DOI: 10.38146/BSZ.2022.2.11

Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei

Security awareness within the cyberspace – results of the 2020 national survey among the population

Palicz Tamás
Dr. igazgató-helyettes, Semmelweis Egyetem, Egészségügyi Menedzserképző Központ
palicz.tamas@emk.semmelweis.hu

Bonnyai Tünde
Dr. PhD, biztonsági szakértő, MVM Services Zrt.,
bonnyai.tunde@mvm.hu

Bencsik Balázs
Dr. igazgató, Szabályozott Tevékenységek Felügyeleti Hatósága
balazs.bencsik@sztfh.hu

Pintér Levente
Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet
levente.pinter@nki.gov.hu

Dombrádi Viktor
PhD, adjunktus, Semmelweis Egyetem, Egészségügyi Menedzserképző Központ
dombradi.viktor@emk.semmelweis.hu

Joó Tamás
ügyvivő szakértő, Semmelweis Egyetem, Egészségügyi Menedzserképző Központ
joo.tamas@emk.semmelweis.hu

Bor Olivér
PR és kormányzati kapcsolatok vezető, biztributor
obor@biztributor.hu

Hornyik Zsuzsanna
Dr. főszerkesztő-helyettes, Belügyminisztérium, Belügyi Szemle Szerkesztősége
zsuzsanna.hornyik@bm.gov.hu

Absztrakt

Cél: A tanulmány célja, hogy a Nemzeti Kibervédelmi Intézet által 2020-ban országosan végzett lakossági kérdőív eredményein keresztül bemutassa, milyen jelentőséggel bír a kiberbiztonság a mai magyar társadalomban, miként befolyásolják azt szociodemográfiai tényezők és a biztonságtudatosság egyes elemei.

Módszertan: A dolgozat a Magyarországon végzett lakossági felmérés eredményeinek, a témában megjelent szakirodalomnak a feldolgozásával, elemzésével, összevetésével összegzi a vizsgálat célját képező biztonságtudatosságot, biztonsági szokásokat.

Megállapítások: A kitöltött kérdőívek feldolgozását követően többek között megállapítható, hogy a nemek eloszlása tekintetében inkább a férfiakra jellemző a legfrissebb IT-hírek olvasása, a jelszavak rendszeres frissítése, amely szokást a magasabb iskolai végzettség is jelentősen befolyásolt. Az idősebb generáció képviselői biztonsági okokból elsők között végeznek frissítéseket, veszik igénybe az ezirányú automatikus rendszereket, alkalmazásokat. A női felhasználók

pedig – jelen felmérés tükrében – kevesebb olyan információt osztanak meg magukról, amelyek révén hamis profilt lehetne róluk készíteni.
Érték: A Nemzeti Kibervédelmi Intézet által kivitelezett felmérés kiértékelése, elemzése valódi érték, nélkülözhetetlen alapja a jövőbeni hasonló témájú felméréseknek és a nemzeti kiberbiztonsági stratégia fejlesztésének, illetve annak céljaihoz illeszkedő beavatkozások és akciótervek kidolgozásának.

Kulcsszavak: biztonságtudatosság, kiberbiztonság, lakossági felmérés, nemzeti stratégia, Európai Kiberhónap

Abstract
Aim: The goal of this study is to present the importance of cybersecurity in the present-day Hungarian society and to show how social demographic factors and certain aspects of security awareness influence this. This goal is achieved by presenting the results of the national survey conducted in 2020 by the National Cyber Security Center.
Methodology: This paper presents the findings of the Hungarian survey conducted among the population. By processing, analysing and comparing the results of the survey with the relevant literature, it presents a summary regarding security awareness and safety habits.
Findings: After evaluating the completed questionnaires, among many things, it can be stated that regarding gender distribution males are more likely to read the latest IT news and update their password regularly. These habits are also considerably more favourable for those having a higher education. Because of security reasons the members of the older generation are the ones who are among the first to do updates, and to utilize systems and applications that do this automatically. According to this survey females share less personal information about themselves which could be used to create a fake profile.
Value: The evaluation and analysis of the survey conducted by the National Cyber Security Center can be considered a true value, and is an essential basis for similar surveys in the future, for improving the national cybersecurity strategy, and for developing interventions and action plans for achieving the specified goals of this strategy.

Keywords: security awareness, cybersecurity, population survey, national strategy, European Cybersecurity Month (ECSM)

Bevezetés

A 21. század egyik legnagyobb kihívása, hogy folyamatosan változó környezetünkre megtanuljunk reagálni – lehetőségeinkhez képest hatékonyan és eredményesen. A technológiai fejlődés révén be kell látnunk, hogy számtalan dinamikusan változó körülménnyel kell szembesülnünk életünk során, amelyek jelentős része a kibertérben, az online felületeken ér el bennünket, és sok esetben komoly hatást gyakorol a mindennapjainkra. A modern kor generációi számára eszközök, alkalmazások, platformok ezrei nyújtanak kényelmes, gyors és fejlődési lehetőségekben gazdag közeget, miközben óhatatlanul beszivárognak a magánéletünkbe, a privát szféránkba is. Ez a fajta kényelem veszélyeztető tényezők és kockázatok széles skáláját hozza magával, és a nem megfelelő reakciók esetén akár súlyos következményeket vonhat maga után. Rendkívül fontos, hogy a kibertér által hordozott veszélyek tekintetében az infokommunikációs eszközöket használók széles körében rendszeres, közérthető és célirányos figyelemfelkeltő tevékenységeket végezzünk annak érdekében, hogy a legfiatalabb generációtól a legtapasztaltabbon át, a legkevésbé érdeklődőig igyekezzünk rávilágítani az online tér előnyei mögött meghúzódó, lehetséges csapdákra is. Jelen tanulmánnyal azt a célt tűztük ki magunk elé, hogy egy hazai lakossági felmérésen keresztül érzékeltessük, miként befolyásolja az emberi tényező és a biztonságtudatosság a mai modern társadalmak működését. Biztonságtudatossággal kapcsolatos felmérések elemzésén keresztül láttatni szeretnénk, hogy a biztonságtudatosság szerte a világban ténylegesen befolyásolja a kiberbiztonságot.

