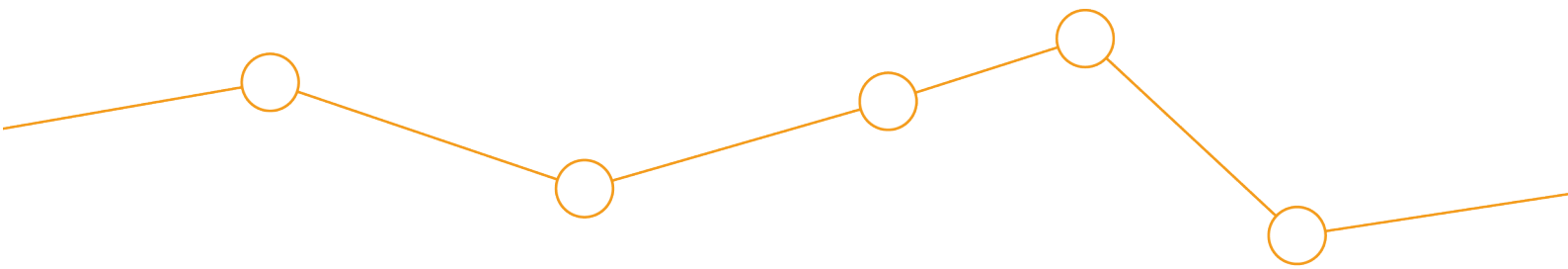
ÁTVERÉSEK ÉS CSALÁSFELDERÍTÉS ONLINE PLATFORMOKON TANULMÁNY A NEMZETI MÉDIA- ÉS HÍRKÖZLÉSI HATÓSÁG RÉSZÉRE

Készítette: eNET Magyarország Kft.

Székhelye: 1095 Budapest, Ipar utca 5.



TARTALOMJEGYZÉK

1 KIBERBŰNÖZÉS ÉS EZEN BELÜL AZ ONLINE ÁTVERÉSEK, CSALÁSOK GAZDASÁGI JELENTŐSÉGE, TERHE

A Mastercard és a KiberPajzs közös jelentése, „A kiberbűnözés kora 2025” szerint a kiberbűnözés globális gazdasági kára 2028-ra meghaladhatja a 14 000 milliárd amerikai dollárt, ami jól mutatja, hogy a digitális térben zajló bűncselekmények immár a világgazdaság egyik legjelentősebb kockázati tényezőjévé váltak (Kiberpajzs, 2025). A tanulmány szerint a támadások jellemzően a pénzügyi szektort, az online kereskedelmet és az adatkezeléssel foglalkozó szolgáltatókat érintik legnagyobb mértékben.

A Check Point 2024-es elemzése ezt a tendenciát megerősíti: a kutatók szerint a kibertámadások száma világszinten 44%-kal nőtt egyetlen év alatt, döntően a mesterséges intelligencia által vezérelt, automatizált támadások terjedése miatt (Check Point, 2024). Becslések szerint 2024 végére a kiberbűnözés okozta világszintű gazdasági kár elérhette a 9500 milliárd USD-t.

Fontos megjegyezni, hogy a kibertámadások nem csupán a legfejlettebb digitális gazdaságokat érintik: a kiberfenyegetettség globális jelenség és Magyarország sem kivétel. A KiberPajzs 2025 adatai szerint 2024-ben több mint 220 000 internetes csalást regisztráltak hazánkban, az ezekkel összefüggő anyagi veszteség pedig 41,9 milliárd forint volt. Miközben a válaszadók 48%-a már találkozott kibertámadással (például: adathalász e-maillel, hamis weboldallal vagy telefonos csalással), csupán 22% mondta azt, hogy képes lenne felismerni és elkerülni az ilyen helyzeteket – ami jelentős biztonsági tudatossághiányra utal (Mastercard, 2025).

Ezek az adatok jól mutatják, hogy a kiberbűnözés nem csupán technológiai, hanem társadalmi probléma is, hiszen a felhasználók biztonságtudatossága és digitális kompetenciája közvetlenül befolyásolja a gazdasági veszteségek mértékét.

Az MNB 2025-ös Fizetési Rendszer Jelentése szerint 2024-ben a pénzforgalmi visszaélésekhez kapcsolódó ügyek száma 36%-kal emelkedett, és a csalások összértéke meghaladta az 54,7 milliárd forintot. Ez több mint kétszerese a 2021-es értéknek. A bankkártyás visszaélések aránya a pénzforgalmi csalások közel felét tette ki, míg a legnagyobb pénzügyi kárt továbbra is az internetes adathalászat (phishing - banki vagy piactéri csalás, ahol a támadók a fogyasztók pénzügyi adatait, jelszavait vagy bankkártyaadatait szerezték meg) és a hamis ügyfél-hitelesítés okozta (MNB, 2025a, 2025b).

A magyarországi trendek illeszkednek az európai folyamatokhoz. Az online átverések terjedése nem csupán a pénzügyi veszteségek miatt aggasztó, hanem azért is, mert aláássa a digitális szolgáltatásokba vetett bizalmat. Az Eurostat 2023-as adatai szerint az online vásárlók 33%-a tapasztalt valamilyen problémát internetes vásárlás során, és Magyarországon is hasonló arányt mértek. A problémák között kiemelt szerepet kapnak a szállítással összefüggő

nehézségek (késedelmes kézbesítés, nem leszállított termék), a minőségi kifogások, valamint a félrevezető online hirdetések; ezek egy része közvetlen pénzügyi veszteséghez is vezet (Eurostat, 2024a).

A kiberbűnözés gazdasági terhei nem csupán az egyénekre, hanem a gazdasági szereplőkre is jelentős hatással vannak. A vállalatok számára a kibertámadások átlagos költsége 2023-ban meghaladta a 4,45 millió USD-t globálisan, ami 15%-os növekedés az előző évhez képest (Check Point, 2024). Magyarországon a vállalati incidensek elsősorban adathalászat, zsarolóvírus-támadás és piactéri csalások formájában jelentkeznek.

A csalásokkal szembeni sebezhetőség szorosan összefügg a lakosság digitális felkészültségével (természetesen más tényezők is befolyásolják a sebezhetőséget, mint a csalásokkal kapcsolatos ismeretek, a biztonságtudatos viselkedés stb.). Az Eurostat 2023-as digitális készségfelmérése szerint Magyarországon a 16–74 éves lakosság 59%-a rendelkezik legalább alapvető digitális készségekkel, ami gyakorlatilag megegyezik az EU27-es 56%-os átlaggal. A biztonsági kompetenciák terén a magyarok 75%-a rendelkezik legalább „basic or above basic” (alap vagy azt meghaladó) szintű készségekkel, vagyis a lakosság 25%-ának nincsenek még alapvető online biztonsági ismeretei sem (Eurostat, 2024b). Ez a csoport különösen sérülékeny az adathalász és online átverési formákkal szemben.

A kiberbűnözés elleni fellépésben Magyarországon az utóbbi években megerősödött az intézményi együttműködés. A 2023-ban indított KiberPajzs program az MNB, a rendőrség, a Nemzeti Kibervédelmi Intézet és a Bankszövetség közös kezdeményezése, célja a lakossági és vállalati tudatosság növelése. Bár a KiberPajzs program jelentős előrelépést jelent az edukáció terén, az online csalások számának növekedése alapján továbbra is kihívást jelent a gyakorlati hatékonyság és a lakosság szélesebb körű elérése.

A gazdasági veszteségek mértéke mellett a kiberbűnözés bizalomromboló hatása is jelentős. Az online csalások aláássák a digitális fizetések és e-kereskedelem iránti bizalmat, ami – ha nem párosul hatékony megelőzéssel – hosszabb távon akár a digitális gazdaság növekedési ütemét is lassíthatja. A visegrádi országokat összehasonlító tanulmány szerint Magyarországon a fogyasztók 28%-a számolt be arról, hogy bizalmatlanabbá vált az online vásárlással kapcsolatban az elmúlt két évben (Fedorko & Kráľ, 2021).

A csalások formái gyorsan követik a társadalmi és gazdasági trendeket. Az Index (2025a) megállapítása szerint a kiberbűnözők egyre gyakrabban használnak mesterséges intelligenciát hang- és képhamisításra („deepfake”), így a csalások sokkal hitelesebbnek tűnnek.

Az MNB (2025a) adatai szerint a pénzforgalmi visszaélések 62%-a online indítású volt, az esetek 80%-ában az áldozat maga hagyta jóvá a tranzakciót, mert elhitte, hogy hivatalos személlyel beszél.

Az online csalások és kiberbűnözés gazdasági terhei már nem csak technológiai, hanem makrogazdasági problémát is jelenthetnek. A jelenség kezelése nem csupán bűnüldözési,

hanem pénzügyi stabilitási és társadalompolitikai kérdés is, amely átfogó oktatási, szabályozási és technológiai együttműködést igényel.

2 ONLINE ÁTVERÉSEK TÍPUSAI, FAJTÁI

Az online tér rohamos digitalizációja az elmúlt években új bűnözési formák megjelenését és elterjedését hozta magával. Az internetes csalások jellemzője, hogy gyorsan alkalmazkodnak a technológiai környezethez és a társadalmi-gazdasági helyzethez. A kiberbűnözők ma már nem csupán technikai tudással, hanem pszichológiai manipulációval is dolgoznak – az emberi tényező kihasználása lett az egyik legfontosabb eszközük (Solymos, 2025).

A KiberPajzs 2025 jelentés szerint a kiberbűncselekmények 80–85%-a felhasználók megtévesztésén alapul, vagyis valamilyen online átverés formájában valósul meg (KiberPajzs, 2025). A Magyar Nemzeti Bank 2025-ös adatai szerint a pénzforgalmi visszaélések száma egyetlen év alatt több, mint 36 %-kal nőtt, az okozott kár pedig meghaladta az 54,7 milliárd forintot (MNB, 2025b). Ezek túlnyomó része online környezetben történt, jellemzően adathalászat vagy hamis ügyfél-hitelesítés útján.

2.1 AZ ONLINE CSALÁSOK FŐBB TÍPUSAI

Halász Viktor, az ORFK Kiberbűnözés Elleni Főosztályának szakértője szerint a kiberbűnözők minden évben új technikákkal próbálkoznak. Gyakoriak a hamis banki telefonhívások, a hamis online webshopok, a hamis csomagküldéssel és a hamis befektetésekkel kapcsolatos csalások. "A módszereknek az alapvető magja gyakorlatilag ugyanaz: megpróbálnak valahogy az áldozat bizalmába férkőzni, hiszen a leggyengébb láncszem mindig az ember" (Kanizsa Médiaház, 2024).

2.1.1 Adathalászat (phishing)

Az adathalászat a legelterjedtebb online csalási forma. Célja, hogy a csalók hamis e-mailek, weboldalak vagy üzenetek segítségével személyes, pénzügyi adatokat (például: banki azonosító, jelszó, kártyaadat, személyes adatok) szerezzenek meg.
A leggyakoribb phishing-típusok:

- Banki vagy szolgáltatói adathalászat, amikor a támadó ismert intézmény (pl. bank, futárszolgálat, közműcég, Magyar Posta) nevében küld hamis értesítést, fizetési vagy vámfizetési felszólítást.
- Közösségi média-adathalászat, amikor a felhasználókat üzenetküldő alkalmazásokon, (Messenger, WhatsApp stb.) keresztül próbálják rávenni érzékeny adatok megadására.
- QR-kódos adathalászat, ahol a csalók hamis kódokat helyeznek el, amelyek adathalász oldalakra irányítanak.

Ezek a támadások jellemzően bizalomra épülnek, és gyakran valós, hitelesített weboldalak, e-mailek kinézetét utánozzák. A magyar felhasználók több mint fele már találkozott adathalász próbálkozással (Mastercard, 2025, MNB, 2025c).

2.1.2 Telefonos és SMS-alapú csalások (vishing, smishing)

A vishing (voice phishing) a telefonos megtévesztés egyik formája, amikor a csaló banki ügyintézőnek, hatósági személynek vagy futárszolgálat munkatársának adja ki magát. A smishing SMS-üzenet formájában történik, gyakran „sürgős" linket tartalmazva. A smishing egyik speciális módja, ha a hívószámot hamisítják, egy valódi banknak vagy más szolgáltatónak kiadva magukat: a másolt intézménybe vetett bizalomra alapozva veszik rá az áldozatokat, hogy átadják személyes, bankszámla- vagy kártyaadataikat, telepítsenek távoli hozzáférést engedő alkalmazást, vagy akár konkrétan pénzt utaljanak a csalóknak.
Az MNB és a Kiberpajzs közleményei alapján 2024–2025-ben a leggyakoribb ilyen csalások a csomagküldésre hivatkozó hamis üzenetek, és a bankbiztonsági riasztások, amelyek célja, hogy a címzett belépjen egy adathalász oldalra.

2.1.3 Online piactéri és hamis webáruházas csalások

A hamis webáruházak és piactéri csalások aránya meredeken nőtt az elmúlt években Magyarországon is. A 2024. első félévi Revolut Consumer Security and Financial Crime Report szerint a vásárlási csalások az összes engedélyezett csalás 68%-át tették ki Magyarországon (Pénzcentrum, 2024. november 11.). A csalók jellemzően olcsóbban kínálják a népszerű termékeket másoknál, vagy nehezen ellenőrizhető, esetleg nehezen elérhető (például: már kifutott vagy gyűjtői) termékeket kínálnak, és az áru kifizetése után eltűnnek. Ide sorolhatóak az online vagy applikációs piactereken (például: Jófogás, Facebook Marketplace, Vinted) fizetett hirdetésekkel operáló csalók is, akik aztán egy hamis webshop oldalára továbbítják az érdeklődő kattintókat. Pár éve még a vevők megkárosítása volt a gyakoribb, manapság azonban már az eladók is a visszaélések céltáblájává válhatnak: a csaló hamis csomagküldési linket küld a vevőnek, vagy olyan banki adatokat kér az „utaláshoz", amelyekkel azután visszaél.

Az Európai Unió fogyasztóinak csaknem fele találkozott csalással és átveréssel az interneten 2024-ben (European Comission, 2025).

2.1.4 Befektetési és kripto-csalások

Az online befektetési csalások új hullámát a kriptoeszközökkel kapcsolatos visszaélések indították el, és ezek az utóbbi két évben ugrásszerűen terjedtek. A csalók olyan, a valós platformokat utánzó weboldalakat hoznak létre, amelyek magas hozamot ígérnek, de valójában nincs mögöttük tényleges befektetés, és (akár) mesterséges intelligenciával generált reklámokkal igyekeznek becsalogatni az áldozatokat. A közösségi médiában és üzenetküldő platformokon emellett megjelentek az ún. influencer-alapú átverések, ahol a csalók ismert emberek nevével vagy arcképével visszaélve hirdetnek hamis befektetési lehetőségeket vagy pénzügyi termékeket.

A KiberPajzs (2025) szerint a bejelentett kripto-befektetési csalások száma 2024-ben megduplázódott és több mint 5 milliárd forint kárt okoztak.

2.1.5 Ártó applikáció vagy kód telepítésén alapuló csalások

Ennek a csalástípusnak a során a csalók vishing (hamis banki hívások), phishing (adathalász levél), smishing (adathalász sms) felhasználásával, QR kód segítségével ráveszik az áldozatot, hogy telepítsen olyan eredetileg legitim távsegítség-szoftvereket (például: TeamViewer, AnyDesk), amelyeken át távoli hozzáférést szereznek az eszközhöz és a bankszámlához. Volt, akiknek percek alatt akár több százezer forintot vontak le a számlájáról. Egyre gyakoribb, hogy az elkövetők informatikai támogatást (például: Microsoft, telekom szolgáltató) vagy banki, pénzügyi biztonsági ellenőrzést (például: MNB, NAV) színlelnek, és ennek kapcsán kérik meg a felhasználót, hogy telepítsen távoli hozzáférést biztosító szoftvert. Az MNB adatai szerint 2025 első negyedévében már a pénzforgalmi csalások 8 %-át tették ki az ilyen típusú támadások (MNB, 2025b).

Egy ilyen támadási hullámban több magyar áldozat számolt be arról, hogy „Microsoft-technikai támogatás” nevében hívták fel őket, és miután a távoli elérést engedélyezték, perceken belül kiürítették a bankszámlájukat (HVG, 2025. május 23.). Egy másik friss csalássorozatban az MBH Bank ügyfeleinek megtévesztésére a csalók hamis online felületeket és telefonos kommunikációt használtak, hogy bizalmat keltsenek az áldozatokban. Az így megszerzett banki adatokkal a csalók önállóan indítottak átutalásokat. A kár több tízmillió forintra rúgott (Válasz Online, 2025. július 11.).

2.1.6 Romantikus vagy „nigériai” csalások

A digitális kommunikáció térnyerésével párhuzamosan egyre elterjedtebbek a bizalmi és érzelmi kapcsolatépítésen alapuló online csalások, az ún. „nigériai csalások”, illetve ennek egy válfaja, a „romantikus csalások”. A „nigériai csalás” klasszikusan olyan átverést jelent, ahol az elkövetők valamilyen fantasztikus, erős érzelmi szálakat megpendítő izgalmas történettel – örökség, humanitárius krízis, sürgős segítség – próbálják rávenni az áldozatot pénz utalására. A romantikus csalás esetében például a csaló egy online ismerkedés keretében épít ki érzelmi kapcsolatot, majd „kilátástalan helyzetére” vagy „közös jövőre” hivatkozva kér pénzügyi támogatást (Dívány, 2024. február 24.).

Ezek a csalások gyakran hosszú idő alatt, bizalmi alapon épülnek fel, és jellemzően érzelmileg kiszolgáltatott helyzetben lévő áldozatokat céloznak meg – például egyedülálló időseket, özvegyeket, magányosan, társas támogatástól messze élő embereket.

Ezek során az elkövetők hamis profilt hoznak létre, gyakran külföldi katonának, orvosnak vagy jómódú üzletembernek adják ki magukat, majd hosszan tartó online kapcsolatot építenek ki az áldozattal. Miután kialakult a bizalom, valamilyen ürüggyel – sürgős egészségügyi helyzetre,

utazási nehézségre, csomagküldésre vagy hatósági ügyintézésre hivatkozva – pénzt kérnek, amelyet az áldozat önként utal át.

A hazai sajtóbeszámolók több hasonló esetet is ismertetnek. Egy zalaegerszegi nő például egy „amerikai katona” nevében fellépő csalónak utalt át több millió forintot, és feltártak olyan esetet, ahol egy magyar áldozat öt éven keresztül tartotta a kapcsolatot egy soha nem látott, külföldinek mondott férfival („Tom Michael”), és ez idő alatt összesen mintegy 75 millió forintot utalt át különböző számlákra. A cikk szerint a rendőrség 36 hasonló, online szerelmi csalás ügyében nyomozott, a károsszeg pedig összesen több százmillió forintot tett ki (Kiberpajzs, 2025b; Economx, 2024. február 14.). A romantikus/nigériai csalások nem egyedi, elszigetelt esetek: a hosszú időn át fennálló érzelmi manipuláció miatt az áldozatok gyakran teljesen valósnak élik meg a kapcsolatot, és még a nyilvánvaló ellentmondások ellenére sem gyanakodnak. Mindkét esetben a csalók hónapokon keresztül fenntartották a kapcsolatot, és pszichológiai manipulációval érték el, hogy az áldozatok fokozatosan egyre nagyobb összegeket utaljanak át.

