Habók Lilla
üzleti elemző
Enelis Informatikai Zrt.
habok.lilla@gmail.com

Az információbiztonsági tudatosság mérése-értékelése Bloom-taxonómiával

Kutatási eredmények gazdasági szervezetek dolgozói körében

Measuring and evaluating information security awareness with Bloom's Taxonomy

Research findings among employees of economic organizations

Abstract

Raising awareness of information security can help economic organizations keep their information more secure and prevent employees from exposing information to attackers without intention. But how can we measure how aware the organization's employees are? What areas do they still need to train? The measurement and development can be facilitated by Bloom's taxonomy. It is widely used in the field of education and describes learners' progress through a pyramid of interdependent levels. Information security experts have previously suggested the use of the Bloom taxonomy in the field, but so far there has been no publication on measurement results. The research surveyed 220 employees from economic organizations in questionnaire form, measuring their knowledge on cognitive levels, as well as on the affective domain, which has been given less weight in information security research so far. Affective levels can help determine the users' emotions and how well information security is integrated into their value system. Do they recognize the problems but are unwilling to deal with them? Or are they interested in the topic but lack sufficient knowledge about it? The study presents in detail the results of the cognitive and affective levels achieved by the respondents, such as how familiar they are with types of electronic information security, whether they can recognize a fake tax authority website, or how often they read about current security issues and discuss them with their contacts. Furthermore, the results reveal whether information security knowledge is correlated with age or IT work. With the help of these results, professionals working on information security awareness can get guidance on how to design their training programs, what kind of knowledge assessment tools to use, and which areas require training for users based on the current survey.
Keywords: information security, social engineering, Bloom's Taxonomy

Absztrakt

Az információbiztonság tudatosításával érhető el a gazdasági szervezetek számára, hogy az információik nagyobb biztonságban legyenek, és a munkavállalók ne szolgáltassák ki azt óvatlanul a támadóknak. De vajon hogyan mérhető, hogy a szervezetnél dolgozók mennyire tudatosak, és milyen területen lenne még szükségük képzésre? A mérésre, valamint az erre épülő fejlesztésre nyújt lehetőséget a neveléstudomány területén elterjedt Bloom taxonómia-rendszer, amely piramis-szerűen egymásra épülő szintek formájában írja le a tanuló haladását. Az információbiztonság szakértői már korábban is tettek javaslatot a Bloom taxonómia-rendszer használatára a területen, de ez idáig nem készült publikáció a témával kapcsolatos mérési eredményekről. A kutatás kérdőíves formában 220 gazdasági szervezetnél dolgozót mért fel, egyrészt a kognitív területen, vagyis az információbiztonsági tudásuk mérésére alkalmas szinteken, másrészt az affektív tartományban, amely a kutatásokban eddig sokkal kisebb súllyal szerepelt. Az affektív szintek segítségével a felhasználók érzelmei határozhatók meg, hogy mennyire épült be az információbiztonság az értékrendszerükbe. Ismerik a problémákat, de nem szívesen foglalkoznak vele? Vagy éppenséggel érdekelné őket a téma, de nincs arról elegendő ismeretük? A tanulmány részletesen bemutatja a válaszadók kognitív és affektív szinteken elért eredményeit, hogy például mennyire vannak tisztában az elektronikus információbiztonság típusaival, felismernek-e egy hamis NAV weboldalt, vagy hogy mennyire szoktak az aktuális biztonsági problémákról olvasni, és megbeszélik-e ezt ismerőseikkel. Továbbá az eredményekből kiderül, hogy az információbiztonsági tudás összefüggésben áll-e az életkorral vagy az informatikai munkával. Az eredmények segítségével az információbiztonsági tudatosítással foglalkozó szakemberek támpontot kapnak a képzéseik összeállításához, hogy milyen tudásfelmérő eszközt használhatnak, és jelen felmérés szerint milyen területeken szükséges a felhasználók képzése.
Kulcsszavak: információbiztonság, social engineering, Bloom taxonómia-rendszer

Bevezetés

Hogyan lehet felmérni a felhasználók információbiztonsági tudását és tudatosságát, amire célzott tudatosító programok építhetők? A tanulmánnyal ebben a témakörben teszek javaslatot, elsősorban a gazdasági szervezetekben az információbiztonság oktatással foglalkozók számára. Kutatásom a Budapesti Metropolitan Egyetem Executive MBA for IT képzése keretében készült, amelynek szakdolgozatát a korábbi, Digitális Állampolgárság területén végzett kutatásainkra építettem (OLLÉ ET AL, 2013).

A vizsgálathoz a DÁ-modell mintájára a kibővített Bloom taxonómia-rendszert (ANDERSON–KATHWOHL, 2001) használtam fel, ezúttal kifejezetten az információbiztonság tudatosítás területére fókuszálva. A módszer relevanciáját mutatja, hogy több információbiztonsági szakcikk követendő mintaként említette a Bloom modelljének használatát az információbiztonság tudatosítás területén (pl. VAN NIEKERK–VON SOLMS, 2013; RAMSOONDER ET AL, 2020; WHITE, 2024), azonban nem találtam példát, hogy más kutató erre a rendszerre épített volna információbiztonság tudatosság mérő kérdőíves vizsgálatot, így ebben jelen kutatás az első.

Az információk biztonságának megőrzése minden korban fontos feladat volt, de a téma jelentőségét adja, hogy manapság az internet segítségével könnyen megoszthatók információink, ezáltal a támadók nagy mennyiségben hozzáférhetnek az információkhoz. Ha pedig a gazdasági szervezetek dolgozói nem elég elővigyázatosak, akkor könnyű célpontot, támadási felületet adhatnak a rosszindulatú aktoroknak. Ez pedig nem csak saját információik megőrzésére jelent veszélyt, hanem az egész gazdasági szervezetre vonatkozóan is. Fontos tehát felmérni és fejleszteni a dolgozók információbiztonsági tudását.

Hipotézisek

Kutatási kérdés: Hogyan lehet a Bloom taxonómia-rendszert felhasználni az információbiztonsági tudatossági (kognitív) és viszonyulási (affektív) szint értékelésére?

A kutatási kérdés megválaszolásához a következő hipotéziseket fogalmaztam meg:

- *H1:* A gazdasági szervezetek dolgozói alapvetően nyitottak az információbiztonsági területre (magas affektív szint), de a gyakorlatban keveset tesznek a tudatosság növeléséért (alacsony kognitív szint).
- *H2:* Az információbiztonság tudatosság szintje nem életkorfüggő.
- *H3:* Közép- és nagyvállalatoknál gyakoribb az információbiztonsági tudatosság növelésére irányuló tevékenység, mint kisvállalatoknál.
- *H4:* Informatikai munkakörökben magasabb az információbiztonság tudatossági szint, mint más foglalkozások esetében.
- *H5:* Az elektronikus információbiztonsági területek közül a megtévesztésen alapuló csalás az egyik legkevésbé ismert terület.

Módszer bemutatása

A hipotézisek elfogadhatóságának megállapításához kérdőíves módszert használtam. A kérdőív 2023.03.03. és 2023.04.03. között volt kitölthető, összesen 15 kérdést tartalmazott Google Formban. A kérdőív terjesztését elsősorban saját kapcsolati hálómban végeztem a gazdasági szervezeteknél dolgozó ismerősök direkt megkeresésével, továbbá ismerőseimet megkértem, hogy a kérdőívet továbbítsák saját munkatársaik és releváns kapcsolati hálójuk körében. A kérdőívet így a rendelkezésre álló egy hónapos intervallum alatt 220 fő töltötte ki.

A kérdéssor nem tartalmazott kötelezően, sem szövegesen megválaszolandó kérdéseket, a kitöltés nagyjából 5-15 percet vett igénybe. Valószínűleg az említett tényezők következtében kérdésenként magas volt a válaszadási arány. A legtöbb esetben mind a 220 fő választ adott a kérdésekre, a legkisebb arányban megválaszolt kérdésnél is 216 fő adott választ. Az eredmények bemutatásában jelzem a kitöltők arányát kérdésenként.

A kérdőív tartalmi felépítését a hipotézisek alapján a következőképp határoztam meg.

- A demográfiai változók közt találhatók:
  - 1. kérdés – Életkor: az életkori csoportok meghatározásához a generációs elméletet használtam: Baby Boom, X, Y, Z generáció (DIMOCK, 2019).
  - 2. kérdés – Munkakör: a munkakör szempontjából arra voltam kíváncsi, hogy a kérdőív kitöltő saját bevallása szerint informatikai területen dolgozik-e, vagy ettől eltérő munkakörben.
- Gazdasági szervezetre vonatkozó információk:
  - 3. kérdés – Cégméret: a cégméret meghatározásához a makro-, kis-, közép- és nagyvállalati kategóriákat használtam fel.
  - 4. kérdés – Céges információbiztonság tudatosító kezdeményezések: az információbiztonsági tudatosság növelésére irányuló tevékenységek közül több választós felsorolásból lehetett választani.
- 5-10. kérdés – Tudatossági szintre vonatkozó kérdések Bloom taxonómia-rendszere alapján: minden Bloom tudatossági szinthez, a szintnek megfelelő feladatot készítettem.

Az *1. táblázatban* jelöltem, hogy melyik szinten összesen mennyi pontot lehetett elérni. Az összesített pontszám megadja, hogy a kérdőív kitöltői milyen Bloom kognitív szinten állnak egymáshoz viszonyítva információbiztonság témában. A Bloom kognitív szinten összesen 15 pont volt elérhető a kérdőívben.

Bloom szint	**Bloom kognitív szinthez kapcsolódó feladat**	**Max. pont**
Emlékezés	Jelölje be az alábbi felsorolásban, hogy melyek tartoznak az elektronikus információbiztonsági problémák típusai közé! (Több választ is bejelölhet.) (Adathalászat, zsarolóvírus, irodai betörés, kéretlen levél, DDoS támadás, adathordozó lopás (pl. iratok))	4 – az 1., 2., 4., 5. lehetőség bejelölése ér pontot
Megértés	Válassza ki az alábbi felsorolásból, hogy a definíció melyikre vonatkozik: *„a bűnelkövető megbízható személynek vagy szervezetnek adja ki magát annak érdekében, hogy bizalmas információkat csaljon ki az áldozattól” (ESET, s.a.).*	1 – ha az adathalászatot választotta
Alkalmazás	Az alábbi állításokkal kapcsolatban jelölje 1–4 skálán, hogy mennyire jellemző az internetes tevékenységére (1 – egyáltalán nem, 2 – inkább nem, 3 – inkább igen, 4 – teljes mértékben): • Kétfaktoros azonosítást használok. • Képeket osztok meg az életemről az interneten. • Beállítom, hogy ki láthatja a bejegyzéseimet a közösségi oldalon. • Az alapján döntök egy mobilalkalmazás használatáról, hogy az milyen hozzáféréseket kér.	4 – minden kérdésben 1 pont jár. Az 1., 3., 4. állítás esetében az inkább igen és teljes mértékben lehetőségre. A 2. állításnál az egyáltalán nem és inkább nem lehetőségre.
Elemzés	A képen látható oldal hamis vagy valódi a megítélése szerint?[1]	1 – ha a „hamis”-t választotta
Kiértékelés	Melyik wifire csatlakozna a felsoroltak közül, ha az alábbi lehetőségek állnának rendelkezésére egy nyilvános helyen? • Gyorséttermi wifire, ami beleegyezést kér. • Hotel wifire, aminél jelszót kell megadni. • Arra, ami semmilyen jelszót/beleegyezést nem kér, mert az a legegyszerűbb. • Egyikre sem, inkább a saját mobilnetem használom.	1 – csak az utolsó válasz ér pontot
Létrehozás	Milyen formában hozott létre tartalmat az információbiztonsággal kapcsolatban az elmúlt 1 évben? (Több választ is bejelölhet.) (Előadás tartás, Cikk/Blogbejegyzés írás, Podcast létrehozás, Egyéb, Nem hoztam létre ilyen tartalmat)	4 – Minden válasz pontot ér, az utolsó kivételével

1. táblázat
Saját mérőeszköz Bloom kognitív területén: feladatok és pontszámok
(Forrás: saját szerkesztés)

[1] A kérdőívben szereplő kép forrása: Nemzeti Kibervédelmi Intézet, 2020.01.14.

- 11-15. kérdés – Érdeklődési szintre vonatkozó kérdések Bloom taxonómia-rendszere alapján: minden Bloom tudatossági szinthez, a szintnek megfelelő feladatot készítettem. A *2. táblázatban* jelöltem, hogy melyik szinten összesen mennyi pontot lehetett elérni. Az összesített pontszám megadja, hogy a kérdőív kitöltői milyen Bloom affektív szinten állnak egymáshoz viszonyítva információbiztonság témában. A Bloom affektív szinten összesen 16 pont volt elérhető a kérdőívben.

