GAZDASÁG ÉS PÉNZÜGY • 12. ÉVF. 3. SZ. • 2025. SZEPT. • DOI: 10.33926/GP.2025.3.6

INTERNETES PÉNZÜGYI CSALÁSOK ÉS A BIZTONSÁGTUDATOSÍTÁS FEJLŐDÉSE MAGYARORSZÁGON

A kiberpajzs programban bemutatott csalások ismertsége felhasználói oldalról

Solymos Ákos[1]

ABSZTRAKT

A tanulmány célja az internetes pénzügyi csalások magyarországi fejlődésének és az ezekre adott társadalmi, intézményi válaszok vizsgálata, különös tekintettel az ügyféloldali biztonságtudatosság alakulására. A történeti áttekintésen túl a kutatás empirikus elemekre is épít: 2025 tavaszán 220 fő részvételével anonim, online kérdőíves felmérés készült a KiberPajzs program ismertségéről, az internetes csalásokkal kapcsolatos ismeretekről és az észlelt pénzügyi veszteségekről. Az eredmények azt mutatják, hogy bár a KiberPajzs kezdeményezés ismertsége biztató, a válaszadók jelentős része túlzott önbizalommal ítéli meg saját védettségét a csalásokkal szemben. A megkérdezettek közel ötöde számolt be tényleges pénzügyi veszteségről. A tanulmány rámutat az oktatás és a célzott, korosztály-specifikus tudatosítás fontosságára, valamint a jelenlegi kommunikációs csatornák hatékonyságának kérdéseire. A kutatás alapján javasolt a prevenciós kampányok adaptálása a digitális médiát aktívan használó fiatalabb generációkhoz is. A jövőbeli vizsgálatoknak célszerű lenne a tudatossági szint változásainak longitudinális követésére, valamint a kampányok tényleges hatásának mérésére fókuszálni.

JEL-kódok: A20, O30, M53, I22, I31, L30

Kulcsszavak: pénzügyi kultúra, kiberbűnözés, adathalászat, kockázatok, tudatosítás, biztonságtudatosság

1 *Solymos Ákos* CISM, CRISC, CDPSE.Kiberbiztonsági szakértő, „A pénzügyi kultúra nagykövete" Magyar Bankszövetség 2025, „Az év útmutató szakembere" ITBN díj 2022. E-mail: soanfoto75@gmail.com.

1. A TÉMA TÁRSADALMI ÉS GAZDASÁGI JELENTŐSÉGE

A kiberbűnözés nem különbözik más bűncselekményektől: amíg pénzt termel, folyamatosan növekedni fog – és a becslések szerint 2028 végére az okozott károk globálisan elérhetik a 14000 milliárd dollárt (Nemes, 2025:3). Magyarországon 2023-ban és 2024-ben közel 55 milliárd forint kárt okoztak a kiberbűnözők az elektronikus pénzforgalomban (MNB, 2025).

A pénzügyi csalások párhuzamosan fejlődtek az emberiséggel. A nyereségvágy, a mások pénzére és vagyonára való áhítozás korokon átívelő motivációt jelentett mindig is a bűnözőknek. A „pénznek nincs szaga", tartja a mondás. A digitális formában tárolt pénznek, amelyek bitekben és számokban jelennek meg, úgyszintén nincsen. A pénzhamisítók, a csalók folyamatosan problémát jelentettek minden társadalomban. A digitalizáció és a felgyorsult világunk, az internet határokon átívelő működése alapjaiban változtatta meg a pénzhez való hozzáállásunkat. A pénzügyi műveltség és a technológiai újdonságok megjelenése is összefüggésben van egymással, hiszen az embereknek új fogalmakkal, új folyamatokkal kellett megismerkedni és ez bizony nem ment mindig zökkenőmentesen. Ahogy a 20. század közepén megjelentek a készpénzhelyettesítő digitális eszközök (bankkártyák és hitelkártyák), a hitelezés mint pénzügyi tevékenység jól jövedelmezett számos szolgáltatói iparágnak. Nem belemélyedve a hitelezés és a hitelkártyák fejlődésének történelmébe, de meglepő módon nem a bankok és pénzintézetek voltak az elsők, akik hitelkártyákkal látták el ügyfeleiket. Azonban mind az ügyfeleknek, mind a bankoknak meg kellett tanulniuk a hitelkártyák kibocsátásával és használatával járó veszélyeket. Az egyik ilyen nevezetes eset volt, a Dine and Sign hitelkártyák esete az 1950-es évek elejéről. A Diners Club, hogy bővítse prémium kategóriás ügyfélkörét, megvásárolta a Cadillac autók tulajdonosainak név és címjegyzékét és előzetes hitelvizsgálat és részletes tájékoztatás nélkül hitelkártyákat postáztak részükre. Ezek a kártyák még papírból készültek és az ügyfeleknek maguknak kellett ráírniuk a nevüket. Sokan azonban ezt egyrészt olvashatatlanul tették meg, megnehezítve azt, hogy a költéseket kinek a részére is kell számlázni. Másrészt voltak, akik a lehetőséget ingyenpénznek gondolták és a kártyákat kölcsönadták. Ebből fakadóan számos visszaélés történt. A Diners Clubnak végül magánynyomozókat kellett fogadni, hogy megállítsák a csalárd kártyahasználatokat (Chakravorti, 2000).

A pénzintézeti oldal felelőtlenségét pedig a chicagói bankok által a '60-as évek közepén-végén tömegesen kiküldött hitelkártyák példázzák: A Life magazin 1970. március 27-i számában részletes cikket közölt a hitelkártyák témájáról, amelyben leírták: „Egyes családok az 1966-os karácsonyt megelőzően hat vagy hét kártyát is kaptak chicagói bankoktól, és néha teljesen meg voltak zavarodva, amikor észrevették, hogy a műanyag darabkán kiskorú gyermekük neve szerepelt… Több ezer

kártya került a kidobás sorsára… Küldtek munkanélkülieknek, alkoholistáknak, kábítószerfüggőknek, notórius adósoknak, …" (Jurík, 2007:67).

Manapság, amikor a lakosság jelentős része használ elektronikus pénzügyi szolgáltatásokat (internetbank, bankkártyás fizetés, digitális pénztárca), vagy nyitott ilyen megoldásokra, az internetes pénzügyi visszaélési esetek is jól mutatják az alap problematikát, mely szerint össztársadalmi szinten az ügyfeleknek szüksége van mind a pénzügyi-, mind a biztonságtudatosságra. Főleg azért, mert az elektronikus fizetésre nyitott lakosok aránya már az összlakosság mintegy 80%-át teszi ki (MNB, 2023). És teszik ezt okostelefonnal, számítógéppel, okosórával, mindezt úgy, hogy alapvetően nincsenek tisztában ezen eszközök biztonságával és veszélyeivel.

Napjainkban egyre nagyobb azon összegek volumene, amit a kiberbűnözők ellopnak az állampolgároktól és ez hasonló szituációkat okoz, mint a hetvenes években, amikor a károsult ügyfelek és a pénzintézetek egymásra mutogatnak és perek sokasága indul, hogy eldőljön, ki volt a hibás és kinek kell a károkat viselnie. Aktuális példa a tanulmány írása közben is zajló eseménysorozat, ahol egy nagy magyar kereskedelmi banknak több mint 600 ügyfelét érte kár. A vizsgálatok még zajlanak, de a sajtóban eddig megjelent információk jól példázzák, hogy az ügyfelek figyelmetlensége, egy nagy internetes kereső szolgáltató fizetett hirdetésekben megjelenő adathalász linkjei és az érintett pénzintézet között megoszlanak a felelősségi kérdések és a témában minden szereplőnek van tere a fejlődésre.

Összességében társadalmi szinten is jelentős hatása van a pénzügyi- és informatikai biztonságtudatosságnak, illetve ezek hiányának. Tekintve, hogy a fizetések, nyugdíjak bankszámlára érkeznek és sokan tartják a megtakarításaikat is bankszámlákon különböző formákban, számos embernek az ilyen veszteség a mindennapi megélhetését kockáztatja. Az ilyen esetek és a riasztó veszteségadatok megrengethetik a bankokba vetett bizalmat, növelhetik a készpénzhasználatot, aminek szintén megvannak a saját veszélyei és költségei.

2. AZ ADATHALÁSZAT ÉS PÉNZÜGYI CSALÁSOK GYORS FEJLŐDÉSE, DIGITALIZÁCIÓS KONTEXTUS

Magyarországon az 1990-es évek legvégén indultak meg az internetbanki rendszerek pilot projektjei (Lemák, 2016) Ekkortól lett szempont a pénzintézetek számára, hogy a digitalizációval az internetes bankolás irányába tereljék az ügyfeleket. Ennek eredménye jól látszódott, hiszen 2000 decemberétől 2022 decemberéig, röpke két év alatt az internetbanki ügyfelek száma 60.000-ről 235.000-re nőtt (GKIeNET, 2002). Bár pontos és aktuális 2024-2025-ös számadat nem érhető el kifejezetten a lakosság körében internetbankot használók számosságára, az, hogy a lakosság 80%-a nyitott valamilyen elektronikus fizetési megoldásra

azt mutatja, hogy ők potenciális célpontjai lesznek a jövőben a támadásoknak és hogy ez az arány nehezen bővíthető, hiszen szinte minden cselekvőképes állampolgár érintett.

A digitalizációval együtt azonban megjelentek a fenyegető árnyak is. 2005-re elérte a hazai internetbankoló ügyfelek száma azt a szintet, amikor a kiberbűnözők már úgy gondolták, hogy érdemes ezt a célcsoportot is támadni. Ekkor már több mint 600.000 lakossági és mintegy 96.000 vállalati ügyfél rendelkezett internetbanki szolgáltatások igénybevételére vonatkozó szerződéssel (Prim.hu, 2005). Ezen időszakot megelőzően is voltak adathalász próbálkozások már 2004-ben is. Azonban 2005 decembere volt az a vízválasztó, amikortól egyre növekvő intenzitással, majd a későbbi években és napjainkban is szinte folyamatosan zajlottak és zajlanak az adathalász támadások.

Ezen támadások kezdetben a pénzintézeti ügyfelek ellen, majd később, ahogy a különböző szolgáltatók is átváltottak az elektronikus kommunikációra, az ő ügyfeleik ellen is elindultak. Természetesen ez a két csoport részben fedi egymást, így az érintetteknek azzal kellett szembesülniük, hogy egyre több olyan üzenetet kapnak, amelyekben a támadók a bankkártya adataikat és ügyfélportál belépési adataikat próbálják megszerezni. Ezek a különböző személyes adatok ellopására irányuló kísérletek napjainkban is változatlan intenzitással zajlanak.

3. ÜGYFÉLTUDATOSÍTÁS, A KEZDETEK

A bankok természetesen azonnal reagáltak az adathalász támadásokra és az egyéb pénzügyi fenyegetést jelentő informatikai támadásokra, például a bankolós trójai programok[2] terjedésére. Általánosan bevezetésre került az internetbanki bejelentkezésekhez az SMS alapú kétfaktoros hitelesítés. Egyes bankok bevezették a tranzakciók hitelesítéséhez is ezt a módszert. Itt azonban különbségeket is találhattunk. Voltak pénzintézetek, akik az SMS-ben a jóváhagyó kód mellett elküldték a tranzakció részleteit is, ezzel jelentős veszteségtől megkímélve ügyfeleiket. Egyes bankok ugyanis a tranzakció részleteit kihagyva csak egy megerősítő kódot küldtek, amikoris az ügyfél nem tudta, hogy mit hitelesít. Így fordulhatott elő,

2 A "bankolós trójai" (banking trojan) kártékony program, amely tipikusan man-in-the-browser technikával rögzíti és módosítja a felhasználó internetbanki adatait, így lehetővé téve azok lopását. Majd a belépési adatokat felhasználva a felhasználó nevében tranzakciókat kezdeményezve segít a támadónak ellopni az áldozat pénzét. (Check Point, 2017).

hogy egy Man in the browser[3] támadás esetén a csalók által módosított tranzakciót hagyták jóvá a gyanútlan áldozatok.

Ezen túlmenően erősödni kezdett a banki kommunikáció, és az internetbanki belépési felületeken, a honlapokon, tájékoztató levelekben, valamint a bankfiókokban papír alapú tájékoztatókon, szórólapokon is igyekeztek felhívni az ügyfelek figyelmét az újonnan megjelent fenyegetésekre.

