Polgári Szemle, 17. évf. 1–3. szám, 2021, 358–373., DOI: 10.24307/psz.2021.0726

Legárd Ildikó

Játék a jövőért

Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével

A Game for the Future

Possibility of Developing Information Security Awareness with the Help of a Gamified Application

Összefoglalás

Az információbiztonsági tudatosság napjainkban egyre nagyobb jelentőséggel bír. Már régóta közhelynek számít, hogy az információbiztonság területén a humán faktor, tehát a felhasználó maga a leggyengébb láncszem. Hiába védjük rendszereinket a legmodernebb és legerősebb fizikai és logikai védelmi intézkedésekkel, ha az elektronikus információs rendszereket használók nem tartanak lépést a technológiai fejlődéssel, illetve nem kellően tudatosak és elővigyázatosak a rendszerek használata során. A felhasználók digitális és információbiztonsági tudásának, kompetenciáinak fejlesztésére a tudatosítási programok nyújtják a leghatékonyabb megoldást. Számos vizsgálat megerősíti azt a tényt, hogy a tudatosítás módszerei közül azok a technikák bizonyulnak a leghatékonyabbnak, amelyek gyakorlatias, élményszerű tanulási lehetőséget biztosítanak a felhasználók számára. Egyetlen magyar nyelvű tudatosító applikációként, a 9-13 éves korosztály számára fejlesztett Mongu for Teen sikeressége is bizonyítja, hogy egy gamifikált alkalmazás képes pozitív irányba befolyásolni a felhasználók biztonságtudatosságát. A tanulmány végén ajánlásként megfogalmazásra és bemutatásra kerül egy olyan magyar nyelvű tudatosító applikáció, a „Célpont vagy" terve, amely tartalma és felépítése szempontjából a legfrissebb tudományos eredményekre, valamint a már működő applikációk tapasztalataira támaszkodik, és alkalmas lehet a társadalom széles körű, élményszerű tudatosítására.

Journal of Economic Literature (JEL) kódok: I250, O31, Y8

Kulcsszavak: információbiztonság, IT biztonság, információbiztonsági tudatosítás, gamifikáció, applikáció

Legárd Ildikó, PhD hallgató, Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi Doktori Iskola (ildiko.legard@gmail.com).

Summary

Information security awareness is becoming increasingly important these days. Many experts agree that the weakest link in the field of information security is the human factor, namely the user. It is pointless to protect our systems with the strongest, state-of-the-art physical and logical measures, while the users of these systems do not keep up with technological development and are not sufficiently aware or cautious when using the systems.

Information Security Awareness Programs provide the most expedient way to improve the digital and information security knowledge and competence of users. Numerous studies confirm that the most efficient awareness raising techniques are those which provide practical and experiential learning opportunities for users. The success of Mongu for Teen, developed as a single Hungarian-language awareness raising application for 9-13-year-olds, also proves that a gamified application can positively influence users' security awareness. At the end of the study, a Hungarian-language awareness raising application plan, the so-called 'You are Target', is presented as a recommendation. The content and structure of the application rely on the latest scientific results as well as the experience of existing applications and may be appropriate for raising the awareness of a wide segment of society in an experiential manner.

Journal of Economic Literature (JEL) codes: I250, O31, Y8

Keywords: information security, IT security, information security awareness, gamification, application

Bevezetés

A kibertámadások az elmúlt években egyre összetettebbé, kifinomultabbá és kiszámíthatatlanabbá váltak, melyek jelentős fenyegetést jelentenek a digitális technológia által átszőtt világunkra. A támadók folyamatosan újabb technikákat alkalmaznak céljaik elérése érdekében. A Trend Micro 2020. évi jelentése[1] is megerősíti a szakemberek által régóta hangsúlyozott tényt, mely szerint továbbra is az emberi hiszékenységre és együttműködési képességre épülő social engineering típusú támadások a legelterjedtebbek.

Aszerint, hogy a támadó milyen módszereket használ, humánalapú és számítógép-alapú technikákat különböztethetünk meg (Muha–Krasznay, 2014:54). A humánalapú technikák alkalmazása a támadó és áldozata között közvetlen kapcsolatot feltételez, ugyanakkor nem igényli feltétlenül informatikai eszközök használatát. Humán módszerek például: segítség kérése; segítség nyújtása (fordított social engineering); megszemélyesítés, vagyis az identitás lopás; thumbstone theft, azaz a „sírkő lopás", mely a megszemélyesítés egy speciális fajtája. További technikák például a shoulder surfing (képernyő lelesése); az irodai hulladék átvizsgálása, azaz a dumpster diving; tailgating, vagyis a szoros követés módszere a bejáraton történő bejutáshoz; illetve piggybackin, azaz, amikor a támadó az áldozat segítségével és tudtával jut át a bejáraton (Deák, 2017a; Bányász, 2018).

A számítógép-alapú technikák esetében a kapcsolat közvetett, a támadó valamilyen informatikai eszközön keresztül lép kapcsolatba az áldozattal. Számítógép-alapú támadások például: adathalászat – phishing; kártékony programok (például trójai programok, veszélyes csatolmányok, billentyűzetnaplózás); Wi-Fi hálózaton keresztül kivitelezett támadások; okostelefon alkalmazások általi hozzáférés – alkalmazásengedélyekből eredő kockázatok (Deák, 2017b; Bányász, 2018).

A kibertámadásokra vonatkozó nemzetközi statisztikák is megerősítik a social engineering típusú támadások népszerűségét és eredményességét. Az Interpol 2020. augusztus 4-én megjelent, az év első négy hónapját vizsgáló jelentése kifejezetten az adathalászat, a malware-ek (rosszindulatú alkalmazások), a rosszindulatú domainek (tartomány nevek), valamint az álhírek számának növekedésére figyelmeztet, mely támadások közös jellemzője, hogy minden esetben a sikerességhez nélkülözhetetlen a felhasználó aktív közreműködése.

A támadások sikeressége nem csak az igénybe vett logikai és fizikai védelmi intézkedésektől függ, hanem nagy mértékben a felhasználók biztonságtudatosságától is. Amennyiben ismerik a lehetséges támadási és védekezési alternatívákat, a megfelelő biztonsági követelményeket és eljárásokat, illetve azokat képesek alkalmazni is, akkor a támadások bekövetkezésének valószínűsége is csökkenthető.

A tudományos probléma megfogalmazása

Az Európai Unió és hazánk is az elmúlt években kiemelt figyelmet fordít a biztonságtudatosításra, és tudatosító kampányok sorával, plakátokkal, videókkal igyekeznek felhívni a felhasználók figyelmét a kibertér felől érkező fenyegetésekre. Minden erőfeszítés ellenére, az Európai Bizottság által 2020. júniusban nyilvánosságra hozott, a digitális gazdaság és társadalom fejlettségét mérő mutató, a Digital Economy and Society Index (DESI) alapján Magyarország a 28 uniós tagállam között a 21. helyen áll.[2] A humán tőkét illetően a DESI megállapítja, hogy a lakosság több mint fele nem rendelkezik alapvető digitális, és a szoftverek használatához szükséges készségekkel, mely nem csak hazánkban jelent kihívást a kormányzat számára, mivel az EU lakosságának közel felénél még mindig hiányoznak az alapvető digitális ismeretek, és így a szükséges információbiztonsági tudatosság is. A 2020-ban elfogadott Nemzeti Biztonsági Stratégia is kiemeli, hogy általános jelenség „a felhasználók információbiztonsági tudatosságának alacsony szintje, holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme."[3] Az elektronikus információs rendszerek biztonságát a jogalkotók jogszabályokkal igyekeznek garantálni, azonban jelenleg nem léteznek olyan tartalmi és módszertani ajánlások, tudatosítási megoldások, amelyek érdemileg biztosítanák az áttörést az átlagfelhasználók biztonságtudatosságának növelésében.