Bloom szint	**Bloom affektív szinthez kapcsolódó feladat**	**Max. pont**
Befogadás	Milyen forrásokból tájékozódik az információbiztonsági hírekről? (Több választ is bejelölhet.) (Konferencia/meetup előadásokat hallgatok, Cikkeket/Blogbejegyzéseket olvasok, Podcastot hallgatok a témában, Egyéb, Nem foglalkozom a témával)	4 – Minden válasz pontot ér, az utolsó kivételével
Reagálás	Milyen rendszerességgel ellenőrzi a megfelelő oldalakon (pl. https://haveibeenpwned.com/), hogy kiszivárgott-e a jelszava? (Legalább hetente, Havonta, Félévente, Évente, Soha)	4 – Gyakoriság alapján csökkenő pont
Értékelés	Jelölje az alábbi skálán, mi állna közelebb a reakciójához a következő helyzetben: Ismerőse elmondja, hogy törölte magát a Twitterről egy közelmúltbeli adatszivárgás miatt, amelyben az ő adatai is kiszivárogtak. (Túlzónak találom, más megoldást is találhatott volna / Teljesen megértem, én is így tettem volna)	1 – ha az 5 fokú skálán 4., 5. értéket választott
Érték-szerveződés	Milyen rendszerességgel beszél ismerőseivel az aktuális elektronikus információbiztonsági problémákról, pl. vírusok, adatlopás? (Legalább hetente, Havonta, Félévente, Évente, Soha)	4 – Gyakoriság alapján csökkenő pont
Érték alapú viselkedés	Hány alkalommal jelentett be gyanús e-mailt munkahelyén a céges IT biztonsági felelős számára az elmúlt 1 évben? (0, 1-2, 3-4, 5+)	3 – Gyakoriság alapján csökkenő pont

2. táblázat
Saját mérőeszköz Bloom affektív területén: feladatok és pontszámok
(Forrás: saját szerkesztés)

A kérdőívet annak figyelembevételével állítottam össze, hogy az egyes Bloom szintek külön-külön is elemezhetőek legyenek, továbbá kognitív és affektív területenként összesítve, valamint ezek kombinációjával egy Bloom összesített átlagban is. A hipotézisek elfogadását vagy elutasítását pedig demográfiai és szervezeti változók, valamint a Bloom taxonómiához kapcsolódó különböző összesített eredmények támogatják, amelyekhez a hipotézisek elemzése során szórást, korrelációszámítást, kereszttábla-elemzést és varianciaanalízist is használok a statisztikai módszerek közül.

A kutatási eredmények

A fejezetben részletezem az információbiztonság tudatosságot felmérő kérdőívem eredményeit 220 fő kitöltése alapján. Az első alfejezetben leíró statisztikai módszerrel elemzem a demográfiai és gazdasági szervezetekre vonatkozó adatokat, továbbá az egyes Bloom kognitív és

affektív szintek eredményeit. Az alfejezet választ ad arra kérdésre, hogy a kérdőív alapján kirajzolódik-e Bloom piramisa, vagy bizonyos szinteken a kérdéssor további fejlesztése szükséges, ha azt tudatosság felmérésre szeretnénk használni.

A második alfejezetben a hipotézisek mentén elemzem az eredményeket összetettebb statisztikai módszerekkel, hogy választ kapjak a kutatási kérdésemre. A számításokat Excel függvények és az Excelbe beépített Analysis Tool Pak segítségével végeztem el.

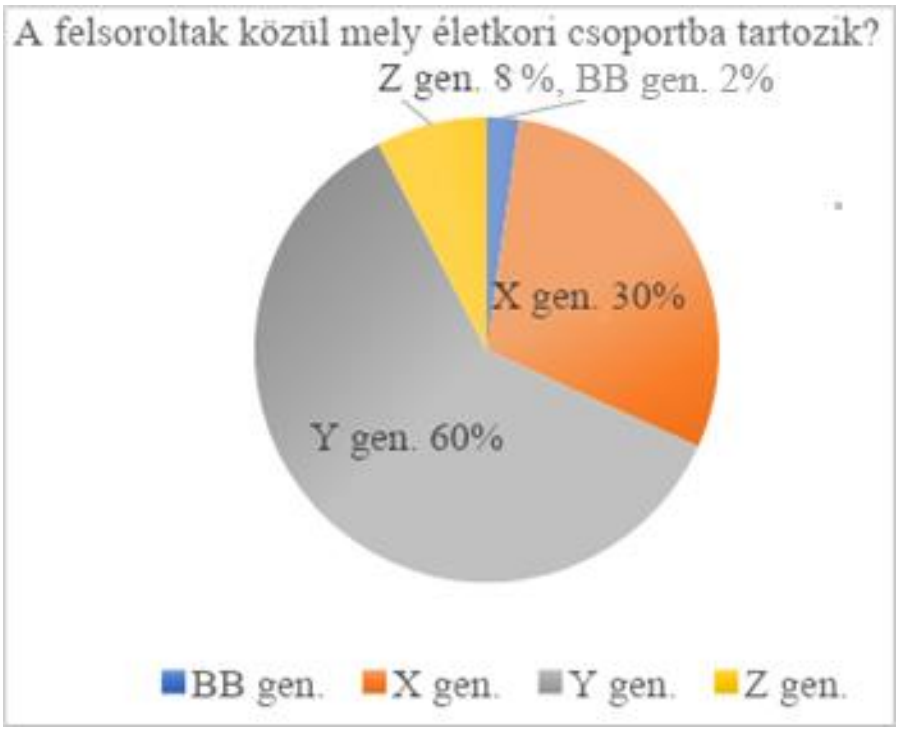
Az eredmények bemutatása leíró statisztikai módszerrel

Az alfejezetben a kérdőívben szereplő kérdésenként elemzem az információbiztonság tudatossági felmérő eredményeit. Minden esetben feltüntetem, hogy melyik kérdésben a válaszadók hány százaléka választotta az adott választ. Továbbá, hogy a Bloom szintekkel kapcsolatban a válasz pontot érő vagy pontot nem érő megoldásnak számít, ami alapján összesítem kognitív és affektív részenként, valamint a teljes Bloom eredményre vonatkozóan a pontokat.

A demográfiai változók

A hipotézisem alapján összesen két demográfiai változó vizsgálatára volt szükség a kérdőívben, az életkorral és a munkakörrel kapcsolatban. Az életkor esetében az információbiztonsági területen megszokott Baby Boom, X, Y, Z generációs csoportosítást használtam Dimock (2019) felosztása alapján (*1. diagram*).

Az életkoráról mind a 220 fő nyilatkozott, így megállapítható, hogy a kitöltők 2,27 százaléka tartozik a Baby Boom generációba (59 éves vagy idősebb), 29,55 százalék az X generációba (43-58 éves), a legtöbben az Y generációhoz (27-42 éves) tartoznak 60,45 százalékkal, míg a legfiatalabb munkavállaló Z generációs korosztályból (26 éves vagy fiatalabb) 7,73 százalék adott választ.



1. diagram
A kérdőív kitöltőinek életkori eloszlása (n=220)
(Forrás: saját szerkesztés)

Fontos megjegyezni, hogy a kérdőív csak a gazdasági szervezetekben dolgozó munkavállalókat vizsgálta. Ezzel a szűkítéssel nem találtam elfogadható reprezentatív adatot a korcsoportokra vonatkozóan. A Központi Statisztikai Hivatal (2023.03.24.) foglalkoztatottságra vonatkozó 2023. februári adatai alapján viszonyíthatjuk részlegesen az adatokat, de a KSH más életkori csoportosítást használ, amely szerint a 4,58 milliós foglalkoztatotti szám 16,6 százalékát képezi az 55-64 éves idősebb korosztály, míg 77,4 százalékát a 25-54 éves korcsoport, végül 5,9 százalékát a 15-24 éves munkavállalók. Ezek alapján a saját kérdőívemben az idősebb munkavállalók csoportja alulreprezentált lehet, de ezt befolyásolja, hogy a kérdőívben a Baby Boom generáció még idősebb korosztályt jelent, mint amivel a KSH számol.

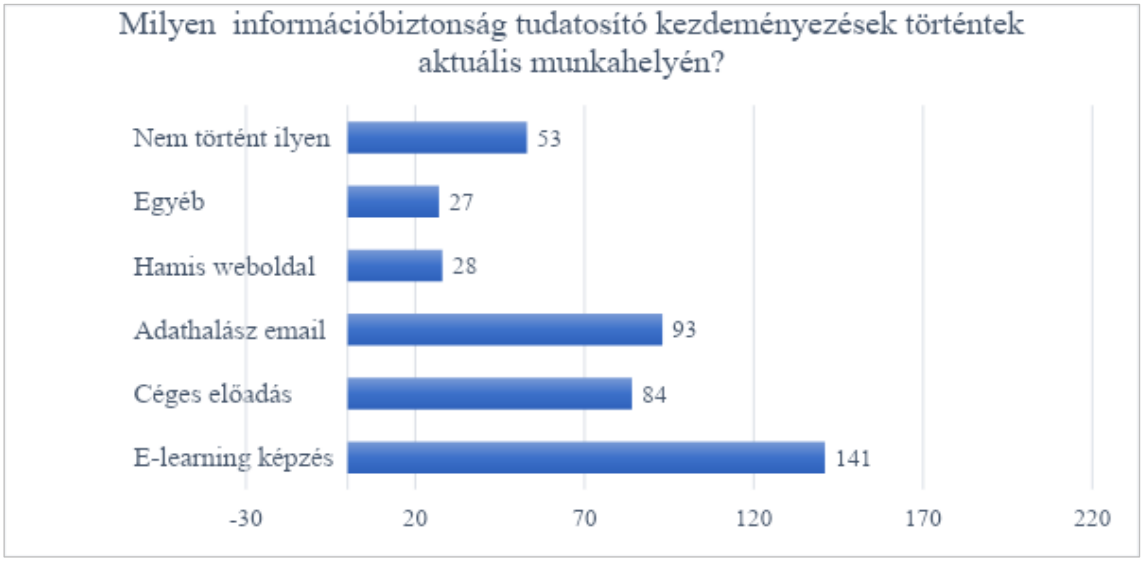
A kérdőív másik demográfiai kérdése a munkakörre vonatkozott, és ezen belül is az informatikusként dolgozók kiemelésére. A kérdés 217 kitöltőjének 29 százaléka dolgozik informatikai területen, míg 71 százalék valamely más területen. Az Eurostat 2020-as adatai alapján (hivatkozza: CSATH, 2022.04.13.) Magyarországon a foglalkoztatottak 3,8 százaléka dolgozik informatikai munkakörben. Így elmondható, hogy az információbiztonság tudatosság kérdőív kitöltői között felülreprezentált az informatikusok száma, amelyet az ismerősi körben történő mintavétel okoz.

Gazdasági szervezetek változói

A kitöltők munkahelyére, azaz a gazdasági szervezetekre vonatkozóan szintén két kérdés jelent meg a kérdőívben, a cégmérettel és a céges információbiztonság tudatosító kezdeményezésekkel kapcsolatban.

A cégmérettel kapcsolatos kérdésre 218 fő adott választ, akiknek 11,47 százaléka dolgozik makrovállalatnál, továbbá 12,84 százalékuk kisvállalatnál, míg 23,85 százalékuk középvállalatnál és végül 51,83 százalékuk nagyvállalatnál. A KSH 2021-es adatai alapján (KSH, 2022.11.15.) a kérdőívemben elért aránynál jóval magasabb (39,54%) a mikrovállalatoknál és valamivel magasabb a kisvállalkozásoknál dolgozók aránya (17,58%), viszont alacsonyabb a középvállalatoknál (11,46%) és nagyvállalatoknál (31,42%) dolgozóké. A kérdőív eredményeinek értékelésekor figyelembe kell venni ezt az eltérést.

A válaszadókat a cégen belüli információbiztonság tudatosító kezdeményezések típusával kapcsolatban is megkérdeztem, amelyre mind a 220 kitöltőtől érkezett válasz (*2. diagram*). Ezek alapján a cégek közel negyedénél (24,09%) nem végeztek még semmilyen jellegű tudatosítást. Szintén nagyjából ekkora arányban történt egy (22,73%), két (22,73%) vagy háromféle (21,36%) típusú tudatosító kezdeményezés ebben a témában, csak 8,18 százaléknál 4 és 0,91 százaléknál 5 különböző formában.



2. diagram
Információbiztonság tudatosító kezdeményezések típusai a válaszadók munkahelyén, többes választási lehetőséggel (n= 220)
(Forrás: saját szerkesztés)

Méghozzá a tudatosítás típusai közül a legnépszerűbb az e-learning képzés, a megkérdezettek közül 141 fő (64,09%) munkahelyén történt már ilyen. Céges előadást 84 fő (38,18%) munkahelyén tartottak. Egészen magas arányt ért el az a lehetőség, hogy a cég adathalász e-mailt küldött a dolgozók tudatosságának tesztelésére, amit 93-an is bejelöltek (42,27%), viszont hamis weboldalt ebből a célból már jóval kevesebb cég hozott létre, ezt 28 fő jelölte be (12,73%). Végül egy Egyéb lehetőséget is feltüntettem, amit 27 fő jelölt (12,27%), de ehhez szöveges válasz nem kapcsolódott, mivel nem a kutatási kérdés szoros részét képezi az összes lehetséges típus megadása.