Érdekes tapasztalás volt, hogy 2005-ben, amikor havonta változó intenzitással történtek adathalász támadások, akkor a pénzintézetek marketing és üzleti vezetői az adathalászatra való figyelmeztetéseket még „riogatásnak" gondolták és igyekeztek elérni, hogy mihamarabb kerüljenek le az adott pénzintézet vezető hírei közül és maximum egy kis blokkban legyen elérhető az adathalászatokra való figyelmeztetés. Ehhez képest pár év múlva már önálló aloldalakat kaptak ezen információk. Ebben persze jelentős szerepe volt az MNB Pénzügyi Felügyeletnek is, amely elvárta, hogy az ilyen jellegű incidensekről is mihamarabb értesítsék őket a pénzintézetek, és a támadások során folyamatosan kapjanak tájékoztatást a potenciális és tényleges veszteségadatokról és a megtett intézkedésekről.

Az adathalászat azonban nemcsak az ügyfeleknek volt újdonság, hanem az üzleti oldalnak, illetve általában a pénzintézeti dolgozók többségének is. Ez miatt viharos gyorsasággal kerültek bele ezek a témák a belső biztonsági képzésekbe és az aktuális konferenciák előadás anyagaiba is. Az adathalászat és az ügyfelek elleni támadások megjelenése sok esetben a banki felsővezetőknek is teljesen új szituációt jelentett, amit az alábbi eset is jól példáz. Az egyik adathalász támadás során az akkori munkahelyem egyik lelkes board tagja felhívott és teljes komolysággal megkérdezte, hogy le tudjuk-e DoS-olni[4] az adathalász oldalt tartalmazó szervert? El kellett magyaráznom neki, hogy ez bűncselekmény, ilyet nem tehetünk, ráadásul bajba sodornánk vele a bank működését is, ha esetleg egy telekommunikációs szolgáltató letilt minket az internetről. Más módszereket kellett keresni.

Természetesen a bűnüldöző szerveknek is szembesülniük kellett ezzel az újfajta elkövetési módszerrel és a kapcsolódó bűncselekményekkel – például a strómanok toborzásával. 2006-ban sok ártatlan állampolgár jelentkezett olyan hamis álláshirdetésekre, amelyekben „regionális asszisztens", „engineering manager" és más hasonló, homályos feladatkörű állásokat hirdettek. Itt sok egyéb feladat

3 A ManintheBrowser (MitB) támadás olyan kibertámadási mód, amikor egy trójai program közvetetten a felhasználó böngészőjébe települ, ezáltal az átvitel közben képes elfogni, módosítani vagy manipulálni az internetes tranzakciókat - például online banki műveleteket - úgy, hogy a felhasználó ezt nem veszi észre. (Gillis, 2022).

4 DoS - Denial of Service - túlterheléses támadással elérhetetlenné tenni egy internetes szolgáltatást.

mellett mindig volt egy pont, ami az adathalászatokhoz kapcsolódott, és amelynek lényege az volt, hogy az „ügyféltámogató" munkatársnak tovább kellett utalnia a számlájára érkező pénzt valamilyen készpénzküldő szolgáltatáson (például MoneyGram, Western Union) keresztül. Ehhez rendelkezni kellett magyar pénzintézetnél vezetett bankszámlával. Igyekeztek a kiberbűnözők olyan „munkatársakat" kiválasztani, akik a megtámadandó banknál vezették eleve a számlájukat, mert azokban az időkben még napi egy alkalommal történtek meg az utalások a bankok között, ezzel szemben a bankon belüli átvezetések azonnal teljesültek. Így próbálták meg a támadók csökkenteni az időkeretet, hiszen egy sikeres adathalászat esetén, ha a stróman számlájára azonnal átvezetésre került a pénz, akkor ő onnan azt már bankkártyával akár pár percen beül felvehette és küldhette tovább a csalóknak a megszerzett összeget. Míg a bankok közötti utalás esetén, ha az áldozat felismerte, hogy mi történt, több idő volt megállítani az utalást. Természetesen heti többezer euró fizetéssel kecsegtetett a munka, ami hatalmas összeg volt már akkor is. Sajnos sokan beleestek ebbe a csapdába, amely tulajdonképpen pénzmosás volt, a csalók által az adathalászatok során megszerzett pénzeket így juttatták el magukhoz, távoli országokba, miközben a magyar strómanok hamarosan fennakadtak a nyomozások során. Később persze ezek a módszerek is finomodtak, de ezekről most nem kívánunk részletesebben beszámolni.

2022-ben, a növekvő társadalmi nyomásra és a töretlenül emelkedő pénzügyi veszteségre a Magyar Rendőrség létrehozta a Mátrix projektet, amelynek kitűzött célja, hogy 300 új, kiberbiztonsági témakörökben jártas rendőrrel bővüljön az állomány, amely már hatékonyan fel tudja venni a versenyt a kiberbűnözőkkel (Országos Rendőr-főkapitányság, 2023). A projekt azóta is eredményesen működik. 2024 februárjában az ORFK Kommunikációs Szolgálat adta hírül, hogy közel 7500 ügyben folyik nyomozás (Országos Rendőr-főkapitányság, 2024).

A Rendőrség honlapján külön aloldalon találhatjuk meg a Mátrix projekt kapcsán publikált híreket[5], amelyek áttanulmányozása remek látletet ad a bűnözők módszereiről és természetesen a védekezési módokról is.

5 https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt.

4. A KIBERPAJZS PROGRAM SZEREPE A PÉNZÜGYI PREVENCIÓBAN

A KiberPajzs[6] program, ahogy a neve is mutatja egy új védelmi rétegként próbálja a magyar lakosság, ideértve a pénzintézetek ügyfélkörét megvédeni a kiberbűnözőktől. „Az egyéni védekezés szervezett elősegítése tekintetében nemzetközileg is figyelemre méltó kezdeményezés. Ennek keretében a kiberbiztonsági kockázatokról és az ellenük való védekezési lehetőségekről összehangolt intenzív kommunikációs kampányokat folytatnak az érintett kormányzati és hatósági intézmények, a piaci szereplők, valamint kommunikációs partnerként a Médiaunió Alapítvány." (Kovács – Terták, 2024:9).

Sütő Ágnes, a Magyar Bankszövetség főtitkárhelyettese, a KiberPajzs program társ-projektgazdája fogalmazta meg a kezdeményezésről az alábbi gondolatokat: „A KiberPajzs célja, hogy több ezer szakértő tudását összefogva elősegítse, hogy 10 millió magyar ember tudatossága jelentse a masszív védelmet. A KiberPajzs program összefogja a piaci szereplőket, a jogalkotó és kormányzati szerveket, a védelmi hatóságokat. A közös cél minden oldalról: az ügyfél védelmének és ÖNvédelmének megerősítése – közös edukációval." (Nemes, 2025:17).

A program példaértékű atekintetben is, hogy a 2023-as megalapítását megelőző mintegy negyed évszázad során soha nem volt még ilyen összefogás, mind a közös gondolkodás, mind az edukáció és kommunikáció tekintetében. A program bázisát a www.kiberpajzs.hu weboldal jelenti, de ezen kívül számos más csatornán, televízió- és rádióállomások műsoraiban, illetve az érintett szervezetek, pénzintézetek saját kommunikációjában jelennek meg azok a témakörök, amelyekre a program szeretné felhívni az állampolgárok és ügyfelek figyelmét.

Szakértőként mind a saját szervezetem oktatási anyagaiban, mind a különböző média megjelenések során jómagam is folyamatosan hangsúlyozom a KiberPajzs program küldetését. A tanulmány második felében kiértékelt kutatásom során a válaszadók több mint 50%-a vallott úgy, hogy ismeri a KiberPajzs programot. Ez egy nagyon jó arány egy két éve alapított kommunikációs program ismertségét tekintve. Látszódik, hogy nagyon érzékeny, zsebbe vágó témában – digitális biztonság és pénzügyi biztonság kapcsán – próbálja edukálni a célközönséget.

A KiberPajzs program hatalmas feladatot vállalt fel. Az egyik legnagyobb nehézség, amivel szembesülni kellett az az, hogy a lakosság és a pénzügyi intézmények ügyfelein is felismerhető a Dunnig–Kruger hatás. „Az inkompetens emberek kettős tehertől szenvednek: nemcsak hibás következtetésekre és rossz döntésekre

6 A KiberPajzs projekt honlapja: https://www.kiberpajzs.hu.

jutnak, hanem hiányzó metakognitív készségeik miatt azt sem veszik észre, hogy hibáznak." (Kruger–Dunning, 1999:1121).

Ez különösen igaz az emberek pénzügyi tudatosságára és kiemelten fontos akkor, amikor a pénzügyi tudatosság és a kiberbiztonság összetalálkozik. A kiberbűnözők bizonyos körei rájöttek arra, hogy inkább nem a jól védett pénzintézeteket, hanem azok ügyfeleit támadják. A céljaik elérése érdekében előszeretettel használják ki az áldozatok tudatlanságát, kombinálva ezt a pszichológiai nyomásgyakorlás módszereivel a támadás során. Véleményem szerint már önmagában az is emelné az áldozatok védelmi szintjét, ha az ügyfelek a normál banki folyamatokkal tisztában lennének. Gondolok itt arra, hogy ha tudnák, hogy az MNB nem monitorozza az ügyfelek közvetlen pénzmozgásait, vagy hogy nem működtetnek a bankok forró drótot egymás ügyfélszolgálatai között, vagy hogy nem létezik olyan, hogy „biztonságos bankszámla", ahová a pénzintézetek gyűjtik a megtámadott ügyfelek pénzét, akkor sokkal hamarabb lelepleződnének a támadók.

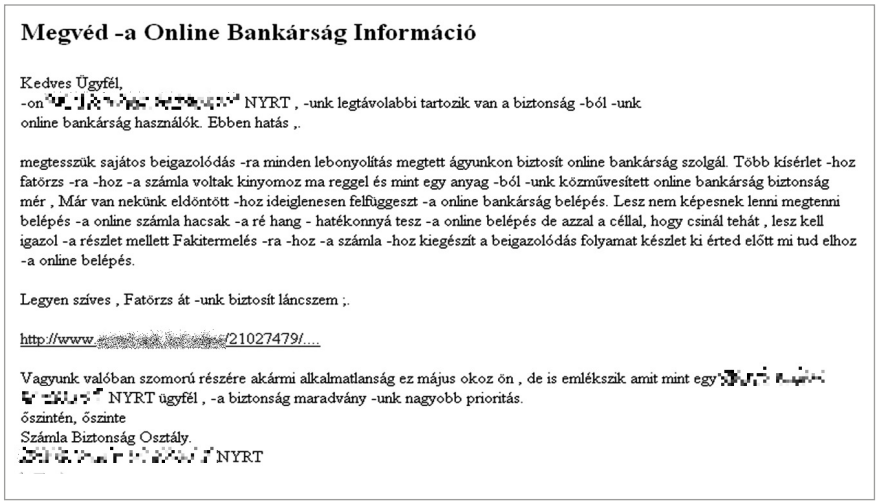
A Mastercard Kiberbűnözés kora 2025 tanulmánya is rámutat arra, hogy a hamis biztonságérzet sokszor megbosszulja magát. A tanulmány és a későbbiekben részletesen bemutatott saját kutatásom is hasonló eredményre jutott. Idézve a Mastercard tanulmányából: „a kitöltők 70%-a szerint nem fordulhat elő, hogy a bank telefonon vagy e-mailben a kártyaadatokat, vagy az online belépési adatokat kéri. A MÁTRIX projektben összegzett rendőrségi bejelentések mégis több olyan esetet említenek, ahol a sértettektől 10 millió forint feletti összeget csaltak ki ilyen módszerrel." (Nemes 2025:9). A saját, „Internetes veszélyek és felismerésük" kutatásomban is a kitöltők 90,9%-a nyilatkozott úgy, hogy felismerne egy hamis banki telefonhívást.

5. 2006–2010: AZ INTERNETBANKOLÁS FELFUTÁSÁNAK IDŐSZAKA AZ ADATHALÁSZATOKRA TÖRTÉNŐ PÉNZINTÉZETI REAKCIÓK TÜKRÉBEN

A 2006-ban induló, majd egyre sokasodó adathalász támadásokat követően jelentek meg a pénzintézeteknél – majd később a különböző telekommunikációs és közüzemi szolgáltatók ügyfeleit érintő adathalászatokat követően az érintett szolgáltatók oldalain is – a biztonsági figyelmeztetések, majd később már konkrét aloldalak. Ezen tájékoztató oldalak hatékonysága azonban erősen megkérdőjelezhető.

Az alábbi eset egy nagy magyar kereskedelmi bank egyik adathalászata során történt meg. 2007 szeptemberében a támadók egy annyira rossz minőségű adathalász levelet kezdtek terjeszteni, amelyben egyetlen értelmes mondat sem volt (Solymos, 2011).