A kiberbiztonság a modern információs társadalom, és az abban életre hívott szervezetek működőképességének és rugalmas alkalmazkodóképességének (rezilienciájának) egyik kulcsterülete. A kibertér létezésének, fenntartásának, és működésének sajátosságai miatt – az emberi kommunikációs csatornák markáns változásait, a diszlokációtól és időtől való függetlenséget, és különösen a COVID–19 pandémia következményeit figyelembe véve – fokozott figyelmet kell fordítani az úgynevezett „átlagfelhasználó" szokásaira, magatartásformáira, összességében arra, hogy a rendelkezésre álló csatornákon és módszereken keresztül a személyi ellenálló képességet, a biztonságtudatos attitűdöt fokozatosan fejlesszük a társadalom lehető legszélesebb körében. A kibertér által hordozott számos fenyegetés, amely az elmúlt másfél évben, a pandémia alatt jelentősen megnőtt (Szabó, 2021; Palicz, Bencsik & Szócska, 2021), egyértelműen alátámasztja, hogy a felhasználói magatartás, azon belül is a biztonságtudatosság a kibertér biztonságos használatának egyik alapja.

A biztonságtudatosság növelése – elsősorban ismeretterjesztés, képzések és készségfejlesztés révén – minden esetben javítja az információs rendszerek

biztonságát, nemcsak a munkahelyen, hanem az otthoni környezetben is. Ezen kampányok, tevékenységek és módszertanok tervezése kapcsán szükséges figyelembe venni, hogy a megszólítani kívánt egyén vagy csoport milyen ismeretekkel és attitűdökkel rendelkezik ezen a területen (Oroszi, 2020), és törekedni kell arra, hogy a leginkább személyre szabott tartalommal valósítsuk meg a tudatosítási programunkat. A szakirodalmakban fellelhető adatok alapján kijelenthetjük, hogy a kiberbiztonsággal kapcsolatos nem megfelelő attitűd és tudás hiánya jelentős mértékben hozzájárulhat a szervezetnél – és a magánéletben – jellemző biztonsági szint csökkenéséhez (Sasse & Flechais, 2005; Nyikes, 2019).

Mindezekre tekintettel Magyarországon is egyre nagyobb hangsúlyt kapnak a kiberbiztonsági tudatosítással kapcsolatos kérdések. Ezt mutatja az is, hogy Magyarország Kormánya 2018 végén a 1838/2018. (XII. 28.) Korm. határozattal elfogadta Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiáját, amelyben egy úgynevezett „irányítási keretrendszert" hívott életre. Az ennek jegyében meghatározott stratégiai szintű feladatokat a digitális környezet iránti bizalom erősítése, a digitális infrastruktúra védelme, illetve a gazdasági szereplők támogatása köré csoportosíthatjuk, amelyeken alapulva külön intézkedési terv rögzíti a részletes tevékenységeket és felelősségi köröket. Ezek között találhatunk olyan törekvéseket, mint olyan fórumok kialakításának szükségessége, amelyek révén lehetőség nyílik a társadalmi párbeszédre és a széles körű tájékoztatásra, vagy annak biztosítása, hogy a lakosság és a gazdasági szereplők ismerjék azokat a forrásokat (helyek, szervezetek stb.), ahol hiteles információhoz juthatnak, illetve támogatást kaphatnak abban, hova fordulhatnak további segítségért. Mindehhez nélkülözhetetlen, hogy az illetékes szervezeteknél rendelkezésre álljanak megalapozott, követéses adatok a lakosság és a gazdasági szereplők tájékozottságáról, tudatosságáról, felkészültségéről, fenyegetettségi helyzetéről. Ennek biztosítására az intézkedési terv a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete számára előírta, hogy minden évben szükséges a lakosság és a kis- és középvállalati szektor biztonságtudatosságának felmérése. Ennek első vizsgálata 2020 októberében, az Európai Kiberbiztonsági Hónap keretében történt meg (URL1).

A felmérés célcsoportjainak kiválasztása nem volt specifikus, általános értelemben célozta a lakosságot – kortól, nemtől, lakóhelytől és munkavégzéstől függetlenül –, illetve gazdasági társaságokat szólított meg. Jelen tanulmány ennek a felmérésnek a lakossági eredményeit mutatja be, mint egy olyan kiterjedt felmérést, amely a teljes lakosságot vette górcső alá, illetve tervezetten, a kormány előírásának megfelelően, évente ismétlésre kerül. Ugyanakkor fontos hangsúlyozni, hogy nem ez az első felmérés Magyarországon, amely az adott kérdéskörrel foglalkozik, és több hazai publikáció (Nyikes, 2017a, 2017b) és

egy PhD-értekezés (Nyikes, 2019) is elemezte a lakosok attitűdjét és szokásait a kiberbiztonsággal kapcsolatosan.

A mostani tanulmány fő célja, hogy a 2020-ban, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (továbbiakban: Intézet) irányításával végzett lakossági felmérés eredményeit összefoglalja, azok felhasználásával bemutassa, hogy a mai magyar társadalomban milyen jelentőséget tulajdonítanak a kiberbiztonsági kérdéseknek felhasználói szinten. A hazai és nemzetközi irodalom feldolgozásán keresztül azt is vizsgáljuk és bemutatjuk, hogy a jelenleg rendelkezésre álló kutatások eredményei alapján a kibertérben meglevő biztonságtudatosság milyen szerepet tölt be a modern társadalmakban, miként befolyásolják annak összetevőit a szociodemográfiai tényezők. A felmérés során a célcsoportokat a stratégiai dokumentumokban meghatározott feladatok definiálták (általános lakossági és gazdasági társaságok körében végzendő felmérés), azonban az így nyert információk hasznosak lehetnek a stratégia további fejlesztése és az annak alapján meghatározásra kerülő kezdeményezések, intézkedések tervezésénél és végrehajtásánál egyaránt.

Módszer

A lakossági felmérés során alkalmazott módszerek tekintetében ismertetésre kerül, hogy milyen viszonyítási alap mentén történt fejlesztés szerint készültek a kérdőívek, miként került meghatározásra a célcsoport, milyen időszakban zajlott, mely kommunikációs csatornákon keresztül és milyen módon a felmérés.

A feladat végrehajtásának tervezésekor figyelembe kellett vennünk, hogy országos szintű adatgyűjtést kell végezni, ezért az információgyűjtést kvantitatív módszertani megközelítéssel, a célközönség számára könnyen hozzáférhető online kérdőíves felmérés keretében valósítottuk meg. Két online kérdőív készült – külön a lakosság és külön a közigazgatási szervek, valamint gazdasági társaságok számára – az Európai Bizottság által működtetett EUSurvey (URL2) webes platform felhasználásával, amelyet az Európai Uniós Kiberbiztonsági Ügynökség (European Union Agency for Cybersecurity – ENISA) is alkalmaz.

A kérdőívek három kommunikációs csatornán kerültek publikálásra: az Intézet weboldalán, az Intézet Facebook-oldalán – amellyel kapcsolatban a kérdések minél szélesebb célközönséghez történő eljuttatásához hirdetési rendszert is igénybe vettünk –, valamint a gazdasági szereplőknek és a közigazgatási szférában dolgozóknak szóló kérdőív elektronikus úton, az Intézet ügyfélkörébe tartozó szervezetek és partnerintézmények számára pedig külön került megküldésre.