A romantikus vagy „nigériai” természetükből fakadóan az ilyen csalások elkövetői felhasználhatnak más típusú csalási elemeket is, például befektetési vagy kriptovaluta-csalásokkal, amikor a bizalmi kapcsolat végül egy „közös befektetésbe” torkollik. Legnagyobb veszélyük, hogy nehezen felismerhetők: az áldozatok sokszor nem tekintik magukat bűncselekmény elszenvedőinek, tagadják, hogy becsapták őket, mivel az elkövetés módja személyes és érzelmi szinten hat rájuk. A szakértők szerint ezek az esetek a bejelentett online csalásoknak csupán a töredékét teszik ki, mivel sok áldozat szégyenérzetből nem tesz feljelentést.

2.1.7 Wangiri vagy visszahívásos csalások

A Wangiri (japán eredetű szó, jelentése: egy csörgés és leteszik) típusú csalások lényege, hogy a csalók külföldi vagy emelt díjas számokról rövid ideig megcsörgetik az áldozat telefonját, majd megszakítják a hívást, abban bízva, hogy az illető visszahívja a számot. A visszahívás azonban jelentős díjat generál, amiből a csalók bevételt szereznek – ez akkor is így van, ha az áldozat foglalt jelet vagy akár semmit sem hall, amikor megpróbálja visszahívni a számot.

Bár a módszer több, mint egy évtizedes, a 2020-as években ismét tömegesen megjelent Magyarországon. A Nemzeti Kibervédelmi Intézet (NKI) 2020-ban külön figyelmeztetést adott ki, miután magyar felhasználók tömegesen kaptak hívásokat külföldi (például: +252 – Szomália, +216 – Tunézia, +685 – Szamoa) körzetszámokról. Az NKI tájékoztatása szerint ezek a hívások automatikus rendszerek által generáltak, amelyek célja, hogy a felhasználót visszahívásra ösztönözzék (NKI, 2020).

2025-ben is előfordult nagyobb szabású wangiri csalássorozat, sok magyar telefonszám tulajdonosa jelezte, hogy külföldi, számára ismeretlen számról keresték, de a hívás szinte azonnal megszakadt. „A mostani hullám során elsősorban +44-es, vagyis az Egyesült

Királysághoz tartozó telefonszámokról érkeznek a hívások. Ez sokakat megtéveszt, hiszen előfordulhat, hogy valaki valóban vár egy hívást egy angol számról – például egy külföldön élő ismerőstől vagy egy hivatalos intézménytől. Fontos azonban tudni, hogy a csalók bármilyen előhívót használhatnak, és időről időre változtatják a módszereiket" (Origo, 2025).

A csalók módszerei az utóbbi években tovább finomodtak:

- SMS-ben vagy chatüzenetben küldenek „visszahívást sürgető" üzeneteket („Sürgős ügyben keresem", „Csomagszállítási probléma", „Családtag bajban van"),
- vagy automatizált robothívásokkal próbálják elérni, hogy a felhasználó azonnal visszahívja a számot.

Külön veszély, hogy az ilyen típusú visszahívásos csalások akár a spoofing, vagy számhamisításos csalással egybekötve közvetlen pénzügyi veszteséget okoznak, és egyben adatszerzési célt is szolgálhatnak: a hívás során rögzített hangmintát vagy a telefonrendszer metaadatait és a telefonszámot későbbi személyazonosításra, sőt, további csalásokhoz is felhasználhatják (Blikk, 2024).

2.2 MAGYARORSZÁGI TRENDEK ÉS JELLEMZŐK

A magyar felhasználók sérülékenyek az olyan csalásokkal szemben, amelyek hivatalos kommunikációnak tűnnek. A csalók üzenete gyakran már magyar nyelvű, helyesírása is korrekt, jó magyar nyelvhasználat jellemzi. A csalások formái gyorsan követik a társadalmi és gazdasági trendeket. A kiberbűnözők egyre gyakrabban használnak mesterséges intelligenciát hang- és képhamisításra („deepfake"), így a csalások sokkal hitelesebbnek tűnnek (Index, 2025. június 6.).
A legtöbb csalás a banki és logisztikai szektor nevével visszaélve történik, ahogy azt a 2.1 alfejezetben bemutattuk. Az internetes csalások számának magas előfordulása Magyarországon összefügg a digitális készségek alacsony szintjével is – a lakosság több, mint fele nem rendelkezik alapvető biztonsági ismeretekkel (Eurostat, 2024b).

Az online csalások Magyarországon és Európában egyaránt a kiberbűnözés leggyorsabban terjedő formáját jelentik. Közös jellemzőjük, hogy technológiai eszközök helyett elsősorban az emberi tényezőt célozzák, így a felhasználói tudatosság kulcstényező a megelőzésben. Az adatok azt mutatják, hogy a pénzügyi kárért legnagyobb arányban az adathalász és befektetési csalások felelősek, míg a legtöbb esetszám az online piactéri átverésekhez köthető. A tendencia egyértelmű: az online átverések diverzifikálódnak, a támadók pedig egyre kifinomultabb pszichológiai és technológiai módszereket alkalmaznak a magyar felhasználókkal szemben. Ez a dinamikusan változó fenyegetési környezet azt is jelenti, hogy a védekezésnek mind technológiai, mind oktatási és szabályozási szinten is lépést kell tartania.

3 JELLEMZŐ CSALÁSOK, ÁTVERÉSEK A KÖZÖSSÉGI PLATFORMOKON

3.1 A KÖZÖSSÉGI PLATFORMOKON JELLEMZŐ ONLINE CSALÁSOK

Magyarországon a Facebook, az Instagram és a TikTok a legnépszerűbb közösségi platformok, így ezek a felületek váltak az online csalások elsődleges terepévé a 2020-as évek közepére.

A Nemzeti Média- és Hírközlési Hatóság (NMHH) megbízásából 2024-ben készült kutatás feltárta, hogy a 18 év feletti magyar internetezők 88%-a használja legalább hetente a Facebook-ot, 73% a YouTube-ot, 38% az Instagram-ot, és 36% a TikTok-ot (Impetus Research, 2024, p. 5). E magas aktivitás jól magyarázza, hogy a közösségi felületek az online visszaélések leggyakoribb helyszínei: a válaszadók 68%-a tapasztalt már valamilyen online problémát, közülük 31% adathalászatot, 18% illegális tartalmat, és 8% adatvisszaélést (Impetus Research, 2024).

3.2 ADATHALÁSZAT A KÖZÖSSÉGI MÉDIÁBAN – PÉLDÁK MAGYARORSZÁGON

Az adathalászat (phishing) továbbra is a legelterjedtebb csalástípus Magyarországon. E-mail mellett már SMS-ben, közösségi médiás üzenetben és kommentekben is megjelennek az adathalász próbálkozások (NKI, 2025. szeptember 25.). A közösségi platformokon a csalók gyakran munkaajánlatokra, nyereményjátékokra vagy közérdekű felhívásokra hivatkozva szereznek jelszavakat és banki adatokat (Mastercard, 2025).

A csalók egyre inkább személyre szabott, úgynevezett social profiling módszerrel dolgoznak: közösségi oldalakon nyilvános adatokból építenek profilt, majd az így szerzett információk alapján célzott üzeneteket küldenek (Tudás.hu, 2024, HunCERT, 2024).

A felhasználók egy része ugyan felismeri a gyanús jeleket, de a panaszkezelés nehézkes: a 2024-es NMHH-felmérésben a bejelentést tevők többsége inkább elégedetlen volt a platformok reakcióival (Impetus Research, 2024).

A Meta platformok (Facebook, Messenger, Instagram) 2025-re a leggyakrabban célzott rendszerekké váltak az adathalászat (phishing) kapcsán. Az elmúlt években a kibercsalások egyik újabb hulláma a felhasználói és hirdetési fiókok ellopását célozta, amely a magánszemélyek mellett vállalkozásokat, hirdetőket és tartalomkészítőket is érintett. E támadások közös jellemzője, hogy a csalók a Meta nevében küldenek megtévesztő üzeneteket, valójában azonban adathalász vagy kártevőt tartalmazó linkek segítségével szerzik meg a fiókok feletti irányítást. A magyar sajtó számos cikkben hívta fel erre a magyar felhasználók figyelmét.

A Blikk egy 2025-ös cikke szerint a csalók a „Meta Business Support” hamis profilról tömegesen küldenek üzeneteket, akár több ezer magyar felhasználót is elérve. Privát üzenetben kérik a

felhasználókat, hogy „erősítsék meg fiókjukat”, amivel valójában átadják hozzáférésüket (Blikk, 2025. szeptember 22.).

A HVG 2024. decemberi figyelmeztetése szerint egy új típusú Messenger-üzenet terjedt „Meta AI” néven, amely hivatalosnak tűnő értesítés formájában érkezett a felhasználókhoz. Az üzenet arra hivatkozott, hogy a Facebook-fiók valamilyen szabálysértést követett el, és azonnali bejelentkezést kért egy linkre kattintva. A felhasználók azonban egy hamisított bejelentkezési oldalra kerültek, ahol az adataik megadása után a csalók teljes hozzáférést szereztek a fiókokhoz (HVG, 2024). Az így ellopott profilokat nemcsak további adathalász üzenetek terjesztésére használják, hanem gyakran a felhasználó nevében vásárolnak hirdetéseket vagy újabb megtévesztő kampányokat indítanak, közvetlen anyagi kárt is okozva.

A probléma 2025-re tömeges méretet öltött. A Qubit 2025. szeptemberi beszámolója szerint többmagyar Facebook-profilt törtek fel az év során, a támadások mögött pedig hamis „admin” profilok és valódinak tűnő támogatási értesítések álltak. A cikk részletesen leírja, hogy a támadók először a személyes fiókot veszik át, majd annak segítségével az ismerősöket is megkeresik, vagy üzleti oldalakhoz próbálnak hozzáférést szerezni (Bodnár, 2025). Az esetek többségében a felhasználók nem észlelik időben a jogosulatlan bejelentkezést, mert a támadók gyorsan módosítják a helyreállítási e-mail-címet és a kétlépcsős azonosítást.

A fiókok ellopása mellett egyre gyakoribb az úgynevezett hirdetési fiókok feltörése és a hirdetési keretek eltulajdonítása (ad-spend theft). Ezek során a csalók a megszerzett hozzáférések segítségével vállalkozások vagy hirdetési ügynökségek Meta Business Manager felületein keresztül hamis kampányokat indítanak, gyakran ismeretlen céloldalakra mutató hirdetésekkel. A The Hacker News 2024 novemberében arról számolt be, hogy a NodeStealer nevű kártevő kifejezetten a Facebook-hirdetési fiókokat célozza, és a bejelentkezési, valamint bankkártyaadatok megszerzése után automatikusan aktivál hirdetéseket a támadók nevében (Lakshmanan, 2024). Ugyanezt a jelenséget írta le több nemzetközi marketingügynökség is, amelyek szerint akár néhány órán belül több ezer eurónyi hirdetési költés tűnhet el a feltört fiókokból (Two Story Media, 2024).

A magyar felhasználók és vállalkozások túlnyomó többségben heti rendszerességgel használják a Facebook-ot. A profilok ellopása nem elszigetelt jelenség, hanem a hazai felhasználói körben is megjelenő, rendszerszintű kockázat a digitális interakciók e gyakori terepein.

A szakértők szerint a támadások egyik fő oka, hogy sok felhasználó nem aktiválja a kétlépcsős azonosítást (2FA), és a vállalkozásoknál sem megfelelő a hozzáférések menedzsmentje a Meta Business Manager környezetben. A védekezés alapvető lépése a biztonsági beállítások megerősítése, az ismeretlen linkek kerülése, valamint a gyanús hirdetési aktivitások folyamatos figyelése.

A Meta platformok nevével visszaélő csalások új szintet értek el: a cél a személyes adatok megszerzése mellett a fiókok és hirdetési profilok anyagi kihasználása.

3.3 HAMIS NYEREMÉNYJÁTÉKOK ÉS MÁRKANÉVVEL VALÓ VISSZAÉLÉSEK

2023-tól kezdve megsokszorozódtak a nagy márkák (például: Decathlon, Lidl, Spar, Penny) nevében folytatotthamis Facebook-kampányok, amelyek az adathalászat egyik kifinomultabb formáját képviselik (Kreatív Online, 2025a. augusztus 6.).

A csalások lényege, hogy egy hitelesnek tűnő oldalon „nyereményt" vagy ajándékutalványt ígérnek, majd a résztvevőket egy hamis oldalra irányítják, ahol bankkártya adatokat kérnek.

2023-ban például több tízezer magyar Facebook-felhasználó találkozhatott a Decathlon nevében indított hamis nyereményjátékkal, amelyben a csalók egy valódinak tűnő oldalon „ingyen hátizsákot" ígértek, mindössze néhány száz forintnyi postaköltségért cserébe. A link azonban egy hamis fizetési oldalra vezetett, ahol a felhasználók bankkártyaadataikat adták meg, így érdemi pénzügyi kár is keletkezett (Kreatív Online, 2023. augusztus 8.).

Előfordult, hogy a Fővárosi Állatkert nevében indítottak hamis nyereményjátékot, amely során a felhasználóktól „postaköltség" címén kértek pénzt vagy banki adatokat (KiberPajzs, 2025c).

2025-re az ilyen „márkaimitációs" csalások gyakran mesterséges intelligenciával generált képi elemeket használnak, és remarketing-szerű hirdetésekkel célozzák a felhasználókat, ami tovább növeli a hitelesség látszatát (Kreatív Online, 2025b. augusztus 7.). A jelenség nem csupán pénzügyi, hanem reputációs kárt is okoz a vállalatoknak, mivel sok felhasználó a valódi márkát hibáztatja, amiért „nem figyelmeztetett időben".

3.4 ONLINE KÖZÖSSÉGI TEREKEN PIACTÉRI ÁTVERÉSEK ÉS HAMIS HIRDETÉSES CSALÁSOK

Az elmúlt években a Facebook Marketplace és a Jófogás-felületek váltak a piactéri csalások központi helyszínévé, mivel a magyar internetezők többsége vásárolt az elmúlt évben valamilyen online piactéren (Impetus Research, 2024).

A BlueVoyant kiberbiztonsági cég már 2023-ban jelezte, hogy csalók hamis futárszolgálati oldalakat használnak, amelyek bankkártya adatokat és netbanki belépéseket próbálnak megszerezni a felhasználóktól a közösségi médiában (HVG, 2023. július 22.).

A KiberPajzs–Médiaunió által bemutatott „A kulcs te vagy" kampány egyik példájában is felhívják az ilyen csalásokra a figyelmet: az online hirdetési oldalakon, közösségi platformok piacterein feltett hirdetésekre válaszolva – akár telefonon felhívva az áldozatot – a csalók egy linket küldenek, amely egy hamis fizetési oldalra visz, és a kártyaadatok, illetve SMS-ben érkező hitelesítő kód bediktálásával / beíratásával digitális pénztárcát nyitnak, majd készpénzt vesznek fel az áldozat számlájáról (Kiberpajzs 2025c).

3.5 HAMIS INTÉZMÉNYI, SZOLGÁLTATÓI ÉS KÖZSZOLGÁLATI PROFILOK

2024–2025-ben Magyarországon is terjedtek a banki, hatósági és közszolgálati szervezetek nevében létrehozott hamis profilok.

Ennek ékes példája, hogy csalók a Magyar Nemzeti Bank nevében „ügyfél-elégedettségi kérdőívet" küldtek ki, valójában azonban adathalász kampányról volt szó (MNB, 2025d). Ugyanebben az évben a KiberPajzs és egy élelmiszerlánc nevében hamis biztonsági ellenőrzéseket is hirdettek (MNB, 2025e).

A Budapesti Közlekedési Központ nevét is felhasználták hamis profil készítéséhez, és egy nyereményjáték keretében az első 500 vásárlónak 950 forintért ígértek Budapest-bérletet hat hónapra. Ahhoz, hogy részt vehessenek a nyereményjátékban egy űrlapon banki és személyes adataikat kellett megadniuk az embereknek, amelyeket felhasználva károsították meg az áldozatokat (KiberPajzs, 2025c).

3.6 ROMANTIKUS VAGY „NIGÉRIAI" CSALÁSOK

Ezek az emberi kapcsolatokat kihasználó csalások a közösségi platformok egyik legstabilabb visszaélési formái. A csalók érzelmi manipulációval, hosszú távú bizalomépítéssel, majd sürgető pénzkéréssel érik el céljukat, mint a korábban ismertetett zalaegerszegi áldozat esetében is, akitől egy magát Szíriában állomásozó katonának kiadó csaló számos technikát felhasználva közel 1,5 millió forintot szerzett. A csaló az áldozatot rávette, hogy hamis csomagküldő szolgálati linkre kattintva fizessen „díjakat", és hitelfelvételhez is felhasználta az áldozat adatait (KiberPajzs, 2025b).

A rendőrség is számos romantikus csalásról beszámolt, mint például egy vasi áldozat esetéről, akit nyilvánosan, közösségi médiában megosztott érdeklődési köre mentén tipikus social-profiling technikával környékezett meg egy csaló. Olyan álprofilt készített, amely illeszkedett az áldozat sport iránti rajongásához, és emellett vonzó, sikeres ember látszatát keltette, aki volt sportolóként most egy játékügynökség vezetője. Különböző indokokkal, mint például, hogy utazáskor otthon hagyta bankkártyáját, végül 36 millió forintot csalt ki áldozatától. 2025-ben egy újabb, hasonló esetben Szíriában szolgáló katonának adta ki magát és 2,5 millió forintot szerzett áldozatától egy csaló „csomagszállításra" (Police.hu, 2024).

4 MILYEN ESZKÖZÖKET, MÓDSZEREKET HASZNÁLNAK AZ ONLINE PLATFORMOK A CSALÁSOK, CSALÁSI KÍSÉRLETEK KISZŰRÉSE, KEZELÉSE ÉRDEKÉBEN

A korábbi fejezetekben főként a csalástípusokra és a felhasználói sebezhetőségre koncentráltunk; ebben a részben azt vizsgáljuk, mit tesznek maguk a platformok – bankok, piacterek, közösségi szolgáltatók – a visszaélések felismeréséért és kezeléséért. A hangsúly kifejezetten a magyarországi gyakorlaton van.

4.1 BANKOK ÉS PÉNZÜGYI SZOLGÁLTATÓK (MNB, KERESKEDELMI BANKOK, REVOLUT)

A magyar bankrendszerben a Magyar Nemzeti Bank az elmúlt években látványosan erősítette a kiberbiztonsági és csalásmegelőzési fókuszt. A kiberbűnözésről szóló jelentésekben és sajtóközleményekben visszatérő elem, hogy a pénzforgalmi visszaélések száma és összértéke gyorsan nő, ezért a jegybank egyrészt technikai eszközökkel, másrészt szabályozói ösztönzőkkel próbál nyomást gyakorolni a szolgáltatókra. Az intézkedés része az is, hogy az első veszteséget bizonyos feltételek mellett a bank viseli (Index, 2025. június 4.).

Az MNB és a KiberPajzs-program keretében létrejött központi visszaélésszűrési és lakossági edukációs rendszer, az „öt csapás” program részeként, a banki oldalon azt jelenti, hogy a nagyobb szereplők egységes, mesterséges intelligenciára épülő csalásszűrő logikát alkalmaznak a tranzakciók előszűrésére, és egyre inkább valós időben próbálják kiszűrni a gyanús utalásokat (MNB, 2025f. július 1.). Ezek a rendszerek gyakran viselkedéselemzésen alapulnak – például felismerik, ha az ügyfél szokatlan időpontban vagy új eszközről kezdeményez tranzakciót –, és gépi tanulással folyamatosan javulnak.