A Bloom kognitív terület eredményei

A Bloom taxonómia-rendszer kognitív területén 6 szint található, amelyhez a kérdőívben 6 kérdés kapcsolódott, az *Alkalmazás* szint esetében alkérdésekkel. Az alfejezetben részletezem, hogy a válaszadók melyik szinten milyen válaszokat adtak, és ez a Bloom-alapú felmérés szempontjából hány pontnak felel meg az elemzésben.

Emlékezés szintje

Az első szinten az *Emlékezés* jelenik meg, melynek kapcsán 6 információbiztonsági területet soroltam fel a kérdőívben, és kértem a felhasználókat, hogy jelöljék közülük az elektronikus információbiztonsági területeket. Az elektronikus típusú fenyegetések közé a következők tartoznak a listából: adathalászat, zsarolóvírus, kéretlen levél (spam), DDoS támadás, míg kettő a hagyományos fenyegetések része: irodai betörés, adathordozó lopás (pl. iratok).

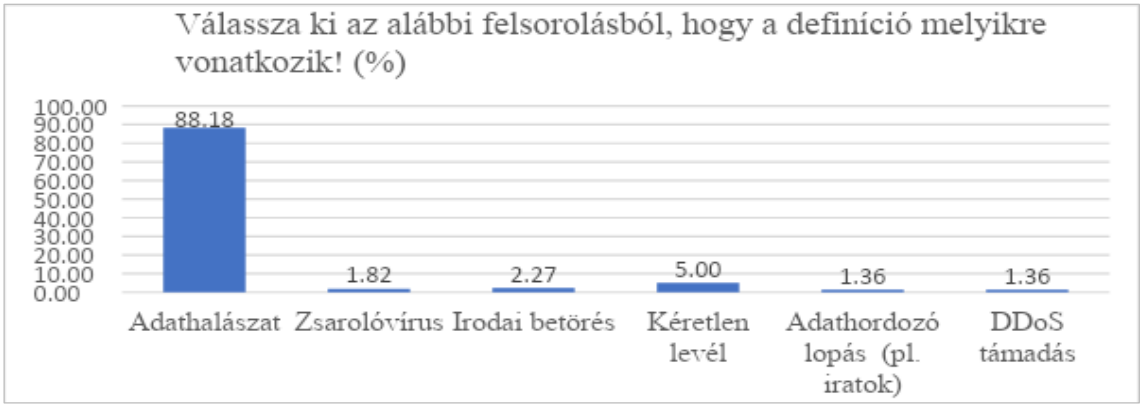
A kitöltők közül csak 1 fő volt (0,46%), aki egyik típust sem jelölte megfelelően, így 0 pontot ért el. További 12 fő (5,48%) csak 1 pontot kapott, 52 fő (23,74%) pedig 2 pontot. A legtöbben 3 pontot szereztek, azaz 86 fő (39,27%), és egészen sokan, 68 fő (31,05%) jelölte mind a 4 kategóriát helyesen (*3. diagram*). Ez esetben nem alkalmaztam levonást a helytelen válaszokért.

3. diagram
Az Emlékezés szintjén a megadott típusok elektronikus információbiztonság típusként való kiválasztások száma (n=219)
(Forrás: saját szerkesztés)

Legtöbben az adathalászatot ismerték fel az elektronikus információbiztonsági kockázatok közül (98,17%), ami pozitívum a megtévesztésen alapuló csalás ismerete szempontjából. Szintén sokan jelölték a zsarolóvírusokat (88,13%), de a DDoS támadást már ennél kevesebben (58,9%). Utóbbival kapcsolatban volt olyan kitöltő, aki privát üzenetben érdeklődött erről a típusról. Ebből is lehet arra következtetni, hogy valószínűleg ez kevésbé ismert, speciális információbiztonsági terület. A legkevesebben viszont a kéretlen leveleket jelölték be a területek közül, amelynek oka valószínűleg nem az, hogy a hagyományos levelekre gondoltak közben. A köztudatban a kéretlen levelek kevésbé az információbiztonsági kockázatok közt szerepelnek, pedig a legtöbb adathalászat ezekre vezethető vissza. A témáról több szakirodalom ír, amely szerint komolyan kell venni a fenyegetést (CORMACK, 2008), különösen Európa több országában, például Egyesült Királyság, Írország vagy Finnország (AMIN ET AL, 2021).

Megértés szintje

A második a kognitív területen belül a *Megértés* szintje, amelynek kapcsán az ESET (s.a.) adathalászati definíciója[2] alapján kértem a kitöltőket (az *Emlékezés* szintjén is használt típusok közül) a definícióhoz tartozó információbiztonsági típus kiválasztására (*4. diagram*).



4. diagram
A Megértés szintjén megadott definíció felismerésre adott válaszok aránya (%) (n=220)
(Forrás: saját szerkesztés)

[2] *„a bűnelkövető megbízható személynek vagy szervezetnek adja ki magát annak érdekében, hogy bizalmas információkat csaljon ki az áldozattól”*

A kitöltők 88,18 százaléka ismerte fel helyesen az adathalászat definícióját, a többi típus közt megoszlottak a százalékok. A kéretlen levelet a kitöltők 5 százaléka választotta, az irodai betörést 2,27 százalék, a zsarolóvírust 1,82 százalék, míg az adathordozó lopást és a DDoS támadást fej-fej mellett 1,36 százalék. Tehát a Megértés szintjén is a kitöltők nagy százaléka jó eredményt ért el az információbiztonság területén.

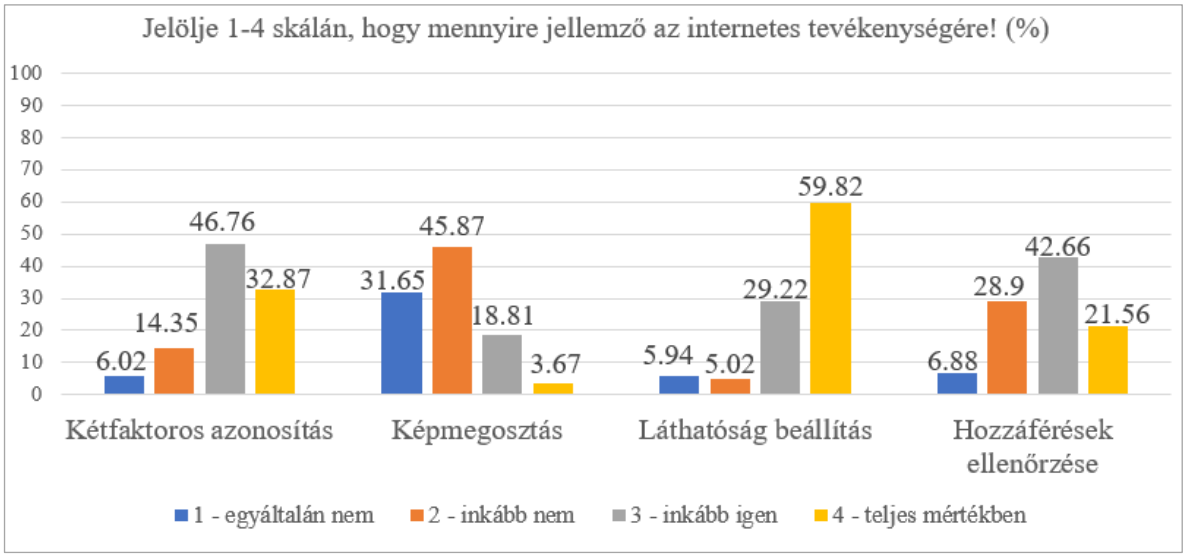
Alkalmazás szintje

Az *Alkalmazás* kognitív szintjén négy különböző állítással kapcsolatban kellett a kitöltőknek bejelölni 1-4 skálán, hogy mennyire jellemző rájuk (*5. diagram*). A skálán az 1-2 az egyáltalán nem vagy inkább nem állítást jelentette, míg a skála másik felén az inkább igen (3) és teljes mértékben (4) állítás szerepelt.

Az alkérdések közt megjelent a kétfaktoros azonosítás beállítása, képmegosztás az interneten, közösségi oldalakon a bejegyzések láthatóságának beállítása és az alkalmazások letöltésekor a hozzáférések figyelembevétele. Az 1., 3. és 4. alkérdésnél az inkább igen és a teljes mértékben ért pontot. Míg a 2. kérdésnél tudatosan megfordítottam az értékelést, így az egyáltalán nem és az inkább nem választásra adtam 1-1 pontot a Bloom szint értékelésekor.

A kétfaktoros azonosítást (n=216) a kérdőív kitöltői saját bevallásuk szerint jellemzően be szokták állítani, ha van erre lehetőségük. A többség a skálán a 3-as értéket választotta (46,76%), a második helyen pedig a skála 4-es értéke végzett (32,87%). Mindössze a válaszadók 20 százaléka nyilatkozott úgy, hogy jellemzően nem állítja be a kétfaktoros azonosítást.

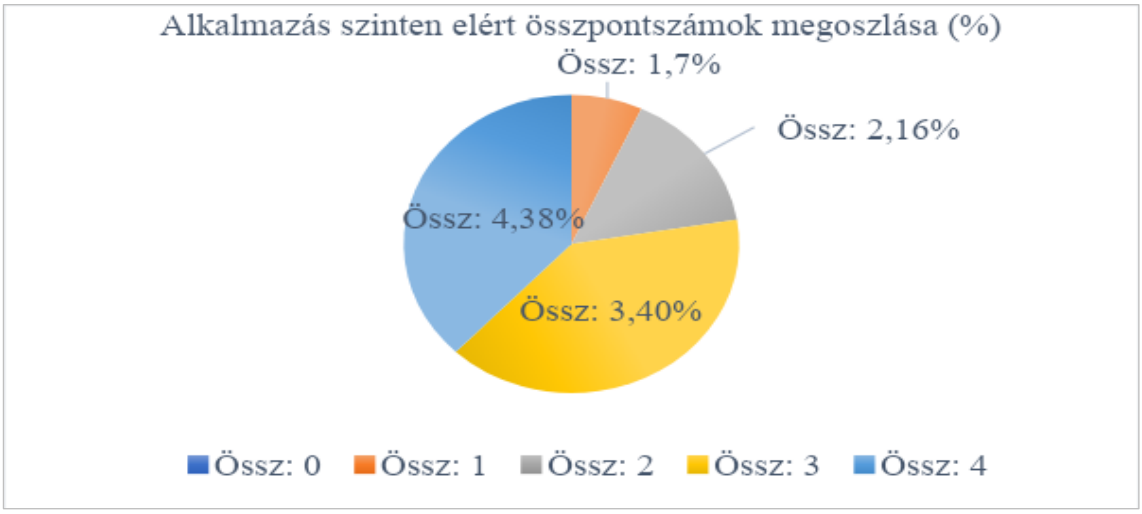
A képekkel kapcsolatban szintén a válaszadók (n=218) több mint háromnegyede gyűjtött pontot a Bloom szinten, ugyanis 45,87 százalékuk inkább nem és 31,65 százalékuk egyáltalán nem oszt meg az életéről képet a válasza alapján. Azaz alig több mint 22 százalék szokott képeket publikálni bármely internetes felületen.



5. diagram
Az Alkalmazás szintjén az alkérdésekre adott válaszok aránya (%)
(Forrás: saját szerkesztés)

A kitöltők (n=219) még az előző alkérdéseknél is nagyobb arányban kaptak pontot a közösségi oldalakon közzétett bejegyzéseik láthatóságának beállítására, mivel 59,82 százalékuk saját bevallása szerint szabályozza azt, és további 29,22 százalék is inkább figyelmet fordít rá. Alig több mint a válaszadók 10 százaléka nem veszi figyelembe a lehetőséget.

Végül a negyedik kérdés bizonyult a leginkább megosztónak (n=218), melyben arra kérdeztem rá, hogy az alkalmazások letöltésekor mennyire veszik figyelembe, hogy azok milyen engedélyeket kérnek. A legtöbben 42,66 százalékkal ebben az esetben is inkább figyelembe veszik ezt a szempontot, de csak 21,56 százalék dönt teljes mértékben ez alapján. Azonban 28,9 százalék jellemzően nem veszi figyelembe ezt a kérdést, és további 6,88 százalékot egyáltalán nem érdekel ez letöltéskor.