A kutatás célkitűzései

A tanulmány célja, hogy a bevezetést követően bemutassa az információbiztonság-tudatosság és tudatosítás fogalmának koncepcionális kereteit, rámutatva arra, hogy tartalmuk különféleképpen értelmezhető más-más aspektusokból, és azok tovább gazdagíthatók, bővíthetők újabb tudományos eredményekkel. Az írás külön kitér a biztonságtudatosság magyarországi helyzetére, jogszabályi vonatkozásaira, valamint röviden bemutatja a tudatosításban kiemelkedő szerepet betöltő Nemzeti Kibervédelmi Intézet tevékenységét. A tanulmány vizsgálja a gamifikáció, valamint a gamifikált applikációk szerepét a biztonságtudatosításban, valamint esettanulmány segítségével elemzi az egyetlen magyar nyelvű, hazai fejlesztésű alkalmazás működési tapasztalatait. A kutatás eredményei alapján végezetül ajánlásként megfogalmazásra kerül a „Célpont vagy" applikáció terve. Az alkalmazás bemutatásával a szerző egy olyan játék fejlesztésére tesz javaslatot, amely a legfrissebb tudományos eredményekre támaszkodik és tartalmazza a legújabb kibertámadás típusokhoz kapcsolódó ismereteket is. Az applikáció célja, hogy minél szélesebb körben megismertesse az elektronikus információbiztonság alapjait, a potenciális, kockázatot jelentő kiberfenyegetéseket, valamint a megelőzéshez, a védekezéshez és a kockázatok kezeléséhez szükséges ismereteket.

Kutatási hipotézisek

A kutatás céljainak megvalósításához az alábbi kérdések részletes vizsgálata és megválaszolása szükséges.

H1. Egy gamifikált applikáció képes biztosítani a hatékony tudástranszfert és a megszerzett tudás magabiztos alkalmazását, ezáltal pozitív irányban befolyásolja a felhasználók biztonságtudatosságát.

H2. Az egyetlen magyar nyelvű, hazai fejlesztésű biztonságtudatosító applikáció hatékonyan növeli a célcsoport biztonságtudatosságát.

H3. A biztonságtudatosság fejlesztéséhez szükséges, hogy az applikáció tartalmilag az általános elektronikus információbiztonsági és informatikai ismeretek átadására, a kapcsolódó készségek kialakítására, valamint a megfelelő eszközhasználat biztosítására koncentráljon.

H4. A tudatosság naprakészen tartásához szükséges, hogy az applikáció nyomon kövesse és folyamatosan hírt adjon a legfrissebb, kiberbiztonságot érintő kérdésekről.

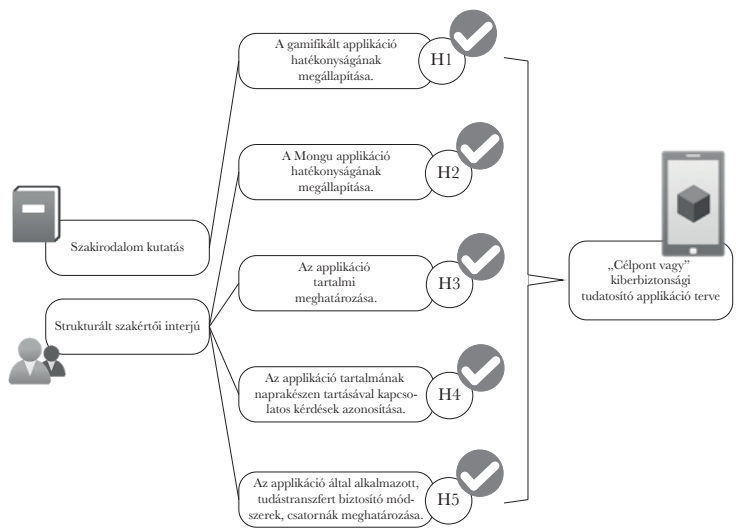
H5. Az applikáció által alkalmazott, tudástranszfert biztosító módszerek, csatornák változatos alkalmazása pozitív irányban befolyásolja a felhasználók biztonságtudatosságát.

Kutatási módszertan

A kutatás szekunder és primer vizsgálatokra épül. A szekunder kutatás széleskörű nemzetközi és hazai irodalomkutatásra, illetve a hazai jogszabályok, a nemzetközi ajánlások, valamint a kibertér felől érkező fenyegetésekkel, támadásokkal kapcsolatos statisztikák vizsgálatára, elemzésére és rendszerezésére támaszkodik. A szekunder kutatás célja egy konzisztens fogalomkészlet létrehozása az információbiztonság-tudatosság, a biztonságtudatosítás és a gamifikáció fogalmai tekintetében, valamint az első hipotézis megválaszolása.

A primer kutatás során strukturált szakértői interjú segítségével, esettanulmány keretében kerülnek elemzésre a Mongu for Teen magyar nyelvű, hazai fejlesztésű biztonságtudatosító applikáció működési tapasztalatai és eredményei. A szakértői interjú célja a H2-H5 hipotézisek megválaszolása, továbbá a H2 hipotézis igazolásával a H1 hipotézis validálása, majd a vizsgálat eredményei alapján egy a szerző által megtervezett, tudományos alapokon nyugvó applikáció tervének felvázolása.

1. ábra: A hipotézisek bizonyításának módszerei



Forrás: a szerző szerkesztése

Információbiztonság-tudatosság (information security awareness)

Az információbiztonság-tudatosságnak (information security awareness) nincs egy általánosan elfogadott fogalma, annak összetevőit több magyar és nemzetközi kutatás is megkísérelte meghatározni (Legárd, 2020:95), Veseli (Veseli, 2011), Chen és társai (Chen et al.,2009). Aldawood és Skinner (Aldawood et al., 2018; 2019:73) a fogalom egyéni aspektusait hangsúlyozzák, míg Nemeslaki és Sasvári (Nemeslaki–Sasvári, 2014), valamint Bulgurcu és társai (Bulgurcu et al., 2010) annak szervezeti vonatkozásait emelik ki.

Összességében az információbiztonság-tudatosság fogalmát úgy lehetne összefoglalni, mint amely a tudás, a képességek és a viselkedés olyan hármasa, amely biztosítja az egyén számára a megfelelő szintű informatikai és információbiztonsági ismereteket, az ezekre épülő és alkalmazásukat biztosító képességeket, valamint e két elemnek megfelelő, belső igényként megjelenő, az információbiztonság jelentőségét elismerő viselkedést (Legárd, 2020:95). Ugyanakkor az információbiztonság-tudatosság a szervezet kultúrájának része, olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a szervezetek alkalmazottai elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják azokat, és másokkal is megismertetik, illetve betartatják (Nemeslaki–Sasvári, 2014:169).