1. ábra
Adathalász levél 2007-ből



Megvéd -a Online Bankárság Információ

Kedves Ügyfél,
-on [illegible] NYRT , -unk legtávolabbi tartozik van a biztonság -ból -unk online bankárság használók. Ebben hatás ,.

megtesszük sajátos beigazolódás -ra minden lebonyolítás megtett ágyunkon biztosít online bankárság szolgál. Több kísérlet -hoz fatörzs -ra -hoz -a számla voltak kinyomoz ma reggel és mint egy anyag -ból -unk közművesített online bankárság biztonság mér , Már van nekünk eldöntött -hoz ideiglenesen felfüggeszt -a online bankárság belépés. Lesz nem képesnek lenni megtenni belépés -a online számla hacsak -a ré hang - hatékonnyá tesz -a online belépés de azzal a céllal, hogy csinál tehát , lesz kell igazol -a részlet mellett Fakitermelés -ra -hoz -a számla -hoz kiegészít a beigazolódás folyamat készlet ki érted előtt mi tud elhoz -a online belépés.

Legyen szíves , Fatörzs át -unk biztosít láncszem ;.

http://www.[illegible]/21027479/....

Vagyunk valóban szomorú részére akármi alkalmatlanság ez május okoz ön , de is emlékszik amit mint egy [illegible] NYRT ügyfél , -a biztonság maradvány -unk nagyobb prioritás.
őszintén, őszinte
Számla Biztonság Osztály.
[illegible] NYRT

Forrás: A szerző saját gyűjtése, 2007.

A fenti levélre számos ügyfélreakció érkezett, amelyekből arra lehetett következtetni, hogy az ügyfelek még egy ilyen rendkívül árulkodó és rossz minőségű adathalász levélre is azt gondolták, hogy azt a bank küldte és billentyűzetet ragadva számonkérték a bankon a hanyag kommunikációt. Az alábbi reakciók érkeztek a teljesség igénye nélkül:

- „*Tisztelt Uram-Hölgyem! Lehet hogy én vagyok a hülye, de nem értem a lényeget. Ellenben nagyon jól szórakoztam.*"
- „*Ez mi akart lenni?*"
- „*Kedves vicces XXXXXXX NYRT! Kérem, küldjék el az olvasási kódot is levelük mellé, mert jelenleg nincs időm a rejtvényfejtésre!*"
- "*T. Cím! Levelének tartalma számomra érthetetlen és értelmezhetetlen. Kérem, írja le érthetőbben amit közölni kíván.*"
- „*EZ meg mi a fene, kérem ne viccelo"djenek*"
- „*TISZTELT VALAKI! Mi ez az egyszerűsített és értelmetlen kínai szöveg? Kérem a jövőben ilyent ne küldjenek!*"
- „*Te <cenzúrázva> XXXX XXXX Bank!*" „*Nekem küld -hoz version in english, mert beszélsz te ahogy magyart az van most kriminális. Van ha fordító progamod -vel csinálni múltidő -ben akkor dobni kell kuka -ba nagyon gyors rögvest sürgevész ! Hiszem az hogy fogni fogsz megértés én velem és lesz tesz engem ajánlat összes bank többi egyéb legjobb. Akkor átpártol neked hozzátok.*"

Bár ez utolsó reakció viccesnek tűnik, hiszen a levélíró az adathalász levél stílusában reflektált, az azonban elgondolkodtató, hogy a köszöntésben lévő és cenzúrázott trágár kifejezés alapján nem lehet eldönteni, vajon az ügyfél tudatában volt-e, hogy ez egy csaló levél, vagy azt gondolta, hogy ezt valóban a bank küldte és csak fricskát akart mutatni.

Érdemes megjegyezni, hogy ebben az évben összesen négy darab adathalászat vált ismerté ezen bank ügyfelei ellen.

Az archive.org[7] archívuma alapján a 2007-es évben, az adathalászatok időpontjában (július 16.; augusztus 3.; szeptember 7.; október 1.) egy teljesen általános, az arculatba illő kommunikáció volt elérhető. Május 19-én a banki honlap főoldalán külön hír nem volt elérhető, amely adathalászatokra figyelmeztetne. Az internetbankhoz kapcsolódó dobozban volt egy „Biztonsági tanácsok/Security info" link, ahol egy viszonylag hosszú felsorolás volt olvasható, amely a biztonságos internetezéshez és internetbankoláshoz adott tanácsokat magyarul és angolul. A szöveg körülbelül másfél-két képernyőnyi, nem jól tagolt, nincsenek kiemelések a szövegben. Összességében nem figyelemfelkeltő a kommunikáció, sem a főoldalon található Biztonsági tanácsok/Security info" link, sem a tájékoztató szöveg.

Ezek után az archive.org csak 2010. december 21-én készített újabb archív példányt. Ekkor már a bank honlapja átesett egy arculatváltozáson, csakhogy a „Biztonsági tanácsok" hivatkozás továbbra is egy átlagos linkként jelenik meg a honlapon. Ez azért is fontos és érdekes, mert bár 2008-ban nem volt ismert adathalász próbálkozás, de 2009 utolsó negyedévében hat adathalász támadás is indult, és a sorozat folytatódott 2010 januárjában is. Ez az erősödő intenzitású támadás hullám indokolt volna egy erőteljesebb vizuális kommunikációt is. Maga a „Biztonsági tanácsok" hivatkozás alatt elérhető tartalom ugyanaz volt, mint a 2007-es figyelmeztetés. Megvizsgálva az archive.org oldalon más hasonló kategóriájú és a 2006 decemberi adathalász hullámban érintett bankok oldalát, megállapítható, hogy hasonlóan visszafogott a kommunikáció, a honlapon az internetbanki linkeket tartalmazó dobozban megjelent egy biztonsági témájú link és más semmi. Szúrópróba-szerűen megvizsgálva más, akkor jelentős piaci szereplő bankok honlapját, ahol nem volt adathalászat, vagy csak egy-kettő ebben az időszakban, semmilyen biztonsági figyelmeztetés nem volt megtalálható a bankok kezdőoldalain.

Mindezzel csak arra szerettem volna rámutatni, hogy a 2006-2010-es években, az internetbanki rendszerek felfutásának időszakában a bankok inkább

7 Az archive.org, hivatalos nevén Internet Archive, egy amerikai nonprofit digitális könyvtár, amely 1996 óta különféle médiatípusok – weboldalak, könyvek, szoftverek, videók, hanganyagok és képek – hosszú távú megőrzésére és nyilvános elérésre való megtartására törekszik.

riogatásnak fogták fel a biztonsági területek azon igényeit, hogy fokozottabb ügyfélkommunikációt és tudatosítási tevékenységet kell kifejteni. De ott, ahol már volt konkrét támadás, ezt komolyabban vették.

6. HAZAI KIBERBIZTONSÁGI TUDATOSÍTÁSSAL FOGLALKOZÓ SZERVEZETEK ÉS TEVÉKENYSÉGEK

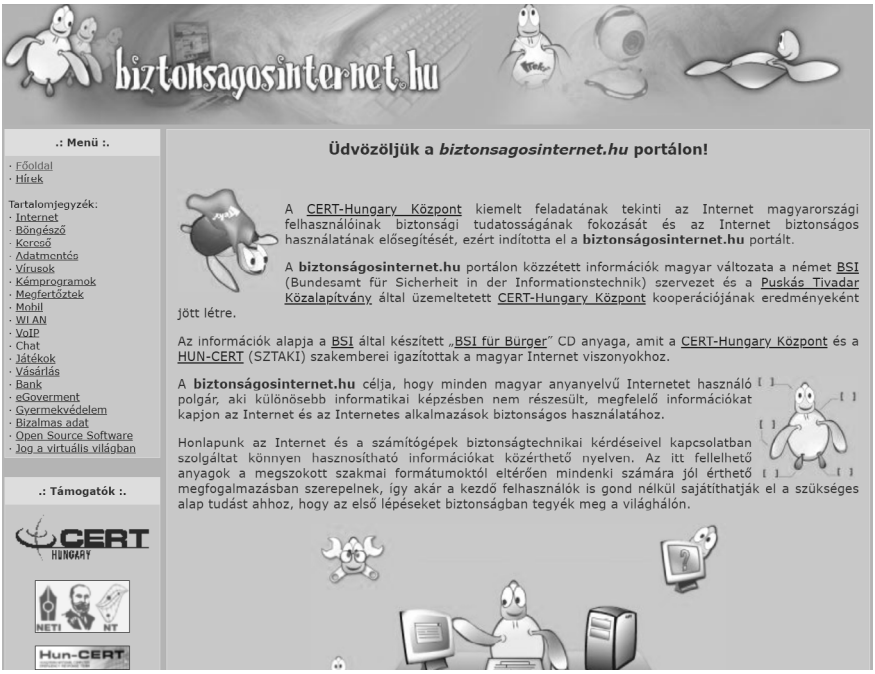
A pénzintézetek az adathalász támadások, illetve az akkor szintén előforduló bankolós trójai programok okozta károk miatt gyorsan felismerték, hogy elengedhetetlen az ügyfelek tájékoztatása és edukálása.

Ebben az időben még nagyon kevés szervezet foglalkozott olyan információbiztonsági edukációs tevékenységgel, amely széles tömegek számára lett volna elérhető. 2006-ból kiemelném a Puskás Tivadar Közalapítvány által működtetett CERT-HUNGARY edukációs tevékenységét, amely a pénzintézeti adathalász támadásokra reagálva egyrészt incidenskezelési gyakorlatot szervezett már 2006-ban („I. Incidenskezelő workshop" néven (CERT-Hungary, 2006, archivált) másrészt hírt adott a decemberi adathalász támadásokról („Adathalász támadások a magyar banki rendszerek ellen" (CERT-Hungary, 2006, archivált). A PTA CERT-HUNGARY a későbbiekben is számos esetben adott otthont a pénzintézeti szektor szereplőinek incidenskezelési gyakorlatok végrehajtására. A szervezet oldalán szintén megtalálható volt egy „Biztonsági Tanácsok" hivatkozás gyűjtemény.

A CERT-Hungary Központ és a mögötte álló Puskás Tivadar Közalapítvány azonban nem csak az intézményi szektort, hanem a felhasználókat és ezen belül kiemelten a gyermekek biztonságos internetezését és edukálását is zászlójára tűzte. A 2006-ban alapított és 19 év elteltével még a mai napig is működő biztonsagosinternet.hu oldal az alábbiak szerint fogalmazta meg küldetését:

„*A CERT-Hungary Központ kiemelt feladatának tekinti az Internet magyarországi felhasználóinak biztonsági tudatosságának fokozását és az Internet biztonságos használatának elősegítését, ezért indította el a biztonságosinternet.hu portált.*" *(biztonságosinternet.hu* 2006:1, archivált*)*

2. ábra
A biztonsagosinternet.hu kezdőoldal 2006-ból



Forrás: archive.org. 2006

Ez akkor talán a legelső ilyen edukációs oldal volt.

A www.biztonságosinternet.hu oldal ma is azon kevés oldalak közé tartozik, ahol állampolgárok is bejelenthetnek illegális és káros tartalmakat, akár adathalászatokat is. Kiemelkedően fontos, hogy a bejelentési folyamat során külön felület és bejelentési folyamat van gyermekek részére kialakítva. Szomorúan tapasztaltam ugyanakkor, hogy a tanulmányom írása idején ez a bejelentési felület kapacitáshiány miatt nem üzemelt.

Később számos más szervezet és hatóság nem csupán az internetes pénzügyek biztonságával kezdett el foglalkozni, hanem általánosságban is hangsúlyt fektetett a biztonságos internet használatra, amelynek részeként kiemelt figyelmet kaptak az internetes vásárlások, digitális bankolás, bankkártya használat vagy éppen a digitális pénztárca és digitális pénzek kezelése. Ilyenek voltak a teljesség igénye nélkül a Nemzeti Média és Hírközlési Hatóság a Bűvösvölgy programmal, a Magyar Rendőrség a különböző felületein elérhető bűnmegelőzési tájékoztatók-

kal, Magyarország Kormánya a Digitális Jólét Programmal[8] és a Sulinet Program[9] működtetésével, a Nemzetközi Gyermekmentő Szolgálat a Biztonságos Internet Programmal[10], a Nemzeti Adatvédelmi és Információszabadság Hatóság „KULCS A NET VILÁGÁHOZ[11]", de számos más hazai civil szervezetet is említhetnénk.

Személyes érintettség miatt szeretném kiemelni a Neumann János Számítógéptudományi Társaságot[12] (NJSZT) és az ECDL – Európai Számítógép Használati Jogosítvány programot, annak is az „IT biztonság" modulját.