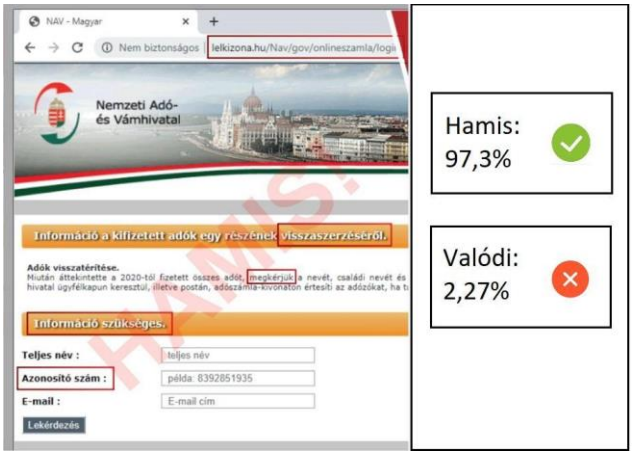


6. diagram
Az Alkalmazás szintjén elért összpontszámok megoszlása (%) (n=219)
(Forrás: saját szerkesztés)

Az *Alkalmazás* szint (n=219) összesítésében növekvő sor látható a 0-4 közt elérhető pontszámokban (*6. diagram*). Egyik kitöltő sem szerzett 0 pontot az alkérdésekre adott válaszai alapján és mindössze 6,86 százalék kapott 1 pontot, további 15,53 százalék pedig 2 pontot. A legtöbb válaszadó 3 pontot (39,73%) vagy 4 pontot (37,9%) kapott nagyjából hasonló arányban.

Elemzés szintje

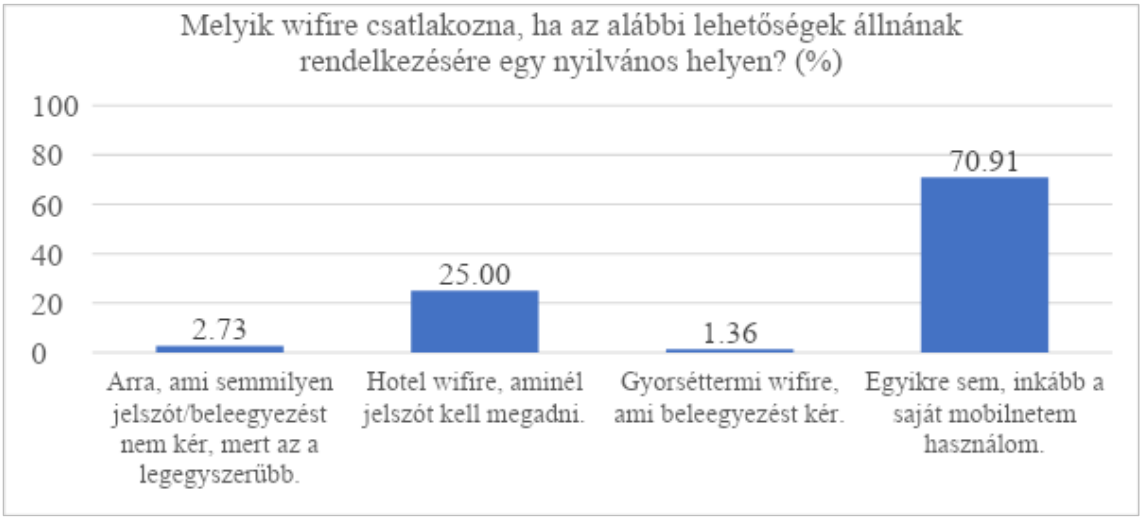
Az *Elemzés* szintjén egy hamis NAV weboldalról kellett a válaszadóknak felismerni, hogy a weboldal hamis vagy pedig valódi (*1. ábra*). A kitöltők (n=220) egészen magas aránya, meghozzá 97,73 százalék felismerte, hogy a képen hamis weboldalt lát, amelyre például az URL-cím és az oldal szövegezési stílusa utalt.



1. ábra
Az Elemzés szintjén mutatott hamis NAV weboldal
(Forrás: Nemzeti Kibervédelmi Intézet, 2020.01.14.)
a megoldás aránya (n=220) (Forrás: saját szerkesztés)

Kiértékelés szintje

A kognitív terület *Kiértékelés* szintjén a kérdőív kitöltőinek a felsorolt lehetőségek közül kellett kiválasztaniuk, hogy milyen WiFi hálózatra csatlakoznának (n=220). Pontot egyedül az a lehetőség ért, hogyha egyikre sem szeretnének csatlakozni, inkább a saját mobilnetüket használnák, amelyet a válaszadók 70,91 százaléka választott (*7. diagram*).

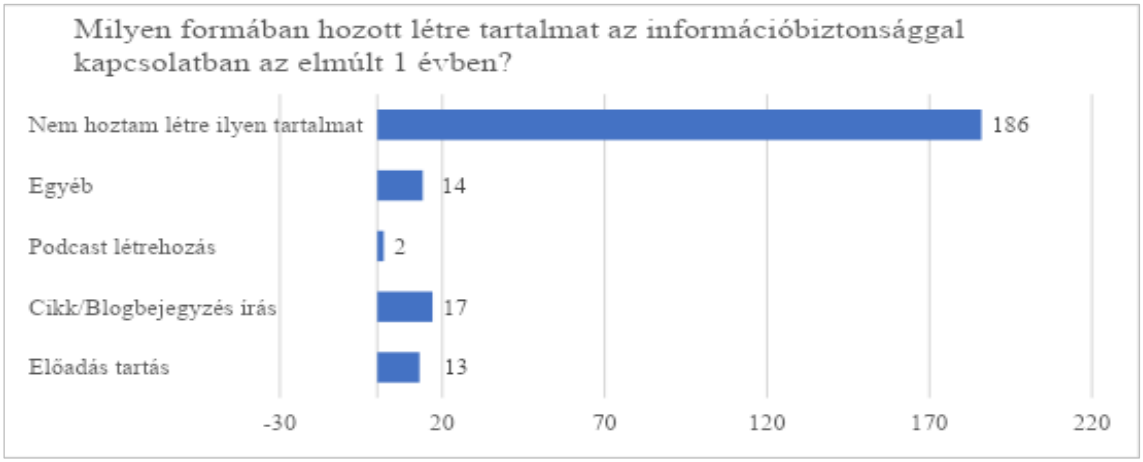


7. diagram
A Kiértékelés szintjén a WiFi-csatlakozással kapcsolatban adott válaszok megoszlása (%) (n=220)
(Forrás: saját szerkesztés)

A második leggyakoribb válasz, 25 százalékkal a hotel wifije volt, aminél jelszót kell megadni, így valóban biztonságosabb megoldás a következőknél, de ez sem teljesen biztonságos. A kérdőív kitöltőinek 2,73 százaléka belátta, hogy a semmilyen jelszót vagy beleegyezést nem kérő hálózatra csatlakozna, mert azt tartja a legegyszerűbbnek. Legutolsó helyen pedig a felhasználói beleegyezést kérő gyorséttermi wifi végzett 1,36 százalékkal.

Létrehozás szintje

A *Létrehozás* a legmagasabb a kognitív szintek közül, amelyen a felhasználók a saját tudásuk alapján mások számára is tudnak új tartalmat előállítani az adott területen. A kérdőív kitöltői (n=220) különböző lehetőségek közül választhattak, milyen formában készítettek már információbiztonsági tartalmat, úgy mint előadás tartás, cikk/blogbejegyzés írás, podcast létrehozás és egyéb. Ezek mindegyike 1-1 pontot ért a Bloom-szintek kiértékelésekor. Ezen a szinten a legmagasabb jelölési arányt a „nem hoztam létre ilyen tartalmat” válasz érte el 186 fő jelölésével (84,55%), a kiértékeléskor 0 pontszámmal, ami jól mutatja, hogy a Bloom-piramis legfelső szintjén már kevesek érnek el eredményt (*8. diagram*).



8. diagram
A Létrehozás szintjén adott válaszok száma a tartalomtípus-létrehozással kapcsolatban (n=220)
(Forrás: saját szerkesztés)

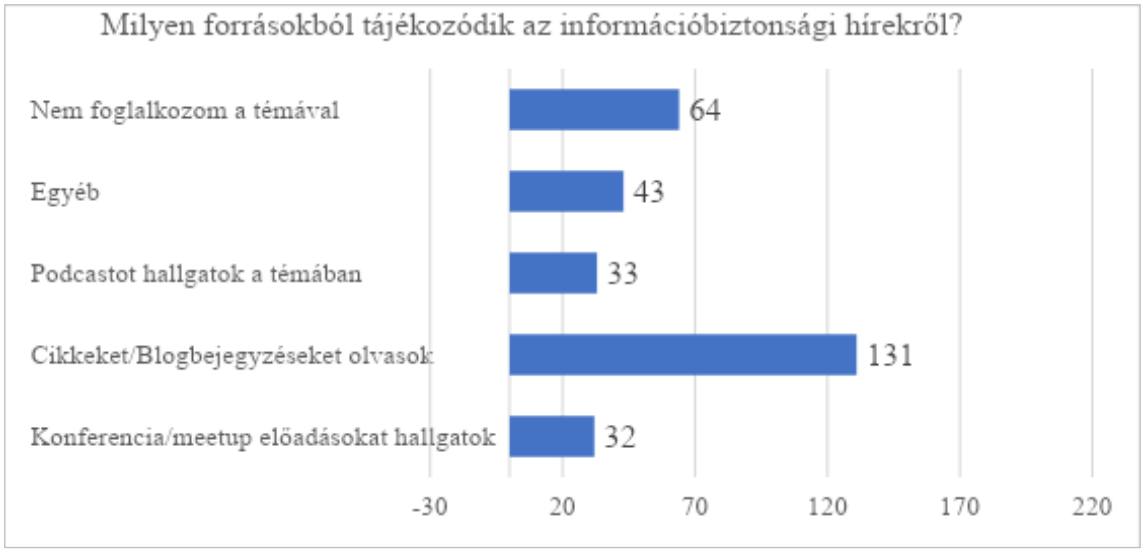
A válaszadások alapján 17 fő (7,73%) írt már cikket vagy blogbejegyzést az információbiztonság kapcsán, 13 fő (5,91%) tartott már előadást a témában, 2 fő (1%) hozott létre podcastot és 14 fő (6,36%) valamilyen egyéb formában is állított elő tartalmat.

Az összesített eredmény tekintetében tehát a *Létrehozás* Bloom-szinten 84,55 százalék nem ért el egyáltalán pontot. További 10,91 százalék 1-1 pontot gyűjtött a tartalom előállítással, mindössze 3,64 százalék ért el 2 pontot és csak 0,9 százalék (azaz 2 fő) kapott 3 pontot, de 4 pontot senki nem gyűjtött a kitöltők közül.

A Bloom affektív terület eredményei

A Bloom taxonómia-rendszer affektív területén 5 szint jelenik meg, amelyhez a kérdőívben öt kérdés kapcsolódott. Az alfejezetben részletezem, hogy a kérdőív kitöltői milyen válaszokat adtak az egyes szinteken, és ez mennyi pontnak felelt meg a válaszadók Bloom szintjének megállapításakor.

Befogadás szintje



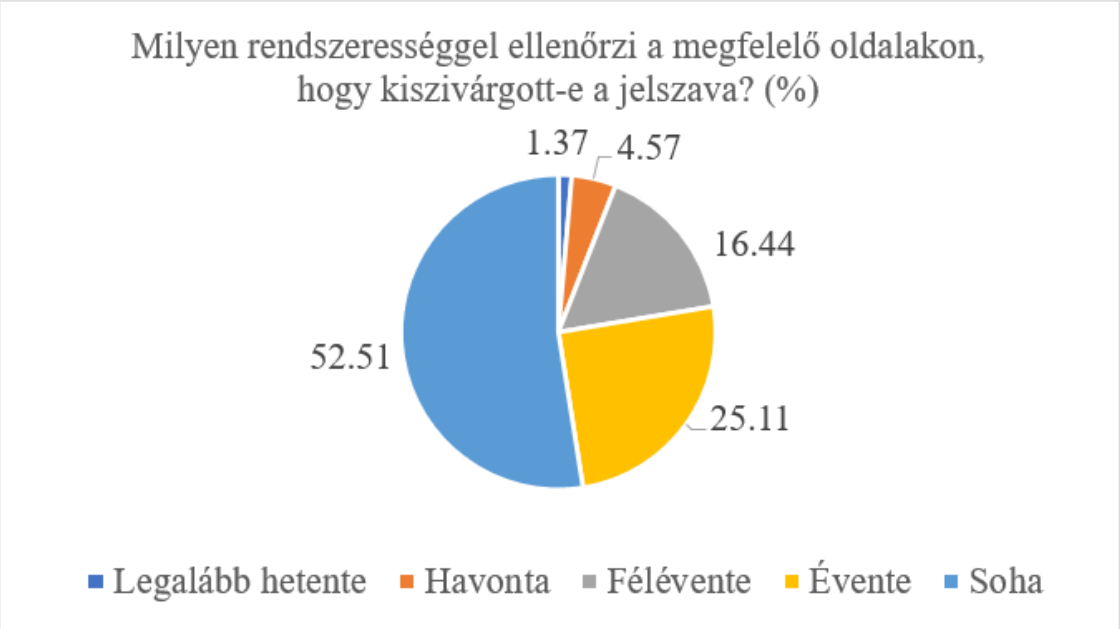
9. diagram
A Befogadás szintjén adott válaszok száma az információbiztonsági hírek fogyasztásával kapcsolatban (n=220)
(Forrás: saját szerkesztés)

A Bloom affektív terület *Befogadás* szintjén arra kerestem a választ, hogy a kérdőív kitöltői (n=220) mennyire nyitottak az információbiztonságról szóló tartalomfogyasztásra. Azaz szoktak-e a témáról előadást hallgatni (pl. konferencia, meetup formájában), olvasnak erről szóló cikkeket vagy blogbejegyzéseket, esetleg podcastot hallgatnak, vagy valamilyen egyéb formában informálódnak az információbiztonsági kérdésekről (*9. diagram*).