A biztonságtudatosság helyzete Magyarországon

A kiberbiztonságra vonatkozó magyarországi dokumentumokban, szabályozásokban kiemelt figyelmet fordítanak a tudatosság és a tudatosítás jelentőségének hangsúlyozására. A 2013-ban elfogadott Nemzeti Kiberbiztonsági Stratégia a kiberbiztonság fogalmi elemeként határozza meg a tudatosságnövelő eszközök folyamatos és tervszerű alkalmazását[4]. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L törvény (továbbiakban Ibtv.) kimondja, hogy az elektronikus információs rendszerek védelme érdekében a szervezet vezetője köteles gondoskodni „az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról”[5]. Magyarország 2020-ban kiadott Nemzeti Biztonsági Stratégiája kiemeli, hogy „elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális kihívások, kockázatok és fenyegetések azonosítása és nyomon követése, a kormányzati koordináció erősítése, a kibertér jogi szabályozásának fejlesztése, a felhasználók biztonságtudatos viselkedésének elősegítése (…)”.[6]

A 2015. október 1-jén alakult, Nemzetbiztonsági Szakszolgálat irányítása alatt működő Nemzeti Kibervédelmi Intézetnek (továbbiakban: NKI) kiemelkedő szerepe van az információbiztonság-tudatosság növelésében. Tevékenysége számos réteget céloz: a döntéshozókat (szervezeti vezetőket, akik a rendszerek védelméért felelősek), az üzemeltetőket (akik ellátják a rendszerek működtetését) és a felhasználókat, akiket pedig meg kell tanítani az internet és az információs technológiák biztonságos használatára, a saját és a rájuk bízott adatok felelős és szakszerű kezelésére. Az NKI szakmai anyagokat és útmutatókat tesz közzé, oktatási vagy képzési tevékenységet folytat, valamint a médiában megjelenő tudatosítási kampányokkal segíti a cél elérését.[7]

Biztonságtudatosítás

A megfelelő biztonságtudatosság kialakításához számos út vezethet, módszerek és technikák széles választéka áll rendelkezésre.

Az Aldawood és Skinner által alkalmazott kategorizálás alapján megkülönböztethetjük a hagyományos és a modern módszereket (Aldawood et al., 2019:7-8). Az előbbihez olyan eszközök tartoznak, mint a belső vagy külső képzések, tréningek, poszterek, emlékeztetők és az online kurzusok. Meglátásuk szerint a hagyományos tréningek eszköztára általában unalmas, fárasztó, nem tartják fenn a figyel-

met, túl általánosak, formálisak és a tartalmat túl komoly környezetben közvetítik, valamint a módszerek egyáltalán nem alkalmazkodnak a résztvevők egyéni tanulási képességeihez. Ezek a tréningek egyszerűen csak elmondják a tudnivalókat a támadásokról, ugyanakkor nem mutatnak be valódi, megtörtént eseteket és nem adnak praktikus tanácsokat, hogy hogyan ismerjenek fel, illetve kezeljenek a résztvevők egy ilyen támadást. Ezzel szemben a modern módszerek, mint a szimulációs technikák, interaktív játékok, virtuális laboratóriumok, valamint tematikus videók és modulok, kreatív, gyakorlatias megközelítést alkalmaznak, élményszerű tanulás segítségével mutatják be a social engineering típusú támadásokat, valamint a megelőzésükhöz és kezelésükhöz szükséges intézkedéseket.

Parsons és társai vizsgálata megerősíti azoknak a módszereknek a hatékonyságát, amelyek a napi rutinhoz, feladatokhoz kapcsolódó ismereteket, közérthetően és szemléltetve közvetítenek a felhasználók felé, mivel szerintük csak így biztosítható a mindennapi munkát támogató, jól hasznosítható tudás megszerzése, és a megfelelő motiváció az ismeretek alkalmazására (Parsons et al., 2010). A tréningeknek helyzetorientáltnak, gyakorlatiasnak kell lenniük, valamint esettanulmányokat kell alkalmazni annak érdekében, hogy a felhasználók megértsék az információbiztonság jelentőségét (Parsons et al., 2014).

Pattinson és társai a forgatókönyvalapú szerepjáték tudatosításban betöltött hatékony szerepét hangsúlyozták, adathalász e-mailek felismerésében végzett vizsgálatuk során (Pattinson et al., 2012).

Szász Antónia és Kiss Gábor jelszó-visszafejtő programok oktatási célú felhasználásával kapcsolatos mérése szintén bebizonyította, hogy a programhasználattal kiegészített, interaktív tevékenykedést támogató módszernek nagyobb hatása volt a hallgatók információbiztonsági attitűdjére, gyakorlatára és tudatosságára, mint a csak videóval támogatott módszernek (Szász–Kiss., 2018).

Gamifikációs applikációk alkalmazása a biztonságtudatosság növelésére

A gamifikáció alapjai azon az elven nyugszanak, hogy az ember alapvető természetéhez hozzátartozik a „játékos én" is, így a játék segít az információk megszerzésében, feldolgozásában és továbbításában (Pacsi–Szabó, 2017:59). Ugyanakkor a játékosítás nem pusztán a játékok alkalmazását jelenti, hanem a játékmechanizmusok beépítését a hétköznapok gyakorlatába, a munkahelyi folyamatokba vagy az oktatásba. A gamifikációs technikák alapvetően a belső motivációs mechanizmusra hatnak, és azt aktiválják az újdonságokkal, az ismeretlen területek felfedezésével, a kihívásokat jelentő izgalmas kalandokkal és az ún. flow élmény biztosításával, amikor az öröm forrása és így a motivációs eszköz nem más, mint a játék élménye, vagyis maga a tevékenység (Fromann–Damsa, 2016:77).

A gamifikáció meghatározására több tanulmány is kísérletet tett, azonban a legelfogadottabb definíció szerint a „játékosítás" nem más, mint a játékok és játékelemek alkalmazása az élet játékon kívüli területein, célja pedig, hogy az ott zajló folyamatokat érdekesebbé és eredményesebbé tegye (Fromann–Damsa, 2016; Deterding et al., 2011; Domínguez et al., 2013).

A játékosítás egyre szélesebb körben terjed és kiválóan alkalmazható számos területen, mint például az oktatás is (Kovács–Várallyai, 2018; Fromann–Damsa, 2016; Pacsi–Szabó, 2017). Ez utóbbi körben végzett vizsgálatok egy része kifejezetten a gamifikált applikációk biztonságtudatosításban betöltött szerepét vizsgálja.

Scholefield és Shepherd egy jelszóhasználati tudatosság növelését célzó szerepjáték kvíz applikációt fejlesztettek ki és mérték annak hatékonyságát. Vizsgálatuk megállapította, hogy a résztvevők nagyon élvezték az applikáció használatát és a segítségével történő tanulást. Az alkalmazás használata folytán a jelszavak biztonságával kapcsolatos tudás is jelentős fejlődést mutatott (Scholefield–Shepherd, 2019).

Volkamer és társai 2014-ben létrehoztak egy Android alapú interaktív játékot, az úgyneve-

zett NoPhish applikációt, melynek célja, hogy az adathalász oldalakat az átlagfelhasználók könnyebben tudják azonosítani. Az elvégzett mérések alapján elmondható, hogy az applikációt használók sikeresebben detektálták az adathalász weboldalakat és tudásuk hosszú távon is tartósnak bizonyult (Canova–Volkamer et al., 2014; Canova–Volkamer et al., 2015). 2016-ban a tapasztalatok alapján tovább fejlesztették az applikációt, és pre-, illetve poszttesztttel mérték annak hatékonyságát. A vizsgálat megállapította, hogy a résztvevők a játék használatát követően hatékonyabban felismerték az adathalász weboldalakat, növekedett a felhasználók biztonságtudatossága, tehát az applikáció elérte a kitűzött célt (Kunz et al, 2016).

Idegen nyelven, jellemzően angolul, számos applikációt találhatunk, amely a biztonságtudatosság egy-egy specifikus területére fókuszál. A Trend Micro által kifejlesztett „Targeted Attack: The Game" applikáció[8] segítségével informatikai igazgatóként hozhatunk döntéseket arról, hogy hogyan védjük meg érzékeny adatainkat, a „Cybersecurity Lab" játékban[9] pedig egy közösségi hálózatot létrehozó vállalat kiberbiztonsági felelőseként kell megerősíteni a védekezést és kivédeni a növekvő számú, szofisztikált támadásokat. A „Keep Tradition Secure" applikációban[10] egy „Bad Bull" elnevezésű hacker által, a Texas A&M's egyetemi hagyományait veszélyeztető fenyegetéseit kell felderíteni komoly kiberbiztonságot érintő kérdések megválaszolásával. A „Zero Threat" app[11] olyan kockázatokat szimulál a játékosok számára, mint az adathalász e-mailek, social engineering támadások, káros weboldalak és fertőzött USB-k. A „Game of Threats"[12] a PWC (PricewaterhouseCoopers) által kifejlesztett szimulációs játék, mely a támadó vagy a szervezet védekezésért felelős személye bőrébe bújva segít megtapasztalni azokat a legfontosabb döntési helyzeteket, amelyekre fel kell készülnünk egy kibertámadás során.