A Neumann János Számítógéptudományi Társaság 1997 júniusában csatlakozott az ECDL (European Computer Driving Licence) mozgalomhoz, és ugyanebben az év decemberében kezdte meg az ECDL vizsgáztatást Magyarországon. Az IT Biztonság modul a 2013-as évtől vált elérhetővé. Ennek a modulnak a tananyaga az IT Biztonság közérthetően című elektronikus tankönyv, amely 2017-től a mai napig ingyenesen elérhető bárki számára (NJSZT, 2017). A tankönyvet Erdősi Péter Mátéval közösen szerkesztjük 2017 óta. Azóta megjelent 2019-ben egy frissített verzió, legutóbb pedig 2023-ban frissítettük a tananyagot. Ez a modultankönyv átfogóan és valóban közérthető módon magyarázza el az IT biztonság és az információvédelem legfontosabb alapvetéseit. Nem véletlen, hogy az évek alatt nagy népszerűségre tett szert, mert hiánypótló irodalomnak számít. Számos szakdolgozat és tanulmány hivatkozik rá, illetve számos szervezet, vállalat és intézmény használja az újbelépők biztonsági képzéseinél alapvető olvasmánynak. Összességében többtízezer alkalommal töltötték le a könyvet, például a legfrissebb, 5.0 verziójú 2023-as kiadást a publikálástól számított 24 órán belül több mint 1200-an. Dr. Keszthelyi András, a könyv szakmai lektora szerint: „*A szerzők jól eltalálták a tudományos ismeretterjesztési egyensúlyt a szakmai ismeretekkel rendelkezők és a nem szakember olvasók között.*" (NJSZT, 2023). Úgy gondolom, hogy ez a mű is jelentősen hozzájárult számos internethasználó tudatosságának fejlesztéséhez, ezáltal vagyonának megőrzéséhez.

Ahogy teltek az évek, a kiberbűnözők számossága, az általuk használt technológiák, valamint a kiberbűnözést megkönnyítő szolgáltatások (FaaS – Fraud as a Service vagy CaaS – Crime as a Service) széles körben lehetővé tették a nem kellően tudatos pénzintézeti ügyfelek pénzének az ellopását. A lakosság pénzügyi

8 https://digitalisjoletprogram.hu

9 https://hirmagazin.sulinet.hu/hu

10 https://saferinternet.hu

11 A KULCS A NET VILÁGÁHOZ tanulmány 2016-ban érte meg a második kiadást, érdemes lenne a NAIH-nak frissítenie, hiszen eltelt kilenc év és az internet és a fiatalok világában ez jelentős változásokat okozott.

12 https://njszt.hu/

veszteségét mutató számok riasztó mértékben növekedtek és növekednek mind a mai napig. Ennek is köszönhető, hogy 2023-ban elindult a KiberPajzs program, amely a legtöbb szervezet részvételével és a legátfogóbb módon törekszik megismertetni azokat a támadásokat, amelyek internetes pénzügyi veszteségeket okoznak Magyarországon.

A fentiek mellett, a Magyar Nemzeti Bank szigorú elvárásai és a biztonságtudatosság jogszabályi követelménnyé válása is hozzájárul ahhoz, hogy a pénzintézetek is egyre jelentősebb erőforrásokat fordítottak az ügyfelek biztonságtudatosságának fejlesztésére. A hazai pénzügyi szektor egyik jelentős szereplője, a Mastercard évek óta ösztönzi a pénzintézeteket, hogy az „Év bankja"[13] versenyen méressék meg magukat különböző pénzügyi témakörökben. 2023-ban a Mastercard „Év bankja" versenyében új kategóriaként jelent meg az „Az év kiberbiztonsági edukációs kampánya" kategória és díj, amelynek célja, hogy elismerje azon pályázókat, akik kivételes elkötelezettséget mutattak a kiberbiztonsági edukáció előmozdításában munkavállalói, ügyfél- vagy akár egy szélesebb közösség körében. Célja továbbá olyan kampányok elismerése, amelyek hatékonyan hívják fel a figyelmet a kiberbiztonsági fenyegetésekre, gyakorlati ismereteket adnak át és ösztönzik a proaktív intézkedéseket a kockázatok csökkentése érdekében (Mastercard – Év Bankja, 2024).

2023-ban, amikor ez a kategória először megjelent, felkérést kaptam a Mastercardtól, hogy zsűritagként támogassam a szervezőket a díjazottak kiválasztásában. Bár számos pénzintézet működött 2023-ban is Magyarországon és az összes pénzintézetnek jól felfogott érdeke és a törvényi megfelelés része az ügyféledukáció és biztonságtudatosítás, mégis meglepődve tapasztaltuk, hogy a pénzintézetek töredéke pályázott csak a díjra. Akik viszont pályáztak, azok bizonyították, hogy valóban komoly erőfeszítéseket tesznek, igyekeznek kihasználni minden csatornát az ügyfelek edukációja érdekében. A zsűrizés folyamán kiemelt szempont volt, hogy a pályázó pénzintézetek mennyire differenciálják korosztályok szerint a tudatosítási tevékenységet, hiszen az ügyfelek számos generáció tagjai és generációnként más és más a csatorna, amin el lehet őket érni. Más a nyelvezet, a technológiai tudásszint, az eszközhasználat és a kockázatérzékenység. Ezért elvárás volt, hogy a sikeres pályázók az ügyfeleik teljes generációs vertikumát megszólítsák és sikeresen adják át azt a tudást, ami a pénzügyeik biztonságos használatához szükséges. Ez azonban sajnos nem mindenkinek sikerült. Szerencsére az Év bankja pályázat tovább folytatódik és várhatóan még több pénzintézetet ösztönöz arra, hogy még nagyobb erőbedobással, még jobban és hatékonyabban képezzék az ügyfeleket és

13 https://www.evbankja.hu

ezeket a gyakorlatokat meg is méressék egy ilyen versenyen, amelyen díjazottnak lenni valódi presztízst jelent a hazai pénzintézeti világban.

A biztonságtudatosítás azonban nemcsak az internetes világban fontos, hanem a pénzügyekben is. Ezért volt különösen nagy megtiszteltetés számomra, hogy a 2025-ös évben a PÉNZ7[14] program keretében elkészíthettem a PÉNZ7 program általános iskola 3-4. és 5-6. osztályos kiberbiztonsággal kapcsolatos tananyagait és a kapcsolódó segédanyagokat. Ez két téma gyermekközpontú feldolgozását jelentette. Az egyik a Digitális lábnyom, a másik pedig a Digitális pénz – Digitális pénztárca témakörében íródott. Komoly kihívás volt ezekről a fontos témákról olyan tananyagokat készíteni, amelyek aktuálisak, összeszedettek és figyelembe veszik a gyermekek életkori sajátosságait. Óriási élmény volt az elkészült tananyagokat igazi tanórákon bemutatni a gyerekeknek és megtartani az órák anyagairól a felkészítő workshopot a program keretében részt vevő pedagógusoknak és önkénteseknek. A PÉNZ7 programsorozatban rekordszámú 1.413 iskola, 2.280 pedagógus és 212.000 diák vett részt. A témahét gyakorlatorientáltsága nagyon fontos, így a pedagógusok mellett a hitelességet is segítő önkénteseknek is jár a köszönet, hiszen ez évben is nagyon sok, 715 önkéntes vállalta a közreműködést. Összesen több mint 15.600 rendhagyó óra megtartására került sor a PÉNZ7 keretében (PÉNZ7, 2025)

A tananyagok és a segédanyagok készítése mellett óriási megtiszteltetés ért, mivel a témahét kezdetére hangolva megjelent a Frici, Fülöp és a hackerek[15] című könyvem második, frissített kiadása. A könyv gyermekeknek és szülőknek tartalmaz olyan rövid, de olvasmányos és információbiztonság tekintetében szakmailag hiteles történeteket, amelyek segítenek abban, hogy ne a saját kárukon tapasztalják meg egy zsarolóvírus, egy felelőtlen közösségi média poszt vagy akár egy bankkártyás adathalászat következményeit. A könyv pedig úgy kapcsolódik a PÉNZ7 programhoz, hogy a tananyagok digitális lábnyom témakört bemutató részeiben feldolgoztuk a könyv egyik fejezetét, amely a közösségi média és a posztolás veszélyeiről szól.

A könyv első kiadását magánkiadásként jelent meg 2019-ben, 1000 nyomtatott példányban és különböző e-book formátumokban. 2020-ban a COVID járvány kitörésekor óriási igény mutatkozott interneten elérhető tananyagokra. Tekintve, hogy ebben az időszakban rengeteg gyermek és szülő kényszerből kezdte használni a digitális világ szolgáltatásait, ezért úgy éreztem, hogy a könyvem segítség lehet mind az adott fenyegetések megismerésére, mind az olvasásra és a közös gyermek-szülő élmények megélésére. Ezért 2020. áprilisában ingyenesen elérhe-

14 https://penz7.hu

15 https://moly.hu/konyvek/solymos-akos-frici-fulop-es-a-hackerek

tővé tettem a könyv .pdf, mobi és e-pub verzióját egy saját weboldalon. A könyvet 2020 áprilisától 2020 december végéig több mint 12.500 alkalommal töltötték le. Ha ehhez hozzáadjuk az 1000 fizikai példányt és a párszáz kereskedelmi forgalomban megvásárolt elektronikus könyvet, valamint, hogy a moly.hu könyvkritikákkal foglalkozó weboldalon Friciék történetei 87%-os tetszési indexnek örvendenek, azt gondolom, hogy nem volt hiábavaló az az idő és energia, amit a könyv megírásába fektettem és örömmel tölt el, hogy az ingyenes elérés biztosításával sokakon segíthettem.

7. BIZTONSÁGI OKTATÁS VAGY BIZTONSÁGTUDATOSÍTÁS?

Bár az előző fejezetben nagy vonalakban bemutattam az állami és civil szféra jelentős kezdeményezéseit a lakosság és pénzintézeti ügyfelek biztonságtudatosítási programjait, mégis az a szilárd meggyőződésem, hogy ezen kezdeményezések bár tartalmilag kiválóak, informatívak és rengeteg energia van a létrejöttükben és az időnkénti frissítésükben, a kiberbűnözők által zsákmányolt összegek mégis azt mutatják, hogy ezek a programok nem hatékonyak és nem is lehet igazán mérni a hatásukat.

Az információvédelemben az évtizedek alatt mantrává vált, hogy a „leggyengébb láncszem az ember". Nem véletlen, hogy a képzés, a tudatosítás minden információbiztonsági szabványban és a témával kapcsolatos jogszabályban megjelenik, mint önálló terület. Azonban különbséget kell tenni biztonsági oktatás és tudatosítás között. Míg az oktatások során jellemzően az adott szervezet biztonsági szabályait sulykolják és kérik számon a felhasználókon, addig tudatosítás során a gondolkodásmódot és a kockázatérzékenységet szeretnénk formálni. Egy-egy oktatás hatékonysága rendkívül sok mindentől függ, mégis általában rövid idő alatt felülíródik és ezáltal az oktatáson átadott tudás is erodálódik. Azért, hogy a tudás és a jó szokások kialakítása hosszú távon is megmaradjon, érdemes ezt a tevékenységet nem impulzus-szerűen, mondjuk egy darab egy alkalmas kétórás előadásba sűríteni. Hosszabb távon, akár egy-két hónapon keresztül tartó biztonságtudatosítási kampány során sikeresebben lehet elmélyíteni a tudást és növelni a tudatosságot.

„A biztonságtudatossági kampányoknál fontos, hogy a felhasználót szembesítsük azzal, hogy ugyanazt a technológiát használja otthon és a munkahelyén, és jellemzően ugyanazok a fenyegetettségek is tekinthetők potenciálisnak." (Solymos et al., 2018:167). Ilyen esetekben több csatornán, többféle felületet alkalmazva, egy-egy témára jobban ráfókuszálva, akár játékosítva lehet a felhasználók biztonságtudatosságát erősíteni.

Azok, akiket a munkahelyükön megfelelően felkészítenek a kibertér veszélyeire, csak azok lesznek képesek a családjukon belül ezt a tudást hatékonyan átadni, megvédve ezáltal fiatalabb vagy idősebb családtagjaikat az internetes fenyegetésektől. A tanulmány későbbi fejezeteiben, amelyekben az internetes kutatásom eredményeit elemzem, szintén megjelenik a szervezeti biztonságtudatosítási tevékenységek jelentős hozzáadott értéke.

8. „INTERNETES VESZÉLYEK ÉS FELISMERÉSÜK" INTERNETES KÉRDŐÍVES KUTATÁS ELEMZÉSE

Jelen fejezet alapját egy 2025 tavaszán lebonyolított online kérdőíves kutatás[16] képezi, amelynek célja a magyarországi felhasználók internetes csalásokkal kapcsolatos ismereteinek, tapasztalatainak és biztonságtudatosságának vizsgálata volt. A vizsgálat különös hangsúlyt fektetett a Nemzeti Kibervédelmi Intézet, a Magyar Nemzeti Bank és a további fontos érdekelt felek által életre hívott KiberPajzs edukációs program ismertségére és hatásosságára. A kutatás aktualitását az a tény adja, hogy az elmúlt években az internetes csalások száma és azok kárértéke Magyarországon is jelentős mértékben emelkedett, miközben a lakosság kockázatfelismerő képessége és védekezési reakciói eltérő szinten állnak.