A válaszadók közül 64 fő (29,09%) jelezte, hogy egyáltalán nem foglalkozik a témával szabadidejében vagy munkájában, azaz egyik felsorolt tartalomfogyasztási típust sem tudta kiválasztani. Azok közül, akik befogadóak a témával kapcsolatban, a legtöbben (131 fő) cikket vagy blogbejegyzést szoktak olvasni, a második legnépszerűbb az egyéb kategória volt (43 fő) és csak ezt követte a podcast hallgatás (33 fő), majd végül a konferencia / meetup előadás hallgatás (32 fő). Feltételezésem szerint az arányok ettől eltértek volna a pandémia előtti időszakban, és nagyobb arányban választották volna a válaszadók a személyes előadásokat, de ez a kérdés nem szerepelt a hipotézisek között.

A Bloom taxonómia-rendszer kiértékelésekor 0 pontot kapott az a 29,09 százalék, akik semmilyen formában nem érdeklődnek az információbiztonsági hírek, trendek iránt. A kitöltők a legnagyobb arányban 1 pontot kaptak (44,09%), többségében, akik csak olvasni szoktak a témáról. Ennél sokkal kevesebben vannak (18,18%), akik 2 féle formában is fogyasztanak tartalmat, még kevesebben (6,36%) 3 féle formában. Végül csak 2,27 százalék (5 fő) jelölte mind a 4 típust, valószínűleg ők nem csak alkalmi szinten, hanem rendszeresen foglalkoznak az információbiztonsági területtel.

Reagálás szintje



10. diagram
A Reagálás szintjén adott válaszok aránya a jelszó kiszivárgás ellenőrzése kérdésre (%) (n=219)
(Forrás: saját szerkesztés)

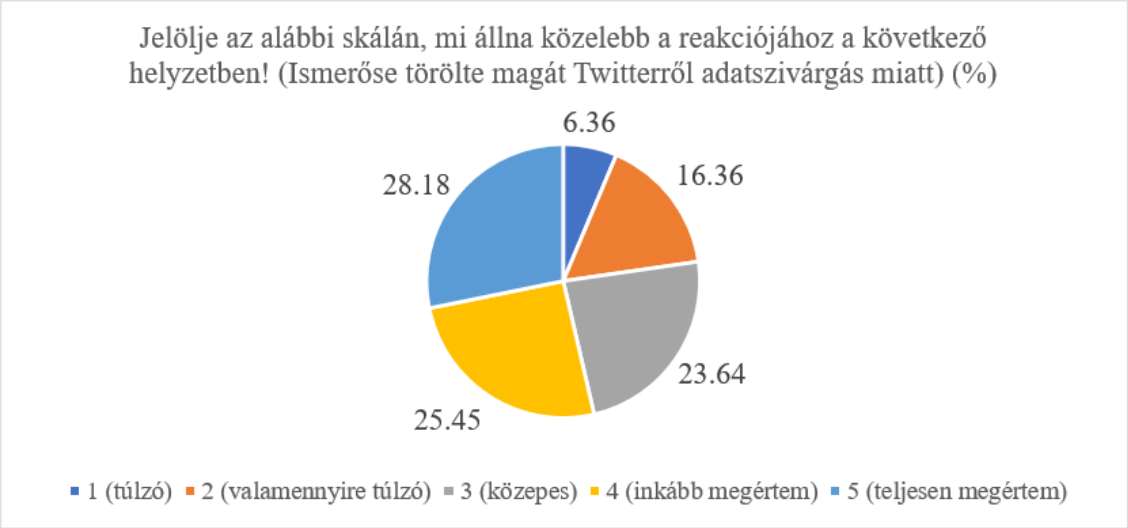
A *Reagálás* affektív szintjén arra voltam kíváncsi, hogy a válaszadók (n=219) egy konkrét elektronikus információbiztonsági területre hogyan reagálnak, azaz milyen gyakran ellenőrzik, hogy kiszivárgott-e a jelszavuk valamely aktuális adatszivárgás közben. Példaként jeleztem, hogy az ilyen ellenőrző oldalak közé tartozik a Have I Been Pwned (https://haveibeenpw

ned.com/), amellyel az informáltabbak számára konkretizáltam a kérdést, az információbiztonság területén kevéssé jártasokat pedig emlékeztettem az ilyen jellegű szolgáltatásokra.

A kérdésre meglepően magas arányban, több mint a kitöltők fele (55,51%) jelezte, hogy soha nem szokta ellenőrizni a hozzá tartozó jelszó kiszivárgását (*10. diagram*). Évente nagyjából a kitöltők negyede szokott (25,11%) erre gondolni, nagyjából félévente 16,44 százalékuk, havi szinten viszont már csak 4,57 százalék ellenőrzi jelszavának kiszivárgását, végül hetente már csak 1,37 százalék (3 fő). Az arány azért is tartható problémásnak, mivel a jelszó ellenőrzése csak egy első lépés a folyamatban, amit a jelszó megváltoztatásának kellene követni ilyen esetben. Feltételezhetnénk, hogy aki nem ellenőrzi a jelszó kiszivárgást, az magától is rendszeresen változtatja jelszavát, de a jelszókezeléssel kapcsolatos kutatások alapján ennek kicsi az esélye. Ennek megállapítása azonban nem jelen kutatás feladata.

Értékelés szintje

Az *Értékelés* szintjén egy szituációval kapcsolatban kérdeztem a kérdőív kitöltőit a véleményükről, hogyan értékelik az adott helyzetet: „Ismerőse elmondja, hogy törölte magát a Twitterről egy közelmúltbeli adatszivárgás miatt, amelyben az ő adatai is kiszivárogtak.” A választ 5 fokú skálán vártam a „túlzónak találom, más megoldást is találhatott volna” (1) és a „teljesen megértem, én is így tettem volna” (5) értékek között. A Bloom szintek értékelésekor a kérdésben az 4-es és az 5-ös jelölésre adtam 1-1 pontot a skálán, míg a többi érték 0 pontot kapott.



11. diagram
Az Értékelés szintjén adott válaszok aránya egy helyzet értékelésével kapcsolatban (%) (n=220)
(Forrás: saját szerkesztés)

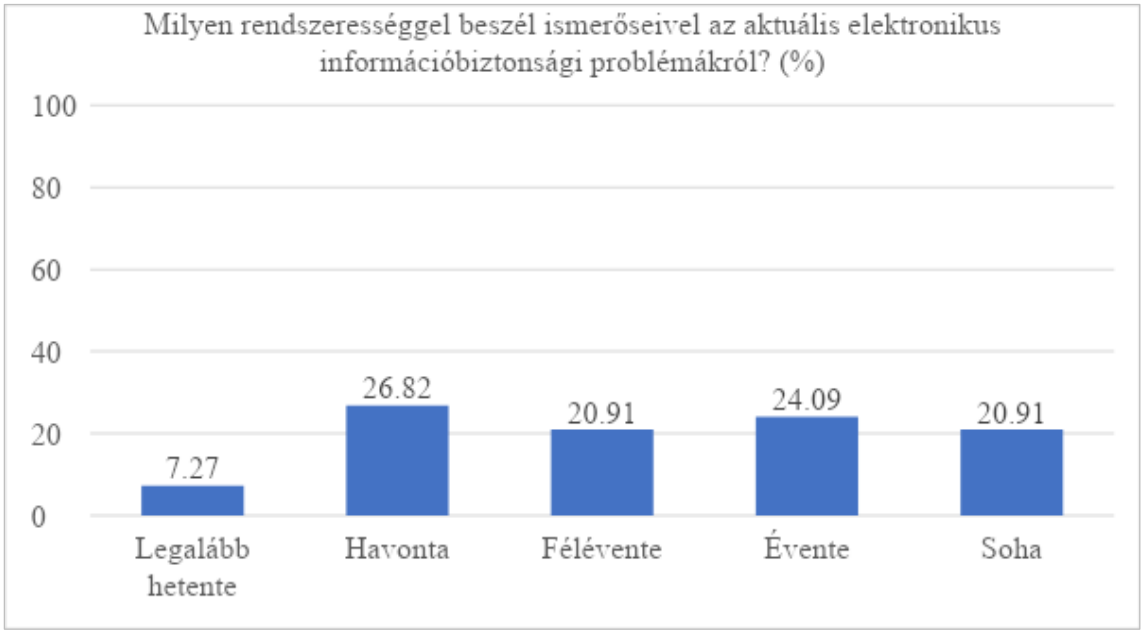
Így valamivel több mint a válaszadók fele, azaz 53,64 százaléka kapott pontot ezen a szinten, közülük 25,45 százalék jelölte a 4-es értéket, tehát inkább megérti a szituációt, míg 28,18 százalék teljesen egyetértett a szituációban szereplő döntéssel (*11. diagram*). Mindez egyébként annak tükrében érdekes eredményt jelent, hogy az előző kérdésre adott válaszok szerint a többség soha nem is szokta ellenőrizni a saját jelszava kiszivárgását, ennek következtében azt gondolhatnánk, hogy nem is jut el a szolgáltatásban a fiókja törléséig.

Azonban az Értékelés szintjén mindössze 6,36 százalék reakciója szerint túlzó viselkedés a fióktörlés egy adatszivárgást követően. További 16,36 százalék értékeli valamelyest túlzónak,

és a válaszadók közel negyede (23,64%) szerint közepes mértékű ez a reakció. Tehát összességében a válaszadók 46,36 százaléka nem kapott pontot ebben a kérdésben.

Értékszerveződés szintje

A Bloom affektív területen belül az *Értékszerveződés* szintjén egy gyakoriságra vonatkozó kérdésben kellett a kitöltőknek jelölni, hogy milyen rendszerességgel beszélnek ismerőseikkel az aktuális elektronikus információbiztonsági problémákról, például vírusokról vagy adatlopásról. A skálán a soha, évente, félévente, havonta és legalább hetente értékek szerepeltek. A Bloom szint értékelésekor a gyakoriság alapján nőtt a pontok száma 0-tól 4 pontig.

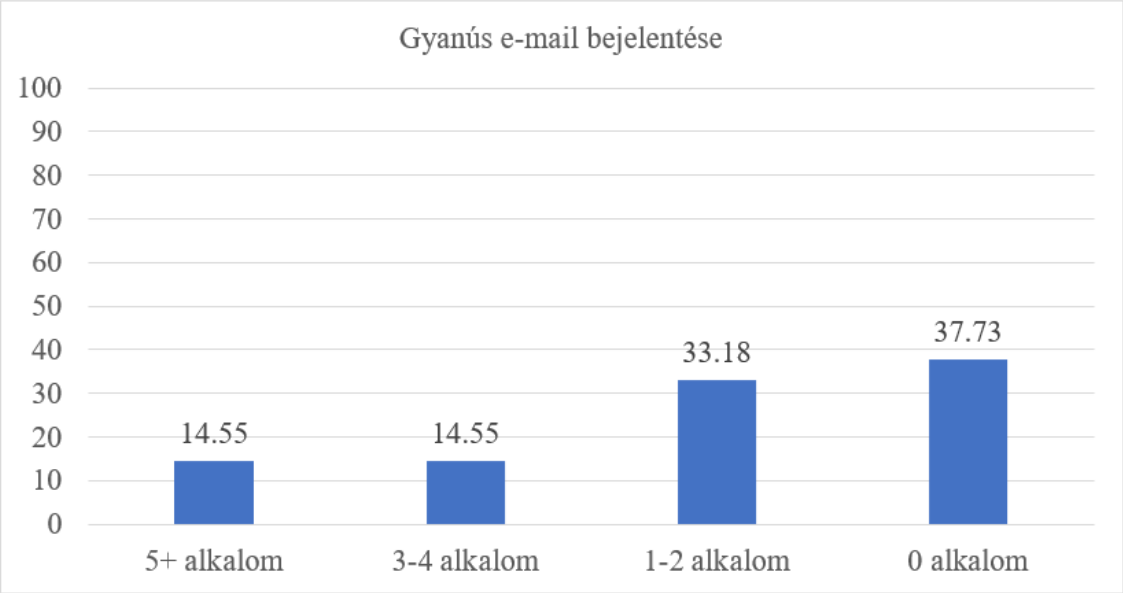


12. diagram
Az Értékszerveződés szintjén adott válaszok az információbiztonságról szóló beszélgetés gyakorisági kérdésében (n=220) (%)
(Forrás: saját szerkesztés)

Az eredmények szerint (*12. diagram*) egészen egyenletesen oszlik el az érték: 20,91 százalék gondolja úgy, hogy soha nem beszél ismerőseivel ezekről a témákról. A kitöltők közel negyede (24,09%) évente beszél erről, míg 20,91 százalék nagyjából félévente, és 26,82 százalék havi rendszerességgel. Egyedül a heti szinten a témát napirenden tartók értéke jóval alacsonyabb a többihez képest a maga 7,27 százalékával.