A nemzetközi szakirodalom és a vizsgált alkalmazások alapján megállapítható, hogy a gamifikációnak helye van a biztonságtudatosításban, és egy megfelelő modulokkal ellátott játékosított applikáció hatékonyan növelheti a felhasználók tudatosságát.

Esettanulmány – A Mongu for Teen applikáció

A Mongu for Teen az egyetlen hazai fejlesztésű, magyar nyelvű alkalmazás, amely egyedülálló megoldást nyújt a 9-13 éves korosztály számára mobileszközük és a közösségi média megfelelő és biztonságos használatához.[13] Az alkalmazás segít a gyermekeknek, hogy felismerjék a közösségi médiában rejlő veszélyeket, és képesek legyenek azokat kikerülni.

A korosztály kiválasztása elsősorban azon az elgondoláson alapult, hogy a 9-13 évesek ebben az időszakban kezdik el használni a közösségi médiát, de még nyitottak a felnőttektől érkező útmutatásra. 15-16 évesen már inkább a leválás történik, így ott már nagyon nehéz rájuk hatni. A gyerekek online védelme érdekében ugyan számos szülői felügyeleti megoldást fejlesztettek ki a kiberbiztonsággal foglalkozó cégek, azonban ezek elsősorban a korlátozásra építenek, illetve adatokat gyűjtenek a gyermek mobilhasználatáról, amiket mi szülők „kielemezhetünk". Az alkalmazás megálmodója és fejlesztője, dr. Dóra László, valamint a fejlesztő csapatban részt vevő szakértők, szülőként, a folyamatos ellenőrzés és korlátozás helyett egy olyan tudatosító módszer fejlesztésében gondolkodtak, amely a gyermekek megfelelő eszköz, és biztonságos internet használatát biztosítja. Így jött létre, a jelenleg még csak iOS operációs rendszer számára elérhető Mongu for teen alkalmazás.

A Mongu a szülők számára szülői, a gyermekek számára pedig gyerek nézetet biztosít, egy applikációhoz több gyermek profilját is hozzá lehet adni. A szülők az egyes gyermekeik profilja alatt nyomon követhetik, hogy milyen alkalmazásaik vannak, illetve milyen oktató feladatokat oldhatnak meg az egyes alkalmazásokhoz kapcsolódóan. Azt is láthatják a szülői nézetben, hogy gyermekeik milyen feladatokat, milyen eredménnyel végeztek el (pl.: maximális ponttal, vagy sem). Amennyiben a gyerekek egy ideje nem használják a Mongut, erről is értesí-

tést kapnak a szülők.

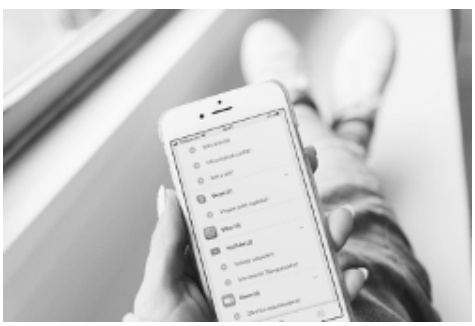
A Mongu alapkoncepciója, hogy olyan alkalmazásokkal kapcsolatban nyújtson technikai és informatív segítséget a gyerekeknek, amelyeket ők maguk valóban használnak, így az ezekkel kapcsolatos tudás ténylegesen releváns és hasznos számukra. Az alkalmazás a telepítést követően felméri az eszköz által használt applikációkat, így az egyes tudatosítási modulok kizárólag ezen appok esetében jelennek meg a telefonon. A fejlesztő a tananyagokat előzetesen priorizálta, így a telefon által használt applikációk és a priorizált ismeretek kombinációjából alakul ki a Mongu által javasolt tudatosító feladatok sorrendje.

Az átadandó ismeretek között számos olyan terület van (pl. jelszókezelés), amely szinte minden alkalmazás használatához szorosan kapcsolódik. Természetesen ezeket a területeket is érintik a tudatosító anyagok, azonban a fejlesztő elsősorban arra törekszik, hogy az általuk kínált megoldások alkalmazás-specifikusak legyenek, az ismeretekben ne legyen ismétlés, hanem mindig a való élethez igazodó, kézzelfogható és releváns tudással gazdagodjanak a gyerekek. Például a posztolás is általános kérdésként merül fel az alkalmazások használata során, mégis a Mongu nem általánosítva közelíti meg a témát, hanem minden egyes applikáció esetében (Facebook, Instagram, Snapchat stb.) kontextusba helyezi azt, és specifikus, gyakorlatias ismereteket igyekszik közvetíteni. A Mongu fejlesztése során kiderült, nem egyszerű feladat ezen ismétlődő, de mégis alkalmazásonként eltérő feltételek szerint működő témáknak a feldolgozása, megfelelő közvetítése a gyerekek felé.

Az egyes alkalmazásokhoz kapcsolódó tananyagot a gyerekek több – jellemzően 4-5 db –, rövid, összefüggő részre osztva kapják meg, játékok formájában. Az egyes részekhez kapcsolódó ismeretek átadására alapvetően kétféle módszert alkalmaznak (videók és párbeszédek), melyre azért van szükség, mert tapasztalataik alapján a tudatosítás során a módszerek megfelelő kombinációja biztosíthatja a hatékony tudástranszfert. A fejlesztő szerint, a videók alkalmazása alkalmas lehet egy kérdés felvetésére, bemutatására (pl. életből vett példa), ugyanakkor a probléma megoldására, kezelésére már nem biztosít megfelelő lehetőséget.

A gyerekek tetszőlegesen tudják kiválasztani

2. ábra: A Mongu applikáció képernyőképe az egyes alkalmazásokhoz kapcsolódó játékokról



Forrás: Mongu for Teen

3. ábra: Mongu for Teen alkalmazás – posztszerűen megjelenő játék

Forrás: Mongu for Teen

az egyes applikációhoz kapcsolódó játékok sorrendjét.

Minden játék két részre tagolódik: az első ún. kaland rész az ismeretek átadását, az oktatást célozza, míg a második részben kihívások teljesítésével mélyíthetik el a gyerekek a megszerzett tudásukat.

A játékok posztszerűen jelennek meg. A játék maga pedig üzenetküldő alkalmazáshoz hasonlóan folyik. A közös, hogy a közösségi média elemeit használják fel.

A kaland rész valamely kérdés felvetésével indul például egy rövid, kb. 40 másodperces videóval, vagy az említett beszélgetéssel. A játék ezen részének célja a tudásátadás, így a gyerekek a kaland során egyre több ismeretet sajátítanak el és folyamatos visszajelzést kapnak az adott témával kapcsolatban.