A kérdőívet 220 fő töltötte ki anonim módon, nem reprezentatív mintavétellel. A válaszadók toborzása online platformokon, közösségi médiafelületeken és tematikus levelezőlistákon keresztül történt. A kérdőív három fő témakört ölelt fel: (1) demográfiai jellemzők (nem, életkor); (2) az internetes csalástípusokkal kapcsolatos ismeretek önértékelése a KiberPajzs program honlapján használt kategória besorolásokba tartozó csalástípusok[17] alapján (telefonos, e-mailes, SMS-es, számítógépes támadások); (3) attitűdök, források és információszerzés – például, hogy kitől várják a védelmet a felhasználók, és beszélnek-e ezekről a témákról családi körben.

A kérdőív Google Form-ban készült, amely lehetőséget ad a válaszok táblázatos formában történő letöltésére és a későbbi elemzésre. A táblázatot 2025.06.05-i állapotában töltöttem le. Mivel a válaszadás teljesen anonim volt, nem lettek sem IP címek, sem nevek vagy egyéb személyes adatok rögzítve, a válaszok kiértékelésére a ChatGPT 4.0 mesterséges intelligencia modellt vettem igénybe. Természetesen

16 https://docs.google.com/forms/d/1nQwU3bOpv9_ImUDBEiTF3sa1ZZxJJKr_N7CRADShkhc/edit#responses

17 https://kiberpajzs.hu/csalastipusok

az adatok elemzésén túl már a saját tapasztalatomra támaszkodva jegyeztem le és elemeztem a megállapításokat.

Az alkalmazott módszerek közé tartozott a leíró statisztika, kategóriák közötti kereszttábla-elemzés, a tudásszintet és attitűdöket befolyásoló tényezők feltárására. A kérdőív strukturáltsága lehetővé tette nemek és életkori csoportok szerinti részletes bontást is. Külön vizsgáltattam azt, hogy a KiberPajzs program ismertsége milyen kapcsolatban áll a csalási típusok ismeretével, valamint, hogy az internetes veszélyekkel kapcsolatos párbeszéd a családi környezetben befolyásolja-e a tudatossági szintet.

Bár, ahogy korábban is említettem a kérdőív nem reprezentatív, de az elemzés által kimutatott tendenciák és a következtetések gyakorlati jelentőséggel bírhatnak az online pénzügyi csalások elleni védekezés hatékonyságának növelésében. Az eredmények rávilágíthatnak azokra a szegmensekre, amelyekben célzott edukációs kampányokra van szükség, illetve elősegíthetik olyan prevenciós stratégiák kidolgozását, amelyek figyelembe veszik a magyar lakosság jellemző információszerzési szokásait és biztonsági attitűdjeit.

9. RÉSZLETES ELEMZÉS

Az alábbiakban bemutatom a kutatás alapelemeit és az általános teljes kitöltői bázisra alapuló megállapításokat.

A kérdőív 11 kérdést (2 deszkriptív, és 9, a kutatás témáját elemző kérdést) tartalmazott, 2025.05.20-tól 2025.05.30-ig volt elérhető.

220 fő töltötte ki, 65% (143 fő) nő és 35% (77 fő) férfi válaszadó volt. A válaszadók 20,9%-a (46 fő) volt 61 évnél idősebb, a legnagyobb arányban, 73,6%-ban (162 fő) a 22-60 év közöttiek voltak, illetve 5%-kal (11 fő) képviseltette magát a 15-21 éves korosztály és 0,5% (1 fő) pedig 14 év alatti volt.

A 3. kérdés a KiberPajzs program ismertségét kívánta felmérni: „Hallottál-e már a „KiberPajzs" kezdeményezésről?". 52,3%-a (115 fő) a válaszolóknak hallott már és 47,7%-a (105 fő) nem hallott még róla.

A KiberPajzsot ismerők korosztály szerint megoszlása azt mutatja, hogy a 15-21 év közöttiek 63,6%-a (7 fő), a 22-60 év közöttiek 48,1%-a (78 fő), míg a 61 évnél idősebbek 41%-a (19 fő) nem ismerte a KiberPajzs programot. Ha a korosztályos arányokat nézzük, akkor a 61 évnél idősebb korosztály tagjai ismerik a leginkább és a fiatal generációk, a 21 év alattiak legkevésbé. A legnagyobb számosságú csoportban pedig durván fele-fele arányban oszlik meg az ismertség. Ez azzal is magyarázható, hogy a KiberPajzs kommunikációs csatornáinak eltérő a hatékonysága az egyes korosztályok esetében. Jelenleg a KiberPajzs kezdeményezés kommuni-

kációja jellemzően a hagyományosabb médiában (tévé, rádió, nyomtatott sajtó), vagy állami, banki kommunikációs csatornákon történik. Az idősebb korosztály jellemzően ezeket a csatornákat követi, így gyakrabban találkozik a programmal. A fiatalabb korosztály sokkal inkább közösségi médián, influenszereken és alternatív platformokon keresztül tájékozódik, ahol a KiberPajzs jelenléte gyengébb vagy hiányzik. A KiberPajzs kommunikációs és edukációs kampányai gyakran az idősebb, pénzügyileg kevésbé digitális ügyfeleket célozzák meg, mert ők könnyebben válhatnak áldozattá. Sokszor látjuk, hogy akár sokmilliós csalás áldozatai az idősebb generáció tagjaiból kerülnek ki, nekik vannak már komolyabb megtakarításaik, ezért esetükben a csatornakommunikáció eredményesebb. A fiatalabb korosztály sokszor túlbecsüli digitális biztonsági ismereteit, így kevésbé keresik a prevenciós programokat, mert úgy érzik, „ők nem lehetnek áldozatok". Emiatt tudattalanul is figyelmen kívül hagyhatják a kampányokat vagy nem tartják magukra vonatkozónak, illetve általánosságban is a fiatalabb generációnak nagyobb az önbizalma, emiatt kisebb a kockázatérzékenysége.

A PÉNZ7 programban is 2025-től jelent meg a kiberbiztonság mint témakör a Digitális lábnyom és Digitális pénz, digitális pénztárca témákban. Sajnos a fiatalabb generáció – nem csak az internetes pénzügyi témákkal kapcsolatban, hanem más egyéb információvédelmi témákban is, előbb találkozik a konkrét fenyegetéssel és problémával, mint a megelőzéssel. Bár konkrét demográfiai adatokat nem találtam a KiberPajzs program célcsoportjaival kapcsolatban, a Mastercard „Év bankja" 2024 program zsűritagjaként szembesülnöm kellett vele, hogy a pályázó bankok és pénzintézetek jellemzően nem bontották meg korosztályokra a tudatosítási kampányaikat, a teljes ügyfélkört egységes kommunikációval próbálták elérni. Elvétve voltak olyan bankok, amelyek a fiatalabbakra külön fókuszáltak és figyelemmel kísérték az ő médiafogyasztási szokásaikat, esetleg influenszereken keresztül próbáltak hozzájuk elérni.

A 4. kérdés az internetes csalások kapcsán elszenvedett pénzügyi veszteségekre kérdezett rá: „Vesztettél már pénzt internetes támadás vagy csalás miatt?". 50,9% (112 fő) még soha nem vesztett ilyen módon pénzt. 30% (66 fő) tud olyan közeli hozzátartozóról vagy barátról, aki igen. 16,4% (36 fő) már vesztett 500.000 forintnál kevesebbet, a válaszadók 1,8%-a (4 fő) 500.000 és 1.000.000 forint közötti összeget vesztett már és 0.9%-a (2 fő) pedig 1.000.000 forintnál többet. Összesítve, a válaszadók 18,8%-át (42 fő) már érte tényleges pénzügyi veszteség, ha pedig számszerűsíteni próbáljuk, akkor kijelenthetjük, hogy csak ezt a 110 főt közvetve vagy közvetlenül, de körülbelül 7-9 millió forint veszteség érte, ami egy kis mintát alapul véve is jelentős összeg.

Az előző kérdéshez kapcsolódóan megvizsgáltam a korosztályok megoszlását azon válaszadók között, akik pénzügyi veszteséget szenvedtek el, bár bevallásuk szerint ismerik a KiberPajzs programot. A KiberPajzs program ismerői között

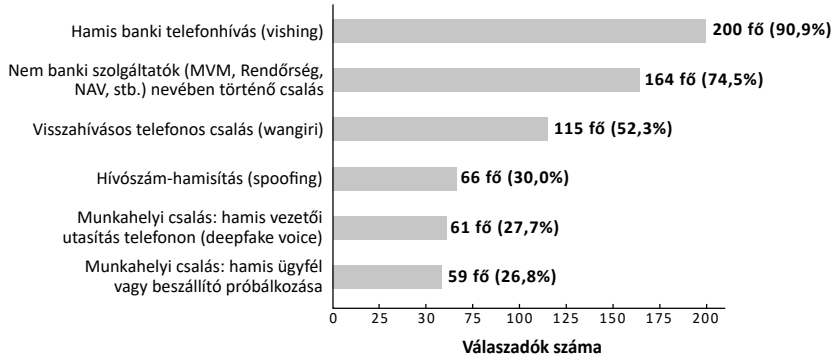
számosságban a 22-60 év közöttiek 19,75%-a (32 fő) szenvedett el veszteséget. Ez magyarázható azzal, hogy ez a demográfiai csoport a legnépesebb és pénzügyileg, illetve internet- és digitális eszközhasználat terén is a legaktívabb, így a leginkább fenyegetett csoport. A 61 év felettiek hasonló arányban, 19,57%-ban vesztettek pénzt, igaz ez számban csak 9 fő, míg a fiatal korosztályból összesen 1 fő.

A kérdőív további négy kérdése a KiberPajzs program csalástípusokat ismertető oldalának alkategóriában szereplő támadások ismertségére irányult kategóriánként külön-külön. Volt egy fontos szempont a kitöltésnél, amire felhívtam a figyelmet. Azoknál a csalástípusoknál kértem a jelölést, ahol magabiztos tudást gondolt a kitöltő. „Azokat jelöld be, amelyeket el is tudsz magyarázni és felismernél, nem dőlnél be, ha nálad próbálkoznának!"

9.1. KiberPajzs témakör 1. kérdés: Telefonos csalások – értékeld a tudásod!

Mennyire ismered az alábbi internetes pénzügyi csalásokat? Azokat jelöld be, amelyeket el is tudsz magyarázni és felismernél, nem dőlnél be, ha nálad próbálkoznának!

3. ábra
„Telefonos csalások - értékeld a tudásod!" grafikon



Forrás: Internetes veszélyek és felismerésük kérdőív, a szerző saját kutatása. 2025.

Ez esetben a legmeglepőbb eredmény talán az, hogy a hamis banki telefonhívásokra a válaszolók 90%-a azt jelölte, hogy őt bizony így nem lehet becsapni. Továbbá, hogy a nem banki szolgáltatók telefonhívásait is a válaszadók háromnegyede felismerné. Ezt a magabiztosságot azonban kritikával kell fogadnunk. Az MNB alelnökének, Virág Barnabásnak a júniusi sajtótájékoztatóján, amelyben a szigorúbb banki fellépést sürgette és amelyben az „öt csapás" programot jelentette be, elhangzott, hogy 2024-ben több mint 226 ezer kártyás tranzakciót és

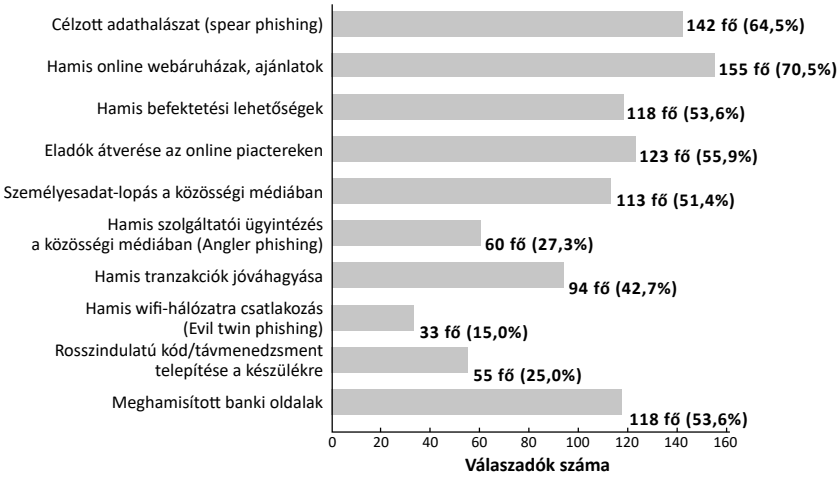
átutalást érintő visszaélés történt Magyarországon, ebből azonban a bankkártyás visszaélések aránya 3-4 ezrelék csupán. „A visszaélések mostanában főként adathalászattal és manipulációval történnek" (MNB sajtótájékoztató, 2025).