A Nemzeti Kibervédelmi Intézet (NKI) mint állami kiberbiztonsági hatóság és incidenskezelő központ, kommunikációs, edukációs és technikai megelőző funkciót lát el: feladatai közé tartozik a lakosság és intézmények tájékoztatása a kibertér aktuális fenyegetéseiről, a tudatos internethasználat elősegítése, valamint a kiberbiztonsági incidensek fogadása, elemzése és riasztása (NKI, n.d.). A Nemzeti Kibervédelmi Intézet rendszeresen ad ki riasztásokat konkrét csalási kampányokról (például: hamis NEAK-SMS-ek), amihez részletes lakossági tájékoztatás társul a csalás felismerési jelekről és a teendőkről.

A KiberPajzs-program keretében a Magyar Bankszövetség ajánlásokat fogalmazott meg technikai lépésekre és útmutatót adott a banki tanácsadók számára a csalás áldozataival való empatikus, strukturált kommunikációra. Az MBH belső útmutatója szerint például a tanácsadóknak, miközben a technikai lépéseket kell ismertetik, figyelmet kell fordítaniuk az ügyfél érzelmi támogatására is (például: nem hibáztatás, segítő nyelvezet) (Fintechzone, 2024. május 30.).

A hazai nagybankok ehhez kapcsolódva több szinten építettek ki védelmi vonalakat. Az OTP, az Erste vagy az MBH esetében már alapvetés a kétfaktoros azonosítás az elektronikus banki belépésnél és a magasabb összegű tranzakcióknál, a mobilbanki alkalmazásokban pedig részletes figyelmeztetések jelennek meg, ha például az ügyfél ismeretlen kedvezményezettnek utal vagy szokatlanul nagy összeget mozgat. A kétfaktoros azonosítás csökkenti a csalási kockázatot, mert az egyszerű jelszólopás önmagában nem elegendő – szükséges hozzá egy második eszköz, például SMS-kód vagy mobilapp megerősítés (OTP Bank, n.d. Erste Bank, n.d. MBH Bank, n.d.).

Ezt egészítik ki az egyre szofisztikáltabb limitek: az Erste például személyre szabott napi átutalási limiteket kínál, amelyek csökkentik a kár nagyságát akkor is, ha a csalók valamilyen módon hozzájutnak a -belépési adatokhoz (Erste Bank, 2025. június 26.). A bankok ügyfélkommunikációja is látványosan átalakult: a csalásmegelőzés külön aloldalakon, figyelmeztető kampányokban, sőt offline rendezvényeken is megjelenik, sokszor konkrét, aktuális csalástípusokra (hamis csomagküldős SMS, call centernek álcázott hívások, kripto-befektetési átverések) reagálva. Az MBH komoly erőfeszítéseket tett az ügyfélkörét érintő nagyösszegű csalássorozat után és külön csalásmegelőzési oldalon foglalja össze az adathalászat elleni alapelveket (erős, egyedi jelszó, kétfaktoros azonosítás, csak hivatalos csatornák használata), és külön figyelmeztetéseket tesz közzé konkrét phishing-kampányok kapcsán. A bank és az ORFK között 2025-ben megújított együttműködés célja, hogy a bank biztonsági csapata és a rendőrség gyors, összehangolt incidenskezelést valósítson meg a felmerülő csalási esetekben (MBH, 2025).

A magyar felhasználók körében külön kategóriát jelent a Revolut, amelyet sokan „bankként” használnak, ugyanakkor jogi és felügyeleti szempontból eltért eddig a hazai hitelintézetektől. A Revolut Bank UAB litvániai székhellyel rendelkezik, EU-s banki engedéllyel működik, és a magyar ügyfelek betétei a litván betétbiztosítási rendszer védelme alatt állnak, legfeljebb 100 000 euróig (Economx, 2025. november 8.).

Az MNB többször figyelmeztette a magyar ügyfeleket, hogy a Revolut nem magyar leánybankként, hanem határon átnyúló szolgáltatóként működik, ezért a magyar felügyelet fogyasztóvédelmi eszközei korlátozottak, a panaszok elsődlegesen a litván felügyelethez tartoznak (MNB, 2024. október 17.). Ez a helyzet megváltozott a közelmúltban: a Magyar Nemzeti Bank hivatalos nyilvántartásában megjelent a Revolut Bank UAB magyarországi fióktelepe, ami lehetővé teszi a helyi IBAN-számok és a magyar ügyfélszolgálat bevezetését (Portfolio, 2025. november 6.).

Ugyanakkor éppen digitális jellege miatt a Revolut kimelt hangsúyt fektet és komoly erőfeszítéseket tesz csalásmegelőző funkciók beépítésére az alkalmazásba (Revolut, n.d.). A legfontosabb eszközök közül több kifejezetten a kártyás visszaélések és az online vásárlási csalások kockázatát csökkenti:

- Kártyabiztonsági beállítások: az alkalmazásban pár érintéssel fagyasztható („freeze”) a kártya, külön kapcsolóval tilthatók az online tranzakciók, az ATM-készpénzfelvétel, a

mágnescsíkos (swipe) és az érintéses fizetés. Emellett „location-based security” funkció is elérhető, amely a telefon helyadatai alapján blokkolhatja az olyan fizetéseket, ahol a terminál földrajzi helye jelentősen eltér a felhasználó tartózkodási helyétől.

- 3D Secure és extra hitelesítés: a Revolut-kártyák támogatják a 3D Secure rendszert, amely online vásárlásoknál az alkalmazásban jóváhagyó értesítést kér, így a lopott kártyaadatok önmagukban nem elegendők a fizetéshez.
- Virtuális és „eldobható” kártyák: a Revolut egyszer használatos virtuális kártyái minden tranzakció után automatikusan új kártyaadatokat generálnak, így a megszerzett adatok azonnal érvénytelenek.
- Felhasználói edukáció: a Revolut saját súgóoldalain részletesen összefoglalja, milyen jelek utalhatnak csalásra, és mit tegyen az ügyfél, ha már áldozattá vált.

A Revolut tehát technikailag fejlett, finomhangolható biztonsági eszköztárat kínál, ugyanakkor a felügyeleti-tulajdonosi struktúra miatt a magyar ügyfelek védelme részben más joghatóságok intézkedéseitől függ. Jó példa arra, hogy a csalásmegelőzés ma már nemcsak technológiai, hanem jogi és intézményi kérdés is.

4.2 ÁR-ÖSSZEHASONLÍTÓ OLDALAK

Az online kereskedelemben az ár-összehasonlító oldalak egyre gyakrabban válnak a visszaélések potenciális terepeivé. Ár-összehasonlítóként működik részben a Google kereső automatikusan felajánlott „szponzorált” terméklistája vagy „Termékek” fül a keresési találatok között. Bár elviekben a legjobb ár megtalálását teszik lehetővé, mégis több fogyasztóvédelmi jelzés mutat arra, hogy az ilyen platformok használata önmagában nem garantál csalásmentességet. Nemzetközi szinten is látszik, hogy az ár-összehasonlító felületek komoly kockázati pontok: az Európai Bizottság úgynevezett „Google Shopping-ügyében” például azt kifogásolták, hogy a Google a saját ár-összehasonlító szolgáltatását előnyben részesítette más szolgáltatókkal szemben. Bár ez elsősorban versenyjogi ügy, az ilyen önpreferálás végső soron a fogyasztói döntéseket torzíthatja, mert a „kiemelt” ajánlatok nem feltétlenül a legkedvezőbb vagy legmegbízhatóbb konstrukciók.

Jellemzően kétfajta csalás kapcsolódik ezekhez az odalakhoz:

1. Félrevezető árak – Az összehasonlító oldalak eredménytábláin szereplő „legolcsóbb” ajánlatok mögött sok esetben olyan webáruház áll, amely még nem rendelkezik megbízható értékelésekkel, vagy a fizetés/más szállítási feltétel miatt extra kockázatot hordoz. Erre figyelmeztet az NMHH is: az ár-összehasonlító oldalak segíthetnek az árak reális piaci szintjének felmérésében, de ha egy ismeretlen webáruház kínálata különleges akcióval vagy kiugróan kedvező árral kiemelkedik a piaci átlagból, az gyanúra adhat okot (Economx, 2024. november 19.)
2. Csaló kereskedők megjelenése az összehasonlító rendszerekben – Az összehasonlító oldalak listáin feltűnő kereskedők között olyan szerepelhet, amely

valójában nem teljesít, vagy az árverésre hívó kommunikációval él. A szakirodalom szerint e területen a legnagyobb probléma az, hogy az aggregátorok nem mindig vizsgálják részletesen az eladó múltját, és az értékelés- vagy visszajelzés-mechanizmusok mögött nem feltétlenül áll független audit (Mai Világ, 2019. május 27.).

A magyar példák között nem ritka, hogy a keresőben első helyen megjelenő ajánlat olcsónak tűnik, de a fizetési mód korlátozott (csak előreutalás), vagy a szállítási költség átláthatatlanul magas – ami azt eredményezi, hogy végső soron a vásárló veszteséggel szembesül. Egy hazai blogpéldában egy olyan webshop került elő, amely a Google-keresőben „ajándék kerékpár" kulcsszóra dobta ki magát elsőként, de a rendelést követően soha nem teljesített (BikeMag, 2025. február 11.).

Kiemelt szereplő az Árukereső.hu, amely ár-összehasonlító oldalból gyakorlatilag fogyasztóvédelmi referenciaponttá vált. A cég által működtetett „Megbízható Bolt" program lényege, hogy a minősítés kizárólag valós vásárlásokhoz kapcsolódó értékelésekre épül: csak azok a fogyasztók kapnak a vásárlások után kérdőívet, akik ténylegesen rendeltek az adott webshopból (Árukereső, n.d.-a).

Ugyanakkor 2024-ben komoly rendszerkockázatra derült fény: a Kockabolygó és Kockaváros nevű LEGO-webshopok hosszabb ideig „Megbízható bolt" címkével, 4,5 feletti átlagértékeléssel és több, mint háromezer véleménnyel szerepeltek az Árukeresőn, miközben a vásárlók egy része egyáltalán nem kapta meg a kifizetett árut, több tízezer forintot veszítve. A csalók ki tudták játszani a rendszert, mivel a sok ötcsillagos értékelés kiegyensúlyozta a negatív bejegyzéseket, és a minősítés elnyeréséhez szükséges numerikus küszöbértékek teljesültek (Trade Magazin, 2024. december 6.).

A Shoprenter technikai leírása alapján a „Megbízható bolt" program minősítése továbbra is főként az értékelések számán és átlagán alapul, így a tartalmi elemzés vagy az extrém mintázatok szűrése (például: nagyszámú „nem kaptam meg az árut" típusú komment) jelenleg nem része az automatizmusnak (Shoprenter, 2024. augusztus 23.). A Kockabolygó-ügy tanulsága tehát kettős: egyrészt a „Megbízható bolt" minősítés továbbra is fontos bizalmi jelzés a fogyasztók felé, másrészt nem helyettesíti a tudatos vásárlói óvatosságot, különösen új vagy ismeretlen webshopok esetében.

Ezt követően az Árukereső kommunikációjában erősítette a csalásmegelőzési és értékelési transzparenciát célzó intézkedéseit: 2025-ben több nyilatkozat és interjú is arról szólt, hogy a vállalat automatizált szűrőkkel és IP-alapú anomália-detektálással „szinte nullára" csökkentette a hamis vélemények arányát. A vállalat újabb kommunikációs kampányaiban azt is hangsúlyozta, hogy a bizalom növelése már nem csupán technikai, hanem reputációs kérdés is (Digital Hungary, 2025. június 19. és október 8.).

Az ár-összehasonlító oldalak között sajátos pozíciót foglal el a Gazdasági Versenyhivatal (GVH) által működtetett Árfigyelő rendszer. Nem klasszikus ár-összehasonlító oldal, hanem állami,

piaci szereplőktől független online adatbázis, amelyet kifejezetten közérdekű céllal hoztak létre. A GVH hivatalos tájékoztatása szerint az Árfigyelő alapját a 163/2023. (V. 8.) Korm. rendelet és a 11/2023. (VI. 22.) GFM rendelet adja; a rendszer feladata, hogy a fogyasztók számára napi árakat tegyen nyilvánosan hozzáférhetővé az alapvető élelmiszerek széles körében, és egyúttal segítse a piaci verseny erősítését, az infláció fékezését (GVH, n.d.-a).

Az Árfigyelőben az adott napra érvényes napi ár, a korábbi ár és – ahol van – a törzsvásárlói ár érhető el, amely adatokat a kereskedőknek naponta kell feltölteniük. Adatszolgáltatásra az a kereskedő kötelezett, amely a rendelet alapján a legnagyobb üzletláncok közé tartozik, de ehhez önként más piaci szereplők is csatlakozhatnak (GVH, 2023. július 19.). A rendszer 2023. július 1-jei indulása óta fokozatosan bővült: 2025 novemberében már 160 termékkategóriában, több mint 15.000 különböző élelmiszer- és háztartási termék ára követhető nyomon, kilenc nagy kiskereskedelmi lánc országszerte több, mint 1200 boltjában (Árfigyelő, 2025. november 11.). A GVH értékelése szerint az Árfigyelőnek kimutatható piacélénkítő, illetve árcsökkentő hatása van: a Makronóm Intézet elemzése alapján 2023 decembere és 2024 februárja között közel 20 milliárd forint megtakarítást jelenthetett a magyar háztartásoknak, részben azáltal, hogy transzparensebbé tette az árakat, részben pedig azáltal, hogy az üzletláncok árcsökkentéssel reagáltak az összehasonlíthatóság nyomására (GVH, 2025. január 24.).

Az Árfigyelő egyedi értékekkel van jelen az online ár-összehasonlító oldalak között:

- Piaci érdekektől független működés: az Árfigyelő nem hirdetési felület, a GVH kifejezetten rögzíti, hogy a honlap nem minősül reklámnak vagy ajánlattételnek, és a kereskedők fizetett megjelenés útján sem tudják előrébb sorolni magukat.
- Kötelező és ellenőrzött adatszolgáltatás: a legnagyobb kiskereskedelmi láncok számára jogszabály írja elő az adatküldést, amelyet a fogyasztóvédelmi hatóság (kormányhivatalok) is ellenőriz; ha az üzletben feltüntetett ár magasabb, mint az Árfigyelőben szereplő, az hatósági eljárást vonhat maga után.
- Makrogazdasági és fogyasztóvédelmi funkció: az állami szervek az Árfigyelő adatai alapján részletes képet kapnak az árak alakulásáról, így célzottan tudják vizsgálni az inflációs folyamatokat, az esetleges kartellgyanús vagy tisztességtelen kereskedelmi gyakorlatokat.

Ha rendeltetésszerűen működik, az Árfigyelő egyszerre fogyasztóvédelmi és versenypolitikai eszköz. A klasszikus ár-összehasonlító oldalakkal szemben itt nem az a cél, hogy egy adott kereskedő forgalmát növeljék, hanem hogy transzparensebbé tegyék az árakat – vagyis pontosan azt nyújtja, amiért a fogyasztók az ár-összehasonlító oldalakhoz fordulnak.

Ugyanakkor sajnos az Árfigyelővel kapcsolatban is előfordult már a fogyasztók kárára indított csalás. 2023 augusztusában a GVH külön sajtóközleményben figyelmeztetett arra, hogy internetes csalók az online Árfigyelőre megtévesztésig hasonlító mobilapplikációval próbálják félrevezetni a fogyasztókat. A „csaló-app” a hivatalos arculati elemeket és az Árfigyelő nevet

használta, miközben a letöltése nem valós, sőt félrevezető árinformációkat közölt, és adatbiztonsági kockázatot is jelenthetett. A GVH a közleményben jelezte, hogy megtette a szükséges jogi lépéseket, kezdeményezte az illegális alkalmazás eltávolítását a Google és az Apple áruházából, és azt kérte a fogyasztóktól, hogy az Árfigyelővel kapcsolatos információkért mindig csak a hivatalos webcímet (arfigyelo.gvh.hu) használják (GVH, 2023. augusztus 5.).

4.3 KÖZÖSSÉGI ÉS KOMMUNIKÁCIÓS PLATFORMOK: AUTOMATIKUS SZŰRÉS ÉS BEJELENTÉSI RENDSZEREK

A közösségi oldalak és üzenetküldő alkalmazások az online csalások egyik leggyorsabban terjedő terepévé váltak, mint azt előzőleg bemutattuk. A visszaélések – hamis hirdetések, nyereményjátékok, befektetési átverések, vagy személyazonosság-lopások – terjedése ellen a platformok különféle technikai megoldásokra és felhasználói visszajelzésekre támaszkodó megoldásokat vezettek be. A szolgáltatók összetett módon reagáltak ezekre a kihívásokra, különböző eszközöket bevetve a felhasználók védelmére:

1. Algoritmikus, automatizált tartalomszűrés
2. Felhasználói jelentésekre támaszkodó megoldások
3. Felhasználói edukáció és tájékoztatás

Algoritmikus, automatizált tartalomszűrés: a legnagyobb szereplők – köztük a Meta (Facebook, Instagram, WhatsApp), a YouTube, a TikTok és a X (korábban Twitter) – gépi tanulásra épülő moderációs rendszereket működtetnek. Ezek célja a gyanús tartalmak (például: „könnyű pénzszerzést” ígérő posztok, befektetési hirdetések vagy adathalász üzenetek) korai felismerése és eltávolítása még azelőtt, hogy a felhasználók széles köréhez eljutnának (Facebook, 2025 augusztus; TikTok, 2025. október 10.).

A Meta 2024-es jelentései szerint naponta több millió problémás tartalmat távolított el a rendszer, és a problémás tartalmak 80–95%-át már bejelentés előtt automatikusan észlelték (Facebook, 2025 január 7). A rendszer azonban korántsem tévedhetetlen: független elemzések szerint a mesterséges intelligenciával támogatott tartalomszűrés sok esetben téves pozitív vagy téves negatív eredményt ad. Ez azt eredményezi, hogy ártalmatlan tartalmakat is letilt, miközben a kifinomult csalások egy része észrevétlenül marad, különösen, ha ehhez a felületnek anyagi érdeke is fűződik (Reuters, 2025. november 6.).

Felhasználói jelentésekre támaszkodó megoldások: A Meta és más nagy platformok minden felhasználó számára elérhetővé tették a gyorsjelentési lehetőségeket. Egyetlen kattintással bejelenthetők a gyanús hirdetések, profilok, üzenetek. Ezek a visszajelzések kulcsszerepet játszanak a moderációs algoritmusok fejlesztésében. A magyar felhasználók körében végzett felmérések szerint ugyanakkor sokan tapasztalják, hogy a bejelentett csaló oldalak lassan vagy egyáltalán nem tűnnek el, ami a rendszer túlterheltségére és a tartalomellenőrzés korlátozott humán kapacitására utal (Impetus Research, 2024).

Felhasználói edukáció és tájékoztatás: Az elmúlt években a Meta és más technológiai cégek is nagy hangsúlyt fektettek a felhasználók tudatosítására és edukálására. A vállalat magyar nyelvű Help-rendszerei (Facebook és Instagram súgóoldalak) külön tájékoztatókat tartalmaznak az online csalások felismeréséről, a biztonságos bejelentkezésről és az adathalász üzenetek elkerüléséről.

A Facebook „Biztonsági központja" például részletes útmutatást ad arról, hogyan lehet azonosítani a gyanús üzeneteket, hogyan működik a kétfaktoros azonosítás, valamint miként lehet visszaszerezni a feltört fiókokat (Facebook, n.d.-a). Az Instagram súgóoldalán szintén megtalálhatók az adathalászat elleni tippek, a gyanús üzenetek jelentésének menete, és a hivatalos biztonsági beállítások (Instagram, n.d.).