Érték alapú viselkedés szintje

Az Érték alapú viselkedés szintjén szintén gyakoriság alapú kérdést alkalmaztam, abban a témában, hogy a válaszadó hányszor jelentett be gyanús e-mailt a munkahelyén a céges informatikai biztonsági felelős számára az elmúlt egy évben (*13. diagram*). A jelölhető értékek között a 0, 1-2, 3-4 és 5+ alkalom szerepelt, amelyet a Bloom szintek kiértékelésekor a gyakoriság alapján vettem figyelembe, így 0-tól 3 pontig terjedt az értékelési skála.



13. diagram
Az Érték alapú viselkedés szintjén adott válaszok aránya a gyanús e-mail bejelentésről szóló gyakorisági kérdésben (n=220) (%)
(Forrás: saját szerkesztés)

A kitöltők több mint harmada (37,73%) jelölte, hogy nem tett ilyet az elmúlt egy évben, és további harmada (33,18%) egy-két alkalommal jelentett be gyanús e-mailt. Három-négy alkalommal jelentett be ilyet a kitöltők 14,55 százaléka, aminek megfelelően 2 pontot kaptak, és szintén ennyien (14,55%) jelölték az 5-nél több alkalmat, és így 3 pontot kaptak az affektív terület legmagasabb szintjén.

Bloom összesített eredmények

A kérdőív kitöltőinek válaszait átszámítottam a Bloom szinteken elért eredményekre kognitív és affektív területen egyaránt. A fejezetben részletezem, hogy a válaszadók az egyes szinteken milyen eredményt értek el a pontszámokban, és ez az összesen megszerezhető pontszámhoz képest milyen arányban van.

Az eredményeket az egyes szintek mellett tovább összesítem, hogy a számítással a kognitív és az affektív területek összeredménye is látható legyen. Az összeredmények alapján csoportokat képeztem az alacsony, közepes és magas szint megállapítására mindkét területen, mivel a csoportképzés a H4 hipotézisem szempontjából is jelentőséggel bír.

Kognitív szint

Az összesített szinteredmények és átlagaik alapján (*3. táblázat*) nem lenne felrajzolható Bloom piramisa, mivel az eredmények nem csökkennek az emlékezéstől a létrehozásig. Megnéztem azt az esetet is, ha nem az összes pontszámot veszem figyelembe, hanem a 4 pontot érő kérdésekben csak a 3 vagy 4 pontot elérők arányát, de ez sem hozott a piramis formájához közelebbi eredményt.

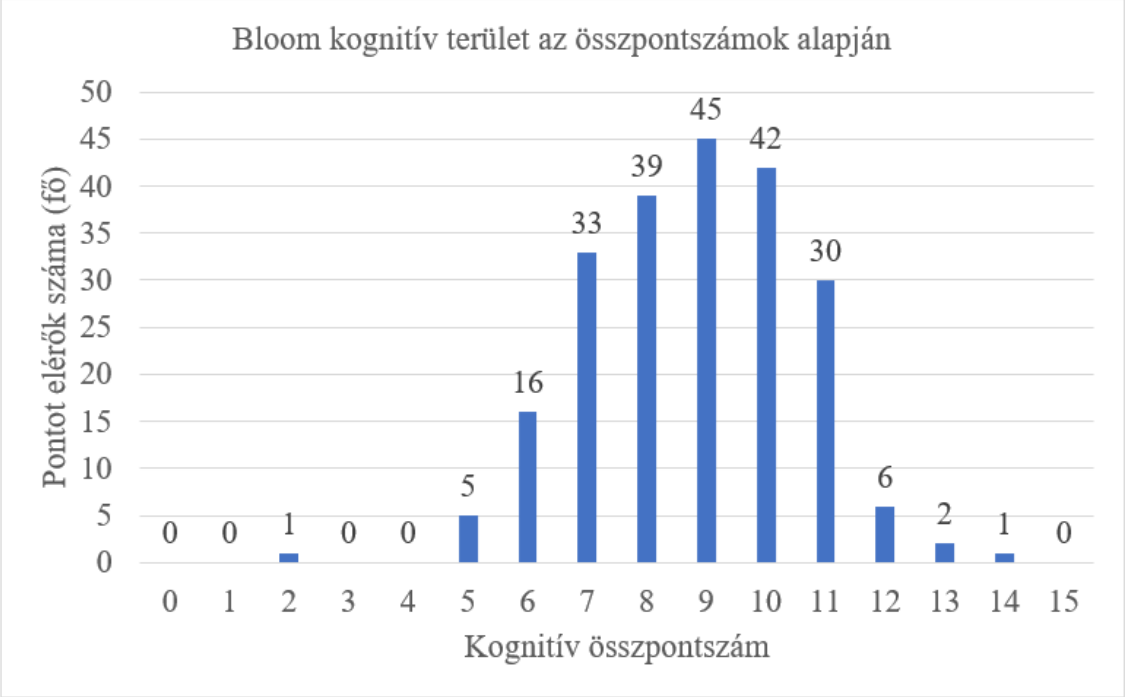
Szint neve	Összesen elérhető pontszám	Kitöltők által elért összpontszám	Elérhető és elért pontszám aránya (%)
Emlékezés	4x219=876	646	73,74%
Megértés	1x220=220	194	88,18%
Alkalmazás	4x219=876	676	77,17%
Elemzés	1x220=220	215	97,73%
Kiértékelés	1x220=220	156	70,91%
Létrehozás	4x220=880	46	5,23%

3. táblázat
Kognitív szint összesített eredménye
(Forrás: saját szerkesztés)

A kutatás folytatásában érdemes lenne az egyes szinteken egyenlő mértékben elérhető pontszámok kialakítása (a váltakozó 4 és 1 pontérték helyett) a könnyebb összehasonlíthatóság érdekében. Ha megnézzük az eredményeket, akkor az 1-1 pontot érő kérdésekben tapasztalható főként a vártnál magasabb eredmény, ezért ezek a szintek további feladatokkal lennének pontosíthatók a felmérésben.

Továbbá a kérdőívben szereplő kérdések átgondolása is szükséges jelen eredmények alapján. Az Elemzés szintjén kiugróan magas eredmény született, amit tovább lehet pontosítani más hamis weboldalak és adathalász e-mailek elemzésével, a jelen példában szereplő hamisított NAV weboldalnál nehezebben felismerhető esetekkel.

A kutatásban nem csak az egyes szintek eredményeit érdemes megállapítani, hanem az összeredményekből csoportok is képezhetők az alacsony, közepes és magas kognitív szinten álló válaszadók meghatározására. Ennek megállapítására összesítettem (*14. diagram*), hogy a kitöltők összes pontszáma milyen arányban oszlott meg a megszerezhető 0-15 pont között. Ahogy az ábrán is látható, a legtöbben 7-11 pontot kaptak a kognitív területen.



14. diagram
Bloom kognitív terület összpontszámok alapján (n=220)
(Forrás: saját szerkesztés)

A kognitív területen a módusz értéke 9 és a szórás 1.80, így a móduszhoz viszonyítottam a közepes szintet, és a közvetlen mellette elhelyezkedő értékeket (7 és 10 pont) vettem számításba a közepes Bloom kognitív szint meghatározásához. Ez alatt alacsony, efölött magas kategóriába sorolom a szintet. A módszerrel a *4. táblázatban* látható csoportokat képeztem.

	Elért pontszám intervallum	**Válaszadók száma**	**Válaszadók aránya**
Alacsony kognitív szint	0-7	55	25,00%
Közepes kognitív szint	8-10	126	57,27%
Magas kognitív szint	11-15	39	17,73%

4. táblázat
Bloom kognitív területen alacsony, közepes és magas szintet elérők száma és aránya
(Forrás: saját szerkesztés)

Tehát számításaim szerint információbiztonsági kérdésekben, Bloom kognitív területen a kérdőívem válaszadóinak negyede sorolható az alacsony szinten lévők csoportjába. A közepes szinten a kitöltők 57,27 százaléka található. Magas kognitív szintet pedig a válaszadók 17,73 százaléka ért el.

Affektív szint

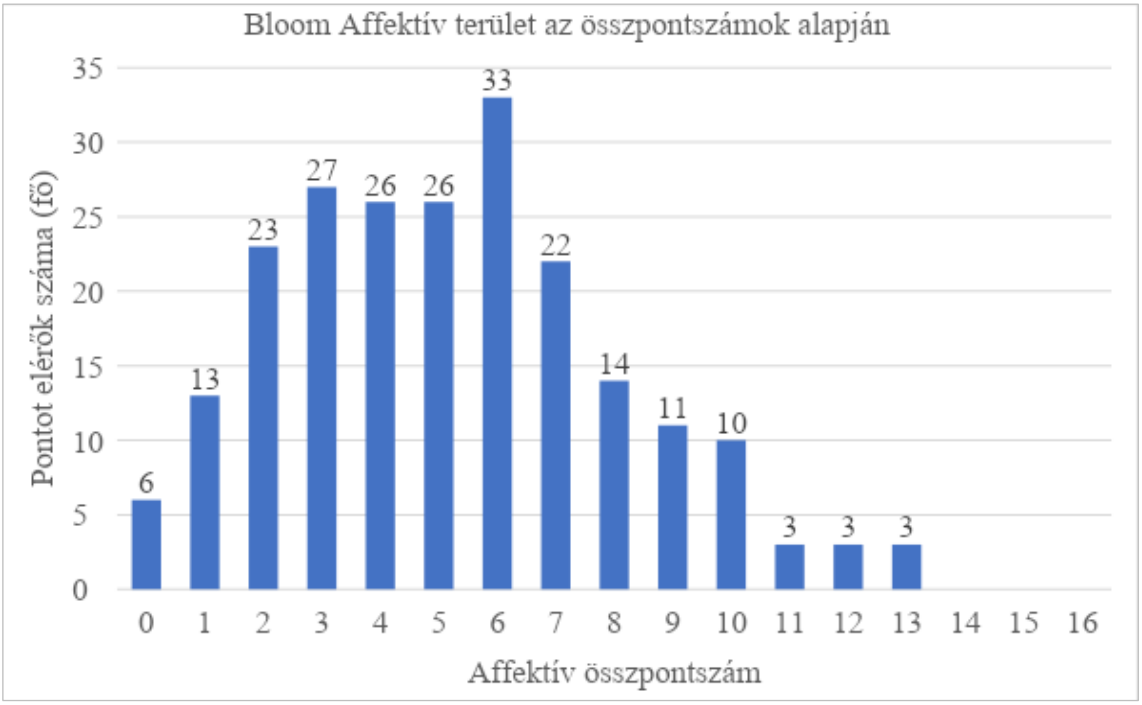
A piramis alakja a Bloom affektív területen sem állt össze az összeredmények és átlagaik alapján (*5. táblázat*), de a kognitív területnél valamelyest jobban megközelíti a formát, főleg az értékekkel kapcsolatos felső három szinten. A Befogadás és a Reagálás szintek meglepően alacsony eredményt értek el, amely okának megállapításához további vizsgálat szükséges.

Szint neve	**Összesen elérhető pontszám**	**Kitöltők által elért összpontszám**	**Elérhető és elért pontszám aránya (%)**
Befogadás	4x220=880	239	27,16%
Reagálás	4x219=876	169	19,29%
Értékelés	1x220=220	118	53,64%
Érték-szerveződés	4x220=880	386	43,86%
Érték alapú viselkedés	3x220=660	96	14,55%

5. táblázat
Affektív szint összesített eredménye
(Forrás: saját szerkesztés)

Ahogy a leíró statisztikai eredmények mutatják (5.1.4 fejezet), *a válaszadók látszólagos értékítéletben egyetértenek az információbiztonság fontosságával* (pl. profil törlésével egy adatszivárgást követően), *de alacsony hajlandóságot mutatnak arra, hogy gyakorlati szinten tegyenek érte*, pl. kövessék az információbiztonsági híreket, ellenőrizzék a jelszavuk kiszivárgását vagy jelentsék az információbiztonságért felelős szakértő számára a gyanús e-maileket. Egy következő kutatásban ezt a kettősséget is érdemes lenne tovább vizsgálni.

Az összeredmények alapján az affektív területen az eredmények a *15. diagramon* láthatók, ami jól szemlélteti az eredmények szórását is. A kitöltők a kérdőívben 0-16 pont közötti eredménnyel végezhettek, és mint látható, 0-tól 13-ig mindenféle összpontszám megtalálható. A legtöbben 2-6 pont közötti eredménnyel zártak, de a legmagasabb 14-16 pontot senki nem érte el az affektív területen.