A munkahelyi csalások, a deepfake[18] telefonhívások és videó-meetingek, valamint a beszállítók és ügyfelek nevében történő csalások a legkevésbé ismertek a kitöltők között. Ennek oka lehet, hogy talán ebből van a legkevesebb, viszont, ha egy-egy ilyen eset sikeres, akkor akár többszázmilliós kár is történhet. Az ilyen munkahelyi jellegű csalások általában jól megtervezett és előkészített támadások, az áldozatot olyan kényszerhelyzetbe hozzák technológiai eszközökkel és pszichológiai nyomásgyakorlással, amely során csak a mentálisan nagyon erős és nagyon felkészült munkavállalók tudnak ellenállni.

9.2. KiberPajzs témakör 2. kérdés: Számítógépes csalások – értékeld a tudásod!

Mennyire ismered az alábbi internetes pénzügyi csalásokat? Azokat jelöld be, amelyeket el is tudsz magyarázni és felismernél, nem dőlnél be, ha nálad próbálkoznának!

4. ábra
„Számítógépes csalások - értékeld a tudásod!" grafikon



Forrás: Internetes veszélyek és felismerésük kérdőív, a szerző saját kutatása. 2025.

18 A szó maga a „deep learning" (mély tanulás) és a „fake" (hamis) szavak összevonásából 2017- ben keletkezett (Erdősi–Solymos, 2023).

A számítógépes csalások egy hatalmas kategória, talán ennek a kategóriának van a legtöbb és a legrégebbi csalásfajtája, s bár emiatt számos további alkategóriára lehetne bontani, erre most nem volt lehetőség.

A hamis online webáruházak és ajánlatok a COVID időszak egyik legnépszerűbb csalási formája volt, mivel az utazás és fizikai érintkezések korlátozott időszakában szinte mindenki online vásárolt. A bezárások és korlátozások miatt az e-kereskedelmi vásárlások volumene jelentősen megnőtt. Az ACI adatai szerint 2020 januárja és júniusa között az e-kereskedelmi vásárlások volumene 15%-kal, 2020 májusában pedig 81%-kal nőtt az előző év májusához képest. Ez a hirtelen ugrás ideális környezetet teremtett a csalók számára (ACI Worldwide, 2021).

Ez pedig azt jelentette, hogy sokan áldozatul is estek az ilyen jellegű csalásoknak. Az internetes vásárlások azonban összegszerűen nem ütötték meg azt az érzékenységi kategóriát, amellyel az áldozatok már segítségért is fordultak volna a hatóságokhoz. Sokan magukat hibáztatták és nem tettek feljelentést, illetve elmondható, hogy tanultak a saját kárukon és a következő alkalommal nem követték el ezt a hibát.

Az interneten egyre több online csalással foglalkozó, potenciális csaló oldalakat ellenőrző weboldal lett elérhető (https://www.scamdoc.com, https://www.scamadviser.com), másrészt a KiberPajzs kommunikáció, a vállalati képzések és a közösségi oldalakon az önszerveződő csoportok (például a Marketplace csalók Facebook csoport körülbelül 10.000 taggal) és önálló oldalak (mint a https://kamuwebshopok.hu) is segítettek. Jómagam is működtetek a Facebookon egy Mindennapi biztonságunk blog[19] nevű oldalt, ahol a több mint 840 követőnek igyekszem hasznos biztonsági tippeket adni.

A kérdőív adatait tovább elemezve látszik, hogy a válaszadók mintegy negyede ismerné csak fel, ha egy szituációban rosszindulatú kódot vagy távmenedzsment programot próbálnának az eszközére telepíteni. Ha egy támadás során idáig eljut valaki, akkor az azt jelenti, hogy a támadóknak sikerült fenntartani a figyelmet és az áldozat nem ismerte fel, hogy épp egy internetes támadás potenciális áldozata.

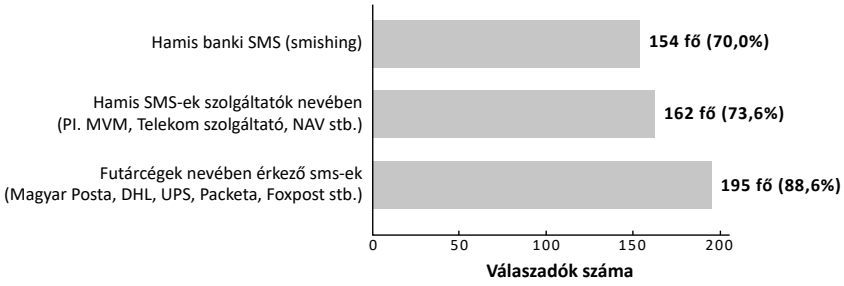
A felmérésben a másik technológiai jellegű csalás – a hamis wifi hálózatra csatlakozás – végzett a legutolsó helyen. Ez egyszerűen abból fakad, hogy az emberek nem értenek hozzá és nem is igazán foglalkoznak ezzel, egyre elterjedtebb a saját mobilinternet használat.

19 https://www.facebook.com/mindennapibiztonsagunk/

9.3. KiberPajzs témakör 3. kérdés: SMS csalások – értékeld a tudásod!

Mennyire ismered az alábbi internetes pénzügyi csalásokat? Azokat jelöld be, amelyeket el is tudsz magyarázni és felismernél, nem dőlnél be, ha nálad próbálkoznának!

5. ábra
„SMS csalások - értékeld a tudásod!" grafikon



Forrás: Internetes veszélyek és felismerésük kérdőív, a szerző saját kutatása. 2025.

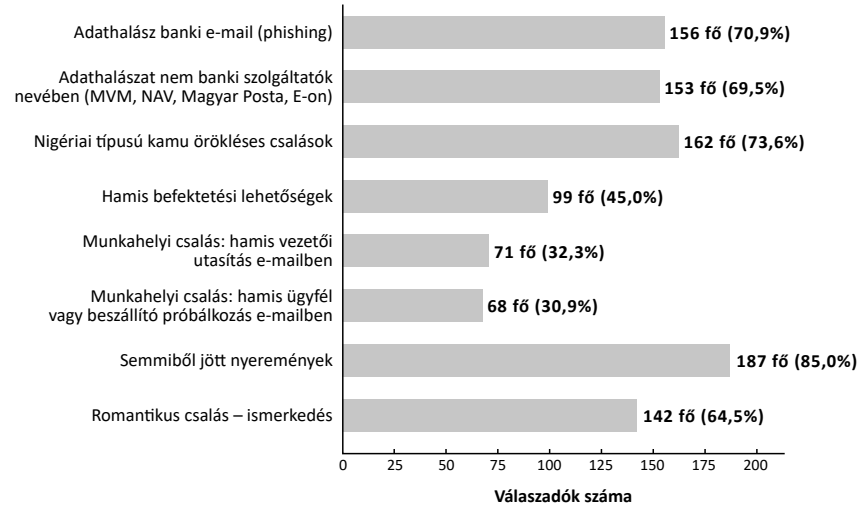
Az SMS-ben érkező adathalász támadások is a COVID időszakában, az online vásárlások felfutásával váltak egyre gyakoribbá és a mai napig is jellemzőek napi szinten előfordulnak. Összességében az ezen a csatornán történő adathalászatok felismerése kimagasló, hiszen a hamis banki SMS csalásokat is a válaszadók 70%-a felismerné, ez pedig jó arány. Ennek egyik oka lehet, hogy az SMS üzenetek rövidek, tömörek, a csalók általában valamilyen webcím rövidítési szolgáltatást használnak, amelynek két oka van. Az egyik, hogy elrejtsék a valódi hivatkozást a felhasználó elől, a másik, hogy beleférjenek az előírt karakterszámba. Maga a csatorna, a furcsa hivatkozásokkal, a jellemzően nyelvtani, fogalmazásbeli hibákat tartalmazó szövegekkel és a szinte mindig megjelenő sürgetéssel okkal kelt gyanút a fogadó felekben.

A futárcégek nevében történő adathalász támadások kimagasló ismertsége annak is köszönhető, hogy rendszeresen jellennek meg a sajtóban ilyen eseteket bemutató cikkek. („Elindult a hullám, veszélyes e-mail és SMS terjed Magyarországon" HVG, 2023). Vagy: „Ismeretlen számról kaptak sms-t a DPD futárcég nevében, bankszámlájuk bánta" (168.hu, 2024). A Mátrix projekt oldalán a Magyar Rendőrség is beszámol ilyen esetekről: „Egy futárszolgálat nevében kapott adathalász SMS-t" (Országos Rendőr-főkapitányság, 2024). Csak a police.hu oldalán rákeresve az „sms csalás" kifejezésre több mint 400 ilyen jellegű hír érhető el.

9.4. KiberPajzs témakör 4. kérdés: E-mailben érkező csalások – értékeld a tudásod!

Mennyire ismered az alábbi internetes pénzügyi csalásokat? Azokat jelöld be, amelyeket el is tudsz magyarázni és felismernél, nem dőlnél be, ha nálad próbálkoznának!

6. ábra
„E-mailben érkező csalások - értékeld a tudásod!" grafikon



Forrás: Internetes veszélyek és felismerésük kérdőív, a szerző saját kutatása, 2025.

Az e-mail-es csalások talán az egyik legszélesebb körű internetes csalási forma. Tekintve, hogy maga a levelezés mint kommunikáció egyidős az írásbeliség megjelenésével, a levelezésen keresztüli csalások és manipulációs technikák megjelenése is ezzel egyidős. Mindössze annyi változott, hogy felgyorsult az üzenetváltások sebessége és a papír mint hordozó átváltott az elektronikus formátumra. Fenti állítást igazolja, hogy az Amerikai Egyesült Államokban a postai szolgáltatások népszerűbbé válásával párhuzamosan olyan mértékben nőtt meg a hamis nyereményjátékokkal, csaló ajándékokkal kapcsolatos levelek száma, hogy a Kongresszus egy 1868-os szabályozás után, 1872-ben konkrétan a postai csalások elleni védelem kapcsán alkotott jogszabályt. A „18 U.S.C. § 1341 – Mail Fraud Statute" ma is hatályos és folyamatosan frissítik az aktuális csalásokra reagálva (18 U.S.C. § 1341, 2023).

Az e-mail-es csalások közül a korábban tárgyalt adathalászatokat nem tekintve, a „nigériai" típusú csalások szintén régi múltra tekintenek vissza, amelyek őse

ugyancsak postai levelezésre alapult. Az ilyen csalások őse a „spanyol fogoly" (Spanish Prisoner) csalás, amely a 16-19. században volt elterjedt Európában. Ennek lényege az volt, hogy a csalók leveleket küldtek gazdag embereknek, azt állítva, hogy egy gazdag politikai fogoly (gyakran egy spanyol arisztokrata) van fogságban, akinek hatalmas vagyonát csak némi előzetes anyagi segítséggel lehetne kiszabadítani vagy átmenteni. Az áldozatoknak a segítségért cserébe hatalmas jutalmat ígértek. Ez az alapmotívum a mai napig változatlan.

Mivel a scambaiting[20] az egyik hobbim, én is számos ilyen csalóval leveleztem egy külön erre a célra fenntartott postafiókkal. A tapasztalatom szerint a csalók jól felépített rendszert, többször is felhasznált fiókokat használnak minden csalástípusra (például afrikai menekülttáborban szenvedő örökös, aki csak akkor kapja meg a pénzét, ha talál európai partnert a pénz befektetésére, vagy a híres amerikai katonanő, aki az iraki sivatagban talált trezorban lévő pénz megszerzése kapcsán ajánl busás összeget, vagy a török bankban hagyott milliók, amit a potenciális áldozat nevéhez hasonló elhunyt hagyott hátra és a jószándékú bankár megpróbálja az összeget eljuttatni a valódi örököshöz). Előfordult, hogy ugyanaz az „ügyvéd" kapcsolódott be két teljesen más jellegű csalás levelezésébe.

A különböző levelezéses csalási formák sokszor keverednek a romantikus csalásokkal, befektetési csalásokkal. Bár a kutatásom szerint ez a két e-mailes csalási forma (a „nigériai" és a „Semmiből jött nyeremények") a legismertebbek, a különböző csalásformák még a mai napig szedik áldozataikat, sajnos ilyenkor akár több milliós veszteséget is okozva.