Az online kérdőívek 2020. október 28. és 2020. november 30. között voltak elérhetők. Összesen 1792 kitöltött kérdőív került benyújtásra, amelyek közül a lakossági szereplők kérdéseire összesen 1104 válasz érkezett.

A kérdések kialakításánál célunk a legalapvetőbb IT-biztonsági ismeretek és szokások feltérképezése volt. A lakossági és a gazdasági társaságok tekintetében egyaránt 20–20 kérdést készítettünk. Természetesen a témakör mélysége jóval hosszabb kérdőív elkészítését is lehetővé tette volna, azonban szem előtt tartottuk, hogy a hosszú kérdőívek esetében a válaszadók motivációja egy idő után csökken, és nagyobb valószínűséggel születnek sztereotipikus válaszok (Herzog & Bachman, 1981).

A stratégiai intézkedési terv által előírt négy fő vizsgálati kategória (tájékozottság, tudatosság, felkészültség, fenyegetettségi helyzet) tekintetében az alábbi szempontokat vettük figyelembe.

- Tájékozottság. Ebben a témakörben arra helyeztük a hangsúlyt, hogy a lakossági szereplők mennyire követik az IT-biztonsági híreket, informálódnak-e. Arra is kerestük a választ, hogy vajon mennyien vannak tisztában azzal, hogy a Nemzeti Kibervédelmi Intézethez segítségért fordulhatnak, amennyiben adatbiztonsági incidensben érintettek, valamint, hogy mennyire tájékozottak a különböző online szolgáltatások által végzett adatgyűjtéssel kapcsolatban.
- Tudatosság. A kategóriában az egyének által alkalmazható legalapvetőbb IT-biztonsági védelmi lépések (vírusirtó szoftver használata, biztonsági frissítések telepítése) alkalmazásáról tettünk fel kérdéseket. Az adatvédelmi tudatosság tekintetében arra voltunk kíváncsiak, hogy a mindennapokból jól ismert weboldal sütik és az okoseszközök adatvédelmi beállításai, valamint az online szolgáltatások kiválasztása során a lakossági szereplők mennyire járnak el tudatosan.
- Felkészültség. Az alapszintű IT-biztonsági jó gyakorlatok vizsgálatakor jelszóalkalmazási, és az e-mail csatolmányok kezelésére vonatkozó jó gyakorlatokat vizsgáltuk, mivel ezek – bár alapszintű IT-biztonsági ismeretek – kiemelt jelentőséggel bírnak a kibertámadások elleni védekezésben.
- Fenyegetettség. A kibertámadásoknak való kitettséget befolyásoló olyan tényezőket vizsgáltunk, mint például a lakossági szereplők mennyire tartják elképzelhetőnek azt, hogy rosszindulatú felek a közösségi média profiljukat lemásolva megszemélyesítik őket.

A beérkezett adatok adattisztítási folyamata során a születési évet átalakítottuk életkorra (életkor = 2020-évszám), majd ezt követően az életkorokat korcsoportokba és generációkba soroltuk (Baby-boom, X, Y, Z generációk). Korrigálható

hibák esetén az értékeket átírtuk, viszont az értelmezhetetlen adatokat tartalmazó rekordokat töröltük (például 0 életév). Feltehetően ezek a hibák a kitöltés során kerültek az adatbázisba.

Az összehasonlító statisztikai elemzések kivitelezésére a demográfiai adatokat és a válaszlehetőségeket dichotomizáltuk, vagyis két csoportba soroltuk (lásd 2–10. táblázatokat az Eredmények fejezetben). A csoportok kialakításánál figyelembe vettük a válaszadók és a válaszok megoszlását, valamint törekedtünk arra, hogy szakmailag is informatívak legyenek a következtetések. Ennek keretén belül például az általános iskolai és középiskolai végzettséggel rendelkezők egy csoportba kerültek.

Az eredeti lakossági kérdőív feldolgozásakor nem elemeztük az összes kérdést, mivel bizonyos kérdések válaszai ugyan érdekesek, viszont szakmai szempontból nem tekinthetők relevánsnak. Ilyen kérdés volt például, hogy *„Az alábbi lehetőségek közül Ön melyiket preferálja okoseszközök képernyőzárának feloldásához?”*. Ebből adódóan az eredeti húsz kérdésből kilencet vizsgáltunk meg összehasonlító statisztika segítségével.

A statisztikai elemzés keretén belül elsőnek leíró statisztikával megnéztük a demográfiai adatok elemszámát és százalékos megoszlását, majd szisztematikusan megnéztük Khí-négyzet próba segítségével, hogy a dichotomizált demográfiai adatok milyen kapcsolatban állnak a dichotomizált kérdések válaszaival. Végezetül mátrix elemzéssel azt is megnéztük, hogy a különböző kérdések között milyen lehetséges kapcsolat található. A mátrix elemzés során is Khí-négyzet próbát alkalmaztunk. A szignifikancia szintjét $P<0,05$ értékben határoztuk meg. Az összes statisztikai elemzéshez SPSS 27 programot használtunk (IBM Corp. Released 2020. IBM SPSS Statistics for Windows, Version 27.0. Armonk, NY: IBM Corp).

Eredmények

Összesen 1104 kitöltő válaszait dolgoztuk fel a vizsgálatunk során (1. számú táblázat). A kitöltők több mint háromnegyede férfi (77,2%), egyötöde nő (21,8%) volt, míg 11-en nem adták meg a nemüket (1,0%). A legtöbben a 35–44 (30,1%), 45–54 (18,1%) és 25–34 (15,8%) korcsoportokban voltak. A kitöltők több mint felének (58,7%) főiskolai vagy egyetemi diplomája volt. A lakóhelyet tekintve a kitöltők 35,5%-a Budapestről, 24,1%-a valamelyik megyei jogú városból, míg 40,1%-a egyéb településről származik. Ezen adatok alapján kijelenthető, hogy a felmérés nem volt reprezentatív az általános lakosságra vonatkozóan, így a felmérésből származó következtetéseket csak óvatosan szabad általánosítani.