A játék második részében megjelenő kihívások segítségével a gyerekek tovább mélyíthetik és ellenőrizhetik a kaland rész során elsajátított tudásukat. A kihívások során olyan gyakorlatias feladatokat kell megoldaniuk a gyerekeknek, mint például (a http sütik kapcsán): „Keress rá, hogy néz ki egy http süti!"; „Ezek közül melyek nem http sütik?"; „Hogyan tudsz cookie-t kitörölni?". Mindezt természetesen ki is próbálhatják és az applikáció iránymutatásai alapján saját magukat ellenőrizni is tudják. Amennyiben azonban rosszul válaszolnak az ellenőrző kérdésekre, újra kell kezdeniük az adott feladatot. Számos feladat az egyéni felfedezés örömére épít, így például ahhoz, hogy egy küldetést teljesítsenek, utána kell nézniük az interneten néhány információnak és egyénileg kell a megoldást megtalálniuk. (Ezzel elkerülhető, hogy a gyerekek csak egyszerűen addig kattintgassanak a lehetséges megoldások között, amíg a helyes választ meg nem találják.) Nem véletlen, hogy a fejlesztő tapasztalatai és a visszajelzések alapján a leghatékonyabb tudástranszfert a kihívások képesek biztosítani.

Az adott játék végén motiváló, gratuláló üzenet és digitális jutalom (pl. arany skorpió) fogadja a gyerekeket, illetve lehetőségük van a beszélgetés újraindítására, és a játékok ismétlésére, vagy a kilépésre.

A visszajelzések a „beszélgetés" első felében, a kaland során folyamatosan jelen vannak, hiszen ez a rész az alapvető ismeretek átadására, az oktatásra irányul, így a feltett kérdésekre és válaszokra folyamatosan érkezik reakció és magyarázat. Azonban a játék második, kihívás részében már nem kap a gyermek visszajelzést arról, hogy miért nem jó az adott válasz, annak saját magának kell utánajárnia az internet segítségével. Ennek a módszernek a kétségtelen erőssége az önfelfedezés élménye, ellenben hátránya lehet, hogy esetleg a gyermekek megunják, elveszi a kedvüket, és felhagynak a válaszok keresésével.

Az applikáció kiemelten foglalkozik az általános informatikai ismeretek fejlesztésével is, mivel ha a felhasználók értik, mi, hogyan működik, ennek birtokában képesek megérteni azt is, hogyan tudnak „jól cselekedni" az online térben. Az általános informatikai ismereteket játékos formában, a használt alkalmazásokhoz kapcsolódva továbbítják a gyerekek felé. Például a megfelelő eszközhasználat biztosításához olyan kérdésekről is tanulhatnak, mitől lesz jó egy fénykép az Instán? A hatékony tudatosításban egyébként is kiemelkedő jelentősége van annak, hogy a biztonság kérdését, ne egyfajta „vészmadárként" kommunikáljuk a gyermekek és szüleik felé, sokkal hatékonyabb és motiválóbb, ha az érdekességeket is kiemeljük és hozzákapcsoljuk az adott témához. Ezzel elérhetjük, hogy „akit esetleg annyira nem érdekel a biztonság, az is azt érezze, hogy kap valamit"!

A fenti tapasztalatokból kiindulva, elkerülendő, hogy folyamatosan negatív hírekkel terheljék a felhasználókat, a legfrissebb, kiberbiztonságot érintő kérdésekről az applikáció jelenleg nem küld értesítéseket a szülőknek, gyerekeknek. A jövőben azonban a nagy nyilvánosságot kapott, széles körben terjedő, gyermekeket érintő esetekről (pl. Kék bálna, Momo) szeretnének egy riasztórendszer részeként értesítéseket küldeni, de kizárólag csak ezekről az esetekről. Fontos szempont maradna továbbra is, hogy „a biztonság ne csak a negatív hírekről szóljon".

Az applikáció nem tartalmaz kifejezett teszt-

rendszert a tudatossági szint változása mérésére, ugyanakkor objektív visszajelzési pontok a sikeresen elvégzett modulok és a megszerzett pontok száma. Jelenleg az applikáció által alkalmazott ellenőrző kérdések, melyek megválaszolásához önálló munkára, utánajárásra van szükség, csak a gyerekek számára biztosítanak visszajelzést, „önbevalláson" alapulnak. Későbbi fejlesztési cél például az ellenőrzési lehetőségek bővítése. Ugyanakkor meg kell jegyezni, hogy alapesetben is, de egy applikáció esetében kifejezetten nehéz kérdés annak megválaszolása, hogy hogyan lehetne a tudatossági szint változását mérni.

A fejlesztő hangsúlyozza, hogy az applikáció jelenleg is fejlesztés alatt áll, elsősorban a játékélményt, valamint a párbeszédek átalakítása segítségével az ismeretek átadását szeretnék javítani.

Következtetések

Összességében elmondható, hogy a 9-13 éves korosztály tekintetében a Mongu applikáció jelentősen hozzájárul mobileszközük és a közösségi média megfelelő és biztonságos használatához, mellyel bizonyítást nyert a H2 hipotézis.

Az esettanulmány alátámasztja és validálja a nemzetközi kutatások által megfogalmazott eredményeket, melyek szerint egy gamifikált applikáció képes biztosítani a hatékony tudástranszfert és a megszerzett tudás magabiztos alkalmazását, ezáltal pozitív irányban befolyásolja a felhasználók biztonságtudatosságát (H1 hipotézis). Ugyanakkor Dr. Dóra László hangsúlyozza, hogy „bár egy gamifikált applikáció mindenképpen hozzátesz a biztonságtudatossági szint növekedéséhez", azonban tapasztalatai szerint „a megfelelő tudatosság kialakítását kizárólagosan egy applikáció nem tudja biztosítani. Elsősorban a gyerekeknél igaz az, hogy egy alkalmazás képes informatív tudást átadni, azonban az igazi alapokat, a valós biztonságérzetet, a pszichológiai eredetű veszélyekre való reagálás képességét a biztonságos háttér, egy közösségnek (család, barátok) a biztonsága tudják megadni. Általában azok reagálnak rosszul, ahol ez a biztonságos környezet nem biztosított. Nagyon sok mindent meg lehet tanulni egy applikáció segítségével, ha rendkívül tudatos az illető, technikailag védeni is tudja magát, de ez nem helyettesíti a pszichológiai támogatást. A támadható emberekből pont az a fajta stabilitás hiányzik, amely alapján támadható." Így összességében bár a H1 hipotézis helyesnek bizonyult, a biztonságtudatosítás tervezése során nem szabad elfeledkezni a tudatosítás egyéb módszereiről és a biztonságtudatos környezet kialakításáról, legyen az a család, vagy egy szervezet biztonságtudatos kultúrája.

A H3 hipotézis az esettanulmány alapján igaznak mondható, tehát nagyon fontos tényező a biztonságtudatosság fejlesztése szempontjából, hogy az applikáció ne csak elektronikus információbiztonsági ismereteket, hanem általános informatikai, valamint a megfelelő eszközhasználatot biztosító tudást is közvetítsen a felhasználók felé. A fejlesztő hangsúlyozza, hogy az alkalmazásnak „a megcélzott személyek számára releváns, gyakorlatias és legfőképpen az őt érdeklő, valódi problémákra választ nyújtó tudást kell nyújtani" annak érdekében, hogy a felhasználó valóban hasznosnak érezze az applikáció használatát.

A H4 hipotézis a vizsgálat alapján csak részben bizonyult helyesnek. A legfrissebb, kiberbiztonságot érintő kérdésekről történő tájékoztatás egyúttal azt is jelenti – a kibertámadások nagy számára tekintettel –, hogy folyamatosan negatív, olykor félelmet keltő híreket kommunikálunk a felhasználók felé. Dóra László szerint kiemelkedő jelentősége van annak, hogy a biztonság kérdését, ne egyfajta „vészmadárként" kommunikáljuk, sokkal hatékonyabb és motiválóbb, ha az érdekességeket is kiemeljük és hozzákapcsoljuk az adott témához.

A H5 hipotézis megerősítést nyert az interjú során. A Mongu applikáció tapasztalatai szerint a tudatosítás során a módszerek megfelelő kombinációja biztosíthatja a hatékony tudástranszfert, tehát az ismeretek átadását biztosító módszerek, csatornák változatos alkalmazása szükséges a biztonságtudatosság pozitív irányú befolyásolásához.