A Meta 2024 decemberében globális szintű csalásmegelőzési kampányt indított, az ünnepi időszak előtt, hogy felkészítse a felhasználókat a lehetséges csalásokra. A kezdeményezés a Facebook, az Instagram és a WhatsApp felületein a tipikus online visszaélések, mint a hamis hirdetések, az adathalászat és a kereskedelmi, nyereménysorsolásos csalások felismerését célozta. A kampány részeként a Meta edukációs anyagokat és biztonsági útmutatókat tett közzé, valamint frissítéseket vezetett be a Marketplace és más platformfunkciók működésében, a visszaélések kockázatának csökkentése érdekében. A Meta csak 2024-ben több mint kétmillió fiókot törölt alkalmazásaiból, amelyek csalóközpontokhoz tartoztak (Facebook, 2024. december 10.).

A WhatsApp és a Viber hasonló edukációs irányt követ: mindkettő beépített „Spam-ellenőrzés" és „Ismeretlen számok némítása" funkcióval rendelkezik, valamint külön oldalt működtet az átverések felismerésére. A WhatsApp hivatalos blogján rendszeresen tesz közzé figyelmeztetéseket az aktuális csalástípusokról, beleértve az álnyereményjátékokat és a „barát vagy rokon nevében" küldött hamis üzeneteket is (WhatsApp, n.d.).

E platformoknál is kulcsfontosságú a felhasználói tudatosság: a vállalatok erőfeszítései ellenére a közösségi médiában terjedő csalások visszaszorítása csak akkor lehet hatékony, ha a technikai szűrés és a digitális írástudás fejlesztése kéz a kézben halad.

A felhasználói tapasztalatok alapján sajnos messze nem tökéletes a rendszer: hasznosnak tartják a jelentési funkciókat, de a csaló hirdetések és fiókok gyakran lassan vagy egyáltalán nem tűnnek el. Az elmúlt években több újságcikk is feltárta, hogy a Meta platformok rendszereiben a jelentett csaló hirdetések nagy része hetekkel, sőt hónapokkal később is aktív maradt, és a tiltások vagy törlések gyakran csak ismételt jelzések után történtek meg. Egy, a Meta belső dokumentumaira hivatkozó 2025-ös riport szerint a vállalat a felhasználók által bejelentett csalások ellenére bizonyos (általában magas költésű) hirdetőket még több alkalommal is engedett tovább hirdetni, mielőtt fellépett volna ellenük. Előfordult, hogy akár 500 bejelentés is szükséges volt a leállításhoz. „A Meta tavalyi becslése szerint a csalárd hirdetések akár a cég bevételének 10 százalékát is kitehetik, ami összesen körülbelül 16 milliárd dollárt, vagyis mintegy 5356 milliárd forintot jelentene. Ez magában foglalja a „csalárd e-kereskedelmi és befektetési rendszerek, illegális online kaszinók és tiltott gyógyászati termékek

értékesítésének” hirdetéseit. (Reuters 2025. november 6.). Ugyanakkor a vállalat a felhasználók által bejelentett csalások mintegy 96%-át figyelmen kívül hagyta vagy tévesen utasította el. Ez jól mutatja, hogy a jelentési mechanizmusok technikailag elérhetők ugyan, ám a humán moderációs rendszer kapacitáskorlátai, az automatizált rendszer szituációs-értékelési hiányosságai és a felületek anyagi ellenérdekeltsége miatt a felhasználók biztonságérzete, illetve a helyi jogszabályok érvényesítése továbbra sem prioritás.

4.4 JELENTÉSI CSATORNÁK, SZABÁLYOZÁSI KÖRNYEZET ÉS FELHASZNÁLÓI TAPASZTALAT

A platformok belső rendszereit Magyarországon több külső, intézményi eszköz egészíti ki. Az NMHH által működtetett Internet Hotline például 0–24 órában fogadja a jogsértő vagy káros online tartalmakról szóló bejelentéseket, ideértve az átverésgyanús vagy csaló oldalakat is (NMHH, 2025. április 30.).

Az Eurobarométer és hazai közvélemény-kutatások alapján a magyar felhasználók jelentős része továbbra is úgy érzi, hogy a digitális platformok nem nyújtanak elég védelmet, és erősebb fellépést vár a kockázatos tartalmakkal és szolgáltatásokkal szemben (Impetus Research, 2024).

5 MAGYARORSZÁGON HASZNÁLT ONLINE PIACTEREK ÉS ÁTVERÉSEK, CSALÁSFELDERÍTÉS ONLINE PIACTEREKEN

Magyarországon számtalan magyar és nemzetközi online piacteret használnak a fogyasztók, lehetetlen lenne ezek közül mindegyikre kitérni. Mégis, a legfontosabb felületeket lehetséges egyfajta tipizálás mentén csoportosítani: 1, a másodlagos és apróhirdetési piacterek (Jófogás, Vatera, Vinted), 2, aukciós/gyűjtői oldalak (Galéria Savaria, és bizonyos kategóriák mentén a Vatera), 3, zárt tematikus Facebook adás-vételi csoportok és a közösségi piacterek (Facebook Marketplace), 4, elsősorban kereskedők által használt piacterek (eMag, Alza) képezik az e-kereskedelem legsűrűbben használt terepeit. Bár több nemzetközi piactér (például: Temu, eBay, Amazon) is népszerű, jelen tanulmány a lokálisan használt vagy helyi eladó-vevő kapcsolatokra épülő rendszerekre fókuszál és ilyen értelemben a Facebook Marketplace is releváns, mivel a kapcsolatok többnyire helyi szinten jönnek létre. A korábbi fejezetekben ismertetett általános csalás, megtévesztés trendek itt konkrét piactéri mechanizmusok útján valósulnak meg.

A piactéri csalások többsége a bizalom és a korlátozott verifikáció kihasználására, valamint a felületek kontrolljának hiányosságaira épít: (1) hamis vagy nem létező termék hirdetése („előre utalás → eltűnés”), (2) hamis csomagszállítási/nyomonkövetési linkek, amelyek adathalász oldalra vezetnek, (3) hamis fizetési/“biztonsági” oldalak, ahol a kártyaadatokat gyűjtik, (4) eladó/fiókeltérítés -feltörés, amely után a megtámadott fiókból további csalások indulnak, és (5) szándékosan manipulált értékelési rendszerek (hamis pozitív visszajelzések) a látszólagos hitelesség növelésére.

A hazai platformok több, kombinált technikát alkalmaznak felhasználóik védelmére: beépített vevővédelem és „letét-szerű” megoldások (a vételárat a platform ideiglenesen kezeli), tranzakció- és üzenetelemzés (automatizált phishing-link felismerés), felhasználói értékelési/rangsorolási rendszerek és gyors bejelentési csatornák. A Jófogás például saját vevővédelmi rendszert és adathalászat-ellenes útmutatót működtet; a Vatera hangsúlyozza a vevővédelem szerepét és a kockázatos tranzakciók rendőrség felé továbbítását; a Vinted pedig a termék megérkezésének visszaigazolásáig a vevő oldaláról visszatartja a vételárat, és emellett dedikált phishing-bejelentési útvonalat tart fenn. Ezek intézkedések jelentősen csökkentik a rutinszerű kockázatokat, de nem teszik lehetetlenné a célzott, kifinomult támadásokat (Jófogás, 2025. november 24.; Vatera, 2025. július 3. és 2023. november 15.; Vinted, n.d.-a és n.d.-b). Ugyanakkor a gyakorlatban a tranzakciók gyakran a hirdetésben megadott telefonszámon vagy e-mailen keresztül vagy privát üzenetváltásban folytatódnak, majd közvetlenül történik banki utalás vagy készpénz átadása az adásvétel kapcsán – így a platformok beépített biztonsági eszközei nem minden esetben érvényesülnek és ezt ki is használják a csalók.

A piacterek belső eszközein túl külső, független intézmények is védik a magyar fogyasztókat az online csalásoktól. A GVH Árfigyelője fogyasztóvédelmi szerepet tölt be, ugyanakkor maga is célponttá vált (hamis appokkal), ami rávilágít a platformokhoz kapcsolódó, hamisított harmadik-fél szolgáltatások veszélyére (Index, 2023. augusztus 5.). Az NMHH Internet Hotline pedig 0–24-ben fogadja a gyanús tartalmak bejelentését, ami fontos jogi-operatív híd a felhasználói jelentések és a hatósági eljárások között (NMHH, 2025 április 30.).

5.1 APRÓHIRDETÉSI PIACTEREK: JÓFOGÁS

A Jófogás „Biztonságos vásárlás" aloldalán részletesen ismerteti a vásárlók számára a leggyakoribb csalási mintákat (például: irreálisan alacsony ár, előre utalás, nem létező termék) és ad konkrét tanácsokat a megelőzésre.

A platform továbbá részletesen foglalkozik az adathalászattal is („Adathalászat" aloldal) és lehetőséget biztosít a „Szabálysértés jelentése" funkció keretében a felhasználók részére.

A vevővédelem folyamatát („Vevővédelem – Biztonságos vásárlás") is leírják: a vételár csak akkor kerül az eladóhoz, ha a termék megérkezett és rendben van; panasz esetén 48 órán belül jelezni kell (Jófogás, n.d.).

5.2 PIACTÉR-AUKCIÓS PLATFORM: VATERA

A Vatera oldala hangsúlyozza, hogy négyszintű védelmi rendszert működtet: eladó ellenőrzése, értékelési rendszer, csalófigyelő rendszer, pénzvisszafizetési garancia.

2025-ben új fizetési modellt vezettek be: online bankkártyás fizetés + vevővédelem = csak akkor kapja meg az eladó a pénzt, amikor a vevő visszaigazolta a termék átvételét – a megoldás hasonlít a Vinted által alkalmazott rendszerhez (Vatera, 2025. november 24.).

Ezen felül a Vevővédelem blogbejegyzése részletezi a panaszkezelési opciókat: visszaküldés, árcsökkentés, termék megtartása + visszatérítés.

5.3 SPECIALIZÁLT AUKCIÓS/GYŰJTŐI PIAC: GALÉRIA SAVARIA

A Galéria Savaria feltételezi, hogy a felhasználók számára bizonyos „ellenőrzött" státusz elérése növeli a bizalmat, valamint az értékelési rendszer és felhasználói visszajelzések nyilvánossága a tranzakciók megbízhatóságát támogatják. A platform már a regisztrációs folyamatban is ellenőrzi a felhasználók hitelességét, és szabályrendszere kifejezetten a biztonságos működést szolgálja. A vevő a sikeres aukció vagy vételi ajánlat megtétele után a rendszeren keresztül kapja meg az eladó banki adatait, az eladó pedig a vételár beérkezése után küldi el vagy adja át a terméket. Csak regisztrált felhasználók vásárolhatnak, és a regisztráció része érvényes bankkártya rögzítése is. A Galéria Savaria online piacterének teljes felületén a felhasználók nem tehetnek közzé olyan tartalmat, amely elérhetőséget, legyen az telefonszám, e-mail cím, weblaphivatkozás, postacím vagy egyéb olyan adat, amely kapcsolatfelvételre alkalmas információt hordoz, így a biztonságos, ellenőrzött csatornákon tartja a piactér az adásvételt.

Az Általános Felhasználási Feltételek alapján a regisztrált tagok kötelesek valós személyes adatokat megadni, a rendszer pedig korlátozhatja, felfüggesztheti vagy törölheti azon felhasználókat, akik valótlan adatokat adnak meg, illetve a közösségi normákat megszegik (Galéria Savaria, n.d.-a). A platform a valós identitás igazolását és a tranzakciók biztonságát azzal is erősíti, hogy ellenőrzi a fizetési módokat és a vásárlók–eladók közötti kapcsolat hitelességét.

A Gyakran Ismételt Kérdések között szerepel, hogy az újonnan regisztrált tagok csak korlátozott értékű vásárlást hajthatnak végre, amíg hitelesített státuszt nem szereznek, illetve a szolgáltató a gyanús tranzakciókat ellenőrzés alá vonhatja (Galéria Savaria, n.d.-b). Ez a fokozatos bizalmi modell a magyar online aukciós piac egyik legátgondoltabb önszabályozó rendszere, amely kombinálja a technikai verifikációt a közösségi értékeléssel.

5.4 ZÁRT FACEBOOK ADÁS-VÉTELI CSOPORTOK

Itt a védekezési minták eltérők: egyes eladók kézzel írt „név + dátum” feliratot helyeznek el a termék mellé készített fotón, mint saját bizonyítékot arra, hogy a termék valós és az eladó komoly: ez a DIY védekezés a stock fotókat használó csalókkal szemben. Ugyancsak gyakori, hogyha valaki a csoportban csalás áldozatává válik, akkor erről posztol, van, hogy akár képernyőképet is megoszt a profilról, aki kárt okozott neki. Ugyanakkor mivel a moderáció jellemzően közösségi alapon történik, és a tranzakciók gyakran szintén off-platform módon zajlanak, az ilyen csoportokban a csalás kockázata magas lehet.

5.5 NAGY WEBÁRUHÁZAK: EMAG, ALZA

Az eMAG és az Alza a hazai online piactér-ökoszisztéma azon szereplői, amelyek formálisan piactérként működnek, de elsősorban ellenőrzött, regisztrált kereskedők számára biztosítanak értékesítési felületet, nem pedig magánszemélyeknek. Ez lényeges különbséget jelent a nyílt, magánszemélyek által használt apróhirdetési platformokhoz képest, és egyben magyarázatot ad arra, hogy miért nem találhatók a felhasználói feltételekben kifejezett, fogyasztók számára szóló figyelmeztetések az online csalásokkal kapcsolatban.

Az eMAG Általános Felhasználási Feltételei részletesen szabályozzák a vásárlói és eladói jogokat, a termékértékelések és visszajelzések rendjét, a panaszkezelés folyamatát, valamint az elállási jog gyakorlását (eMAG, n. d.). A dokumentum hangsúlyozza, hogy a vásárló az eMAG platformján értékesítő, szerződésben álló partnerektől vásárolhat, akik a platform előzetes jóváhagyásával tehetnek közzé termékeket. A csalásmegelőzés tehát nem a fogyasztói oldal edukációján keresztül, hanem a kereskedői hitelesítés és minőségbiztosítás útján valósul meg. Ezzel együtt a felhasználási feltételek és ügyfélszolgálati anyagok nem tartalmaznak részletes figyelmeztetéseket a potenciális online csalásokra, ami azt sugallja, hogy a platform a csalások kockázatát elsősorban a partner-oldali szűrés révén tartja kezelhetőnek. Ennek ellenére a platform működésében megjelentek kockázatok a fogyasztók számára: a Gazdasági Versenyhivatal 2023-ban ötvenmillió forintos bírságot szabott ki az eMAG-ra a vásárlókat megtévesztő akciós árak és hirdetési gyakorlatok miatt (HVG, 2023 január 30). Ez az eset jól

mutatja, hogy a biztonságosnak tartott, kereskedői alapú piactereken is felmerülhetnek olyan problémák, amelyek – bár nem klasszikus csalási formák – a fogyasztói bizalom sérüléséhez vezethetnek.

Az Alza.hu hasonló modellben működik: az Általános Szerződési Feltételek szerint az Alza saját nevében vagy hivatalosan szerződött partnerei révén értékesít, és minden vásárlás esetében garantálja a biztonságos online fizetési környezetet (Alza, n.d.). Az Alza Szerviz és Reklamáció aloldalak részletes útmutatót adnak a jótállási, visszaküldési és panaszkezelési eljárásokra. A honlapon a biztonságos fizetés kérdése központi elemként jelenik meg. Ez feltehetően szintén a zárt értékesítési modell következménye, amelyben az Alza a vásárlók és a kereskedők közötti teljes folyamatért felelősséget vállal. Az Alza talán emiatt is külön cikket szentelt a figyelmeztetéseknek a fogyasztókat célzó online csalásokkal kapcsolatban (Alza, 2022. június 2.).

Mindkét platform esetében tehát a csalásmegelőzés struktúra-alapú megközelítéssel valósul meg: az eladói kör korlátozásával és a fizetési folyamatok ellenőrzött felületen tartásával. Ugyanakkor a márkanévvel való visszaélés (például: ál-eMAG vagy ál-Alza weboldalak) továbbra is létező kockázat, amely a fogyasztók tudatosságán múlik (Infostart, 2025. június 10.).

Az online piacterek üzemeltetői egyre komplexebb védelmi rendszerekkel dolgoznak annak érdekében, hogy csökkentsék a csalás- és visszaélés-kockázatokat. Magyarországon a következő főbb mechanizmusok figyelhetők meg:

- Felhasználói edukáció és figyelemfelhívás – Például a Jófogás „Adathalászat” aloldala részletesen ismerteti, hogyan ismerhető fel egy adathalász üzenet és mit tesz a platform a visszaszorításuk érdekében.
- Technikai fizetési letét és vevővédelem – Jófogás és a Vinted például akkor utalja át az eladó részére a vételárat, ha a vevő igazolta az átvételt.
- Üzenet- és link-monitorozás, riportálási mechanizmusok – Bizonyos platformok automatikusan figyelik az üzenetváltásokat, a gyanús linkeket blokkolják, és a felhasználóknak lehetőségük van szabálysértést jelenteni.
- Eladó-hitelesítés és értékelési rendszer – A specializált oldalakon (például: Galéria Savaria) a regisztráció során történő adatellenőrzés, valamint az értékelések nyilvánossága szolgál hitelesítési célokat.
- Strukturális modell – zárt kereskedői kör – A nagy webáruház-piacterek (például: eMAG, Alza) elsősorban csak szerződött kereskedőknek engedik az értékesítést, ezáltal csökkentik a magáneladók révén keletkező kockázatokat.

Mindezek ellenére az alábbi korlátok továbbra is fennállnak:

- Off-platform tranzakciók – Ha a felek a piactér szolgáltatója által nem támogatott módon folytatják a kommunikációt (telefon, email, személyes találkozás) és nem

használják a platform fizetési vagy letétfunkcióit, akkor a védelmi mechanizmusok nem érvényesülnek.

- Célzott, kifinomult csalások – A technikai szűrés kevésbé hatásos azokkal a támadásokkal szemben, ahol a csaló személyre szabottan jár el (social engineering, fiókeltérítés).
- Márkával való visszaélés – Még a kereskedői modellben működő platformok sem képesek teljesen kizárni azt, hogy a márkanévvel visszaélve hamis oldalakat, hamis hirdetéseket hozzanak létre, ami a laikus felhasználót megtéveszthetí.
- Ismeret- és tudatosság-hiány – A mechanizmusok technikai működése fontos, de a felhasználói viselkedés (például: ár túl olcsó, link kattintása, személyes adatok megadása) továbbra is döntő szerepet játszik abban, hogy az emberek csalások áldozatává válnak. E szempontokat több hazai elemzés is alátámasztja (ESET, 2025. május 28.; BankNavigator, 2025. február 19.).

A hazai online piactér-ökoszisztémában ugyan létrejöttek a szükséges technikai és szervezeti védelmi intézkedések, ezek hatékonysága azonban korlátozott. A kockázatok jelentős része továbbra is a felhasználói viselkedésből és a szűrési mechanizmusok technikai vagy beállítási határaiból ered. A platformokra jellemző tranzakciós gyakorlatok, mint például az off-platform utalások, az üzenetekben található linkekre történő kattintás vagy a személyes átadás, olyan kockázati pontokat jelentenek, amelyek pusztán technikai eszközökkel nem kezelhetők teljeskörűen. A következő fejezetben (a mystery visit felmérés keretében) empirikus adatokkal vizsgáljuk majd, hogy ezek a mechanizmusok milyen mértékben érvényesülnek a magyar piacon.