1. számú táblázat: *Válaszadók demográfiai adatai*

Nem	**N**	**%**
Férfi	852	77,2
Nő	241	21,8
Nincs adat	11	1,0
Kor	**N**	**%**
<18	46	4,2
18–24	89	8,1
25–34	174	15,8
35–44	332	30,1
45–54	200	18,1
55–64	121	11,0
65–74	121	11,0
75 és idősebb	20	1,8
Nincs adat	1	0,1
Iskolázottság	**N**	**%**
Általános iskola	65	5,9
Középiskola	391	35,4
Főiskola/egyetem	648	58,7
Lakóhely	**N**	**%**
Budapest	392	35,5
Megyei jogú város	266	24,1
Egyéb	446	40,4
Eszközök (többválasztós kérdés)	**N**	**%**
Számítógép	755	68,4
Laptop	1104	100
Tablet	558	50,5
Okostelefon	1061	96,1
Okosóra	280	25,4
Okoskarkötő	169	15,3
Okos háztartási eszköz	212	19,2
Eszközök használata naponta (óra)	**N**	**%**
0–3 óra	164	14,9
3–6 óra	325	29,4
6–9 óra	294	26,6
9 vagy több óra	321	29,1

Forrás: A szerzők saját szerkesztése.

Mindenkinek volt laptopja (100%) és majdnem mindenki rendelkezett okostelefonnal (96,1%). A válaszadók több mint felének volt számítógépe (68,4%) és tabletje (50,5%). Az elektronikus eszközök használatára a kitöltők többsége napi 3–6 órát fordít (29,4%), viszont nem sokkal vannak kevesebben azok, akik naponta 9 vagy több órát használják ezeket az eszközöket (29,1%).

2. számú táblázat: *Válaszadók olvasási gyakorisága IT-biztonság témájában*

Változók	Kategóriák	Ön milyen gyakorisággal olvas IT-biztonsággal kapcsolatos híreket?		Összes válasz	P-érték
		Nem rendszeresen	Rendszeresen		
Nem	férfi	369	483	852	**<0,001**
		43,3%	56,7%	100%	
	nő	172	69	241	
		71,4%	28,6%	100%	
Legmagasabb iskolai végzettség	általános vagy középiskola	244	212	456	**0,035**
		53,5%	46,5%	100%	
	főiskola vagy egyetem	305	343	648	
		47,1%	52,9%	100%	
Generáció	X vagy Baby-boom	358	329	687	**0,046**
		52,1%	47,9%	100%	
	Y vagy Z generáció	191	225	416	
		45,9%	54,1%	100%	
Napi szinten több, mint hat órát használja az eszközeit	0–6 óra	304	185	489	**<0,001**
		62,2%	37,8%	100%	
	6 ≤ óra	245	370	615	
		39,8%	60,2%	100%	
Lakóhely	Budapest vagy megyei jogú város	295	363	658	**<0,001**
		44,8%	55,2%	100%	
	egyéb	254	192	446	
		57,0%	43,0%	100%	
Több, mint három eszközzel rendelkezik	igen	96	170	266	**<0,001**
		36,1%	63,9%	100%	
	nem	453	385	838	
		54,1%	45,9%	100%	

Forrás: A szerzők saját szerkesztése.

3. számú táblázat: *Válaszadók szokása weboldal-regisztráció során*

Változók	Kategóriák	Regisztráció során Ön el szokta olvasni a weboldalak adatvédelmi szabályzatait?		Összes válasz	P-érték
		Igen	Nem		
Nem	férfi	618	234	852	**0,107**
		72,5%	27,5%	100%	
	nő	162	79	241	
		67,2%	32,8%	100%	
Legmagasabb iskolai végzettség	általános vagy középiskola	296	160	456	**0,237**
		64,9%	35,1%	100%	
	főiskola vagy egyetem	398	250	648	
		61,4%	38,6%	100%	
Generáció	X vagy Baby-boom	443	244	687	**0,144**
		64,5%	35,5%	100%	
	Y vagy Z generáció	250	166	416	
		60,1%	39,9%	100%	
Napi szinten több, mint hat órát használja az eszközeit	0–6 óra	319	170	489	**0,146**
		65,2%	34,8%	100%	
	6 ≤ óra	375	240	615	
		61,0%	39,0%	100%	
Lakóhely	Budapest vagy megyei jogú város	401	257	658	**0,109**
		60,9%	39,1%	100%	
	egyéb	293	153	446	
		65,7%	34,3%	100%	
Több, mint három eszközzel rendelkezik	igen	178	88	266	**0,116**
		66,9%	33,1%	100%	
	nem	516	322	838	
		61,6%	38,4%	100%	

Forrás: A szerzők saját szerkesztése.

Az IT-biztonsággal kapcsolatos híreket (2. számú táblázat) szignifikánsan gyakrabban olvassák a férfiak (P<0,001), főiskolai vagy egyetemi diplomával rendelkezők (P=0,035), a fiatalabb generációk (Z vagy Y generációk; P=0,046), akik naponta hat vagy több óránál többet használják az elektronikus eszközeiket (P<0,001), a budapesti vagy megyei jogú város lakosai (P<0,001), és azok, akik több mint három eszközzel rendelkeznek (P<0,001).

Ezzel szemben sehol sem találtunk szignifikáns eltérést annak tekintetében, hogy a regisztráció során elolvassák-e a weboldalak adatvédelmi szabályzatát (3. számú táblázat).

Az idősebb generációra (Baby-boom vagy X generációk) inkább jellemző, hogy amint kijönnek a biztonsági eszközök frissítései, az előre beállított automatikus frissítés következtében azonnal elvégzik a frissítést (P<0,001) (4. számú táblázat). Ugyanez az állítás jellemző azokra is, akiknek három vagy több fajta elektronikus eszközük van (P=0,006).

4. számú táblázat: *Válaszadók szokása a biztonsági frissítést illetően*

Változók	Kategóriák	Ön milyen gyakorisággal végez biztonsági frissítést eszközein?		Összes válasz	P-érték
		Amint kijönnek a frissítések, mert be van állítva az automatikus frissítés	Egyéb		
Nem	férfi	618	234	852	0,107
		72,5%	27,5%	100%	
	nő	162	79	241	
		67,2%	32,8%	100%	
Legmagasabb iskolai végzettség	általános vagy középiskola	318	138	456	0,369
		69,7%	30,3%	100%	
	főiskola vagy egyetem	468	180	648	
		72,2%	27,8%	100%	
Generáció	X vagy Baby-boom	517	170	687	**<0,001**
		75,3%	24,7%	100%	
	Y vagy Z generáció	268	148	416	
		64,4%	35,6%	100%	
Napi szinten több, mint hat órát használja az eszközeit	0–6 óra	350	139	489	0,804
		71,6%	28,4%	100%	
	6 ≤ óra	436	179	615	
		70,9%	29,1%	100%	
Lakóhely	Budapest vagy megyei jogú város	479	179	658	0,154
		72,8%	27,2%	100%	
	egyéb	307	139	446	
		68,8%	31,2%	100%	
Több, mint három eszközzel rendelkezik	igen	207	59	266	**0,006**
		77,8%	22,2%	100%	
	nem	579	259	838	
		69,1%	30,9%	100%	

Forrás: A szerzők saját szerkesztése.