A fejlesztő véleménye szerint, az alkalmazás sikeressége és eredményessége szempontjából a gamifikáció maga másodlagos tényező, önmagában kevés, „csak egy picit tud hozzátenni" a hatékony tudatosítás biztosításához. Természetesen motiváló erővel bírnak a játék során megszerezhető pontszámok, digitális jutalmak, díjak, ezek számszerűsíthető visszajelzést is nyújtanak arról, hogyan halad előre a felhasználó. Azonban az egész alkalmazás csak akkor lesz működőképes és eredményes, csak akkor éri el a célját, ha a célcsoport számára releváns, gyakorlatias tudást olyan formában nyújtja, hogy a felhasználó az applikáció használata közben élvezi, amit csinál, ezért magával ragadja a használata.

„Célpont vagy" – kiberbiztonsági applikáció

A hipotézisek vizsgálata során bizonyítást nyert, hogy egy gamifikált applikáció alkalmas az átlagfelhasználók biztonságtudatosságának pozitív irányba történő befolyásolására. Dóra az interjúban kiemelte, hogy egy applikáció technikailag is megfelelő lehet a szélesebb körű biztonságtudatosítás megvalósítására, mivel telefonra letöltve gyakorlatilag olyan mintha az alkalmazás „beköltözne a lakásunkba", azáltal, hogy folyamatosan mutatja a jelenlétét, üzeneteket küld a feladatokról, emlékeztet az előttünk álló „kalandokra", így sokkal inkább képes szem előtt tartani és elérni a használatát.

Dóra szerint a felnőttek tudatosítása egyébként is nehezebb feladat, mint a gyerekek esetében. A gyermekek még rugalmasabbak, sokkal nyitottabbak az új irányába. A felnőttek jellemzően azt a tudást mélyítik el, ami felé már amúgy is nyitottak, így sokkal nehezebb azokat edukálni, akik a leginkább „rászorulnának". Éppen ezért e csoportot megszólítani és egy önkéntes alapon működő applikáció használatára ösztönözni őket nagyobb kihívás, mint akik érdeklődők az online biztonság iránt.

Ahhoz, hogy a felnőtt lakosság körében szignifikáns javulás legyen kimutatható a biztonságtudatosság terén, egy, a társadalom széles körét – az internetező átlagfelhasználókat – érintő kérdésekre választ nyújtó, gyakorlatias, a mindennapi internethasználatot segítő tudást közvetítő és bárki számára könnyen hozzáférhető applikáció komoly támogatást jelenthet.

4. ábra: „Célpont vagy" applikáció tudatosítási területei

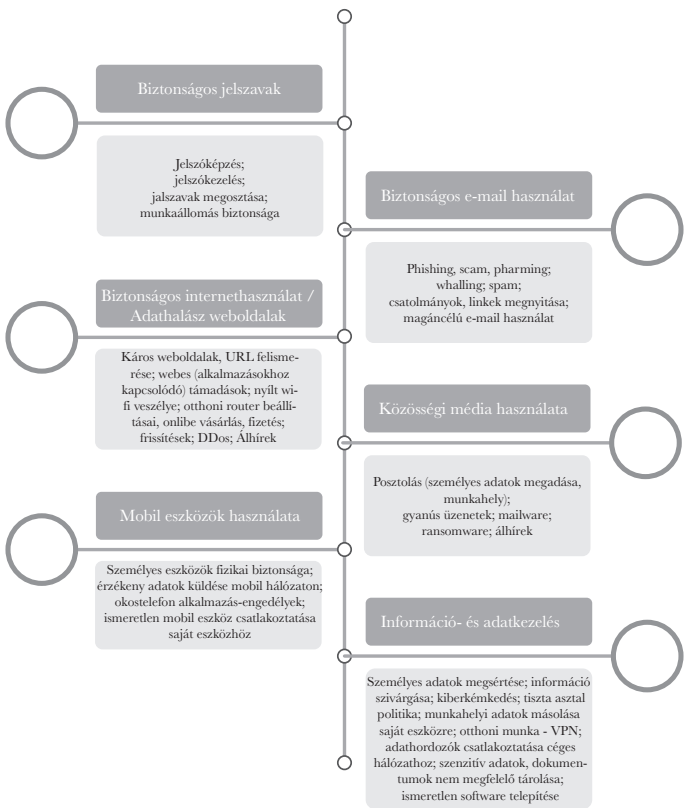
Forrás: a szerző szerkesztése

A tanulmány ezen része bemutatja a „Célpont vagy" tudatosságnövelő applikáció tervét, mely egy olyan magyar nyelvű, tudományos alapokon nyugvó kezdeményezés, melynek segítségével a résztvevők játékos módon ismerkedhetnek meg az elektronikus információbiztonság, valamint a biztonságos internet- és eszközhasználat alapjaival, illetve sajátíthatják el a kibertámadások megelőzéshez és a védekezéshez szükséges legfontosabb ismereteket. Az applikáció célja az átlagfelhasználók bevonása egy fejlesztési programba, mely képes biztosítani a hatékony tudástranszfert és a megszerzett tudás magabiztos alkalmazását. Mivel a megcélzott felhasználói réteg teljes körű bevonása és azonos szintű képzése nem egyszerű feladat, indokolt egy olyan platform létrehozása, mely egységes szempontrendszer alapján biztosítja a szükséges ismereteket és a lehető legegyszerűbb módon elérhető minden felhasználó számára.

A felvázolt applikáció alkalmas lehet arra, hogy össztársadalmi szinten járuljon hozzá az állampolgárok biztosságtudatosságának növeléséhez, akár egy ingyenesen, például a magyarorszag.hu-n keresztül biztosított eléréssel, ezáltal gondoskodva az elektronikus közigazgatás vívmányainak biztonságos és magabiztos használatáról.

Az applikáció az elmúlt évek nemzetközi és hazai szakirodalma, a legjobb gyakorlatok (best practice), valamint a nemzetközi statisztikákban megjelenő legújabb támadás típusok alapján, hat különböző, a mindennapi használat során gyakori kérdéseket felvető területre koncentrál,

5. ábra: Az egyes tématerületek által érintett részkérdések



Forrás: a szerző szerkesztése

melyek a 4. ábrán láthatók.

A hat terület, hat önálló küldetés formájában jelenik meg az alkalmazásban. A játékos egy titkos ügynök, akinek egy számítógépbe rejtett bombát kell hatástalanítania. A hatástalanításhoz egy 6 jegyű kódra van szükség. A kód egyes elemeinek megszerzéséhez teljesíteni kell mind a hat küldetést, melynek jutalma a felfedett egy-egy kódrészlet. Ha a játékos megszerzi mind a hat kódrészletet, hatástalaníthatja a bombát és oklevelet kap a kiváló teljesítményéért.

Minden egyes modul, azaz küldetés azonos felépítésű. A küldetések megkezdésekor, az adott témát érintő rövid ismertetésre, videó vagy animáció megtekintésére kerül sor, majd egyenként érkeznek a feleletválasztós kérdések. Néhány kivételes esetben azonban a feleletválasztós kérdés helyett komplexebb feladat megoldására kerül sor: például adathalász levelek, vagy weboldalak felismerése céljából a játékos két képet kell, hogy összehasonlítson, megtalálja a hibákat, majd megjelölje, hogy mely levél, vagy URL céloz adathalász tevékenységet. Az egyes kérdések megválaszolását követően minden esetben információk, magyarázatok, további segítségek jelennek meg a témához kapcsolódóan, melynek elolvasását egy „OK"-kal szükséges igazolni. Hibás válasz esetén a kérdés újra megválaszolására van lehetőség. Helyes válaszok esetén minden esetben azonnali pozitív visszajelzés történik (pl. Jól csináltad!, Szép munka volt!), a küldetések teljesítését követően a kódrészleten kívül egy serleget is megszerez a játékos. A megszerzett serlegek száma egyenlő a teljesített küldetések számával. A modulok végén rövid áttekintés jelenik meg arról, hogy mit tanultunk az adott küldetés során.