6 A MYSTERY VISIT KUTATÁS: FRISS TAPASZTALATOK 2025 OKTÓBER-NOVEMBERÉBEN

6.1 A KUTATÁS CÉLJA

A digitális kereskedelem térnyerésével és az online piacterek mindennapi használatával az internetes csalások felismerése és kezelése a digitális tudatosság egyik legkritikusabb komponensévé vált. Mivel a felhasználók egyre gyakrabban találkoznak olyan kereskedelmi és kommunikációs helyzetekkel, amelyekben a megtévesztés lehetősége strukturálisan beépül a piactér működésébe, az online csalások működési mechanizmusainak feltárása a hatékony védekezés alapfeltétele.

Az **NMHH 2025-ben próbavásárlásos kutatást** indított annak érdekében, hogy **közvetlen, empirikus megfigyeléseken keresztül** vizsgálja az online térben megjelenő csalásokat, különösen azokat, amelyek vásárlási vagy eladási interakciók során jelentkeznek. A hagyományos kérdőíves vagy interjús megközelítésekkel szemben a próbavásárlás egy olyan módszer, amelyben a vizsgálat alanyai maguk lépnek be a tranzakciós folyamatba, ezáltal **valós interakciók során** figyelhetők meg a csalók működési technikái, a platformok reakciói és az egyes platformokon megjelenő kockázatok.

A kutatás célja az volt, hogy **feltárja az online térben előforduló csalási kísérletek mintázatait**, megértse azok lefolyását, valamint azonosítsa, hogy a különböző piacterek, közösségi felületek vagy kisebb webshopok milyen környezetet teremtenek a csalások számára. A vizsgálat elsősorban a **gyanús, kifejezetten csalásra utaló hirdetésekkel** való interakciókat célozta, a létrejövő tranzakciók tényleges lefolytatásával vagy annak kísérletével. A módszer lehetőséget biztosított arra, hogy az NMHH **első kézből származó adatokat** gyűjtsön a csalások működéséről, a felhasználókra leselkedő kockázatokról, illetve a platformok védelmi mechanizmusainak tényleges működéséről.

6.2 A KUTATÁS MÓDSZERTANA

A vizsgálat **próbavásárlás (mystery shopping)** módszerével zajlott. Ennek lényege, hogy a kutatók szigorúan ellenőrzött keretek között **vásárlói vagy eladói szerepbe lépve** valós tranzakciókat kezdeményeztek, majd dokumentálták a folyamat minden elemét: az első kapcsolatfelvételtől a fizetési kísérletig vagy az interakció lezárultáig.

6.2.1 Kutatási design és mintakeret

A vizsgálat kezdetén 50 próbavásárlási esetet határoztunk meg, amelyből a tervezett megoszlás szerint

- 40 eset vásárlói szituáció,
- 10 eset eladói szituáció lett volna.

A platformok szerinti előzetes elosztás a következő volt:

Platform	Vásárlás	Eladás
Facebook Marketplace	15	5
Jófogás	7	3
Vatera	7	1
Meska	4	1
Google-keresés	7	–
Összesen	**40**	**10**

1. táblázat: A próbavásárlási terv platformok szerint

A vizsgálat fókuszában a kifejezetten csalásgyanús hirdetések álltak. Ennek megfelelően a személyes átvétel lehetőségét minimálisra csökkentettük, és kizártuk a vásárlói védelemmel ellátott hirdetéseket. Előnyben részesítettük az előreutalást preferáló, hiányos leírással vagy stock fotókkal hirdető eladókat.

Mind az eladások, mind a vásárlások során a próbavásárlást végző eladók tapasztalataikat kérdőívben rögzítették.

A statisztikai elemzéseket az IBM SPSS Statistics 22.0 verziójával végeztük.

6.2.2 A módszertan módosítása a terepmunka során

A terepmunka megkezdését követően szükségessé vált az eredeti arányok módosítása. Az eladásra meghirdetett termékekre ugyanis jóval kevesebb, vásárlási szándékot mutató érdeklődő érkezett, mint amennyire számítottunk. Emiatt a 10 tervezett eladás helyett mindössze 3-at sikerült megvalósítani, így ezzel párhuzamosan a vásárlások száma 47-re emelkedett.

Ez az elmozdulás nem rontotta a vizsgálat érvényességét, mivel a cél továbbra is az online csalási kísérletek azonosítása volt, ehhez pedig a vásárlói szerep bizonyult hatékonyabbnak.

6.2.3 Platformhasználat

A vásárlások a következő csatornákon zajlottak:

- Facebook Marketplace
- Jófogás
- Vatera
- Google-keresések nyomán talált webshopok
- Facebook ad hoc adásvételi csoportok

Az eladási próbák Facebook Marketplace-en és Jófogáson történtek.

A Meska platformot – stabil megbízhatósága és sajátos termékprofilja miatt – végül kizártuk a vizsgálatból, a számára tervezett elemszámot pedig átcsoportosítottuk a többi platformra.

6.2.4 Időkeret és előkészítés

A terepmunka 2025. október 15. és 2025. november 12. között zajlott. A munkát előkészítő szakaszban feltérképeztük a potenciálisan csaló eladókat, összeállítottuk a vizsgálathoz szükséges terméklistát, és elvégeztük az első kapcsolatfelvételi kísérleteket.

6.3 AZ ELADÁSI PRÓBAVÁSÁRLÁSOK TAPASZTALATAI

Mindösszesen 3 eladási kísérletre került sor. Mindhárom Piactér jellegű felületen történt, a Facebook Marketplace-en. Mindhárom termék fizikai termék volt, kettő elektronika (12.000 Ft és 15.000 Ft értékben), egy pedig szépség/egészség kategóriában (20.000 Ft értékben). A három eladási kísérletből egy esetben azonosítottunk csalást, a másik két esetben legitim érdeklődők jelentkeztek.

6.3.1 Az érdeklődő fiókok jellemzői:

Három különböző vevő jelentkezett a három termékre. 2 legitim profilból nem derült ki a fiók életkora, a csalást megkísérlő profil életkora 1-6 hónapos sávba esett.

A legitim érdeklődők:

- profiljukban megadták a lakóhelyük települését,
- egyértelműen magyar névvel rendelkeztek.

A csalást megkísérlő profil:

- nem adta meg lakóhelyét,
- egyértelműen külföldi nevet adott meg.

6.3.2 A kommunikáció:

Mindhárom esetben az első kapcsolatfelvételre a hirdetés platformjának megfelelően a Facebook Messenger-en került sor. A kommunikáció során egyik esetben sem volt gyanús a nyelvi minőség, nem merült fel, hogy gépi fordításról lehet szó. Távoli elérés telepítését egyik esetben sem kérték.

A legitim érdeklődők:

- nem javasoltak csatorna váltást,
- a próbavásárlók nem éreztek sürgetést, nyomásgyakorlást,
- nem kértek a szükségnél több adatot,
- nem küldtek file-t vagy bizonylatot fizetésről.

A csalást megkísérlő profil:

- javasolt csatorna váltást,
- a próbavásárló sürgetést, nyomásgyakorlást érzett,
- banki belépést, jelszót kért,
- küldött file-t, bizonylatot fizetésről: egy banki átutalási képernyőképét,
- a tranzakció nem volt ellenőrizhető a számlán, nem jelent meg az állítólag általa küldött összeg.

6.3.3 Specifikus csalási trükkök, mint külső link, „futár" vagy „pénz fogadása":

A legitim érdeklődők:

- nem küldtek külső linket.

A csalást megkísérlő profil:

- a csalási kísérlet során a vevő profil küldött egy külső linket,
- ez futárszolgálatot volt hivatott biztosítani, a GLS nevét felhasználva (gls.order38596.cyou),
- kért továbbá bankkártyaadatot „pénz fogadásához" is linken keresztül (gls.order38596.cyou/bank/mkb/137220657),
- a domainek életkora nem ismert.

6.3.4 A csalási eset ismertetése

A csalási kísérletre a 12.000 Ft értékű elektronikai termék esetében került sor. A csalási kísérlet során hamis futárrendelő és hamis fizetési oldalra mutató külső linkeket használtak, kérték a kommunikációs csatorna váltását és sürgették az eladót. A próbavásárló a külső linkre kattintott annak érdekében, hogy ellenőrizze, valóban csalási kísérlet történt-e, de nem osztott meg semmilyen érzékeny adatot. A próbavásárló szavaival élve: „Hirdetésfeladás után pár pillanat múlva azonnal rám írt és ő akarta intézni a futárt. Kért mailt, sürgetett, hogy ő már intézte a futáron keresztül a fizetést és szállítást. Banki felhasználó nevet és jelszót akart a linken keresztül megszerezni." A csalási kísérletet a platform számára nem jelentette a próbavásárló.

6.4 A VÉTELI PRÓBAVÁSÁRLÁSOK TAPASZTALATAI

Mindösszesen 47 vételi kísérletre került sor. A vásárlások 4/5-e online apróhirdetési felületen történt. 36%-ra a Facebook Marketplace-en, 28%-ra a Jófogáson és 17%-a a Vaterán került sor.

Emellett zajlottak próbavásárlások Google Search Ads-ben megjelenő ajánlatokon keresztül (11%) és webshopokon (9%) is. A webshopok is Google Search Ads segítségével kerültek kiválasztásra a kutatásba. Ez utóbbi két felületen jóval nagyobb arányban azonosítottak a

próbavásárlások csalási kísérleteket a felületen megkísérelt próbavásárlásokon belül is: az összes Google Search Ads vásárlások 60%-a bizonyult csalási kísérletnek, a webshopok esetében ez az arány 75%, szemben a piactereken tapasztalt 3%-kal. Ebben minden bizonnyal szerepe volt annak is, hogy a Google Search Ads, illetve a webshopok esetében jóval könnyebb volt megtalálni a csalási kísérleteket – itt emlékeztetnénk, hogy a kutatásnak nem volt célja reprezentatívan leképezni az online vásárlási szokásokat Magyarországon.

PRÓBAVÁSÁRLÁS HELYE		Total (N=47)		Legitim hirdetés (n=40)		Csalási kísérlet (n=7)	
		elem-szám	oszlop%	elem-szám	oszlop%	elem-szám	oszlop%
Mi a csatorna kategóriája, ahol történt a vásárlás?	Google Search Ads	5	**10,6**	2	**5,0**	3	**42,9**
	Online apróhirdetési felület (Jófogás/Vatera/Facebook Marketplace)	38	**80,9**	37	**92,5**	1	**14,3**
	Webshop	4	**8,5**	1	**2,5**	3	**42,9**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Milyen felületen történt a vásárlás?	Facebook Marketplace	17	**36,2**	16	**40,0**	1	**14,3**
	Google Search Ads	5	**10,6**	2	**5,0**	3	**42,9**
	Jófogás	13	**27,7**	13	**32,5**	0	**0,0**
	Vatera	8	**17,0**	8	**20,0**	0	**0,0**
	Webshop	4	**8,5**	1	**2,5**	3	**42,9**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Hogyan találtad meg?	Ajánlás	1	**2,1**	0	**0,0**	1	**14,3**
	Fizetett hirdetés	1	**2,1**	0	**0,0**	1	**14,3**
	Külső keresés (Google)	9	**19,1**	4	**10,0**	5	**71,4**
	Platformon belüli keresés	36	**76,6**	36	**90,0**	0	**0,0**
	Total	47	**100,0**	40	**100,0**	7	**100,0**

2. táblázat: a megvalósult vételi próbavásárlások platformok szerint

A vizsgált 47 próbavásárlás mindegyike fizikai termékre vonatkozott. A megvásárolt termékek 62%-a elektronikai cikk, 15%-a ruházati termék, míg 23%-a egyéb kategóriába tartozott. A termékek átlagára 9 967 Ft volt (N = 47; SD = 6 653 Ft), az árak 1 900 és 34 395 Ft között mozogtak.

Az eladásra kínált termék ára az esetek 64%-ában megegyezett a piaci árral, 30%-ában alacsonyabb, 6%-ában pedig magasabb volt annál. A csalási kísérletnek minősített hét esetből hatban a kínált ár alacsonyabb volt a piaci árnál. A legitim hirdetések körében az eladási ár az esetek 75%-ában megegyezett a piaci árral, 20%-ában alacsonyabbnak, 5%-ában pedig magasabbnak bizonyult.

Eredményeink összhangban vannak a várakozással, miszerint az online termékértékesítéshez kapcsolódó csalások egyik jellegzetes vonása, hogy az elkövetők a piaci árnál feltűnően kedvezőbb ajánlattal próbálják megtéveszteni a fogyasztókat.

TERMÉKEK ÁRA		Mennyi a meghirdetett termék ára (HUF) a hirdetésben?	Mennyi a meghirdetett termék reális piaci ára (HUF)?
Total (n=47)	n=	47	47
	Átlag	9 697 Ft	12 624 Ft
	Szórás	6 653 Ft	12 601 Ft
	Minimum	1 900 Ft	1 900 Ft
	Maximum	34 395 Ft	60 000 Ft
Legitim hirdetés (n=40)	n=	40	40
	Átlag	8 814 Ft	10 008 Ft
	Szórás	5 998 Ft	7 645 Ft
	Minimum	1 900 Ft	1 900 Ft
	Maximum	34 395 Ft	34 395 Ft
Csalási kísérlet (n=7)	n=	7	7
	Átlag	14 747 Ft	27 571 Ft
	Szórás	8 395 Ft	23 050 Ft
	Minimum	8 000 Ft	3 000 Ft
	Maximum	32 245 Ft	60 000 Ft

3. táblázat: termékek átlagos ára a vételi próbavásárlások során

A próbavásárlások során vizsgált hirdetések minősége összességében kedvező volt: a hirdetések mintegy háromnegyede jó vagy nagyon jó minőségű, részletes információt tartalmazott. A meghirdetett termékek leírásának minőségét egy 1–5-ös skálán értékelték a résztvevők (1 = nagyon gyenge, 5 = nagyon részletes). A teljes mintában az értékelés átlaga 4,09 volt (N = 47; SD = 0,95), az értékek 1 és 5 között szóródtak.

A csalási kísérletként azonosított hirdetések lényegesen gyengébb minősítést kaptak: ezek átlagértéke 3,43 volt (N = 7; SD = 1,27). Bár az értékelési tartomány ebben az alcsoportban is 1–5 között maradt, a hirdetések következetesen kevésbé részletesek voltak.

A csalásgyanús hirdetésekre jellemző továbbá, hogy kevesebb fényképet tartalmaztak, és ezek döntően stock fotóknak bizonyultak, nem pedig az adott termékről vagy webshopról készült eredeti képeknek. Ez a vizuális jellegű egyszerűsítés jól illeszkedik azokhoz a mintázatokhoz, amelyek tipikusan az online csalásokra utalnak.

HIRDETÉS ISMERTETÉSE		Total (N=47)		Legitim hirdetés (n=40)		Csalási kísérlet (n=7)	
		elem-szám	oszlop%	elem-szám	oszlop%	elem-szám	oszlop%
Kérjük, értékeld a meghirdetett termék leírásának minőségét egy 1–5-ös skálán, ahol 1-es azt jelenti, hogy nagyon gyenge a termék leírásának minősége, míg az 5-ös azt, hogy nagyon részletes!	1=Nagyon gyenge	1	**2,1**	0	**0,0**	1	**14,3**
	2	1	**2,1**	1	**2,5**	0	**0,0**
	3	10	**21,3**	8	**20,0**	2	**28,6**
	4	16	**34,0**	13	**32,5**	3	**42,9**
	5=Nagyon részletes	19	**40,4**	18	**45,0**	1	**14,3**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Hány darab fénykép található a meghirdetett termékről? Kérjük, értékeld a meghirdetett termékről feltöltött képek minőségét!	1-2 fénykép	21	**44,7**	18	**45,0**	3	**42,9**
	3-4 fénykép	13	**27,7**	10	**25,0**	3	**42,9**
	5 vagy annál több fénykép	13	**27,7**	12	**30,0**	1	**14,3**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Hogyan találtad meg? Hány darab fénykép található a meghirdetett termékről?	Jó fotó(k)	30	**63,8**	30	**75,0**	0	**0,0**
	Stock fotó(k)	17	**36,2**	10	**25,0**	7	**100,0**
	Total	47	**100,0**	40	**100,0**	7	**100,0**

4. táblázat: hirdetések jellemzése a vételi próbavásárlások során

A kilenc, próbavásárlásba bevont webshop vagy Google Search Ads hirdetés közül mindössze kettőben volt elérhető az Impresszum vagy a cég adatokat tartalmazó oldal. A három legitimnek minősített webshop közül kettő esetében ez az információ szintén hiányzott, ami arra utal, hogy az Impresszum jelenléte önmagában nem alkalmas a hirdetések megbízhatóságának megítélésére.

Ezzel szemben az Általános Szerződési Feltételek (ÁSZF) megléte jóval erősebben különválasztotta a legitim és a csalásgyanús webshopokat. A három legitim webshop mindegyikében elérhető volt az ÁSZF, míg a hat csalási kísérletként azonosított eset közül csupán egynél volt megtalálható, öt esetben pedig teljes mértékben hiányzott. Ez alapján az ÁSZF hiánya potenciálisan fontos jelzőfaktor lehet a kockázatos vagy csalásgyanús online hirdetések azonosításában.

WEBSHOPOK / GOOGLE SEARCH ADS (Bázis: amennyiben a csatornakategória típusa webshop vagy Google Search Ads)		Total (N=47)		Legitim hirdetés (n=40)		Csalási kísérlet (n=7)	
		elem-szám	oszlop%	elem-szám	oszlop%	elem-szám	oszlop%
Kérlek, add meg a webshop domainjét / webcímét!	https://alosangle.com	1	**11,1**	0	**0,0**	1	**16,7**
	https://clickpick.club	1	**11,1**	0	**0,0**	1	**16,7**
	https://ecipo.hu	1	**11,1**	1	**33,3**	0	**0,0**
	https://hajina.shop	1	**11,1**	0	**0,0**	1	**16,7**
	https://www.coach-hungary.com/	1	**11,1**	0	**0,0**	1	**16,7**
	https://www.dellaprint.hu	1	**11,1**	1	**33,3**	0	**0,0**
	https://www.hungarybootsoutlets.com/	1	**11,1**	0	**0,0**	1	**16,7**
	https://www.ralphlaurenhungary.com/[1]	1	**11,1**	0	**0,0**	1	**16,7**
	https://www.skechers.hu/	1	**11,1**	1	**33,3**	0	**0,0**
	Total	47	**100,0**	40	**100,0**	7	**100,0**

5. táblázat: webshopok a vételi próbavásárlások során

A meghirdetett termékek ára széles tartományban mozgott (8 000 Ft–32 245 Ft), jellemzően ruházati vagy egyéb kategóriákból származtak. A csalásgyanús esetekben meghirdetett termékek ára jelentős eltérést mutatott a valós piaci értékhez képest: több esetben a meghirdetett ár lényegesen alacsonyabb volt (például: 9 095 Ft vs. 60 000 Ft), míg egy esetben feltűnően magas árat kértek az adott termékkörhöz képest (11 900 Ft egy ~3 000 Ft értékű termékért).

6.4.1 Az eladói fiókok jellemzői, online apróhirdetési próbavásárlás esetén:

Az online apróhirdetési felületeken 38 eladói fiók vagy profil 79%-a hat hónapnál régebben lett létrehozva, 18%-ról nem lehetett megállapítani, és csupán egy fiók – amelyik csalást kísérelt meg – volt 6 hónapnál fiatalabb. Az online apróhirdetési felületeken legitim hirdetéseket közzétevő fiókok döntő többsége hagyományos magyar személynevet használt. Kis arányban ugyanakkor megjelentek a nem magyaros vagy kevésbé tipikus névszerkezetű fióknevek is. Bár ezek kontextuálisan kevésbé illeszkednek a magyar online piacterek megszokott mintázatához, a próbavásárlások eredményei alapján mind legitimnek bizonyultak, így önmagukban nem tekinthetők kockázati jelnek.