A válaszadók 90,8% válaszolta, hogy van vírusirtó szoftver a számítógépén vagy a laptopján (5. számú táblázat). Ez az arány szignifikánsan magasabb a nőknél (P=0,014), a főiskolai vagy egyetemi diplomával rendelkezőknél (P=0,008) és az idősebb generációnál (Baby-boom vagy X generációk) (P<0,001).

A férfiakra jellemzőbb, hogy inkább több jelszót használnak különböző online felületek használatakor (P<0,001) (6. számú táblázat), továbbá ez jellemzőbb még a főiskolai vagy egyetemi végzettséggel rendelkezőkre is (P<0,001).

5. számú táblázat: *Válaszadók vírusirtó szoftver használata*

Változók	Kategóriák	Használ-e a számítógépén/laptopján vírusirtó szoftvert?		Összes válasz	P-érték
		Igen	Nem		
Nem	férfi	755	85	840	**0,014**
		89,9%	10,1%	100%	
	nő	216	11	227	
		95,2%	4,8%	100%	
Legmagasabb iskolai végzettség	általános vagy középiskola	389	53	442	**0,008**
		88,0%	12,0%	100%	
	főiskola vagy egyetem	590	46	636	
		92,8%	7,2%	100%	
Generáció	X vagy Baby-boom	632	44	676	**<0,001**
		93,5%	6,5%	100%	
	Y vagy Z generáció	346	55	401	
		86,3%	13,7%	100%	
Napi szinten több, mint hat órát használja az eszközeit	0–6 óra	440	41	481	0,501
		91,5%	8,5%	100%	
	6 ≤ óra	539	58	597	
		90,3%	9,7%	100%	
Lakóhely	Budapest vagy megyei jogú város	595	52	647	0,110
		92,0%	8,0%	100%	
	egyéb	384	47	431	
		89,1%	10,9%	100%	
Több, mint három eszközzel rendelkezik	igen	239	20	259	0,350
		92,3%	7,7%	100%	
	nem	740	79	819	
		90,4%	9,6%	100%	

Forrás: A szerzők saját szerkesztése.

6. számú táblázat: *Válaszadók jelszóhasználati szokása*

Változók	Kategóriák	A különböző online felületeken eltérő jelszavakat használ?		Összes válasz	P-érték
		Eltérő jelszavakat használok	Törekszem a minél kevesebb jelszó megjegyzésére		
Nem	férfi	625	199	824	**<0,001**
		75,8%	24,2%	100%	
	nő	141	80	221	
		63,8%	36,2%	100%	
Legmagasabb iskolai végzettség	általános vagy középiskola	288	144	432	**<0,001**
		66,7%	33,3%	100%	
	főiskola vagy egyetem	487	137	624	
		78,0%	22,0%	100%	
Generáció	X vagy Baby-boom	475	190	665	0,054
		71,4%	28,6%	100%	
	Y vagy Z generáció	300	90	390	
		76,9%	23,1%	100%	
Napi szinten több, mint hat órát használja az eszközeit	0–6 óra	329	137	466	0,068
		70,6%	29,4%	100%	
	6 ≤ óra	446	144	590	
		75,6%	24,4%	100%	
Lakóhely	Budapest vagy megyei jogú város	475	154	629	0,058
		75,5%	24,5%	100%	
	egyéb	300	127	427	
		70,3%	29,7%	100%	
Több, mint három eszközzel rendelkezik	igen	189	67	256	0,855
		73,8%	26,2%	100%	
	nem	586	214	800	
		73,3%	26,8%	100%	

Forrás: A szerzők saját szerkesztése.

7. számú táblázat: *Válaszadók jelszómódosítási gyakorisága*

Változók	Kategóriák	Milyen gyakran módosítja az online felületek eléréséhez szükséges jelszavait?		Összes válasz	P-érték
		Nem rendszeresen	Rendszeresen		
Nem	férfi	577	275	852	0,282
		67,7%	32,3%	100%	
	nő	172	69	241	
		71,4%	28,6%	100%	
Legmagasabb iskolai végzettség	általános vagy középiskola	333	123	456	**0,007**
		73,0%	27,0%	100%	
	főiskola vagy egyetem	424	224	648	
		65,4%	34,6%	100%	
Generáció	X vagy Baby-boom	459	228	687	0,112
		66,8%	33,2%	100%	
	Y vagy Z generáció	297	119	416	
		71,4%	28,6%	100%	
Napi szinten több, mint hat órát használja az eszközeit	0–6 óra	346	143	489	0,163
		70,8%	29,2%	100%	
	6 ≤ óra	411	204	615	
		66,8%	33,2%	100%	
Lakóhely	Budapest vagy megyei jogú város	440	218	658	0,140
		66,9%	33,1%	100,0%	
	egyéb	317	129	446	
		71,1%	28,9%	100,0%	
Több, mint három eszközzel rendelkezik	igen	172	94	266	0,115
		64,7%	35,3%	100,0%	
	nem	585	253	838	
		69,8%	30,2%	100,0%	

Forrás: A szerzők saját szerkesztése.

8. számú táblázat: *Válaszadók ismerete a zsarolóvírust illetően*

Változók	Kategóriák	Zsarolóvírusnak nevezzük azokat a rosszindulatú programokat, amelyek…		Összes válasz	P-érték
		titkosítják a számítógépes eszközön tárolt adatokat	ellopják a felhasználók jelszavait / nem tudja		
Nem	férfi	764	88	852	**<0,001**
		89,7%	10,3%	100%	
	nő	144	97	241	
		59,8%	40,2%	100%	
Legmagasabb iskolai végzettség	általános vagy középiskola	359	97	456	**0,002**
		78,7%	21,3%	100%	
	főiskola vagy egyetem	557	91	648	
		86,0%	14,0%	100%	
Generáció	X vagy Baby-boom	556	131	687	**0,022**
		80,9%	19,1%	100%	
	Y vagy Z generáció	359	57	416	
		86,3%	13,7%	100%	
Napi szinten több, mint hat órát használja az eszközeit	0–6 óra	363	126	489	**<0,001**
		74,2%	25,8%	100%	
	6 ≤ óra	553	62	615	
		89,9%	10,1%	100%	
Lakóhely	Budapest vagy megyei jogú város	562	96	658	**0,009**
		85,4%	14,6%	100%	
	egyéb	354	92	446	
		79,4%	20,6%	100%	
Több, mint három eszközzel rendelkezik	igen	233	33	266	**0,021**
		87,6%	12,4%	100%	
	nem	683	155	838	
		81,5%	18,5%	100%	

Forrás: A szerzők saját szerkesztése.