Az egyes küldetések a 5. ábra szerinti részkérdéseket dolgozzák fel játékos formában (a teljesség igénye nélkül)[14].

A küldetések sorrendje tetszőlegesen választható, azonban az adott küldetés csak az összes kérdés helyes megválaszolása esetén teljesített, így a hiányzó kódrészlet csak ebben az esetben szerezhető meg.

A játékosnak öt élete van, minden egyes rossz válaszért elveszít egyet. Ugyanakkor az egyes küldetések végén lehetőség van extra nehézségű, bónusz feladatért járó további élet megszerzésére, küldetésenként egyre. Azonban, ha a játék során elfogynak az életek, a játéknak vége.

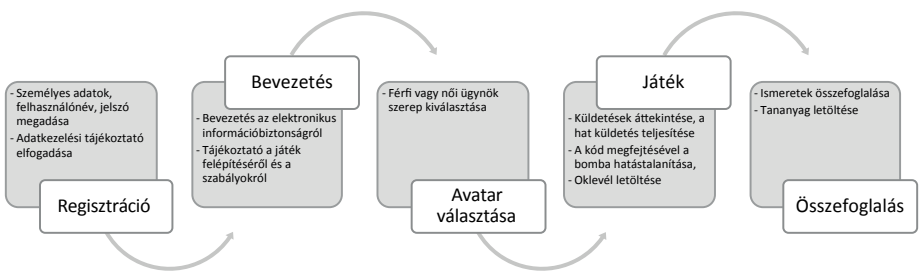
A küldetések teljesítésére időkorlát nélkül van lehetőség. Amennyiben a játék megszakítására kerül sor, az automatikusan menti a teljesített feladatokat és újabb belépés esetén, tovább folytatható a játék az előző állapotról.

A játék végén röviden bemutatásra kerülnek a küldetések során elsajátított legfontosabb ismeretek, valamint lehetőség nyílik egy összefoglaló tananyag letöltésére is.

Összegzés

Magyarországon az elektronikus információbiztonsági tudatosítás különböző formáira számos piaci cég kínál változatos lehetőségeket. A hagyományos tréningek, képzések, online és

6. ábra: Áttekintő ábra a „Célpont vagy" alkalmazás szerkezeti felépítéséről



Forrás: a szerző szerkesztése

blended learning kurzusok mellett már találkozhatunk a tudatosítás modern formáival is, mint a szimulációs technikák, szabadulószoba, vagy tematikus videók alkalmazása, valamint a Nemzeti Közszolgálati Egyetem által üzemeltett Probono felületen létrehozott, „IT Biztonság Angyalai" elnevezésű önfejlesztő csatorna. Ez utóbbi a közösségi oldalak „hírfolyamához" hasonlóan működő felület, melyen a feliratkozók kommentelhetnek, vagy like-olhatják a megjelent cikkeket, blogokat, és szabadon kérdezhetnek a csatorna szerzőitől. A gamifikált applikációk használata ugyanakkor még nem terjedt el hazánkban, magyar nyelvű applikációként csupán a tanulmányban bemutatott Mongu for Teen-nel lehet találkozni.

Az elmúlt években bár egyre többet hallani a tudatos online jelentlétről, és előremutató tudatosító tevékenység indult el mind a privát, mind pedig a közszférában, számottevő áttörést nem sikerült elérni a felhasználók biztonságtudatosságának növelésében. A kibertámadások elkövetői és az átlagfelhasználók tudása között egyre nagyobb hézag jelentkezett, az internethasználók nagyobb százaléka sajnos nem tart lépést a digitális világ felől érkező fenyegetésekkel, ezért egyre nagyobb igény jelentkezik a társadalom jelentős részét átfogó tudatosításra. A Mongu for Teen applikáció működési tapasztalatait bemutató esettanulmány is megerősíti a gamifikált applikációk hatékonyságát a biztonságtudatosítás területén, azonban az interjúból az is kiderült, hogy megfelelő, tartalmilag a felhasználók számára hasznos és élményszerű tanulást nyújtó alkalmazást fejleszteni nem egyszerű folyamat.

A kutatási kérdések megválaszolását követően, az interjú tapasztalatait felhasználva, valamint az írásban bemutatott, az elmúlt évek biztonságtudatosságot, illetve tudatosítást érintő hazai és nemzetközi vizsgálatok eredményeire, a gamifikációs kutatások megállapításaira támaszkodva ajánlásként megfogalmazásra kerül egy magyar nyelvű tudatosító applikáció terve, mely alkalmas lehet a biztonságtudatosság társadalom szintű növelésére. A „Célpont vagy" applikáció segítségével a társadalom széles köréhez eljuttathatók a legfontosabb elektronikus információsbiztonsági ismeretek játékos és élményszerű formában.

Jegyzetek

1 Securing the Pandemic-Disrupted Workplace - Trend Micro 2020 Midyear Cybersecurity Report https://documents.trendmicro.com/assets/rpt/rpt-securing-the-pandemic-disrupted-workplace.pdf (Letöltve: 2020. október 31.)

2 https://ec.europa.eu/digital-single-market/en/human-capital (Letöltve: 2020. 12. 29.)

3 A Kormány 1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, 32. pont

4 Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat

5 Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L törvény 11. § (1)

6 A Kormány 1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, 159. pont

7 https://nki.gov.hu/intezet/tartalom/szolgaltatasok/ (Letöltve: 2020. 10.31.)

8 http://targetedattacks.trendmicro.com/ (Letöltve: 2020.11.03.)

9 https://www.pbs.org/wgbh/nova/labs/lab/cyber/ (Letöltve: 2020.11.03.)

10 https://keeptraditionsecure.tamu.edu/ (Letöltve: 2020.11.03.)

11 https://leolearning.com/leo-grc-academy/ (Letöltve: 2020.11.03.)

12 https://www.pwc.co.uk/issues/cyber-security-services/game-of-threats.html (Letöltve: 2020.11.03.)

13 https://monguforteen.com/hu/ (Letöltve: 2020.11.03.)

14 „Célpont vagy" – kiberbiztonsági applikáció tartalmi elemeinek tudományos megalapozottsága:
- Biztonságos jelszavak: Aldawood – Skinner (2018); Aldawood – Skinner (2019); Illéssy et al. (2014); Kruger- Kearney (2006); Nemeslaki – Sasvári (2014); Parsons et al. (2014); Pattinson et al. (2012); Prah et al. (2016); Som – Papp (2016); Stephanou et al. (2008); Szász – Kiss (2018);
- Biztonságos e-mail használat: Aldawood – Skinner (2018); Aldawood – Skinner (2019); Bányász – Krasznay (2019); Deák (2019); Il-

léssy et al. (2014); Kruger – Kearney (2006); Nemeslaki – Sasvári (2014); Parsons et al. (2014); Pattinson et al. (2012); Prah et al. (2016); Stephanou et al. (2008);
- Biztonságos Internet használat/Adathalász weboldalak: Aldawood – Skinner (2018); Aldawood – Skinner (2019); Bányász – Krasznay (2019); Deák (2019); Illéssy et al. (2014); Kruger – Kearney (2006); Nemeslaki – Sasvári (2014); Parsons et al. (2014); Prah et al. (2016);
- Közösségi média használata: Aldawood - Skinner (2018); Aldawood – Skinner (2019); Bányász (2015); Bányász (2017); Bányász (2018); Bányász – Krasznay (2019); Deák (2017); Deák (2018); Parsons et al. (2014);
- Mobil eszközök használata: Aldawood – Skinner (2018); Aldawood – Skinner (2019); Deák (2017); Deák (2019); Illéssy et al. (2014); Kruger – Kearney (2006); Parsons et al. (2014);
- Információ- és adatkezelés: Aldawood – Skinner (2019); Bányász – Krasznay (2019); Deák (2019); Illéssy et al. (2014); Nemeslaki – Sasvári (2014); Parsons et al. (2014).