15. diagram
Bloom affektív terület összpontszámok alapján
(Forrás: saját szerkesztés)

Az affektív területen a módusz értéke 6 és a szórás sokkal nagyobb, mint a kognitív területen a maga 2,88-as értékével. Ezek alapján a közepes affektív szintet a 4-8 pontot elérők körében határoztam meg. Az alacsony szinten lévők 0-3 pontot értek el, míg a magas szintűek 9-16 pontot, amelyekhez kapcsolódóan a válaszadói eredmények eloszlását a *6. táblázat* mutatja meg.

	Elért pontszám intervallum	**Válaszadók száma**	**Válaszadók aránya**
Alacsony affektív szint	0-3	69	31,36%
Közepes affektív szint	4-8	121	55,00%
Magas affektív szint	9-16	30	13,64%

6. táblázat
Bloom affektív területen alacsony, közepes és magas szintet elérők száma és aránya
(Forrás: saját szerkesztés)

Ezek alapján a kérdőív kitöltőinek 31,36 százaléka, vagyis csaknem a harmada az alacsony affektív szinten lévők közé sorolható. Több mint a válaszadók fele (55%) közepes érdeklődő az információbiztonsági ismeretek megszerzése kapcsán. Mindössze 13,64 százalék sorolható a magas affektív szintűek közé, akiket aktívan foglalkoztat az információbiztonsági terület, szívesen olvasnak új híreket, és beszélik meg azokat az ismerőseikkel.

A hipotézisek megtartása és elvetése

A fentiekben leírt statisztikai módszerekkel végeztem el a hipotézisekhez szükséges elemzéseket, hogy megállapíthassam, melyik hipotézis elfogadható és melyik elvethető.

H1: A gazdasági szervezetek dolgozói alapvetően nyitottak az információbiztonsági területre (magas affektív szint), de a gyakorlatban keveset tesznek a tudatosság növeléséért (alacsony kognitív szint).

A hipotézis elemzéséhez a kérdőíves eredményekben szereplő Bloom taxonómia-rendszer alapján összeállított kérdéssor használható fel. Az 5-10. kérdésre adott válaszok összeredménye kiadja a kitöltők Bloom kognitív szintjét. A 11-15. kérdésre adott válaszok pedig a Bloom affektív szintekre vonatkoznak. A hipotézis alapján az vizsgálandó, hogy a Bloom affektív szinten elért eredmény magasabb értéket ér-e el, mint a Bloom kognitív szinten elért eredmény.

A *Bloom kognitív területen* elért átlageredmény 8,79 az összesen megszerezhető 15 pontból, míg a módusz és a medián is 9, a szórás pedig 1,80. Míg a *Bloom affektív területen* elért átlageredmény 5,21 az összesen megszerezhető 16 pontból, a módusz 6, a medián 5, a szórás pedig 2,88.

Az átlageredmény tehát jóval alacsonyabb, mint a kognitív szinten, viszont magasabb szórásérték mellett, *azaz változó, hogy a válaszadók mennyire érdeklődnek az információbiztonsági terület iránt, de a többség kevésbé érdeklődő.*

ÖSSZESÍTÉS

Csoportok	*Darabszám*	*Összeg*	*Átlag*	*Variancia*
AFFEKTÍV	220	1144	5,20	8,31
KOGNITÍV	220	1933	8,79	3,23

VARIANCIA-ANALÍZIS

Tényezők	*SS*	*df*	*MS*	*F*	*p-érték*	*F krit.*
Csoportok között	1414,82	1	1414,82	245,31	3,19E-44	3,86
Csoporton belül	2526,16	438	5,77			
Összesen	3940,98	439				

7. táblázat
Egytényezős varianciaanalízis a Bloom kognitív és affektív területek közti különbség elemzésére
(Forrás: saját szerkesztés)

Az egytényezős varianciaanalízis (ANOVA) eredménye (*7. táblázat*) szerint a csoportok közötti és csoporton belüli változást mutató F érték 245,31, míg az előfordulási valószínűséget mutató p-érték 3,19E-44 (azaz 3,19 szorozva tízzel a -44 hatvánnyal). Ez a p-érték nagyon alacsony, ami azt jelenti, hogy a csoportok közötti különbség nagy valószínűséggel nem véletlen. Az F érték küszöbértéke 3,86, ami felett a nullhipotézis elutasítható. Mint látható, a 245,31 jóval efelett található. *Azaz a Bloom kognitív és affektív szintek közötti különbség statisztikailag szignifikáns, és így a nullhipotézis elutasítható, mivel van különbség a csoportok között.*

Az első hipotézisemnek tehát az a része elfogadható, hogy a kognitív és az affektív szintek között valóban van különbség. Azonban a Bloom területek eredményeit figyelembe véve elutasítható az a feltevés, hogy a kognitív szint alacsony lenne és az affektív szint magas, az eredmények alapján ennek ellenkezője tapasztalható.

H2: Az információbiztonság tudatosság szintje nem életkorfüggő.

A hipotézis a kérdőív kitöltőinek Bloom kognitív szintje és az életkori csoportok alapján értékelhető. Azaz a megtartásához vagy elvetéséhez az egyes életkori csoportok (1. kérdés) által a kérdőív 5-10. kérdésére adott válaszok eredményét kell összevetni.

Az életkor és a Bloom kognitív szinten elért eredmények keresztkorrelációja -0,02, amely szerint gyenge, negatív, szignifikáns összefüggés van a vizsgált változók között. Az összefüggés egészen gyengének tekinthető, mivel inkább a nullához áll közel.

A korreláció mínusz előjele arra utal, hogy az életkor és a Bloom kognitív szint közt fordított kapcsolat áll fenn, azaz az életkor előrehaladtával valamelyest csökken a kognitív szint.

A Student-féle t-próba alapján egyszélű, kétmintás egyenlő varianciájú típusértékkel az eredmény 5,67E-174 (azaz 5,67 szorozva tízzel a -174 hatvánnyal), míg kétmintás nem egyenlő varianciájú típusértékkel az eredmény 3,58E-133 (azaz 3,58 szorozva tízzel a -133 hatvánnyal). A p-érték mindkét esetben jóval kisebb, mint az általában elfogadott 0,05-ös küszöbérték, amely szerint a nullhipotézist valószínűleg el kell utasítani, mivel a kapott eredmény statisztikailag szignifikáns.

Az eredmény szerint tehát van összefüggés az életkor információbiztonság tudatosság szintje és az életkor közt, ugyanakkor a két érték nagyon gyenge korrelációt mutat. A második hipotézisem tehát részben elfogadható, de az adatokban rejlő mintázatokat érdemes lehet tovább vizsgálni.

H3: Közép- és nagyvállalatoknál gyakoribb az információbiztonsági tudatosság növelésére irányuló tevékenység, mint kisvállalatoknál.

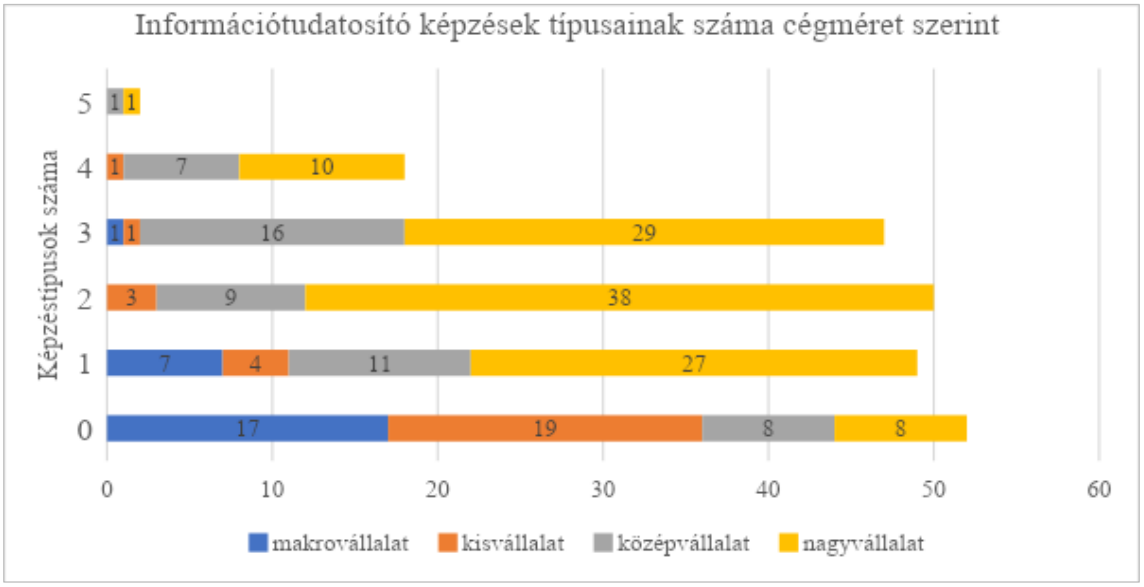
A harmadik hipotézis a gazdasági szervezetre vonatkozó információkkal foglalkozik, ezért a cégméretre vonatkozó kérdés eredményét (kérdőív 3. kérdése) és a céges információbiztonság tudatosító kezdeményezések (4. kérdés) eredményét kell kereszttáblás formában összevetni a hipotézis kiértékeléséhez (*8. táblázat*). A hipotézis alapján összesíteni kellett azokat az eredményeket, ahol történt bármilyen formában információbiztonság tudatosítás.

Cégméret / Képzéstípusok száma	**0**	**1**	**2**	**3**	**4**	**5**	**Végösszeg**
makrovállalat	17	7	0	1	0	0	25
kisvállalat	19	4	3	1	1	0	28
középvállalat	8	11	9	16	7	1	52
nagyvállalat	8	27	38	29	10	1	113
(üres)	1	1	0	0	0	0	2
Végösszeg	**53**	**50**	**50**	**47**	**18**	**2**	**220**

8. táblázat
Cégméret és a cégek által nyújtott képzéstípusszám kereszttáblás elemzése
(Forrás: saját szerkesztés)

Az összesített eredmények alapján látható, hogy a makro- és kisvállalatok közt a legmagasabb annak aránya, ahol egyáltalán nem folytatnak információbiztonsági tudatosítást semmilyen formában. Ezenkívül az egyféle képzés, valamint kisvállalatoknál a kétféle képzés fordul elő. A közép- és nagyvállalatoknál sem végeznek mindenhol tudatosítást, de ezekben a vállalatokban sokkal inkább jellemző az 1-2-3-féle munkavállalói képzési típus, sőt akár a 4-féle tudatosítási kezdeményezés is, és 1-1 esetben még az 5-féle típus is előfordul. A cégméret szerinti különbséget a *16. diagram* is szemlélteti.

Tehát a hipotézis elfogadható, mely szerint közép- és nagyvállalatoknál gyakoribb az információbiztonság tudatosítására irányuló kezdeményezés.



16. diagram
Információtudatosító képzések típusainak száma cégméret szerint
(Forrás: saját szerkesztés)

H4: Informatikai munkakörökben magasabb az információbiztonság tudatossági szint, mint más foglalkozások esetében.

A hipotézis a demográfiai változók közül a munkaköri kérdésre vonatkozik (2. kérdés), amelyet a Bloom taxonómia-rendszer kognitív szinten elért átlageredménnyel (5-10. kérdés) vetek össze a hipotézis megvizsgálásához.

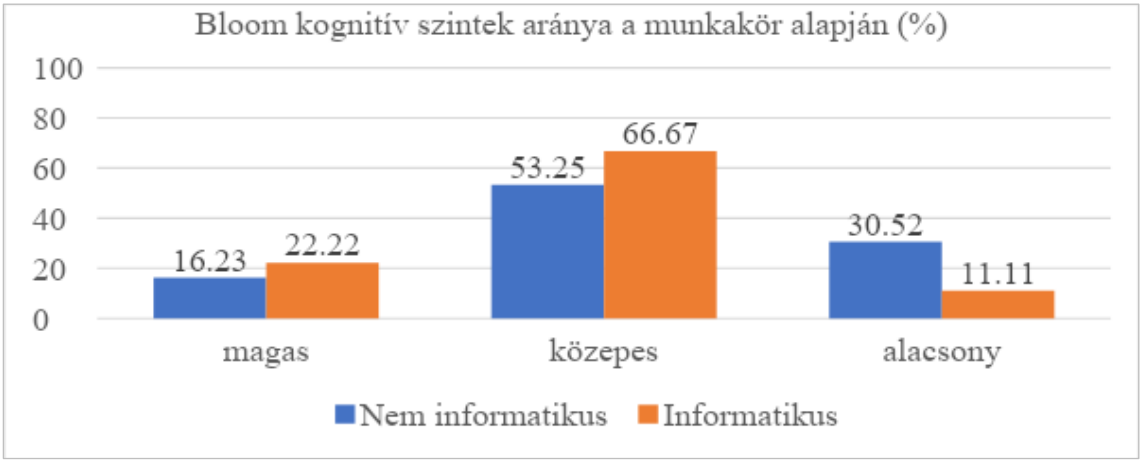
Az összesen elérhető 15 pontból a nem informatikusként dolgozók (n=154) átlageredménye kognitív szinten 8,54, méghozzá 1,79-es szórásértékkel. Az informatikusként dolgozók (n=63) átlageredménye pedig 9,41, melynek szórása 1,7. *Azaz az informatikus kitöltők nagyjából hasonló szórás mellett valamivel jobb átlageredményt értek el a Bloom kognitív területen, mint a nem informatikus kitöltők, így a hipotézis elfogadható.*

További elemzést végeztem a kérdésben az 5.1.5 fejezetben összesített alacsony, közepes és magas kognitív Bloom szintek csoportosítása alapján, amelyet kereszttáblás formában összevetettem a munkaköri változóval (*9. táblázat*).