Egyedül a legmagasabb iskolai végzettség áll azzal kapcsolatban, hogy milyen gyakran módosítanak jelszót online felületek esetén a felhasználók (7. számú táblázat). A felsőfokú végzettség esetén gyakrabban válaszolták azt, hogy rendszeresen változtatnak jelszót (P=0,007), viszont ez az arány náluk is mindössze 34,6%. A kitöltők 83,0%-a válaszolta helyesen, hogy mik a zsarolóvírusok (8. számú táblázat). Ez szignifikánsan kedvezőbb volt a férfiak (P<0,001), főiskolai

vagy egyetemi diplomával rendelkezők (P<0,002), fiatalabb generációk (P=0,022) esetén, továbbá azoknál is, akik legalább napi hat órát használják az elektronikus eszközeiket (P<0,001), valamint, akik Budapesten vagy más megye jogú városban élnek (P=0,009), és akiknek több mint három fajta eszközük van (P=0,021).

A felsőfokú végzettséggel rendelkezőkre (P=0,047) és az idősebb generációkra (P=0,036) inkább jellemző, hogy elfogadhatatlannak tartanák azt, ha valamilyen őket érintő felhasználói adatot kiszivárogtatnának (9. számú táblázat).

9. számú táblázat: *Válaszadók bizalomvesztése adatszivárgás esetén*

Változók	Kategóriák	Milyen mértékű bizalomvesztést eredményezne Önnél, ha kiderülne, hogy egyik szolgáltatója felhasználói adatokat szivárogtat ki?		Összes válasz	P-érték
		Elfogadhatatlannak tartanám és azonnal szolgáltatót váltanék	Nem okozna komoly bizalomvesztést		
Nem	férfi	581	203	784	0,878
		74,1%	25,9%	100%	
	nő	153	52	205	
		74,6%	25,4%	100%	
Legmagasabb iskolai végzettség	általános vagy középiskola	286	117	403	**0,047**
		71,0%	29,0%	100%	
	főiskola vagy egyetem	454	139	593	
		76,6%	23,4%	100%	
Generáció	X vagy Baby-boom	473	145	618	**0,036**
		76,5%	23,5%	100%	
	Y vagy Z generáció	266	111	377	
		70,6%	29,4%	100%	
Napi szinten több, mint hat órát használja az eszközeit	0–6 óra	321	119	440	0,388
		73,0%	27,0%	100%	
	6 ≤ óra	419	137	556	
		75,4%	24,6%	100%	
Lakóhely	Budapest vagy megyei jogú város	463	148	611	0,178
		75,8%	24,2%	100%	
	egyéb	277	108	385	
		71,9%	28,1%	100%	
Több, mint három eszközzel rendelkezik	igen	182	67	249	0,615
		73,1%	26,9%	100%	
	nem	558	189	747	
		74,7%	25,3%	100%	

Forrás: A szerzők saját szerkesztése.

Végezetül a nők (P=0,007) és a fiatalabb korosztály (P=0,012) tartja kevésbé valószínűnek azt, hogy közösségi oldalon róluk valamilyen hamis profilt hozzanak létre (10. számú táblázat). Ugyanakkor fontos megemlíteni, hogy ez utóbbi esetén nem egyértelmű, hogy a különbség arra vezethető vissza, hogy valóban kevesebb személyes információt osztanak meg magukról, vagy egyszerűen nem érzik annak a veszélyét, hogy a profilhamisítás velük is megtörténhet.

A válaszlehetőségek kapcsolatának vizsgálata alapján megállapítható, hogy a válaszok között többségében pozitív irányú szignifikáns kapcsolat található (11. számú táblázat). Ez azt jelenti, hogy ha valaki az egyik kérdésre helyes vagy kedvező választ adott, akkor valószínűleg egy másik kérdés esetén is helyes vagy kedvező választ adott. Ugyanakkor fontos megemlíteni, hogy ez nem minden esetben volt észlelhető, és kettő esetben nem szignifikáns fordított kapcsolatot találtunk. A fordított kapcsolat azt jelenti, hogy ha valaki az egyik kérdésre helyes vagy kedvező választ adott, akkor feltehetően a másik kérdésre helytelenül vagy kedvezőtlenül válaszolt.

10. számú táblázat: *Válaszadók véleménye a hamis profil készítésről*

Változók	Kategóriák	Elképzelhetőnek tartja-e, hogy egy közösségi oldalon valaki az Ön nevében profilt hozzon létre (lemásolja a profilját)?		Összes válasz	P-érték
		Igen, elvégre elég sok nyilvánosan elérhető adatot, képet és információt osztok meg magamról	Nem, mert minimális adatot osztok meg magamról, és azok hozzáférését is szigorúan korlátozom		
Nem	férfi	235	536	771	**0,007**
		30,5%	69,5%	100%	
	nő	44	165	209	
		21,1%	78,9%	100%	
Legmagasabb iskolai végzettség	általános vagy középiskola	102	301	403	0,082
		25,3%	74,7%	100%	
	főiskola vagy egyetem	178	408	586	
		30,4%	69,6%	100%	
Generáció	X vagy Baby-boom	189	417	606	**0,012**
		31,2%	68,8%	100%	
	Y vagy Z generáció	91	291	382	
		23,8%	76,2%	100%	
Napi szinten több, mint hat órát használja az eszközeit	0–6 óra	125	304	429	0,614
		29,1%	70,9%	100%	
	6 ≤ óra	155	405	560	
		27,7%	72,3%	100%	
Lakóhely	Budapest vagy megyei jogú város	165	433	598	0,535
		27,6%	72,4%	100%	
	egyéb	115	276	391	
		29,4%	70,6%	100%	
Több, mint három eszközzel rendelkezik	igen	71	173	244	0,753
		29,1%	70,9%	100%	
	nem	209	536	745	
		28,1%	71,9%	100%	

Forrás: A szerzők saját szerkesztése.