Emellett előfordultak úgynevezett „fantázianevek” is, amelyek tipikusan hobbi- vagy mikrovállalkozói eladókra jellemzőek. Ezek a vizsgálatban szereplő esetekben nem mutattak csalásra utaló mintázatot.

1 2025 december 22-én már az alábbi figyelmeztetés jelent meg e weboldal felkeresésekor:
„Veszélyes webhely
Előfordulhat, hogy az Ön által felkeresni próbált webhelyen a támadók ráveszik Önt valamilyen szoftver telepítésére, illetve olyan adatok megadására, mint a jelszavai, a telefonszámai vagy a bankkártyaszámai. A Chrome kifejezetten javasolja, hogy térjen vissza biztonságos webhelyre. További információ erről a figyelmeztetésről.”

A vizsgált csalási kísérletek közül egy eset kapcsolódott online apróhirdetési felületen létrehozott fiókhoz, amely klasszikus magyar személynevet viselt, ami alátámasztja, hogy a névszerkezet önmagában nem alkalmas megbízhatósági indikátor.

A fiókok többségénél nem álltak rendelkezésre hivatalos értékelések (az esetek 82%-ában), így ebből érdemi következtetés nem vonható le sem a legitim, sem a csalásgyanús eladók vonatkozásában.

Minden vizsgált fiók – beleértve a csalási kísérletet is – megadta a lakóhely települését, ezért ez a tényező szintén nem különböztette meg a legitim és a csalásgyanús eladókat.

A kommunikáció gyorsaságára vonatkozó vizsgálat alapján átlagosan 30,6 perc telt el a próbavásárlói első üzenet elküldése és az eladó válasza között (N = 32; SD = 35,9). A leggyorsabb válasz 1 perc alatt érkezett, míg a leghosszabb válaszidő 180 perc volt. A válaszidő így jelentős szórást mutatott, és nem különült el élesen a legitim és csalásgyanús hirdetők között.

6.4.2 A kommunikáció és gyanús jelek:

A próbavásárlások során az első kapcsolatfelvétel minden esetben a hirdetési platform által biztosított csatornán történt, jellemzően platformon belüli chatfelületen (40,4%), Facebook Messenger-en (25,5%) vagy emailben (14,9%).

A csatornaváltás (off-platform kommunikációra terelés) – amely a csalások egyik tipikus eleme – a legitim hirdetések 5%-ában (2 eset) megjelent, viszont a csalási kísérletek során ez a lépés elmaradt.

A vizsgált esetekben a nyelvi minőség erősen összefüggött a hirdetések megbízhatóságával: a hét csalási kísérlet mindegyikében megjelent valamilyen gyanús nyelvhasználati jel (például: gépi fordításra utaló szerkezetek, szokatlan hibák), míg a legitim hirdetések egyikében sem tapasztaltak ilyen problémát. Bár a minta alapján a nyelvi minőség ígéretes indikátornak tűnik, fontos hangsúlyozni, hogy ez nem tekinthető önmagában tökéletes szűrőnek, hiszen előfordulhatnak kifogástalan nyelvezetű csaló vagy hibásan fogalmazó legitim eladók is. A nyelvi jelek ezért leginkább más gyanús mintázatokkal együtt értelmezhetők.

Az indokolatlan adatigény szintén markáns különbséget mutatott. A teljes mintában hét esetben (14,9%) kértek bankkártya-adatokat, amely a legitim tranzakciók 7,5%-át (3 eset), míg a csalási kísérletek 57,1%-át (4 eset) érintette. A legitim hirdetések körében ez a jelenség különösen figyelemre méltó, mivel a bankkártyaadatok „pénz fogadásához” történő bekérése a csalások egyik leggyakoribb módszere, és a kutatásban legitimként értékelt hirdetéseknél történő előfordulása egy új, eddig kevéssé vizsgált kockázati mintázatra utal. Mégpedig arra, hogy ha a vásárlók a legitim vásárlások során a piactereken hozzászoknak bankkártyaadatok

megadásához akkor, amikor az nem feltétlen szükséges, úgy kevésbé érzékenyen figyelnek majd ilyen, csalást potenciálsan jelző kérésekre.[2]

Sürgetést vagy nyomásgyakorlást egyetlen esetben sem tapasztaltak a próbavásárlók és távoli elérés telepítését sem kértek egyik esetben sem, egy esetben küldtek gyanús linket tartalmazó SMS-t, az egyik hamis webshophoz kapcsolódó csalási kísérlet kapcsán.

GYANÚS KOMMUNIKÁCIÓ		Total (N=47)		Legitim hirdetés (n=40)		Csalási kísérlet (n=7)	
		elem-szám	oszlop%	elem-szám	oszlop%	elem-szám	oszlop%
Milyen kommunikációs csatornát használtak a kapcsolatfelvételhez?	Platform chat	19	**40,4**	19	**47,5**	0	**0,0**
	Facebook Messenger	12	**25,5**	11	**27,5**	1	**14,3**
	E-mail	7	**14,9**	7	**17,5**	0	**0,0**
	Nem releváns	9	**19,1**	3	**7,5**	6	**85,7**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Javasolt-e az eladó csatornaváltást (off-platform)?	Igen	2	**4,3**	2	**5,0**	0	**0,0**
	Nem	36	**76,6**	35	**87,5**	1	**14,3**
	Nem releváns		**0,0**		**0,0**		**0,0**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Megfigyelhetők-e gyanús jelek a nyelvhasználatban (pl. gépi fordítás, sok hiba)?	Igen	7	**14,9**	0	**0,0**	7	**100,0**
	Nem	40	**85,1**	40	**100,0**	0	**0,0**
	Total	47	**47**	47	**47**	47	**47**
Kért-e a személyes adatokon felül a szükségesnél több adatot?	Bankkártya adatok	7	**14,9**	3	**7,5**	4	**57,1**
	Nem kért a szükségesnél több adatot	40	**85,1**	37	**92,5**	3	**42,9**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Kért-e bankkártyára vonatkozó adatot „pénz fogadásához”?	Igen	7	**14,9**	3	**7,5**	4	**57,1**
	Nem	40	**85,1**	37	**92,5**	3	**42,9**
	Total	47	**100,0**	40	**100,0**	7	**100,0**

6. táblázat: kommunikációs elemek a vételi próbavásárlások során

Együttesen a kommunikációs csatornák használata, a nyelvi minőség és az indokolatlan adatbekérés erős prediktív értékkel bírnak a gyanús tranzakciók azonosítására, míg a csatornaváltás ebben a mintában nem bizonyult jelentős megkülönböztető tényezőnek.

6.4.3 Fizetés és szállítás:

A vételi próbavásárlások során a hirdetések többféle fizetési opciót kínáltak, gyakran egyszerre több lehetőséget is. A teljes mintában (N=47) a leggyakrabban felajánlott fizetési mód a banki

2

átutalás volt (63,8%), ezt követte az utánvét (23,4%) és a bankkártyás fizetés (17,0%). A csalási kísérletként azonosított hirdetések esetében (n=7) ezzel szemben a bankkártyás fizetés dominált (71,4%), míg a legitim hirdetések között a banki átutalás volt a legjellemzőbb (72,5%).

A próbavásárlók tényleges választása is ezt a mintázatot követte: a teljes mintában a tranzakciók többsége banki átutalással történt (61,7%), azonban a csalási kísérletek esetében a bankkártyás fizetés vált leggyakoribbá (57,1%). Ez utóbbi arra utal, hogy a gyanús hirdetők aktívan próbálnak olyan fizetési módot ösztönözni, amely lehetőséget teremt az adathalászatra vagy illetéktelen tranzakciókra.

A rendelkezésre álló kevés adat alapján az IBAN-számok többsége magyar számlaszám volt (HU), azonban az IBAN-számok nem bizonyultak használható indikátornak a csalások azonosításában. Ennek elsődleges oka, hogy a csalási kísérletek túlnyomó részében bankkártyás fizetést ajánlottak fel és alkalmaztak (71% ajánlott, 57% ténylegesen választott fizetési mód), ezért az eladók bankszámlaszáma gyakran nem került megosztásra, így nem volt lehetőség az IBAN-adatok ellenőrzésére vagy összehasonlító elemzésére.

A kártyás fizetéseket vizsgálva komoly biztonsági hiányosság rajzolódott ki. A próbavásárlások során ugyanis egyik esetben sem történt kétfaktoros hitelesítés (3D Secure / SCA), sem a legitim, sem a csalási kísérletként azonosított tranzakcióknál. Ez azt jelenti, hogy a kártyás fizetések 100%-a olyan környezetben zajlott, ahol nem alkalmaztak erős ügyfélhitelesítést – jóllehet az európai PSD2 irányelv és az ahhoz kapcsolódó SCA-szabályozás (EU 2018/389) értelmében az online kártyás fizetések túlnyomó többségénél kötelező a kétfaktoros hitelesítés.

Mivel a csalási kísérletek jelentős része kártyaadatok megszerzésére vagy a fizetési folyamat manipulálására épült, a kétfaktoros hitelesítés teljes hiánya súlyos kockázati tényezőt jelent a fogyasztók számára. Ez a mintázat ráadásul egyformán jellemző volt a legitim és a gyanús hirdetések kapcsán lebonyolított fizetésekre is.

FIZETÉS ÉS SZÁLLÍTÁS		Total (N=47)		Legitim hirdetés (n=40)		Csalási kísérlet (n=7)	
		elem-szám	oszlop%	elem-szám	oszlop%	elem-szám	oszlop%
Milyen fizetési lehetőségeket ajánlott fel? (Többválasztós kérdés)	Banki átutalás	30	**63,8**	29	**72,5**	1	**14,3**
	Bankkártya	8	**17,0**	3	**7,5**	5	**71,4**
	E pénztárca (pl. Revolut/Wise)	2	**4,3**	2	**5,0**	0	**0,0**
	PayPal	1	**2,1**	1	**2,5**	0	**0,0**
	Platformos escrow (harmadik fél által kezelt fizetés)	1	**2,1**	1	**2,5**	0	**0,0**
	Utánvét	11	**23,4**	9	**22,5**	2	**28,6**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
	Banki átutalás	29	**61,7**	28	**70,0**	1	**14,3**

Milyen fizetési módot választottál?	Bankkártya	7	**14,9**	3	**7,5**	4	**57,1**
	E pénztárca (pl. Revolut/Wise)	2	**4,3**	2	**5,0**	0	**0,0**
	PayPal	1	**2,1**	1	**2,5**	0	**0,0**
	Utánvét	8	**17,0**	6	**15,0**	2	**28,6**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Melyik országhoz tartozik a feltüntetett IBAN-szám?	EU (nem HU)	1	**2,1**	0	**0,0**	1	**14,3**
	HU	32	**68,1**	31	**77,5**	1	**14,3**
	Nem releváns	14	**29,8**	9	**22,5**	5	**71,4**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Történt-e kétfaktoros hitelesítés vagy azonosítás kártyás fizetés esetén?	Nem	7	**14,9**	3	**7,5**	4	**57,1**
	Nem releváns	40	**85,1**	37	**92,5**	3	**42,9**
	Total	47	**100,0**	40	**100,0**	7	**100,0**

7. táblázat: fizetés és szállítás a vételi próbavásárlások során

A vizsgált hirdetésekben a leggyakrabban felkínált szállítási mód a csomagautomata volt (a hirdetések 51%-ában szerepelt). A csomagautomatás szállítási opció egyértelműen a legitim hirdetésekhez kötődött: a valós eladók 60%-a kínált ilyen lehetőséget, míg a csalási kísérletek egyikében sem szerepelt ez az opció. A csalási kísérletként azonosított hét eset mindegyikében a szállítási mód futárszolgálat volt, amely bár a legitim hirdetéseknél is megjelent (20%), arányaiban lényegesen gyakoribb volt a gyanús esetekben (100%). A személyes átvétel a legitim hirdetések kis részénél (2,5%) fordult elő, a csalási esetekben viszont egyáltalán nem.

Ez azt jelzi, hogy a szállítási opciók mintázata a mintában következetes különbséget mutat a legitim és a gyanús hirdetések között: a csomagautomata felajánlása inkább legitim, míg a kizárólag futáros megoldás fokozott óvatosságot indokolhat, ha más gyanús elemek is megjelentek. Hangsúlyozzuk, hogy a szállítási mód önmagában nem tekinthető bizonyító erejű tényezőnek, de kockázati indikátorként értelmezhető.

A fizetés során keletkező veszteség csak a csalási kísérleteknél fordult elő (n=6), ahol a kár értéke 8 000 Ft és 32 245 Ft között mozgott. A legitim hirdetések esetében minden tranzakció kármentes volt.

Együttesen a fizetési és szállítási mintázatok egyértelmű különbséget mutatnak:

- a legitim hirdetésekre a banki átutalás, magyar IBAN, csomagautomata és a kármentes tranzakciók jellemzők;
- míg a csalási kísérleteknél a bankkártyás fizetés preferálása, a kétfaktoros hitelesítés hiánya, a futárszolgálatra hivatkozás, valamint a pénzügyi veszteség magas aránya volt megfigyelhető.

SZÁLLÍTÁS		Total (N=47)		Legitim hirdetés (n=40)		Csalási kísérlet (n=7)	
		elem-szám	oszlop%	elem-szám	oszlop%	elem-szám	oszlop%
Kiszállítás során melyik szállítási opciót választottad?	Csomagautomata	24	**51,1**	24	**60,0**	0	**0,0**
	Futár	15	**31,9**	8	**20,0**	7	**100,0**
	Posta	7	**14,9**	7	**17,5**	0	**0,0**
	Személyes	1	**2,1**	1	**2,5**	0	**0,0**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Keletkezett-e kár vagy veszteség a fizetés során?	Igen, és nem történt visszatérítés	6	**12,8**	0	**0,0**	6	**85,7**
	Nem	41	**87,2**	40	**100,0**	1	**14,3**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
Ha keletkezett kár vagy veszteség a fizetés során, mi a mértéke (HUF)?	0 Ft	41	**87,2**	40	**100,0**	1	**14,3**
	8 000 Ft	1	**2,1**	0	**0,0**	1	**14,3**
	9 095 Ft	1	**2,1**	0	**0,0**	1	**14,3**
	9 800 Ft	1	**2,1**	0	**0,0**	1	**14,3**
	14 873 Ft	1	**2,1**	0	**0,0**	1	**14,3**
	17 318 Ft	1	**2,1**	0	**0,0**	1	**14,3**
	32 245 Ft	1	**2,1**	0	**0,0**	1	**14,3**
	Total	47	**100,0**	40	**100,0**	7	**100,0**

8. táblázat: szállítás a vételi próbavásárlások során

6.4.4 A vételi próbavásárlások kimenete, a csalások ismertetése

A 47 vételi próbavásárlás közül 7 esetben (15%) azonosítottunk nagy valószínűséggel vagy egyértelműen csalásnak minősíthető magatartást, egy esetben vegyes benyomások mentén semlegesnek minősítettük az interakciót és 39 esetben (83%) biztosan legitimnek értékeltük.

KIMENET ÉS MINŐSÍTÉS		Total (N=47)		Legitim hirdetés (n=40)		Csalási kísérlet (n=7)	
		elem-szám	oszlop%	elem-szám	oszlop%	elem-szám	oszlop%
Hogyan értékeled a vásárlás teljes folyamatát egy 1-5-ös skálán, ahol 1-es azt jelenti, hogy biztosan legitim, míg az 5-ös azt, hogy valószínűleg csalás / csalás történt!	1=Biztosan legitim	39	**83,0**	39	**97,5**	0	**0,0**
	2	0	**0,0**	0	**0,0**	0	**0,0**
	3=Vegyes/semleges	1	**2,1**	1	**2,5**	0	**0,0**
	4	0	**0,0**	0	**0,0**	0	**0,0**
	3=Vegyes/semleges	1	**2,1**	1	**2,5**	0	**0,0**
	Total	47	**100,0**	40	**100,0**	7	**100,0**
	Egyéb					1	**14,3**

A csalástipológiát figyelembe véve, milyen típusú csalásról van szó, és melyik kategóriába sorolnád?	Előre utalásos csalás					2	**28,6**
	Hamis webshop (brand/klón)					4	**57,1**
	Total					7	**100,0**
Próbavásárlás lezárása	Sikeres fizetés – nem kézbesített					5	**71,4**
	Sikeres vásárlás és kézbesítés, de nem a megrendelt termék					2	**28,6%**
	Total					7	**100,0**

9. táblázat: kimenet és minősítés a vételi próbavásárlások során

Saját szavaikkal így írták le röviden a csalásnak minősített eseteket a próbavásárlók:

- „Egyértelmű csalás, a weboldal szövegezése, a nagyon alacsony árak, mind árulkodó. Minimum vásárlási összeg. A weboldal minősége, a hatalmas akciók, a szövegezés, magyartalan megfogalmazás a weboldalon, gyanús fizetési felület."
- „Előreutalás után nem reagált, eltűnt. Nem küldte a dolgot. Nem is volt neki ilyen valószínűleg. Alacsony ár, nem valós képek, más számlaszámon szereplő név."
- „Megkaptuk a csomagot, de turis ruhák voltak benne. Megszűnt a webshop."
- „Gyanús linkes SMS érkezett. Gyanús a webshopban az ÁSZF és a leírások is."
- „Nem érkezett termék. Több pénzt emelt le."
- „Nincs róla hír, többet vont le a fizetésnél. Fizetésnél 3 tranzakció volt, 3. alkalommal vonta le és többet."
- „Kínai nyelvű könyvet küldtek."

A vételi próbavásárlások során feltárt csalási kísérletekhez kapcsolódóan a próbavásárlók jellemzően a következő figyelmeztető jeleket rögzítették:

- Stockfotók használata, hiányos vagy gyenge minőségű hirdetési tartalom, mint például gyanús nyelvhasználat (gépi fordítás, hibás mondatszerkezet)
- A piaci értéktől feltűnően eltérő árképzés
- Indokolatlan adatbekérés a kommunikáció során, például bankkártyaadatok
- Külső link megjelenése – főként hamis futár- vagy fizetési oldalakhoz kapcsolódva.
- Webshopok esetén gyanús domainek és az ÁSZF hiánya
- Fizetés során tapasztalt inkonzisztenciák (gyanús fizetési felület, nagyobb összeget emelnek le a kártyáról, mint ami a hirdetésben vagy webshopon szereplő ár, többszöri tranzakció egyetlen vásárlás során)

7 JAVASLATOK, MEGÁLLAPÍTÁSOK ÖSSZEFOGLALÁSA

A tanulmány átfogó képet nyújt az online csalások gyorsan változó és egyre összetettebb ökoszisztémájáról. A digitális térben zajló megtévesztések ma már nem elszigetelt jelenségek, hanem a pénzügyi stabilitást, a fogyasztói bizalmat és a platformok működőképességét érintő rendszerszintű kockázatot jelentenek. Az online átverések túlnyomó része továbbra is az emberi tényező kihasználásán alapul. Eközben a mesterséges intelligencia megjelenését is kihasználva a támadók technológiai eszköztára gyorsabban fejlődik, mint a védekezésre szolgáló társadalmi és intézményi mechanizmusok.