A két legkevésbé ismert kategória, a munkahelyi jellegű csalások (hamis vezetői utasítások e-mailben és hamis ügyfélszolgálati vagy beszállító próbálkozás e-mailben) alacsonyabb mértékére az lehet a magyarázat, hogy ez eleve feltételez aktív munkatapasztalatot, ami a fiatalabb korosztályokat kevésbé érinti (a korosztály 27,3%-a, 3 fő ismeri fel), a legidősebb, hatvan év felettiek aktív dolgozói időszakában nem volt elektronikus levelezés.

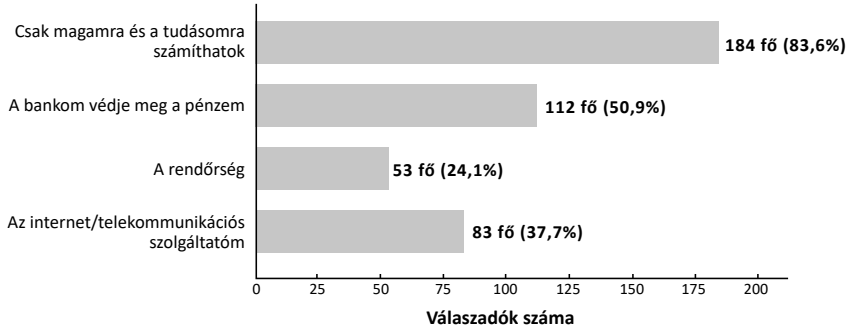
Az elemzés ugyanakkor kimutatja, hogy a 22-60 éves korosztály közül is mindössze a 42%-uk (68 fő) ismerné fel az ilyen jellegű csalási próbálkozásokat.

20 A scambaiting olyan preventív védekezési gyakorlat, amelynek során a felhasználók szándékosan kapcsolatba lépnek az online csalókkal annak érdekében, hogy lekössék azok erőforrásait, valamint információkat gyűjtsenek a csalási módszereikről és kampányaikról *(Charnsethikul–Crotty, 2025)*.

9.5. A következő három kérdés pedig az előzőekben értékelt tudás megszerzésének forrásaira irányult.

Kérdés 1. „Kitől várod, hogy megvédjen az Interneten?"

7. ábra
„Kitől várod, hogy megvédjen az Interneten?" grafikon



Forrás: Internetes veszélyek és felismerésük kérdőív, a szerző saját kutatása, 2025.

Ez a kérdés egy fontos témakörre világít rá, nevezetesen az emberek biztonságérzetének az alapjaira. Ki véd meg engem az interneten? Mivel több válaszlehetőség is adott volt, ezért elemzési szempontként az egyes válaszadási variációkat vizsgáltam. Terjedelmi okokból nem lehetséges az összes kombináció elemzése, az azonban jól látható, hogy pénzügyek kapcsán az emberek jelentős része bizalmatlan és leginkább csak a saját tudásában és éberségében bízik. Meglepő eredmény, hogy a „Bankom védje meg a pénzemet" opciót a válaszadók mindössze fele választotta. Ezen érdemes elgondolkodni, mivel a bankok alapvetően „bizalmat árulnak". Ha az emberek nem bíznak abban, hogy a bankba tett pénzüket nem lopják el, akkor nem is fogják odatenni, vagy csak a legminimálisabb mértékig.

Az elemzés alapján azok közül, akik kizárólag a bankoktól várják a védelmet, vagyis csak ezt az egy opciót jelölték meg, 85,7%-uk a 61 év feletti korosztályból származik. A maradék 14,3% pedig a 22-60 éves korosztály. Ebből az következik, hogy az aktívan dolgozó és internetbankoló korosztály kevésbé gondolja azt, hogy csak és kizárólag a bankoktól kell várni a védelmet. A 22–60 év közötti válaszadók általánosan több szereplő (pl. bank, rendőrség, szolgáltató) együttes védelmére számítanak.

Most vizsgáljuk meg részletesebben, kik azok, akik úgy gondolják, hogy csak magukra számíthatnak. Közülük is kik azok, akik semelyik más opciót nem gondolták relevánsnak. Számosság tekintetében 102 válaszadó nyilatkozott így. Válaszaikat elemezve, körükben a KiberPajzs program ismertsége az alábbi módon

oszlik meg. 43,1% (44 fő) ismeri a programot, míg a maradék 56,9% (58 fő) nem. Érdemes elgondolkodni azon, hogy ez a 44 fő, bár ismeri a KiberPajzs programot, mégis csak magában bízik. Ebből az következik, hogy esetükben nem volt meggyőző a pénzintézetek, vagy akár a Rendőrség segítségnyújtási tevékenysége. Erre utalhat a következő eredmény is, miszerint a 102 fő válaszadó 24,5%-a (25 fő) már szenvedett el pénzügyi veszteséget, míg a többség 75,5% (77 fő) nem. Elképzelhető, hogy rossz a tapasztaltuk az elszenvedett veszteség kezelése kapcsán banki és/vagy rendőrségi oldalról.

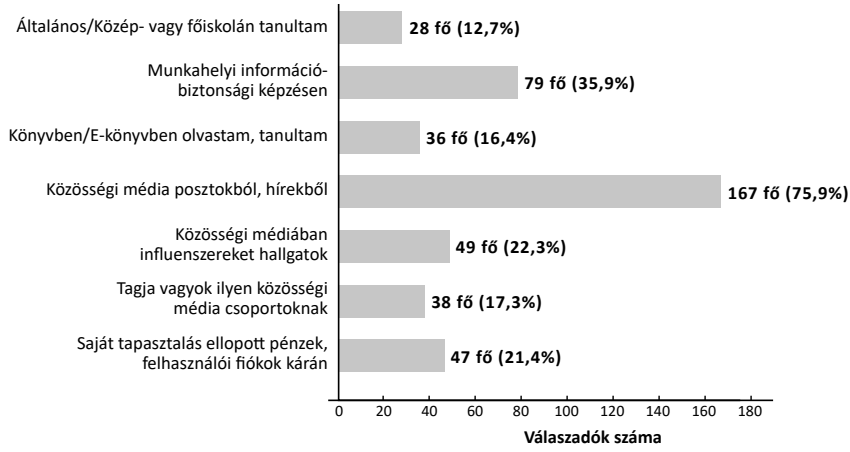
Kérdés 2. „Szoktatok otthon a családban internetes veszélyekről beszélgetni?"

A válaszadók 68,8%-a (151 fő) rendszeresen beszélget a témáról és figyelmeztetik is egymást, ha szükséges. 29,5% (65 fő) nagyon ritkán beszél a családban internetes pénzügyi veszélyekről, mivel túl sok mindenről kellene beszélni. A kitöltők 1,8%-a (4 fő) gondolja úgy, hogy ezt mindenki tapasztalja meg a saját kárán, nem szoktak ilyenekről beszélgetni a családban.

A válaszadók közel 70%-a rendszeresen beszélget a témáról családon belül. Én ezt pozitívan értékelem. Ez a fajta tudás is egy olyan beszélgetési téma lehet minden korosztály számára, ami építi a belső kapcsolatokat és hasznos tudást transzferál.

Kérdés 3. (Utolsó kérdés): Te honnan szerzed/szerezted a legtöbb, leghasznosabb információkat az internetes csalásokról?

8. ábra
Te honnan szerzed/szerezted a legtöbb, leghasznosabb információkat az internetes csalásokról? grafikon



Forrás: Internetes veszélyek és felismerésük kérdőív, a szerző saját kutatása. 2025.

Ez a kérdéskör is egy nagyon fontos témát dolgoz fel és jól látható, hogy a kitöltők háromnegyede használja ismeretszerzésre a közösségi média felületeket információbiztonsági és pénzügyi biztonsági témákban. Az állami és civil szereplők mellett szerencsére sok olyan szakértő is jelen van, akik tudásátadási céllal rendszeresen posztolnak adat- és információbiztonsági témában, vagy akár saját tematikus közösségi oldalaikon.

Az iskolából származó ismeretszerzés alacsony aránya azzal magyarázható, hogy ez a téma, abban a korban, amikor a kitöltők jelentős része iskolába járt, még egyáltalán nem volt releváns. Mégis elgondolkodtató, hogy azok aránya a legkisebb, akik saját pénzen végeztek el valamilyen képzést (4,5% 10 fő), illetve akik könyvekben olvastak a biztonságról (16,4% 36 fő). Annak, hogy az emberek nem áldoznak pénz a saját biztonságukra és képzésükre, számos oka lehet. Rengeteg biztonsági képzés érhető el a nagy oktatási platformokon (Pl. Udemy, Coursera, Udacity, Thinkfic). Ezek egy jelentős része bár elavult, de a közösségi visszajelzések hatalmas száma alapján mégis hasznosnak ítélik meg a képzést elvégzők. A képzések többsége párezer forint, ezek a legnépszerűbbek és a pár óra alatt teljesíthetők. De ezeken kívül akár ingyenes gyorstalpaló e-learning jellegű képzésektől a komolyabb, többhetes, akár egyetemi végzettséget is adó képzésekig széles a skála. Az olvasás és az információbiztonsággal kapcsolatos könyvek elérhetősége minimális a Magyarországon elérhető könyvek mennyiségéhez képest. Az informatikai és információbiztonsági könyvek nagy része tankönyv vagy ismeretterjesztő jellegű. A magyar lakosság, főképp a fiatalabb generációk ráadásul egyre kevesebbet olvasnak és inkább a hang és videó alapú ismeretszerzés kerül előtérbe (Nagy, 2010).

Fontos jelzés, hogy az ismeretszerzési módok és csatornák közül a munkahelyi információbiztonsági képzések foglalják el a második helyezést a képzeletbeli dobogón (35.9% 79 fő). Magam is úgy gondolom, hogy a cégeknek és szervezeteknek jól felfogott érdeke, hogy biztonságtudatos felhasználóik legyenek. Ráadásul nekik megvannak azok az erőforrásaik, amelyek szükségesek akár saját tananyag elkészítésére, vagy akár a piacról információbiztonsággal foglalkozó cégektől való beszerzésre. Én is azt az álláspontot képviselem, hogy mindenekelőtt a felhasználókat a saját életükre reflektálva, a saját környezetükben előforduló példákon keresztül kell tudatosítani, majd ezután következhet a céges és szervezeti biztonsági szabályok bemutatása. Meggyőződésem, hogy ha a felhasználó a saját vagy gyermekét érintő példákon keresztül megérti az információvédelem fontosságát, akkor sokkal könnyebben meg fogja érteni a szervezeti biztonsági szabályokat és jelentősen csökken majd annak a szándéka, hogy kijátssza vagy megkerülje ezeket. Ez pedig a szervezetek kockázati szintjét jelentősen mérsékli. Az emberi hibák és felelőtlenség hosszú évek óta az információbiztonsági incidensek egyik fő oka. A KnowBe4, az egyik legjelentősebb információbiztonsági tudatosítással

foglalkozó cég blogjában, a Stanford Egyetem kutatásával alátámasztott cikk is úgy fogalmaz, hogy a biztonsági incidensek 88%-a emberi hibára vezethető vissza (KnowBe4, 2020).

A munkahelyi információbiztonsági képzések jelentős része kötelező jellegű, a felhasználóknak el kell végezniük és ez teljesen rendben is van. Jó gyakorlat, ha a szervezet a kötelező tudásanyag mellett további, a munkahelyhez nem, vagy nem szorosan kapcsolódó, de a felhasználók tudatosságát növelő kurzusokat vagy képzési anyagokat is elérhetővé tesz, lehetőséget adva például a gyermekek és a kibertér veszélyei, a mesterséges intelligencia, az internetes pénzügyi csalások és támadások, vagy akár a közösségi média veszélyeinek megismerésére.

A teljes képet vizsgálva, ha a kötelező jellegű iskolai és munkahelyi képzéseket nem vesszük figyelembe, csak az önkéntességen alapuló információszerzést, akkor látható, hogy a közösségi média a felhasználók fő információforrása, erre pedig építeni kell a jövőben.

10. ÖSSZEGZÉS ÉS KÖVETKEZTETÉSEK

A tanulmánnyal az volt a célom, hogy átfogó képet nyújtsak az internetes pénzügyi csalások magyarországi fejlődéséről, különös tekintettel az ügyféloldali biztonságtudatosság alakulására és a KiberPajzs program szerepére. A kiberbűnözés rohamos tempóban növekedik (Kovács–Terták, 2024), miközben az internetes pénzügyi szolgáltatásokat igénybe vevők körének biztonságtudatossága nem tudja tartani a lépést az újabb és újabb támadási és csalási módszerekkel. Emiatt a digitális pénzügyi szolgáltatások kockázatai is nőnek – különösen, ha az ügyfelek biztonsági ismeretei a jövőben is hiányosak lesznek vagy túlbecsült önbizalommal párosulnak.