11. számú táblázat: *Attitűdök, tudás és szokások mátrixelemzése Khí-négyzet próbával*

Kérdés	K2	K3	K4	K5	K6	K7	K8	K9
K1: Ön milyen gyakorisággal olvas IT-biztonsággal kapcsolatos híreket?	**<0,001**	**0,008**	0,459	**<0,001**	**<0,001**	**<0,001**	**0,010**	**0,005**
K2: Regisztráció során Ön el szokta olvasni a weboldalak adatvédelmi szabályzatait?		0,173	**0,002**	**<0,001**	**<0,001**	0,144	0,099	**<0,001**
K3: Ön milyen gyakorisággal végez biztonsági frissítést eszközein?			**<0,001**	**0,002**	**<0,001**	**0,009**	**<0,001**	0,911
K4: Használ-e a számítógépén/laptopján vírusirtó szoftvert?				0,066	**<0,001**	0,678	**0,019**	0,945
K5: A különböző online felületeken eltérő jelszavakat használ, vagy törekszik a minél kevesebb jelszó megjegyzésére?					**<0,001**	**<0,001**	**0,029**	**0,009**
K6: Milyen gyakran módosítja az online felületek eléréséhez szükséges jelszavait?						**<0,001**	**0,016**	**0,011**
K7: Kérjük, fejezze be a mondatot! Zsarolóvírusnak nevezzük azokat a rosszindulatú programokat, amelyek…							0,570	0,850
K8: Milyen mértékű bizalomvesztést eredményezne Önnél, ha kiderülne, hogy egyik szolgáltatója felhasználói adatokat szivárogtat ki?								0,549
K9: Elképzelhetőnek tartja-e, hogy egy közösségi oldalon valaki az Ön nevében profilt hozzon létre?								

Megjegyzés: A zöld jelölés pozitív irányú, a sárga jelölés fordított irányú kapcsolatot jelöl.
Forrás: A szerzők saját szerkesztése.

Összegzés

A mostani kutatás adathalmaza a Nemzeti Kibervédelmi Intézet első olyan felméréséből származik, amely elsősorban az intézetet ismerő populációra irányult, és így feltételezhetően nagy arányban ebből a körből töltötték ki a kérdőívet. Ebből adódóan a 2020-ban, a lakosság körében végzett felmérés csak egy nagyon szűk rétegre korlátozódott. A demográfiai adatok alapján megállapítható,

hogy a vizsgált minta nem tekinthető reprezentatívnak az egész magyarországi lakosságra vonatkozóan, mivel például a férfi és a budapesti kitöltők aránytalanul többen voltak a magyar átlaghoz képest. Bár nagyon nehéz valódi reprezentatív felmérést végezni a lakosság körében, a reprezentativitás mértékét a megfelelő kommunikációs csatornák alkalmazásával lehet javítani (Nyikes, 2017a, 2019). Továbbá azt is figyelembe kell venni, hogy mivel a kérdőív válaszai kategorikusak voltak, nem volt lehetőségünk regresszió elemzés révén a lehetséges zavaró tényezőket figyelembe venni. A reprezentativitás hiánya jelenti a 2020-as vizsgálat egyik legfontosabb korlátját, azonban ezektől eltekintve az összehasonlító statisztika eredményei nagy mértékben összhangban állnak a hazai és nemzetközi kutatások eredményeivel, ezért is gondoljuk fontosnak a mostani eredmények publikálását és bizonyos összefüggések kiemelését.

Vizsgálatunkban arra a következtetésre jutottunk, hogy a férfiak rendszeresebben olvasnak IT-híreket, gyakrabban használnak eltérő jelszavakat és jobban tisztában vannak a zsarolóvírus fogalmával. A nemzetközi tanulmányok is hasonló megállapítással éltek, miszerint a férfiak tudatosabbak és kedvezőbb szokásokkal rendelkeznek a kiberbiztonság tekintetében (Anwar, He, Ash, Yuan, Li & Xu, 2017; Cain, Edwards & Still, 2018; McGill & Thompson, 2018; Fatokun, Hamid, Norman & Fatokun, 2019; Zwilling et al., 2020). Ugyanakkor fontos megemlíteni, hogy a magyar felmérésben a nők esetében jellemzőbb volt, hogy van vírusvédelem a gépükön, illetve kevesebb olyan információt osztanak meg magukról, amelyek révén hamis profilt lehetne róluk készíteni. Ez azért lehet érdekes, mert a kisebb kockázatvállalás javítja a helyes kiberbiztonsági szokásokat (Kennison & Chan-Tin, 2020). Ezt a megállapítást célszerű óvatosan kezelni, mivel a felmérésben a nők kisebb arányban vettek részt az országos megoszláshoz viszonyítva, valamint feltételezhető, hogy inkább azok töltötték ki a kérdőívet, akik érdeklődnek a kiberbiztonság iránt.

Az életkor esetében azt találtuk, hogy az idősebb generációra (Baby-boom vagy X generációk) igaz, hogy rendszeresebben végeznek biztonsági frissítéseket, gyakrabban használnak vírusirtó programot, valamint kevésbé elnézőek, ha felhasználói adatot szivárogtatnak ki. A hazai kutatások is hasonló következtetésre jutottak (Nyikes, 2017a, 2019), viszont a nemzetközi irodalom nem következetes ezen a téren, mivel néhány tanulmány szerint az idősebbek komolyabban veszik a kiberbiztonságot (Cain et al., 2018; Hadlington, 2018), azonban más vizsgálatban nem találtak szignifikáns összefüggést (McCormac et al., 2016; Gratian, Bandi, Cukier, Dykstra & Ginther, 2018). Tekintettel arra, hogy a mi vizsgálatunkban is az idősebb generációra volt jellemzőbb, hogy ritkábban olvasnak IT-híreket, kevésbé vannak tisztában a zsarolóvírus fogalmával, és több olyan adatot osztanak meg, amellyel hamis profilt lehet róluk

készíteni, így nem kizárt, hogy területfüggő, hogy az idősebb generációhoz mikor társul jobb kiberbiztonsági tudás és szokás, és mikor nem. A saját, valamint más hazai és nemzetközi eredmények viszont egyértelműen megkérdőjelezik azt a sztereotipikus gondolkodást, hogy mivel az idősebbek kevésbé jártasak a modern technológia használatában, a kiberbiztonsági szokásaik is rosszabbak (Cain et al., 2018).

Egy nemzetközi kutatás igazolta, hogy a magasabb iskolai végzettség javítja a kiberbiztonsági szokásokat, viszont ugyanabban a tanulmányban azt találták, hogy a nem és a kor sokkal meghatározóbb tényező volt e tekintetben (Fatokun et al., 2019). A mi vizsgáltunkban arra is fény derült, hogy a felsőfokú végzettséggel rendelkezőknél jellemzőbb volt az IT-hírek olvasása, a vírusirtó program használata, az eltérő jelszavak használata különböző online felületeken, a jelszavak rendszeres megváltoztatása, a zsarolóvírus fogalmának ismerete, valamint kevésbé tartották elfogadhatónak az adatok kiszivárogtatását. A vírusírtókkal kapcsolatos megállapítást egy hazai kutatás eredményei is alátámasztják. Ebben a szerző arra a következtetésre jutott, hogy az iskolai végzettséggel lineárisan nő a vírusirtók használatának valószínűsége (Nyikes, 2017a; Nyikes, 2019).