A vizsgálat eredményei alapján megállapítható, hogy Magyarországon az online csalások gyorsan változó és sokrétű fenyegetést jelentenek, amelyek a digitális szolgáltatásokba vetett bizalmat, a lakossági pénzügyi biztonságot és a platformok működésének integritását egyaránt érintik. A tanulmány korábbi fejezetei részletesen bemutatták az egyes csalástípusokat, valamint a hazai sajátosságokat.

A tanulmányban szereplő mystery visit-próbavásárlások primer kutatási eredményei fontos empirikus illusztrációt adnak arról, hogy az elméletben bemutatott csalástípusok hogyan jelennek meg a gyakorlatban.

7.1 A MAGYARORSZÁGI ONLINE CSALÁSOK JELLEMZŐI

A hazai felhasználókat érő online csalások túlnyomó része a megtévesztésre, a pszichológiai manipulációra és a bizalmi helyzetek kihasználására épül. Jellemző, hogy a támadók a banki, logisztikai és közszolgálati szervezetek, illetve nagy márkák nevében kommunikálnak, gyakran kifinomult nyelvi és vizuális eszközökkel. A banki adathalász kísérletek, a hamis csomagküldési értesítések, a közösségi platformokon megjelenő hamis támogatási üzenetek (például: a Meta Support névvel visszaélők) és a profilfeltörések az elmúlt évek legdominánsabb online csalási jelenségei közé tartoznak.

Az online piactereken tapasztalható visszaélések széles körben érintik a magyar felhasználókat. Ezek során a csalók gyakran professzionális kommunikációt folytatnak, majd a tranzakciót külső, hamisított oldalra terelik, ahol a bankkártyaadatok vagy bejelentkezési adatok megszerzése történik meg. A romantikus és bizalmi alapú csalások esetében a károsszegek kiemelkedően magasak, mivel az elkövetők hosszabb távú érzelmi manipulációt alkalmaznak.

7.2 A VÉDEKEZÉSI MECHANIZMUSOK AKTUÁLIS HELYZETE

A bankok és pénzügyi szolgáltatók Magyarországon fejlett technikai szűrőrendszereket alkalmaznak, köztük viselkedéselemzésen alapuló, mesterséges intelligenciával támogatott

csalásfelismerő eszközöket. Ugyanakkor ezek hatékonyságát korlátozza, hogy a megtévesztésen alapuló incidensek túlnyomó részét az áldozatok saját jóváhagyásukkal hajtják végre, így a technológiai védelem nem elegendő önmagában.

A platformüzemeltetők eltérő mértékű és változó megbízhatóságú csalásszűrést valósítanak meg. A vizsgált esetek alapján a gyanús hirdetések, hamis profilok és rosszindulatú linkek gyakran hosszabb ideig észrevétlenül aktívak maradnak. Az állami szervezetek (NKI, KiberPajzs) rendszeres figyelmeztetéseket és edukációs anyagokat tesznek közzé, ugyanakkor ezek nem jutnak el egységes mértékben minden társadalmi réteghez és gyakorlati haszonsulásuk is eltérő lehet társadalmi csoportonként.

7.3 A PRÓBAVÁSÁRLÁSI KUTATÁS TANULSÁGAI

A mystery visit-kutatás eredményei egyértelműen megerősítik, hogy a magyar online piactereken és közösségi felületeken megjelenő csalások szabályos mintázatokat követnek, és ezek a minták nagymértékben átfednek a tanulmány elméleti fejezeteiben bemutatott jelenségekkel.

7.3.1 Eladói oldal tapasztalatai

Az eladási próbavásárlások során a csalók gyorsan kapcsolatba léptek a hirdetővel, majd rövid időn belül egy külső, hamis futárszolgálati vagy fizetési oldalra irányították a kommunikációt. A hamis oldalak felépítése professzionálisnak tűnt, a csalók kommunikációja udvarias, angol nyelvű vagy gépi fordításon alapuló, de következetes volt. A módszerek jól megfeleltethetők a hazai adathalász és online apróhirdetési felületeken megjelenő csalástípusoknak.

7.3.2 Vevői oldal tapasztalatai

A hamis eladók jellemzően indokolatlanul kedvező áron kínálták a termékeket, sürgették a fizetést, vagy kizárólag előreutalást fogadtak volna el. Több esetben már a kommunikáció elején megjelentek gyanús jelek (eltérő név, külföldi telefonszám, bizonytalan termékleírás), amelyek megfelelnek a tanulmányban leírt tipikus, online apróhirdetési felületeken megjelenő csalási mintáknak. A próbavásárlások során több olyan eset is előfordult, amelyeket a platform szűrési rendszerei nem jelöltek gyanúsként.

A kutatás tehát empirikusan igazolta, hogy a platformok jelenlegi védelmi mechanizmusai nem minden esetben képesek időben felismerni a visszaéléseket, miközben a megtévesztési módszerek egységesek és gyorsan terjednek.

7.4 JAVASLATOK A HAZAI VÉDEKEZÉS ERŐSÍTÉSÉRE

1. **Egységes piactéri és közösségi platformszabályozás kialakítása:** Szükséges olyan minimumkövetelmények meghatározása, amelyek a hirdetések előzetes validációját, a külső linkek automatikus szűrését és a profilok hitelesítését hatékonyabbá teszik.

2. **A pénzügyi szektor és a digitális platformok együttműködésének bővítése:** Javasolt olyan integrált figyelmeztetési rendszer kialakítása, amely a felhasználók számára valós időben jeleníti meg a tranzakciókhoz kapcsolódó kockázatokat, beleértve a platformokon indított üzenetalapú interakciókat is.
3. **A lakossági edukáció megerősítése, célcsoportra optimalizált üzenetekkel, edukációval:** A magyar lakosság digitális biztonságtudatossága heterogén; az edukációs kampányokat célcsoportokra (idősek, fiatalok, alacsony jövedelmű felhasználók, kisvállalkozók) szabott formában kell folytatni.
4. **A próbavásárlási módszer rendszeres alkalmazása:** A mystery visit-kutatás eredményei alapján indokolt a vizsgálat rendszeres ismétlése, amely segítené a platformok valós biztonsági teljesítményének mérését és a csalási trendek korai azonosítását.

8 MELLÉKLET

8.1 FORRÁSJEGYZÉK

1. Alza (2022. június 2.) Ne dőlj be az internetes csalásoknak https://www.alza.hu/ne-dolj-be-az-internetes-csalasoknak
2. Alza (n.d.) Általános Szerződési Feltételek Fogyasztók részére https://www.alza.hu/altalanos-szerzodesi-feltetelek-fogyasztok-reszere
3. Árfigyelő (2025. november 11.) Napi termékadatok letöltése https://cdnarfigyeloprodweu.azureedge.net/excel/arfigyelo_napi_termekadatok.xlsx
4. Árukereső (n.d.-a) Megbízható Bolt – Miről szól a szolgáltatás? https://www.arukereso.hu/static/megbizhato_bolt_program.html
5. Banknavigátor (2025. február 19.) Az online piactereken elkövetett csalások és az új pénzügyi átverések trendjei (https://banknavigator.hu/az-online-piactereken-elkovetett-csalasok-es-az-uj-penzugyi-atveresek-trendjei/
6. BikeMag (2025. február 11.) Vigyázat csalás! - Hogyan szűrd ki a kamu webshopokat. https://bikemag.hu/magazin/vigyazat-csalas-hogyan-szurd-ki-a-kamu-webshopokat/
7. Blikk (2024. november 15. Önnél is próbálkoztak? Egy kínai hang hívogatja a magyarokat: rakja le azonnal! https://www.blikk.hu/aktualis/belfold/kinai-hang-hivas-csalas/fwdh2th
8. Blikk (2025. szeptember 22.) Figyelem! A Facebookon vadásznak a magyarokra a csalók. Blikk. https://www.blikk.hu/ferfiaknak/tech/meta-csalas-facebook-adatlopas/be31hwb
9. Bodnár, Zs. (2025. szeptember 21.) Feltörtek egy csomó magyar Facebook-profilt, de a bajt meg lehet előzni. Qubit. https://qubit.hu/2025/09/21/feltortek-egy-csomo-magyar-facebook-profilt-de-a-bajt-meg-lehet-elozni
10. Check Point. (2024). Global cyber attacks surge 44% as AI threats transform the security landscape. https://www.checkpoint.com
11. Digital Hungary (2025. június 19.). Az Árukereső új kampányt indít: a „vásárlás istennőjével” segít a magyaroknak a döntéshozatalban https://www.digitalhungary.hu/marketing/Az-arukereso-uj-kampanyt-indit-a-vasarlas-istennojevel-segit-a-magyaroknak-a-donteshozatalban/28294/
12. Digital Hungary (2025. október 8.) Túl szép, hogy igaz legyen? Így ismerjük fel a hamis vásárlói értékeléseket https://www.digitalhungary.hu/gazdasag/Tul-szep-hogy-igaz-legyen-igy-ismerjuk-fel-a-hamis-vasarloi-ertekeleseket-tippek-az-arukereso-hu-tol/29391/
13. Dívány.hu (2024. február 24.) Évente magyarok tízezreit verik át: így ismerheted fel a módszereiket, hogy ne bukjad mindenedet https://divany.hu/eletem/csalas-online/
14. Economx (2024. november 19.). Novemberben sem pihennek a csalók, ezek az aktuális átverések https://www.economx.hu/tech/blackfriday-csalas-nmhh-webaruhaz-onlinefizetes.799822.html
15. Economx (2025. november 8.) Litván védelem alatt a magyar Revolut-betétek. https://www.economx.hu/gazdasag/litvan-vedelem-alatt-a-magyar-revolut-betetek-de-meddig-birja-vilnius.818558.html

16. eMAG (n.d) Általános felhasználási feltételek https://www.emag.hu/help/altalanos-felhasznalasi-feltetelek/
17. Erste Bank (2025. június 26.) Tovább bővíti csalásmegelőzési arzenálját az Erste. https://www.erstebank.hu/hu/sajto/sajtokozlemenyek/2025/06/26/tovabb-boviti-csalasmegelozesi-arzenaljat-az-erste
18. Erste Bank (n.d.) Őrszem a pénzügyeidhez https://www.erstebank.hu/hu/ebh-nyito/mindennapi-penzugyek/elektronikus-szolgaltatasok/orszem
19. ESET (2025. május 28.) A csaló telefonhívásokon és a nem létező gázszámlákon túl – 7 módszer, amivel ellophatják az adatainkat az interneten https://www.eset.com/hu/hirek/7-modszer-amivel-ellophatjak-az-adatainkat-az-interneten-2025/
20. European Comission (2025. február 2.) Commission gathers key European enforcement network and stakeholders to fight online consumer fraud https://commission.europa.eu/news-and-media/news/commission-gathers-key-european-enforcement-network-and-stakeholders-fight-online-consumer-fraud-2025-02-21_en
21. Eurostat. (2024a). Problems encountered when shopping online (isoc_ec_iprb21). Luxembourg: Eurostat Database. https://ec.europa.eu/eurostat/databrowser/view/isoc_ec_iprb21/default/table?lang=en
22. Eurostat. (2024b). Individuals' level of digital skills and safety by age (isoc_sk_dskl_i21). Eurostat Database. https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i/default/table?lang=en&category=isoc.isoc_sk.isoc_sk_h
23. Exonomix (2024. február 14.) „Tom vagyok, szeretnélek feleségül venni, küldjél pénzt!" - vaksi a szerelem https://www.economx.hu/gazdasag/valentin-online-csalok-atveres-tarskereso-kozosegi-media-brfk-rendorseg-nyomozas.785202.html
24. Facebook (2024. december 10.) Meta Launches Global Anti-Scam Awareness Campaign Ahead Of The Holiday Season https://about.fb.com/news/2024/12/meta-launches-global-anti-scam-awareness-campaign-ahead-of-the-holiday-season/
25. Facebook (2025. augusztus) EU Digital Services Act: Systemic Risk Assessment Results Reports. https://transparency.meta.com/reports/regulatory-transparency-reports/
26. Facebook (2025. január 7.) More Speech and Fewer Mistakes (https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/
27. Facebook (n.d.-a) Védekezés a csalásokkal szemben a Facebookon https://www.facebook.com/help/1674717642789671?locale=hu_HU
28. Fedorko, R., & Kráľ, Š. (2021). Online shopping problems in the context of B2C e-commerce in the Visegrad Four countries. In F. J. Martínez-López & D. López López (Szerk.), Digital Marketing and E-commerce Conference Proceedings (83–94. o.). Springer. https://doi.org/10.1007/978-3-030-76520-0_9
29. Finteczone (2024. május 30.) KiberPajzs: új banki kommunikációs protokoll az online pénzügyi visszaélések kezelésére https://fintechzone.hu/kiberpajzs-uj-banki-kommunikacios-protokoll-az-online-penzugyi-visszaelesek-kezelesere/

30. Galéria Savaria (n.d.-b) Gyakran Ismételt Kérdések https://galeriasavaria.hu/sugokozpont/gyakran-ismetelt-kerdesek/l22/
31. Galéria Savaria (n.d.-a) Általános Felhasználási Feltételek https://galeriasavaria.hu/altalanos-felhasznalasi-feltetelek/
32. GVH (2023. augusztus 5.) Csalókra figyelmeztet a GVH. https://www.gvh.hu/sajtoszoba/sajtokozlemenyek/2023-as-sajtokozlemenyek/csalokra-figyelmeztet-a-gvh
33. GVH (2023. július 19.) A GVH az árfeltüntetési szabályok betartatásával is védi a magyar embereket. https://www.gvh.hu/sajtoszoba/sajtokozlemenyek/2023-as-sajtokozlemenyek/a-gvh-az-arfeltuntetesi-szabalyok-betartatasaval-is-vedi-a-magyar-embereket
34. GVH (2025. január 24.) Az online Árfigyelő bővítése újabb segítség a magyar családoknak. https://www.gvh.hu/sajtoszoba/sajtokozlemenyek/2025-os-sajtokozlemenyek/gvh-az-online-arfigyelo-bovitese-ujabb-segitseg-a-magyar-csaladoknak
35. GVH (n.d.-a). Árfigyelő. https://www.gvh.hu/arfigyelo
36. HunCERT (2024) Megnövekedett a magyar nyelvű online csalások száma https://cert.hu/biztonsagi-szemle/2024-10-31/megnovekedett-a-magyar-nyelvu-online-csalasok-szama
37. HVG (2023. január 30.) Ötvenmilliós bírságot kapott az eMAG https://hvg.hu/gazdasag/20230130_Otvenmillios_birsagot_kapott_az_eMag
38. HVG (2023. július 22.) Újfajta csalás terjed a Facebookon, a bankszámlája bánja annak, aki benézi. https://hvg.hu/tudomany/20230722_bluevoyant_jelentes_kiberbiztonsag_kozossegi_mediaban_terjedo_csalasok
39. HVG (2024. december 23.) „Figyelmeztetés a Meta AI-tól” – veszélyes vírus terjed Messengeren, bele ne kattintson, ellopja a Facebookon mindenét. https://hvg.hu/tudomany/20241223_figyelmeztetes-a-meta-ai-tol-facebook-messenger-uzenet-kartekony-program-virus-adatlopas-ebx
40. HVG. (2025. május 23.) Elindult a hullám, veszélyes e-mail és SMS terjed Magyarországon https://hvg.hu/tudomany/20230523_kamu_email_sms_futarszolgalatok_atveres_adathalasz_levelek_banki_adatok_bankkartyaadatok_csalok
41. Impetus Research (2024) Digitális piacok szabályozásának ismerete a lakosság körében. https://onlineplatformok.hu/cikk/digitalis-piacok-szabalyozasanak-ismerete-a-lakossag-koreben
42. Index (2023. augusztus 5.) Csalókra figyelmeztet a GVH az árfigyelő miatt https://index.hu/gazdasag/2023/08/05/gvh-arfigyelo-figyelmeztetes-applikacio-internetes-csalas/
43. Index (2025. június 4.) Az MNB öt csapása: az első kárt állja a bank, a többi a gondatlan ügyfél terhe https://index.hu/gazdasag/2025/06/04/mnb-kibercsalas-veszteseg-csalok-kibercsalok-first-loss-megtevesztes-bank-kartersites-bankkartya-csalas/

44. Index (2025. június 6.) A látszat már nem csak néha csal, a csalók pedig szinte sosem látszanak https://index.hu/techtud/2025/06/06/ai-mesterseges-intelligencia-buncselekmeny-deep-fake-ugyved-kiberbiztonsag-rendorseg-csalas/
45. Index (2025a, február 24.). Azt hisszük, nem tudnak átverni a kibercsalók, pedig… https://index.hu/gazdasag/2025/02/24/kiberbiztonsag-csalas-mnb-visszaeles/
46. Infostart (2025. június 10.) Már az egyik legismertebb magyar webáruház sem szent a csalóknak https://infostart.hu/bunugyek/2025/06/10/mar-az-egyik-legismertebb-magyar-webaruhaz-sem-szent-a-csaloknak
47. Instagram (n.d.) Visszaélések, kéretlen tartalmak és csalások https://help.instagram.com/165828726894770/?helpref=hc_fnav
48. Jófogás (2025. november 24.) Itt a Jófogás vevővédelem – biztonságos adásvétel, egyszerűen https://blog.jofogas.hu/itt-a-jofogas-vevovedelem-ami-biztonsagossa-teszi-az-adasvetelt/
49. Jogtár (2024) 6/2024. VII. 7. NMHH rendelet az online platform szolgáltatók adatszolgáltatási kötelezettségéről https://net.jogtar.hu/jogszabaly?docid=a2400006.nmh
50. Kanizsa Médiaház. (2024) Online csalások: naponta 72 millió forintot visznek el a kiberbűnözők. https://kanizsamediahaz.hu/hir/202412/online-csalasok-naponta-mar-72-millio-forintot-visznek-el-itthon-a-kiberbunozok
51. KiberPajzs (2025a). A kiberbűnözés kora 2025 – összefoglaló jelentés. Budapest: Magyar Nemzeti Bank és Mastercard. https://kiberpajzs.hu/letoltes/a-kiberbu-no-ze-s-kora-2025-o-sszefoglalo-kiberpajzs-0220fin-mnb.pdf
52. Kiberpajzs (2025b. május 16.) Romantikus csalás: magyar volt az amerikai katona https://kiberpajzs.hu/hirek/romantikus-csalas-magyar-volt-az-amerikai-katona-tippek-es-tanacsok
53. KiberPajzs (2025c) Bárkivel megtörténhet ez 3+3 durva kibercsalás – tippek és tanácsok. https://kiberpajzs.hu/hirek/barkivel-megtortenhet-ez-3-3-durva-kibercsalas-tippek-es-tanacsok
54. Kreatív Online (2023. augusztus 8.) Facebookos átverés: Decathlonos hátizsák 949 forintért – így működnek a hamis nyereményjátékok. https://kreativ.hu/cikk/online-csalas-decathlon-atveres
55. Kreatív Online (2025a. augusztus 6.) Az online csalók a bizalomra és az érzésekre lőnek, de a márkák is sérülnek – 1. rész. Kreatív Online. https://kreativ.hu/cikk/online-csalas-decathlon-atveres
56. Kreatív Online (2025b. augusztus 7.) Az online csalók a bizalomra és az érzésekre lőnek – 2. rész. Kreatív Online. https://kreativ.hu/cikk/online-csalas-decathlon-atveres-2-resz
57. Lakshmanan, R. (2024. november 21.) NodeStealer malware targets Facebook ad accounts, harvesting credit card data. The Hacker News https://thehackernews.com/2024/11/nodestealer-malware-targets-facebook-ad.html
58. Magyar Nemzeti Bank (MNB) (2024. október 17.) Revolut-ügy: másfél millió magyar ügyfél megérdemelne egy hazai bankot. https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2024-evi-

sajtokozlemenyek/revolut-ugy-masfel-millio-magyar-ugyfel-megerdemelne-egy-hazai-bankot

