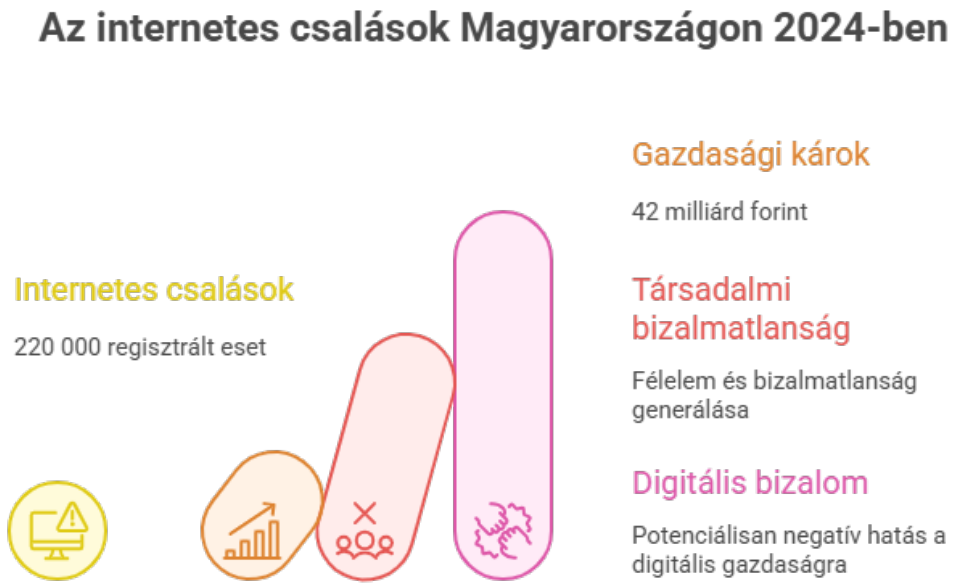
Online csalások és átverések világa: veszélyek, típusok és védekezési lehetőségek a digitális térben

Kiberbűnözés és az online átverések gazdasági jelentősége, terhei

A kiberbűnözés mára jelentős makrogazdasági kockázattá vált: 2024-ben globálisan mintegy 9500 milliárd USD kárt okozhatott, amely 2028-ra 14 000 milliárd USD fölé emelkedhet. A támadások fő célpontja a pénzügyi szektor, az online kereskedelem és az adatkezeléssel foglalkozó szolgáltatók.



(adatok: KiberPajzs, 2025)

Magyarországon 2024-ben több mint 220 000 internetes csalást regisztráltak, közel 42 milliárd forintos kárértékkel. Ez nem csupán gazdasági, hanem társadalmi probléma is. A lakosság kevesebb mint egynegyede érzi magát felkészültnek a csalások felismerésére és ez bizonytalanságot generál, ami már a digitális gazdaság iránti bizalomra is negatívan hat. Az MNB fizetési rendszerről szóló jelentése a pénzforgalmi visszaélések 36%-os éves növekedését jelezte 2024-re.

A magyar tapasztalatok az online vásárlások során előforduló problémákkal, csalásokkal hasonlóak az Eurostat adatai alapján más európai országokhoz. Az online vásárlók harmada tapasztal problémát.

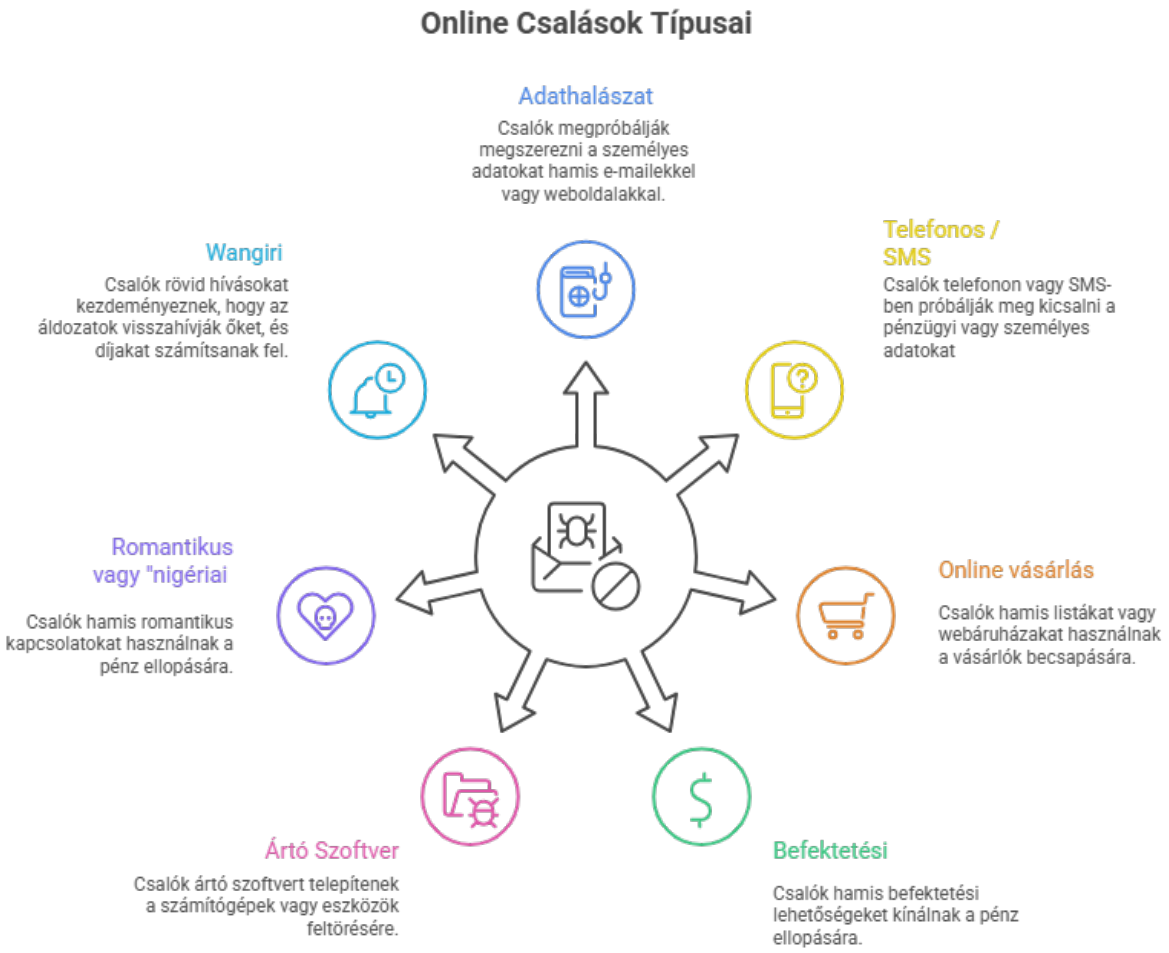
A lakosság digitális készségei a digitális csalások felismerésére hiányosak: a felnőtt magyarok kevesebb, mint egynegyede érzi magát képesnek felismerni és elkerülni az online csalásokat.