Munkakör /Bloom kognitív eredmény				
	Magas	**Közepes**	**Alacsony**	**Végösszeg**
Nem informatikus	25	82	47	154
Informatikus	14	42	7	63
Végösszeg	**39**	**124**	**54**	**217**

9. táblázat
Munkakör és a Bloom kognitív területen elért eredmény kereszttáblás elemzése
(Forrás: saját szerkesztés)

A kitöltők száma alapján is látható a különbség az informatikusok és nem informatikusok közt, de a változók alapján megnéztem a százalékos eredményeket is a könnyebb összehasonlíthatóság érdekében (*17. diagram*).



17. diagram
Bloom kognitív szintek aránya a munkakör alapján (%) (n=217)
(Forrás: saját szerkesztés)

Mindkét munkaköri típusban a közepes szinten teljesítők vannak döntő többségben, méghozzá az informatikus kitöltők közül többen (66,67%) mint a nem informatikusok közül (53,25%). Azonban az alacsony szinten látható, hogy a nem informatikusként dolgozók csaknem harmada (30,52%) ebbe a kategóriába került, míg az informatikusoknak csak 11,11 százaléka jelenik meg itt. Az informatikusok közül valamivel többen jelennek meg a magas kognitív szinten (22,22%) a többi kitöltőhöz (16,23%) képest. Tehát ebből a csoportosításból is látható, hogy a hipotézis elfogadható, mivel az informatikusok értek el jobb eredményt Bloom kognitív szinten az eredményeim szerint.

H5: Az elektronikus információbiztonsági területek közül a megtévesztésen alapuló csalás az egyik legkevésbé ismert terület.

A megtévesztésen alapuló csalással kapcsolatos ismeretek felmérésére a kérdőívben az Emlékezés, a Megértés, az Elemzés és a Kiértékelés szintjén alkalmaztam kérdéseket, ezért a hipotézis elemzéséhez ezen kérdések elemzésére van szükség.

Az *Emlékezés* (5. kérdés) szintjén a válaszadóknak egy megadott listából kellett kiválasztaniuk az elektronikus információbiztonság típusait, köztük a megtévesztésen alapuló csalás témakörébe tartozó adathalászatot. Ezt a típust a kérdőív kitöltőinek döntő többsége, méghozzá 98,17 százaléka választotta ki helyesen elektronikus információbiztonság típusaként. Ehhez képest a többi típust kevesebben azonosították helyesen: a zsarolóvírust (88,13%), a kéretlen levelet (49,77%) és legfőként a DDoS támadást (58,9%), vagyis összesítve a többi típust 65,6 százalék azonosította be helyesen.

A *Megértés* (6. kérdés) szintjén kifejezetten az adathalászat definícióját kellett felismerniük a kitöltőknek, és az előző kérdésben is szereplő listából kiválasztani. A kérdésben a válaszadók 88,18 százaléka választott helyesen. A legtöbben a kéretlen levelet jelölték be a rosszul válaszolók közül, de ez is csak 5 százalékot tett ki.

Az *Elemzés* szintjén egy hamis weboldalt kellett felismerni, amelyet a támadók szintén jellemzően adathalászatra használnak. A kitöltők 97,73 százaléka felismerte a weboldalról, hogy az hamis.

A *Kiértékelés* szintjén pedig a listázott WiFi kapcsolatok és a saját mobilinternete közül kellett kiválasztania a kitöltőknek, hogy melyikhez csatlakoznának. A válaszadók 70,91 százaléka helyesen döntött a saját mobilinternete mellett a publikus WiFi hálózatok helyett, amelyen keresztül szintén könnyedén lehet adathalászati támadást indítani.

A megtévesztésen alapuló csalásra vonatkozó feladatok eredményeit a *10. táblázat* mutatja be összefoglalóan a jó és rossz válaszok megoszlásában, és más típussal való összehasonlításban.

	Megtévesztésen alapuló csalás jó válaszadás %	**Megtévesztésen alapuló csalás rossz válaszadás %**	**Kérdésben szereplő más típusok jó válaszadás %**
5.	98,17%	1,83%	65,6%
6.	88,18%	11,82%	–
8.	97,73%	2,27%	–
9.	70,91%	29,09%	–

10. táblázat
A megtévesztésen alapuló csalással kapcsolatos kérdésekre adott jó és rossz válaszok aránya (Forrás: saját szerkesztés)

Tehát a válaszadások alapján megállapítható, hogy a kérdőív kitöltői viszonylag jól ismerték a megtévesztésen alapuló csalás témakörét, az ebbe a kategóriába tartozó adathalászati definíciót, hamis weboldalt, és aránylag sokan tudják, hogy nem érdemes nyilvános WiFi hálózatra csatlakozni az adathalászat veszélye miatt. Ennek következtében *a hipotézist el kell vetni*, mivel valószínűleg más kategória, amit kevesen ismernek, például ilyen lehet a speciális területnek számító DDoS támadás.

Összegzés

A tanulmány eredményeiből látható, hogy a Bloom taxonómia-rendszer alkalmas az információbiztonsági tudatosítás mérésére és értékelésére, az ismeretekkel foglalkozó kognitív területen, és a felhasználók értékrendszerét vizsgáló affektív tartományban egyaránt. A kérdőíves felmérést kitöltő 220 fő nem jelent reprezentatív mintát az életkorra, a munkakörre és a kapcsolódó gazdasági szervezetek méretére vonatkozóan sem, de megfelelő kiindulópontként szolgált a vizsgálathoz, és a további lehetséges kutatási területek meghatározásához.

A leíró statisztikai eredmények és a hipotézisvizsgálat alapján a következő megállapítások tehetők összefoglalóan:

- A válaszadók látszólag egyetértenek az információbiztonság fontosságával, de a gyakorlatban keveset tesznek érte, például nem követik a biztonsági problémákról szóló híreket, nem ellenőrzik jelszavaik kiszivárgását.
- Ebből is következően a kognitív területen a válaszadók magasabb eredményt értek el, mint az affektív területen. A két terület közt a különbség statisztikailag szignifikáns. Azonban a szórás is nagyobb azzal kapcsolatban, hogy mennyire érdekli a felhasználókat ez a téma.
- Az életkor és az információbiztonsági tudatosság közt gyenge negatív korreláció mutatható ki, tehát valamelyest az idősebbek kevésbé teljesítettek jól a kognitív területen, de az okok és az arányok vizsgálatához további kutatás szükséges.

- Az informatikus válaszadók jobb eredményt értek el az ismeretek mérésekor a többi munkakörhöz képest.
- Továbbá az a hipotézis is elfogadható, mely szerint cégméret szerint nő az információbiztonság tudatosító kezdeményezések száma. A nagyvállalatok sokkal változatosabb formában igyekeznek tudatosítást végezni akár előadásokkal, e-learning anyagokkal, és még adathalász kampányok szimulálásával is a mérés és tudatosítás érdekében.
- Az elektronikus információbiztonsági típusok közül a social engineering ismertnek mondható, legalábbis a felhasználók tisztában vannak az adathalászat definíciójával, vagy a hamis adathalász weboldalak ismérveivel.

Az eredmények pontosítása érdekében a Bloom taxonómia-rendszert alkalmazó mérőeszközt érdemes tovább finomítani abból a szempontból, hogy az egyes szinteken egyenlő arányban jelenjenek meg a pontszámok, és több konkrét feladatot tartalmazzanak a tudás pontosabb felméréséhez, például hamis weboldalak felismerésével, vagy a definíciók azonosításával kapcsolatban.

Az információbiztonság tudatosítással foglalkozó szakemberek számára viszont így is levonható a következtetés, hogy a Bloom taxonómia-rendszer használható az ismeretek és az értékrendszerek mérésére. Az eredményeim alapján főleg a kisebb szervezetek nem informatikusként dolgozó X és Baby Boom generációs dolgozóinak körében lenne szükség nagyobb mértékben a tudatosító kezdeményezésekre.

Az információbiztonság iránti érdeklődést azonban még ennél is szélesebb körben kellene terjeszteni, mivel nem elég, ha a felhasználók tisztában vannak a definíciókkal, de az újabbnál újabb támadások miatt folyamatosan informálódniuk kellene például az adathalászati és vírustámadásokkal kapcsolatban, rendszeresen ellenőrizniük kellene jelszavaik kiszivárgását, és ennek megfelelő lépéseket tenni a saját információik, és ezáltal a munkahelyükkel kapcsolatos információk védelme érdekében egyaránt.

Irodalom

Amin, R. W., Sevil, H. E., Kocak, S., Francia III, G., & Hoover, P. (2021). The Spatial Analysis of the Malicious Uniform Resource Locators (URLs): 2016 Dataset Case Study. *Information 2021., 12*(2)

Anderson, L. W., & Krathwohl, D. R. (szerk.). (2001). *A taxonomy for learning, teaching and assessing: A revision of Bloom's Taxonomy of educational objectives: Complete edition*. Longman.

Cormack, G. V. (2008). *Email Spam Filtering: A Systematic Review.* now. https://ieeexplore.ieee.org/document/8187090 (Utolsó hozzáférés: 2024.05.05.)

Csath M. (2022. április 13.). Hiány van informatikusokból vagy nincs? *növekedés.hu* https://novekedes.hu/mag/hiany-van-informatikusbol-vagy-nincs (Utolsó hozzáférés: 2024.05.05.)

Dimock, M. (2019). Defining generations: Where Millenials end and Generation Z begins. *Pew Research Center* https://www.pewresearch.org/fact-tank/2019/01/17/where-millennials-end-and-generation-z-begins/ (Utolsó hozzáférés: 2024.05.05.)

ESET (s.a.). *Hogyan veszélyezteti ez a támadási forma vállalkozását?* https://www.eset.com/hu/it-biztonsagi-temak-cegeknek/social-engineering/ (Utolsó hozzáférés: 2024.05.05.)

Have I Been Pwned (s.a.). https://haveibeenpwned.com/ (Utolsó hozzáférés: 2024.05.05.)

Központi Statisztikai Hivatal (2022. november 15.). *9.1.1.17. A vállalkozások teljesítménymutatói kis- és középvállalkozási kategória szerint.* https://www.ksh.hu/stadat_files/gsz/hu/gsz0018.html (Utolsó hozzáférés: 2024.05.05.)

Központi Statisztikai Hivatal (2023. március 24.). *4 millió 691 ezer fő volt a foglalkoztatottak száma.* https://www.ksh.hu/gyorstajekoztatok/#/hu/document/fog2302 (Utolsó hozzáférés: 2024.05.05.)

Nemzeti Kibervédelmi Intézet (2020. január 14.). *Tájékoztatás a NAV nevével visszaélő adathalászattal kapcsolatban.* https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-a-nav-nevevel-visszaelo-adathalaszattal-kapcsolatban/ (Utolsó hozzáférés: 2024.05.05.)

Ramsoonder, N. K., Kinnoo, S., Griffin, A. J., Valli, C., & Johnson, N. F. (2020). Optimizing Cyber Security Education: Implementation of Bloom's Taxonomy for future Cyber Security workforce. In *International Conference on Computational Science and Computational Intelligence (CSCI)*. https://ieeexplore.ieee.org/document/9458047 (Utolsó hozzáférés: 2024.05.05.)

Ollé J., Lévai D., Domonkos K., Szabó O., Papp-Danka A., Czirfusz D., Habók L., Tóth R., Takács A., & Dobó I. (2013). *Digitális állampolgárság az információs társadalomban*. ELTE Eötvös Kiadó. https://www.elte-reader.hu/kiadvanyok/digitalis-allampolgarsag-az-informacios-tarsadalomban/ (Utolsó hozzáférés: 2024.05.05.)

Van Niekerk, J., & von Solms, R. (2013). Using Bloom's Taxonomy for Information Security Education. In Dodge, R.C., & Futcher, L. (szerk.). *Information Assurance and Security Education and Training. WISE WISE WISE 2013 2011 2009. IFIP Advances in Information and Communication Technology. vol 406*. Springer. https://link.springer.com/content/pdf/10.1007/978-3-642-39377-8_33.pdf (Utolsó hozzáférés: 2024.05.05.)

White, G., (2024). Higher Education Model for Security Literacy using Bloom's Revised Taxonomy. *Cybersecurity Pedagogy and Practice Journal* 3(1) pp 27-36. https://www.cppj.info/2024-3/n1/CPPJv3n1p27.html (Utolsó hozzáférés: 2024.05.06.)