59. Magyar Nemzeti Bank (MNB) (2025a). Pénzforgalmi visszaélések statisztikája, 2024. https://statisztika.mnb.hu/idosor-4619
60. Magyar Nemzeti Bank (MNB) (2025b). Fizetési Rendszer Jelentés 2025. https://www.mnb.hu/kiadvanyok/jelentesek/fizetesi-rendszer-jelentes/fizetesi-rendszer-jelentes-2025
61. Magyar Nemzeti Bank (MNB) (2025c) Az adathalász csalások legjellemzőbb típusai. Budapest: MNB – Digitális biztonság. https://www.mnb.hu/fogyasztovedelem/digitalis-biztonsag/az-adathalasz-csalasok-legjellemzobb-tipusai
62. Magyar Nemzeti Bank (MNB) (2025d. március 6.) Hamis MNB ügyfél-elégedettségi kérdőívvel támadnak a kibercsalók. https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2025-evi-sajtokozlemenyek/hamis-mnb-ugyfel-elegedettsegi-kerdoivvel-tamadnak-a-kibercsalok
63. Magyar Nemzeti Bank (MNB) (2025e. szeptember 17.) Csalók élnek vissza a KiberPajzs és egy élelmiszeráruház-lánc nevével. https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2025-evi-sajtokozlemenyek/csalok-elnek-vissza-a-kiberpajzs-es-egy-elelmiszeraruhaz-lanc-nevevel
64. Magyar Nemzeti Bank (MNB) (2025f. július 1.) Mesterséges intelligenciát vet be a jegybank a pénzügyi kibercsalások visszaszorításáért https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2025-evi-sajtokozlemenyek/mesterseges-intelligenciat-vet-be-a-jegybank-a-penzugyi-kibercsalasok-visszaszoritasaert
65. Mai Világ (2019. május 27.). Ár-összehasonlító oldalak - Vigyázat! Kész átverés! https://maivilag.com/ar-osszehasonlito-oldalak-vigyazat-kesz-atveres/
66. Mastercard (2025) A kiberbűnözés kora 2025 https://www.mastercard.hu/content/dam/public/mastercardcom/eu/hu/pdfs/A_kiberbunozes_kora_2025.pdf
67. MBH Bank (2025. szeptember 30.) Az MBH Bank és az ORFK együttműködést kötött a digitális csalások elleni fellépés érdekében https://www.mbhbank.hu/sajtoszoba/20250930_2
68. MBH Bank (n.d.) Csalásmegelőzés https://www.mbhbank.hu/csalasmegelozes
69. Nemzeti Kibervédelmi Intézet (NKI, 2025. szeptember) Miért lépnek túl a támadók az e-mail alapú adathalász támadásokon? https://nki.gov.hu/it-biztonsag/hirek/miert-lepnek-tul-a-tamadok-az-e-mail-alapu-adathalasz-tamadasokon/
70. Nemzeti Kibervédelmi Intézet NKI. (2020. április 2.) Tájékoztatás un. „Wangiri” telefonhívások kapcsán https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-un-wangiri-telefonhivasok-kapcsan/
71. Nemzeti Kibervédelmi Intézet.(n.d.) Szolgáltatások https://nki.gov.hu/intezet/feladataink/

72. Nemzeti Média- és Hírközlési Hatóság (NMHH) (2025. április 30.) Az Internet Hotline szolgálatról. https://nmhh.hu/cikk/190105/Az_Internet_Hotline_szolgalatrol
73. Origo (2025. március 23.) Vigyázat! Csalók állhatnak a külföldi számokról érkezett hívások mögött https://www.origo.hu/techbazis/2025/03/csalok-kulfoldi-hivasok-44
74. OTP Bank (n.d.) Adathalász csalások és visszaélések formái https://www.otpbank.hu/portal/hu/adathalaszat
75. Pénzcentrum (2024. november 11.) Te is szoktál online vásárolni? Nagyon vigyázz, mostanában így trükköznek a csalók https://www.penzcentrum.hu/tech/20241111/te-is-szoktal-online-vasarolni-nagyon-vigyazz-mostanaban-igy-trukkoznek-a-csalok-1159078
76. Police.hu (2024. május 7.) Online hazudott szerelem. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/online-hazudott-szerelem
77. Police.hu (2025. november 7.) Újabb romantikus csaló. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/ujabb-romantikus-csalo
78. Portfolio (2025. november 6.) Szép csendben megszerezte a Revolut a magyar engedélyt: jöhet a fióktelep! https://www.portfolio.hu/bank/20251106/szep-csendben-megszerezte-a-revolut-a-magyar-engedelyt-johet-a-fioktelep-797854
79. Reuters (2025. november 6.) Meta is earning a fortune on a deluge of fraudulent ads, documents show. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/
80. Revolut (n.d.) Need a hand? https://help.revolut.com
81. Shoprenter (2024. augusztus 23.) Árukereső Megbízható Bolt beállítása https://support.shoprenter.hu/hc/hu/articles/360021631054-Árukereső-Megbízható-Bolt-beállítása
82. Solymos, Á. (2025). Internetes pénzügyi csalások és a biztonságtudatosítás fejlődése Magyarországon. Gazdaság és Pénzügy, 123, 447–478. https://doi.org/10.33926/GP.2025.3.6
83. TikTok. (2025. október 10.) Community Guidelines Enforcement Report. https://www.tiktok.com/transparency/en/community-guidelines-enforcement-2025-2
84. Trade magazin (2024. december 6.) Átverések a netes vásárlások világában: tanulságos eset a Kockabolygóról és Kockavárosról https://trademagazin.hu/hu/atveresek-a-netes-vasarlasok-vilagaban-tanulsagos-eset-a-kockabolygorol-es-kockavarosrol/
85. Tudás.hu. (2024. június 15.) A kiberbűnözők a közösségi oldalakról felépítik a profilunkat és személyes üzenetet küldenek. https://tudas.hu/a-kiberbunozok-a-kozossegi-oldalakrol-felepitik-a-profilunkat-es-szemelyes-uzenetet-kuldenek/
86. Two Story Media. 2024, október 24. How hackers hijacked my client's Meta Ads. https://twostorymedia.com/9511-2/
87. Válasz Online. (2025. július 11.) MBH, Mészáros Lőrinc és a kriptocsalás: újabb kiberbűnöző hálózat lepleződött le. https://www.valaszonline.hu/2025/07/11/mbh-meszaros-lorinc-kibercsalas-mnb-bunozo-karterites/

88. Vatera (2023. november 15.) Vásárlói tippek Vatera Black Friday-re! https://blog.vatera.hu/2023/11/15/vasarloi-tippek-vatera-black-friday-re/
89. Vatera (2025. július 3.) Vásárolj biztonságban – bemutatkozik a Vatera Vevővédelem https://blog.vatera.hu/2025/07/03/vasarolj-biztonsagban-bemutatkozik-a-vatera-vevovedelem/
90. Vinted (n.d.-a) Hogyan kerüld el, és hogyan jelentsd az adathalász üzeneteket és a csalásokat? https://www.vinted.hu/help/628-az-atvero-es-adathalasz-uzenetek-felismerese
91. Vinted (n.d.-b) Vevővédelem https://www.vinted.hu/help/15/550-vevovedelem?access_channel=hc_topics
92. WhatsApp (2024. február 12.) Hogyan védekezz a gyanús üzenetek és átverések ellen? https://faq.whatsapp.com/573786218075805
93. WhatsApp (n.d.) Biztonságra tervezve https://www.whatsapp.com/security

8.2 PRÓBAVÁSÁRLÁSI KÉRDŐÍVEK

ELADÁS KÉRDŐÍV

A. Adminisztráció

A1. Próbavásárló azonosító

A2. Próbavásárlás dátuma (első kapcsolatfelvétel időpontja)

A3. Próbavásárlás lezárásának dátum

A4. Első gyanús kontakt dátum-idő

B. Platform

B1. Csatornakategória

1. Piactér (Jófogás/Vatera/Facebook Marketplace)
2. Webshop
3. Közösségi hirdetés

B2. Konkrét platform

1. Jófogás
2. Vatera
3. Facebook Marketplace
4. Egyéb (Meska, stb.)

C. Termék jellemzők

C1. Termék típus

1. Fizikai termék
2. Digitális termék
3. Szolgáltatás

C2. Kategória

1. Elektronika
2. Ruházat
3. Bútor
4. Dekoráció
5. Szépség/egészség
6. Egyéb

C3. Meghirdetett ár (Huf)

D. Érdeklődő/vevő fiók jellemzők

D1. Vevő megjelenített neve

D2. Fiók életkora

1. ≤30 nap
2. 1–6 hó
3. =>6 hó
4. Nem ismert

D3. Értékelés átlaga – ha van
D4. Értékelések száma – ha van
D5. Hitelesítési jelvény (igen, nem, nem ismert)
D6. Megadott hely/település
D7. Nyelvi minőség gyanús? (gépi fordítás, sok hiba) (igen, nem)

E. Kommunikáció és gyanús jelek

E1. Kapcsolatfelvétel módja [1=Platform chat, 2=Facebook Messenger, 3=WhatsApp, 4=E-mail, 5=SMS, 6=Telefon, 7=Telegram, 99=Egyéb

E2. Javasolt-e a vásárló csatornaváltást (off-platform)
E3. Nyelvhasználat gyanús (gépi fordítás, sok hiba)?
E4. Sürgetés/nyomásgyakorlás érződött?
E5. Kért-e személyes adatot a szükségesnél többet? [1=Szem. igazolvány, 2=Lakcímkártya, 3=Bankkártya adatok, 4=2 faktoros azonosítás kódja, 5=Banki belépés/jelszó, 6=TAJ/Adóazonosító, 99=Egyéb]
E7. Kért-e távoli elérés telepítését?

E7a. Melyik? 1=Anydesk, 2=Teamviewer, 3=egyéb

E8. Küldött-e fájlt/bizonylatot „fizetésről”? (igen, nem)

E8a. Bizonylat típusa [1=Banki átutalási képernyőkép, 2=PayPal/Stripe visszaigazolás, 3=E-pénztárca (Revolut/Wise), 99=Egyéb]

E8b. Ellenőrizhető tranzakció a számlán? [0=Nem, 1=Igen, 2=Folyamatban]

F. Külső linkek / „futár” / „pénz fogadása” trükkök

F1. Küldött-e külső linket? [0=Nem, 1=Igen]

F1a. Link rövidített? [0=Nem, 1=Igen]

F1b. Link domainje

F1c. Oldal típusa / célja [1=„Pénz fogadása” oldal (kártyaadat kérés), 2=Fizetési oldal, 3=Futárszolgáltatás, 4=Személyazonosítás, 99=Egyéb]

F1d. Melyik „futár” szerepel? [1=GLS, 2=Packeta, 3=DHL, 4=MPL/posta, 5=Foxpost, 99=Egyéb]

F1e. Kért-e bankkártyaadatot „pénz fogadásához”? [0=Nem, 1=Igen]

F2. Domain (pl. .hu/.shop)

F3. (Ha ismert) Domain életkora [1=≤90 nap, 2=91–365 nap, 3=>1 év, 9=Nem ismert]

G. Kimenet/megerősítés

G1. Összbenyomás az érdeklődőről [1=Biztosan legitim, 2=Valószínűleg legitim, 3=Vegyes/semleges, 4=Erős gyanú csalásra, 5=Valószínű csalás / kísérlet]

G2. Feltételezett csalástípus [1=Hamis futár/fizetési oldal, 2=Kártyaadat kérése pénz fogadásához, 3=Off-platform csatornaváltás link használatával, 4=Túlfizetés/refund trükk, 5=Hamis fizetési bizonylat, 6=Személyes adathalászat/KYC, 7=Távoli elérés (tech support), 99=Egyéb]

G3. Döntést alátámasztó fő bizonyítékok (max. 3) [1=Külső link, 2=Kártyaadat kérése, 3=Csatornaváltás kérése, 4=Sürgetés, 5=Hamis bizonylat, 6=Irreális előrefizetési igény, 7=Friss domain (E3=1), 8=Gépi fordítás/hibás nyelv]

G4. Jelentetted-e a platformnak? [0=Nem, 1=Igen]

G4a. Platform reakciója [1=Eltávolítva/letiltva, 2=Nincs intézkedés, 3=Folyamatban, 9=N/A]

G5. Megjegyzés / rövid narratíva

H. Biztonsági események (eladó oldali)

H1. Kattintottál-e a külső linkre? [0=Nem, 1=Igen]

H2. Adtál-e meg kártyaadatot „pénz fogadásához”? [0=Nem, 1=Igen]

H3. Megosztottál-e 2 faktoros azonosítási kódot? [0=Nem, 1=Igen]

H4. Telepítettél-e távoli elérés appot? [0=Nem, 1=Igen]

H5. Történt-e kár / jogosulatlan terhelés? (HUF)) [0, ha nincs]

H6. Intézkedések [1=Kártya letiltása, 2=Jelszócsere, 3=2 faktoros azonosítás bekapcsolása, 4=Eszköz ellenőrzés, 5=Bank értesítése, 6=Platform jelentés, 99=Egyéb]

I. Bizonyítékok

I1. **Csatolmányok** [1=Chat export/képernyőkép, 2=Külső oldal képernyőkép/HTML, 3=Fizetési „bizonylat”, 4=URL-lista, 5=Hirdetés screenshot, 6=Videó, 99=Egyéb]

VÉTEL KÉRDŐÍV

I. Adminisztráció

A1. Próbavásárló azonosító

A2. Próbavásárlás dátuma (első kapcsolatfelvétel időpontja)

A3. Próbavásárlás lezárásának dátuma

J. Platform

B1. Csatornakategória

4. Piactér (Jófogás/Vatera/Facebook Marketplace)
5. Webshop
6. Közösségi hirdetés
7. Google Search Ads

B2. Konkrét platform

5. Jófogás
6. Vatera
7. Facebook Marketplace
8. Google Search Ads
9. Egyéb (Meska, stb.)

B3. Hogyan találtad?

1. Platformon belüli keresés
2. Külső keresés (Google)
3. Fizetett hirdetés

4. Ajánlás
5. Egyéb

K. Termék jellemzők

C1. Termék típus

4. Fizikai termék
5. Digitális termék
6. Szolgáltatás

C2. Kategória

7. Elektronika
8. Ruházat
9. Bútor
10. Dekoráció
11. Szépség/egészség
12. Egyéb

C3. Meghirdetett ár (Huf)

C4. Piaci reális ár becslése (Huf)

C5 Ár-eltérés (%)

C6. Leírás minősége (L1–5) [1=Nagyon gyenge … 5=Nagyon részletes]

C7. Képek száma

C8. Képek minősége (stock fotó)

C10. Webshopnál „Impresszum”/cégadatok megvannak?

1. igen
2. nem
3. nem releváns

C11. Webshopnál ÁSZF van?

C12. Domain

L. Eladó/fiók jellemzők (marketplace esetén)

D1. Eladó megjelenített neve

D2. Fiók életkora

5. ≤30 nap
6. 1–6 hó
7. =>6 hó

8. Nem ismert

D3. Értékelés átlaga – ha van
D4. Értékelések száma – ha van
D5. Hitelesítési jelvény (igen, nem, nem ismert)
D6. Megadott hely/település
D7. Válaszidő (perc) első üzenetre

M. Kommunikáció és gyanús jelek

E1. Kommunikációs csatornák [1=Platform chat, 2=Facebook Messenger, 3=WhatsApp, 4=E-mail, 5=SMS, 6=Telefon, 7=Telegram, 99=Egyéb

E2. Javasolt-e az eladó csatornaváltást (off-platform)
E3. Nyelvhasználat gyanús (gépi fordítás, sok hiba)? Igen, nem
E4. Sürgetés/nyomásgyakorlás érződött? Igen, nem
E5. Kért-e személyes adatot a szükségesnél többet? [1=Szem. igazolvány, 2=Lakcímkártya, 3=Bankkártya adatok, 4=2 faktoros azonosításhoz kód, 5=Banki belépés/jelszó, 6=TAJ/Adóazonosító, 99=Egyéb]
E7. Kért-e távoli elérés telepítését?
E8. Küldött-e külső fizetési/kiszállítási linket
E8a. Link rövidített (bit.ly stb.)?
E8b. Link domainje
E8c. Oldal célja (S) [1=Fizetés, 2=„Pénz fogadása”, 3=Futárszolgáltatás, 4=Személyes adategyeztetés, 99=Egyéb]
E8d. Kért-e bankkártya adatot „pénz fogadásához”?

E9. „Futár” említés / link [1=GLS, 2=Packeta, 3=DHL, 4=MPL/posta, 5=Foxpost, 99=Egyéb]

N. Fizetés és szállítás

F1. Felkínált fizetési módok [1=Platformos escrow (harmadik fél által kezelt fizetés), 2=Utánvét, 3=Banki átutalás, 4=Bankkártya, 6=E-pénztárca (pl. Revolut/Wise), 7=PayPal, 8=Kripto, 9=Ajándékkártya/kupon, 99=Egyéb]

F2. Választott fizetési mód

F3. Kedvezményezett neve (részlegesen rejtve)

F4. IBAN országa [1=HU, 2=EU (nem HU), 3=Nem EU, 9=Nem releváns]

F5. Kedvezményezett név ≈ eladó neve? (S) [0=Nem, 1=Igen, 2=Nem ismert]

F6. 2 faktoros azonosítás történt kártyás fizetésnél? [0=Nem, 1=Igen, 2=Nem releváns]

F7. Szállítási opció [1=Személyes, 2=Futár, 3=Csomagautomata, 4=Posta]

F8. „Futár" linkje valósnak tűnt? (S) [0=Nem, 1=Igen, 2=Nem tudom]

F9. Tranzakció státusza (S)
[1=Sikeres vásárlás és kézbesítés, 2=Sikeres fizetés – nem kézbesített, 3=Fizetés elutasítva/megszakítva, 4=Nem jutott el fizetésig]

F10. Kár/veszteség (HUF) [0, ha nincs]

F11. Megtörtént-e visszatérítés? (S) [0=Nem, 1=Igen, 2=Folyamatban, 9=Nem releváns]

O. Kimenet/minősítés

G1. Összbenyomás [1=Biztosan legitim, 2=Valószínűleg legitim, 3=Vegyes/semleges, 4=Erős gyanú csalásra, 5=Valószínű csalás / csalás történt]

G2. Csalástipológia
[1=Előre utalásos csalás, 2=Hamis futár/fizetési oldal, 3=Ál-escrow/PayPal/Stripe oldalak, 4=Túlfizetés / hamis utalási bizonylat, 5=Hamis webshop (brand/klón), 6=Jegy/booking csalás, 7=Adathalászat, 9=Távoli elérés/„support" csalás, 99=Egyéb]

G4. Jelentetted-e a platformnak? [0=Nem, 1=Igen]
G4a. Platform reakciója [1=Eltávolítva/letiltva, 2=Nincs intézkedés, 3=Folyamatban, 9=N/A]

G5. Megjegyzés/narratíva röviden

P. Biztonsági események

H1. Kattintottál-e gyanús linkre?

H2. Bármilyen csalásra utaló jellel találkoztál-e?

Q. Bizonyítékok

I1. Csatolmány típusa [1=Hirdetés képernyőkép, 2=Chat export, 3=Fizetési oldal képernyőkép/HTML, 4=E-mail, 5=URL-lista, 6=Videó, 99=Egyéb]

I2. Csatolmány