Felhasznált irodalom

Aldawood, Hussain – Skinner, Geoffrey (2018): A critical appraisal of contemporary cyber security social engineering solutions: measures, policies, tools and applications; Conference paper: 2018 26th International Conference on Systems Engineering (ICSEng), p. 6, https://www.researchgate.net/publication/330661441_A_Critical_Appraisal_of_Contemporary_Cyber_Security_Social_Engineering_Solutions_Measures_Policies_Tools_and_Applications

Aldawood, Hussain – Skinner, Geoffrey (2019): Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues, *Future Internet*, vol. 11, no. 3., p. 16.

Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak (2010): Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, vol. 34, no. 3, 523–548, DOI: https:// doi.org/10.2307/25750690

Bányász Péter (2015): A közösségi média, mint a nyílt forrású információszerzés fontos területe, *Nemzetbiztonsági Szemle (Online)*, 3. évf. 2. szám, 21-36., http://real.mtak.hu/72506/

Bányász Péter (2018): Social engineering and social media, *Nemzetbiztonsági Szemle (Online)*, 6. évf. 1. szám, 59-77., http://real.mtak.hu/94335/1/EPA02538_nemzetbiztonsagi_szemle_2018_01_059-077.pdf

Bányász Péter – Krasznay Csaba (2019): Kiberbiztonsági incidensek a magyar közigazgatásban, In: *A jó állam mérhetősége III.*, Szerk,: Kaiser Tamás, Budapest, 249-270.

Canova, Gamze – Volkamer, Melanie – Bergmann, Clemens – Borza, Roland (2014): NoPhish: An Anti-Phishing Education App, International Workshop on Security and Trust Management, 2014. https://www.researchgate.net/publication/300021202_NoPhish_An_Anti-Phishing_Education_App

Canova, Gamze – Volkamer, Melanie – Bergmann, Clemens – Reinheimer, Benjamin: NoPhish App Evaluation (2015): Lab and Retention Study, Workshop on Usable Security, https://www.researchgate.net/publication/300925099_NoPhish_App_Evaluation_Lab_and_Retention_Study (Letöltve: 2020.11.03.)

Deák Veronika (2019): Kártékony programok terjedése social engineering technikákon keresztül, *Hadmérnök* 14. évf. 2. szám, 256-271.

Deák Veronika (2017a): A social engineering humán alapú támadási technikái, *Biztonságpolitika*, 2017. április 10., https://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai

Deák Veronika (2017b): A számítógép alapú social engineer támadási technikák, *Biztonságpolitika*, 2017. április 28., https://biztonsagpolitika.hu/wp-content/uploads/2017/04/biztpol_IT_Deak_Veronika.pdf

Deterding, Sebastian - Dixon, Dan – Khaled, Rilla – Nacke, Lennart (2011): From game design elements to gamefulness: defining gamification. In Proceedings of the 15th International Academic MindTrek Conference, 9–15., https://www.researchgate.net/publication/230854710_From_Game_Design_Elements_to_Gamefulness_Defining_Gamification

Domínguez, Adrián – Saenz-de-Navarrete, Joseba – de-Marcos, Luis – Fernández-Sanz, Luis – Pagés, Carmen – Martínez-Herráiz, José-Javier (2013): Gamifying learning experiences: Practical implications and outcomes; *Computer & Education* vol. 63., no. 1., 380-392.

Fromann Richárd – Damsa, Andrei (2016): Digitális pedagógia – A gamifikáció (játékosítás) motivációs eszköztára az oktatásban; *Új Pedagógiai Szemle* 2016/3-4., 76-81.

Illéssy Miklós – Nemeslaki András – Som Zoltán (2014): Elektronikus információbiztonság-tudatosság a magyar közigazgatásban; *Információs Társadalom* 2014/1., 52–73.

Kovács Tamás – Várallyai László (2018): Gamifikáció, avagy a játékosítás szerepe napjainkban; *International Journal of Engineering and Management Sciences* vol. 3, no. 3, 171-180.

Kruger, Hennie A. – Kearney Wayne D (2006): A prototype for assessing information security; *Computers & Security*, vol. 25, no. 4, 289-296.

Kunz, Alexandra – Volkamer, Melanie – Stockhardt, Simon – Palberg, Sven – Lottermann,Tessa – Piegert, Eric (2016): NoPhish: Evaluation of a web application that teaches people being aware of phishing attacks; In: Mayr, H. C. & Pinzger, M. (Hrsg.), *Informatik 2016*. Bonn: Gesellschaft für Informatik e.V., 509-518.

Legárd Ildikó (2020): Célpont vagy! – A közszolgálat felkészítése a kiberfenyegetésekre, *Hadmérnök*, 15. évf., 1. szám, 91-105.

Muha Lajos – Krasznay Csaba (2014): *Az elektronikus információs rendszerek biztonságának menedzselése*, Budapest: NKE, Vezető- és Továbbképzési Intézet

Nemeslaki András – Sasvári Péter (2014): Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában, *Infokommunikáció és Jog*, 60. sz., 169–177.

Pacsi Diána – Szabó Zoltán (2017): A gamifikáció fejlődése és a magyar gamifikációs trend alakulása; *Studia Mundi – Economica*, vol. 4., no. 1. 57-68.

Parsons, Kathryn – Mccormac, Agata – Butavicius, Marcus – Ferguson Lael (2010): *Human factors and information security: Individual, culture and security environment*; Published by Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation, Edinburgh South Australia, p. 54., https://apps.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf

Parsons, Kathryn – Mccormac, Agata – Butavicius, Marcus – Pattinson, Malcolm – Jerram, Cate (2014): Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), *Computers & Security* 42 (2014), 165-176.

Pattinson, Malcolm – Jerram, Cate – Parsons, Kathryn – Mccormac, Agata – Butavicius, Marcus (2012): Why do some people manage phishing e-mails better than others?, *Information Management & Computer Security*, vol. 20, no. 1, 18-28.

Scholefield, Sam – Shepherd, Lynsay A. (2019): Gamification Techniques for Raising Cyber Security Awareness, In: *Moallem A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science*, vol 11594. Springer, Cham, 191-203.

Shaw, R. S. – Chen, Charlie C. – Harris.Albert L. – Huang, Hui-Jou (2009): The impact of information richness on information security awareness training effectiveness, *Computers & Education*, vol. 52, no. 1, 92–100, DOI: https://doi.org/10.1016/j. compedu.2008.06.011

Som Zoltán – Papp Gergely Zoltán (2016): Információbiztonsági alapok és jelszóhasználati statisztikák. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban, Nemzeti Közszolgálati Egyetem; *Hírvillám-Signal Badge* 2016/1., 47-59., https://www.puskashirbaje.hu/index_html_files/hirvillam_7evfolyam_1szam.pdf

Szász Antónia – Kiss Gábor (2018): Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra, *Információs Társadalom*, 18. évf. 3–4. szám, 82–104.

Veseli, Ilirjana (2011): *Measuring the Effectiveness of Information Security Awereness Program*, M. S. thesis, Gjøvik University College, Gjøvik, p. 87., https://www.semanticscholar.org/paper/Measuring-the-Effectiveness-of-Information-Security-Veseli/4105e146d3e0d13afe62960db6f1157722d824c9

373