel kapcsolatos kurzust, míg 42,4% nyilatkozta azt, hogy nem. Az interjúk végén megállapítottam, hogy kötelező óra keretein belül főképp a tisztjelölt hallgatóknak volt lehetőségük ilyen kurzuson részt venni, az ÁNTK hallgatói inkább szabadon választható tantárgy keretein belül tanulhattak adat- és/vagy kiberbiztonsági tudatosságról.

A kérdőívben szintén a Tudás–Képesség–Viselkedés modell segítségével mértem fel kitöltőim hozzáállását az információk online közlésével kapcsolatosan. Az arányok

a következőképp alakultak (n = 198): a kérdezettek 73,2%-a nyilatkozta azt, hogy mindig ellenőrzi egy weboldal megbízhatóságát, mielőtt információt közölne azon, 15,2% mondta azt, hogy amennyiben segíti a tanulásban, munkavégzésben, nem lényeges, hogy milyen információt közöl egy weboldalon, és a maradék 11,6% választotta azt az opciót, miszerint tudja, hogy rendben van mindenféle információ közlése a különböző weboldalakon, amennyiben az segít a tanulásban, munkavégzésben.

4. Következtetések

Munkám arra próbál rávilágítani, hogy a társkereső alkalmazások használatához rendszerint párosul kevésbé biztonságtudatos attitűd, amely elősegíti az esetleges támadások hatékonyságát.

T1 tézisem igazolta, hogy az NKE hallgatói körében a motivációt nem kizárólag a konkrét társkeresés jelenti, T2 tézisem pedig alátámasztotta, hogy az NKE diákjai nagyobb arányban vallják magukat biztonságtudatosnak adatvédelmi szempontból, mint sem. A kérdőív és az interjú más kérdéseit elemezve azt is láthattuk, hogy a válaszadók több mint fele részt vett eddigi tanulmányai során adat- és/vagy kiberbiztonsági tudatossággal kapcsolatos kurzuson, ennek ellenére a hallgatók rendszerint osztanak meg magukról olyan szenzitív adatokat pluszban, amelyeket a társkereső alkalmazások nem várnak el kötelező jelleggel.

Véleményem szerint mindenki számára komoly problémát jelenthet a társkereső oldalakon megosztott túlzott információhalmaz, hiszen ahogyan a korábbiakban szemléltettem, temérdek mennyiségű támadási módszer áll a támadók rendelkezésére, abban az esetben, ha adatokhoz szeretnének jutni illegális módon. Az NKE hallgatóinak különösen nagy figyelmet kellene fordítaniuk személyes adataik kezelésére az online felületeken, mivel nagy valószínűséggel az egyetemi tanulmányaik elvégzését követően az állami szférában fognak munkát vállalni, akár a hivatásos állomány tagjaként, akár a civil állomány részeként. Amennyiben ezek a fiatalok nem részesülnek olyan, az adat- és információbiztonsági tudatossággal kapcsolatos oktatásban, amelynek segítségével felismerhetik a fenyegetéseket, abban az esetben magas fokú kockázatot jelentenek az őket foglalkoztató szervezet számára. Ezért igazán érdemes körültekintően és megfontoltan dönteni a saját magukról publikált adatokkal kapcsolatban.

A biztonsági kockázatokon kívül azonban az a tény sem elhanyagolható, hogy a virtuális térben történő túlzott időtöltés erőteljesen képes befolyásolni személyiségfejlődésünk szakaszait, kialakított önképünk megítélését, illetve általános habitusunkat. A társkereső oldalak fogalmához gyakran párosul negatív sztereotípia, a külföldi szakirodalom számos esetben emlegeti a társkereső alkalmazásokat biológiai piacként, húspiacként. Nem szabad megfeledkeznünk az álprofilok diverzáns hatásairól sem, amelyek szinte minden közösségi médiában jelentkeznek, annak ellenére, hogy ezt az oldalak közösségi irányelvei szigorúan tiltják.

Felhasznált irodalom

Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36. Online: https://doi.org/10.32561/nsz.2015.2.2

Bányász Péter: *A közösségi média lehetőségei és kihívásai a védelmi szférában.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12483/banyasz_peter_doktori_ertekezes_2018.pdf?sequence=1

Bányász Péter: Social Engineering and Social Media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77. Online: https://doi.org/10.32561/nsz.2018.1.4

Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

Chiles, Barb: Military Romance Scams: Are You a Target? *Military.com,* (é. n.). Online: www.military.com/spouse/military-life/military-romance-scams-are-you-target.html

Comunello, Francesca – Lorenza Parisi – Francesca Ieracitano: Negotiating Gender Scripts in Mobile Dating Apps: Between Affordances, Usage Norms and Practices. *Information, Communication & Society,* 24. (2021), 8. 1140–1156. Online: https://doi.org/10.1080/1369118X.2020.1787485

Greenberg, Andy: Tinder's Lack of Encryption Lets Strangers Spy on Your Swipes. *Wired,* 2019. január 23. Online: www.wired.com/story/tinder-lack-of-encryption-lets-strangers-spy-on-swipes/

Kallis, Rhiannon B.: Understanding the motivations for using Tinder. *Qualitative Research Reports in Communication,* 21. (2020), 1. 66–73. Online: https://doi.org/10.1080/17459435.2020.1744697

Kurnyikova, a féregvírus. *Index.hu,* 2001. február 13. Online: http://index.hu/tech/net/anna/

Luzio, Adriano – Alessandro Mei – Julinda Stefa: Uncovering Hidden Social Relationships through Location-based Services: The Happn Case Study. In *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).* 2018. 802–807. Online: https://doi.org/10.1109/INFCOMW.2018.8406866

Molnár Csaba: Dekoratív hölgyek képével verték át a Hamász hekkerei az izraeli katonákat. *Index.hu,* 2020. február 17. Online: https://index.hu/techtud/2020/02/17/izrael_hadsereg_idf_hamasz_hekkerek_adathalasz_atveres_kamu_nok/

Parsons, Kathryn – Dragana Calic – Malcom Pattinson – Marcus Butavicius – Agata McCormac – Tara Zwaans: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers & Security,* 66. (2017), 40–51. Online: https://doi.org/10.1016/j.cose.2017.01.004

Randy Jay C. Solis – Ka Yee J. Wong: To Meet or Not to Meet? Measuring Motivations and Risks as Predictors of Outcomes in the Use of Mobile Dating Applications in China. *Chinese Journal of Communication,* 12. (2019), 2. 204–223. Online: https://doi.org/10.1080/17544750.2018.1498006

Sajtos László – Mitev Ariel: *SPSS kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.

Tóth Balázs: Titkosítás nélkül pörögnek a képek a Tinderen. *Index.hu,* 2018. január 24. Online: https://index.hu/tech/2018/01/24/titkositas_nelkul_porognek_a_kepek_a_tinderen