A különböző eszközök használatának száma és a lakóhely tekintetében, bár találtunk szignifikáns eltéréseket, de mivel a hazai és nemzetközi irodalomban ezeket nem vizsgálták, nem tudjuk a saját eredményeinket másokéval összevetni. Az eszközhasználat időtartama esetén is csak egy olyan tanulmányt találtunk, amely szerint az internetfüggőség szignifikánsan rontja a kiberbiztonsági szokásokat (Hadlington, 2017). Mivel a függőség nem csak az eszközhasználat idejével áll összefüggésben, így ezen a téren sem tudunk összehasonlítást végezni. Mindenesetre érdemes megemlíteni, hogy a nagyvárosokban élők, a több fajta eszközt használók és az ezeket az eszközöket napi szinten többet használók esetén kedvezőbb válaszokat találtunk.

A módszertani korlátok miatt vizsgálatunkban a válaszokat külön-külön elemeztük, viszont a válaszok közötti szoros kapcsolat világított rá arra, hogy a kiberbiztonsággal kapcsolatos tudás és szokás egy rendkívül összetett kérdés. A nemzetközi vizsgálatok nemcsak ezeket és a demográfiai tényezőket veszik figyelembe, hanem pszichológiai kérdésekkel a kitöltők attitűdjét, személyiségét, a kockázatvállalás mértékét is figyelembe veszik (Herath & Rao, 2009; Shappie, Dawson & Debb, 2020).

A felmérés eredményének feldolgozását követően arra a következtetésre jutottunk, hogy további fejlesztésre van szükség a kérdőívek tekintetében. Célcsoport specifikus kérdésekre, esetleg személyiséget felmérő kérdések beépítésére is szükség lehet a mintanagyság megállapítása mellett, különös figyelemmel a minta reprezentatívitására.

Összegezve, a felmérés kiértékelésekor megállapítást nyert, hogy fontos a lakosság attitűdjének és tudásának folyamatos monitorozása, valamint célszerű a kapott adatokat összehasonlító statisztika segítségével elemezni, mivel a döntéshozók számára releváns információt tudnak nyújtani.

A 2020 októberében Magyarországon végzett nagymintás, elektronikus kérdőívvel végzett lakossági kiberbiztonságra vonatkozó biztonságtudatossági felmérés kapcsán megállapítható, hogy annak eredményei sok tekintetben hasonlóak a hazai és nemzetközi eredményekhez, vagyis számos olyan tényező van (életkori csoport, nem, iskolázottság, lakóhely stb.), amelyek befolyásolják a biztonságtudatosság különböző összetevőit. A felmérés kapcsán fontos kiemelni, hogy a megfelelő statisztikai módszerek alkalmazhatósága érdekében szükséges a felmérési módszertan és a mintavételezés további fejlesztése, a reprezentativitás megteremtése. Az évente rendszeresen végzendő vizsgálatok jól nyomon követhetővé teszik a biztonságtudatosság alakulását, és megfelelő alapot jelentenek olyan célzott intézkedések tervezésére, amely a kibertérben növeli a kiszolgáltatott célcsoportok tudatosságát és ellenállóképességét.

Felhasznált irodalom

Anwar, M., He, W., Ash, I., Yuan, X. H., Li, L. & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*(1), 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Cain, A. A., Edwards, M. E. & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*(1), 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Fatokun, F. B., Hamid, S., Norman, A. & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series, 1339*(1), 012098. https://doi.org/10.1088/1742-6596/1339/1/012098

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*(1), 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hadlington, L. (2018). Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269–281. https://doi.org/10.5281/zenodo.1467909

Herath, T. & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Herzog, A. R. & Bachman, J. G. (1981). Effects of Questionnaire Length on Response Quality. The *Public Opinion Quarterly, 45*(4), 549–559. https://doi.org/10.1086/268687

Kennison, S. M. & Chan-Tin, E. (2020). Taking Risks with Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. Frontiers in *Psychology, 11*(1), 546546. https://doi.org/10.3389/fpsyg.2020.546546

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior, 69*(1), 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McGill, T. & Thompson N. (2018). *Gender Differences in Information Security Perceptions and Behaviour*. Australasian Conference on Information Systems, Sydney.

Nyikes, Z. (2017a). A Közép-Kelet európai generációk digitális kompetencia és biztonságtudatosság vizsgálatának eredményei. *Hadmérnök, 12*(4), 159–174.

Nyikes, Z. (2017b). *A Digitális Kompetencia Értékelési Rendszerének Egyes Kérdései*. XXII. Fiatal Műszakiak Tudományos Ülésszaka, Kolozsvár. Műszaki tudományos közlemények 7. 323–326. https://doi.org/10.33895/mtk-2017.07.73

Nyikes, Z. (2019). *A Közép-Kelet európai generációk digitális kompetencia és biztonságtudatosság vizsgálatának eredményei.* PhD értekezés. Óbudai Egyetem, Biztonságtudományi Doktori Iskola.

Oroszi, E. D. (2020). Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasználó támadási technikák és megelőzésük. *Dunakavics, 8*(5), 5–20.

Palicz, T., Bencsik, B. & Szócska, M. (2021). Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai. *Scientia et Securitas, 2*(1), 78–87. https://doi.org/10.1556/112.2021.00001

Sasse, M. & Flechais, I. (2005). Usable Security: Why Do We Need It? How Do We Get It? In Cranor, L. F. & S. Garfinkel (Eds.), *Security and Usability* (pp. 13–30). O'Reilly Publishing.

Shappie, A. T., Dawson, C. A. & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media, 9*(4), 475–480. https://doi.org/10.1037/ppm0000247

Szabó, H. (2021). Kiberbiztonság a koronavírus-járvány idején – a COVID-19 nemzetbiztonsági aspektusai. *Rendvédelem, 10*(1), 52–70.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F. & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems,* 1–20. https://doi.org/10.1080/08874417.2020.1712269

A cikkben található online hivatkozások

URL1: *A hálózati és információs rendszerek biztonságára vonatkozó Stratégia végrehajtásának 2020-2022. évekre vonatkozó intézkedési terve*. https://2015-2019.kormany.hu/download/3/6d/b1000/Int%C3%A9zked%C3%A9si%20terv%202020-2022.pdf#!DocumentBrowse

URL2: *EUSurvey*. https://ec.europa.eu/eusurvey/home/welcome

Alkalmazott jogszabályok

1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról

A cikk APA szabály szerinti hivatkozása

Palicz T., Bonnyai T., Bencsik B., Pintér L., Hornyik Zs., Joó T., Bor O. & Dombrádi V. (2022). Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei. *Belügyi Szemle*, *70*(2), 395–418. https://doi.org/10.38146/BSZ.2022.2.11