A tanulmányban szerettem volna emlékeztetni az olvasót arra, hogy a támadások elsődleges célpontja ma már nem a bankrendszer, hanem maguk az ügyfelek. Pedagógiai szemléletű kiberbiztonsági szakértőként a téma feldolgozásában nemcsak a szakirodalomra és korábbi eseményekre, hanem saját szakmai tapasztalataimra, többek között a több mint tízéves pénzintézeti információbiztonsági területen szerzett élményeimre és emlékeimre is támaszkodtam.

A téma feldolgozása során az a kép rajzolódott ki bennem, hogy bár a társadalom biztonságtudatosítása kapcsán a KiberPajzs programmal elindult egy komoly felzárkóztatási munka számos érintett szervezet bevonásával, nélkülözhetetlen a további területeken is lépni, gondolok itt a központi visszaélés szűrő rendszer hadrendbe állítására és az MNB oldali követelmények szigorítására. A kutatási eredmények alapján szükségesnek látom a korosztályonként célzott, rendszeres

tudatosítási kampányok erősítését, különösen a fiatalabb generációk sajátos médiafogyasztási szokásainak figyelembevételével.

Ugyanakkor lehetőséget látok arra, hogy a kormányzat ösztönözze a cégeket és szervezeteket, hogy a munkavállalóik részére erősítsék az információvédelmet és az internetes pénzügyi tudatosságot. Bár a GINOP plusz munkahelyi képzéseket támogató program[21] erre kiváló lehetőség volt, javaslom, hogy konkrétan erre a két témára reflektáló képzések támogatására is induljanak pályázatok.

Ezen kívül pedig a közösségi média jelenlét erősítése a másik olyan lehetőség, amiben mind a KiberPajzsnak, mind a teljes magyar szakértői társadalomnak nagyobb erőforrásokat kell mozgósítani. Ezen a területen szintén el tudnék képzelni támogatott szakértőket, akik rendszeresen, hitelesen, már-már influenszeri jegyeket viselve próbálják átadni a tudásukat. Jelenleg ez a tevékenyég teljesen önkéntes alapon, változó intenzitással és változó tudásszinten valósul meg.

A legidősebb korosztályok elérésére szintén nagyobb hangsúlyt kell fektetni, de figyelembe kell venni, hogy tíz év múlva a hatvanas éveiben járó generáció már bőven rendelkezik internetes és technológiai ismeretekkel, ha máshogy nem, akkor saját tapasztalás útján, és ők jelentősen különböznek a mostani hatvanas-hetvenes éveikben járó generációtól. Erre és a megfelelő kommunikációs csatornák kiválasztására már most készülni kell, figyelembe véve a manapság egyre nagyobb figyelmet kapó generációkutatások eredményeit.

A jövőbeni kutatások során célszerű lenne vizsgálni a különböző edukációs formák hatékonyságát, és hosszabb távon nyomon követni, milyen változásokat hoznak a lakosság információbiztonsági attitűdjeiben. Ezen javaslatok megvalósításával, kiegészítve a technológiai fejlesztésekkel és jogszabályi szigorításokkal, hatékonyan fel lehetne venni a versenyt az állampolgárok pénzére pályázó kiberbűnözőkkel.

HIVATKOZÁSOK

168.hu (2024. augusztus 28.): Ismeretlen számról kaptak SMS-t a DPD futárcég nevében, bankszámlájuk bánta. https://168.hu/itthon/adathalasz-sms-magyar-dpd-280780 (letöltve: 2025.05.15.).

ACI Worldwide (2021): Pandemic-Driven Patterns of eCommerce Fraud. https://www.aciworldwide.com/wp-content/uploads/2021/04/pandemic-driven-patterns-of-ecommerce-fraud-article.pdf (letöltve: 2025.05.20.).

21 https://www.palyazat.gov.hu/programok/szechenyi-terv-plusz/ginop-plusz/ginop-plusz-321-21/alapadatok.

biztonsagosinternet.hu. (2006.12.19.): [Weboldal-archívum] biztonsagosinternet.hu (archiválva a *Wayback Machine* által) https://web.archive.org/web/20061012000850/http://www.biztonsagosinternet.hu/ (letöltve: 2025.06.10.).

Chakravorti, S. (2000): Why Has Stored Value Not Caught On? Emerging Issues Series, Supervision and Regulation Department, *Federal Reserve Bank of Chicago*. (S&R-2000-6). https://doi.org/10.2139/ssrn.294516 (letöltve: 2025.05.10.).

Charnsethikul, P., Crotty, C. (et al., 2025): *Puppeteer*: Leveraging a Large Language Model for Scambaiting. *University of Hawaii ScholarSpace*. https://doi.org/10.24251/hicss.2025.131 https://scholarspace.manoa.hawaii.edu/items/86d10c9c-236f-425e-ae86-b917f10b3d9b.

CERT-Hungary (2006.11.16.): *I. Incidenskezelő workshop* [Weboldal-archívum]. cert-hungary.hu (archiválva a Wayback Machine által). https://web.archive.org/web/20070708044324/http://www.cert-hungary.hu/modules.php?name=News&file=article&sid=29 (letöltve: 2025.06.14.).

CERT-Hungary (2006.12.19.): Adathalász támadások a magyar banki rendszerek ellen [Weboldal-archívum]. cert-hungary.hu (archiválva a Wayback Machine által) https://web.archive.org/web/20070708044209/http://www.cert-hungary.hu/modules.php?name=News&file=article&sid=30 (letöltve: 2025.06.14.).

Check Point (2017.09.19.): August's Most Wanted Malware: Banking Trojans and Ransomware That Want Your Money. *Check Point Research Blog.* https://blog.checkpoint.com/security/augusts-wanted-malware-banking-trojans-ransomware-want-money (letöltve: 2025.06.14.).

Erdősi, P. M. – Solymos, Á. (2023): IT Biztonság közérthetően. *Neumann János Számítógéptudományi Társaság (NJSZT)*. https://njszt.hu/letoltheto-it-biztonsag-kozerthtetoen ISBN: 978-615-5036-26-2 (letöltve: 2025.05.10.).

HVG (2023.05.23.): Elindult a hullám, veszélyes email és SMS terjed Magyarországon. *HVG Tech*. https://hvg.hu/tudomany/20230523_kamu_email_sms_futarszolgalatok_atveres_adathalasz_levelek_banki_adatok_bankkartyaadatok_csalok (letöltve: 2025.06.14.).

Gillis, A. S. (2022.05.17.). *What is man in the browser (MitB)?* TechTarget. https://www.techtarget.com/searchsecurity/definition/man-in-the-browser (letöltve: 2025.06.14.)

GKIeNET. (2002): E-bankolás Magyarországon 2002. Budapest: *GKI Gazdaságkutató*. https://enet.hu/jelentes-az-internet-gazdasagrol-fokuszban-a-penzugyi-szektor-2002-iv-negyedev/ (letöltve: 2025.05.30.).

Jurík, P. (2007): Bankkártyaenciklopédia – A kezdetektől napjainkig. *HVG Kiadó Zrt*. ISBN 9789639686311, 67.

Kruger, J. – Dunning, D. (1999): Unskilled and unaware of it: How difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of Personality and Social Psychology*, 77(6), 1121–1134. https://doi.org/10.1037/0022-3514.77.6.1121 (letöltve: 2025.06.03.).

KnowBe4. (2020): Stanford Research: 88% of Data Breaches Are Caused by Human Error. *KnowBe4 Blog*. https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error (letöltve: 2025.06.14.).

Kovács, L. – Terták, E. (2024): A kiberbűnözés legjobb ellenszere: a pénzügyi műveltség. *Gazdaság és Pénzügy*, 11(1), 6–29. https://doi.org/10.33926/GP.2024.1.2 https://bankszovetseg.hu/Public/gep/006-029%20Kovacs_Tertak.pdf (letöltve: 2025.06.10.).

Lemák, G. (2016.09.15.): Nagy magyar FinTechtörténelem (béta). *FinTechZone*. https://fintechzone.hu/a-nagy-magyar-fintech-tortenelem-beta/ (letöltve: 2025.06.10.).

Magyar Nemzeti Bank (2023). Pénzforgalom 2030: Az MNB pénzforgalmi stratégiai célkitűzése és a Pénzforgalmi Fejlettségi Mutatórendszer bevezetése. Budapest: *Magyar Nemzeti Bank*. https://www.mnb.hu/letoltes/penzforgalom-2030-strategia.pdf (letöltve: 2025.06.04.).

Magyar Nemzeti Bank sajtótájékoztató (2025.06.03.): „Öt csapással számolna le a banki csalásokkal az MNB" [HVG cikk]. *HVG*. https://hvg.hu/gazdasag/20250603_Ot-csapassal-szamolna-le-a-banki-csalasokkal-az-MNB (letöltve: 2025.05.30.).

Magyar Nemzeti Bank (2025): Pénzforgalmi visszaélések (2025.03.17.) Visszaélések az elektronikus pénzforgalomban (Excel fájl). https://statisztika.mnb.hu/timeseries/3-visszaelesek.xls (letöltve: 2025.05.30.) 8.

Mastercard – Év Bankja (2024).: Az év kiberbiztonsági edukációs kampánya 2024 – az Év Bankja kategóriái között. https://www.evbankja.hu/kategoriak/az-ev-kiberbiztonsagi-edukacios-kampany (letöltve: 2025.06.15.).

Nemes, M. (2025): A kiberbűnözés kora 2025. *Mastercard* – KiberPajzs. https://kiberpajzs.hu/letoltes/a-kiberbu-no-ze-s-kora-2025-0-sszefoglalo-kiberpajzs-0220fin-mnb.pdf (letöltve: 2025.05.30.) 3-9-17.

Neumann János Számítógéptudományi Társaság (2017.06.27.): IT biztonság közérthetően – új, ingyenes tankönyvet tesz hozzáférhetővé az NJSZT. https://njszt.hu/hu/news/2017-06-27/it-biztonsag-kozerthetoen-uj-ingyenes-tankonyvet-tesz-hozzaferhetove-az-njszt (letöltve: 2025.05.30.).

Neumann János Számítógéptudományi Társaság (2023.12.7.): Ingyenesen letölthető a Neumann Társaság frissített IT biztonsági tankönyve. https://njszt.hu/hu/news/2023-12-07/ingyenesen-letoltheto-neumann-tarsasag-frissitett-it-biztonsagi-tankonyve (letöltve: 2025.06.14.).

Nagy, J. (2010): 9–14 évesek olvasáskultúrája Magyarországon (Szakdolgozat*). Debreceni Egyetem, Informatikai Kar, Könyvtárinformatikai Tanszék*, Debrecen. https://dea.lib.unideb.hu/server/api/core/bitstreams/c83d8ccb-8fef-4cdb-9261-12d57fd33171/content (letöltve: 2025.06.14.).

PÉNZ7 (2025.03.03.): *A PÉNZ7 sikerei 2025ben*. PÉNZ7 – *Pénzügyi és Vállalkozói Témahét* https://penz7.hu. (letöltve: 2025.06.14.).

Prim.hu (2005.11. 21.): Több mint felével nőtt az internetbanki ügyfelek száma. *Prim Online*. https://hirek.prim.hu/cikk/49636/ (letöltve: 2025.05.10.).

Országos Rendőr-főkapitányság (2024.02.16.). *Mátrix Projekt – közel 7 500 ügyben nyomozunk*. Police.hu. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/matrix-projekt-kozel-7500-ugyben-nyomozunk (letöltve: 2025.06.12.)

Országos Rendőr-főkapitányság (2023.11.06.): Mátrix Projekt a kiberbiztonságért. *Zsaru Magazin* / police.hu. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/matrix-projekt-a-kiberbiztonsagert (letöltve: 2025.05.10.).

Országos Rendőr-főkapitányság (2024.03.26.): Egy futárszolgálat nevében kapott adathalász SMS-t. *Police.hu*. https://www.police.hu/hu/hirekesinformaciok/legfrissebbhireink/matrixprojekt/egy futarszolgalatnevebenkapottadathalasz (letöltve: 2025.05.10.).

Solymos, Á. (2011.07.07.): Hazai vizeken – A hazai adathalászatok tapasztalatairól [Előadás]. *IIR Masterclass Pénzintézeti Fraud Management* konferencia, Budapest. (Prezentációs diasor nem publikált formában elérhető a szerzőnél.)

Solymos, Á. (2018): In: Berzsenyi D., Gyaraki R., Hámornik B. P., Hirsch G., Kiss A., Marsi T., Orbók Á., Simon B., Solymos Á., Tikos A., Zsíros P. Incidensmenedzsment – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára *2017. ISBN 978-615-5764-99-8 (PDF). https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/6848/Incidens-menedzsment.pdf?sequence=1*(letöltve: 2025.05.24.) 167.

United States Postal Inspection Service (2023): History of the Mail Fraud Statute (18 U.S.C. § 1341). https://www.uspis.gov/history-spotlight-2023/history-of-the-mail-fraud-statute (letöltve: 2025.05.24.).