A 16-74 évesek 59%-a rendelkezik legalább alapvető digitális készségekkel, de 25%-uk még alapvető biztonsági ismeretekkel sem. Ez a réteg különösen sérülékeny az online átverésekkel szemben.

A KiberPajzs program az MNB, a rendőrség, az NKI és a Bankszövetség együttműködésével próbálja növelni a tudatosságot, több mint egymillió embert elérve, ám a csalások számának növekedése jelzi, hogy az oktatás és a technikai védelem még nem elégséges. A kiberbűnözés nemcsak technológiai, hanem társadalompolitikai és pénzügyi stabilitási kérdés, amely komplex intézményi, szabályozási és edukációs választ igényel.

Az online csalások főbb típusai

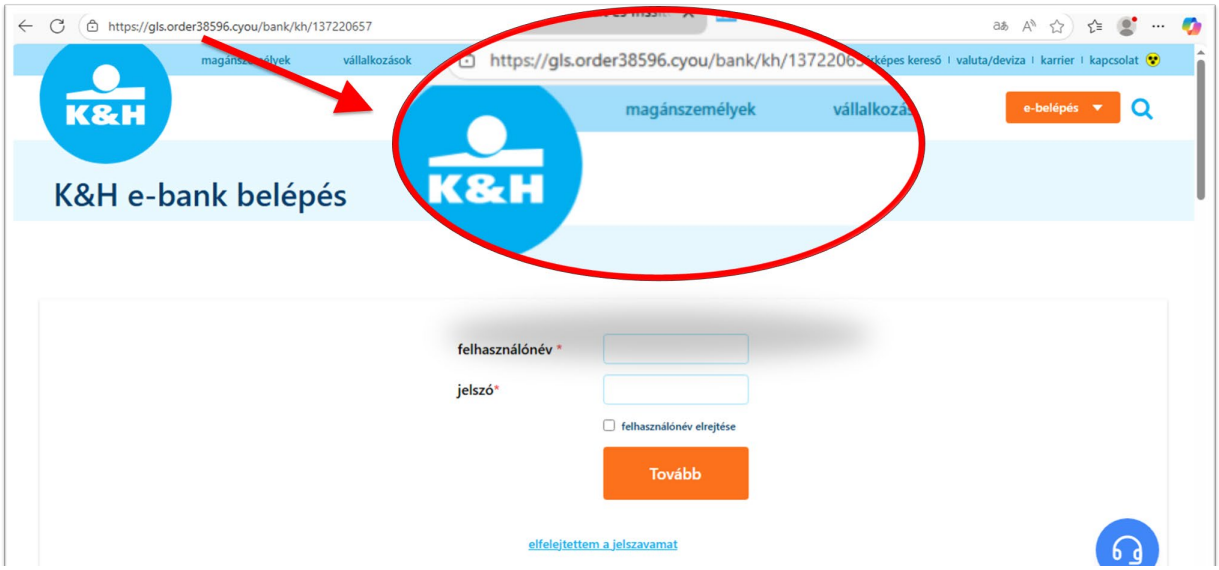
Az online csalások gyorsan alkalmazkodnak a fejlődő technológiához és a változó társadalmi helyzethez: az emberi tényező lett a fő támadási felület, a kiberbűncselekmények 80-85%-a megtévesztésen alapul. A pénzforgalmi visszaélések túlnyomó többsége is online közeget érint. Magyarországon közel 55 milliárd forint kárt okoztak a pénzügyi visszaélésekkel 2024-ben, adathalászathoz és hamis ügyfél-hitelesítéshez kötődően.



Adathalászat (phishing)

Az adathalászat a legelterjedtebb online csalás: a csalók bankok, futárszolgálatok vagy közműcégek nevében küldött üzenetekkel hamisított bejelentkezési vagy fizetési oldalakra irányítják az áldozatokat. Gyakoriak a közösségi médiában megjelenő hamis munkaajánlatok, támogatási felhívások és „Meta" jellegű értesítések, amelyek célja a fiókátvétel. A nagy márkák nevében futó nyereményjátékok és kuponos oldalak szintén gyakran adathalász célúak, és sokszor professzionálisan másolják az eredeti arculatot.

A bankokkal való visszaélés is megjelent a próbavásárlások során:



Mystery Visit kutatás 2025

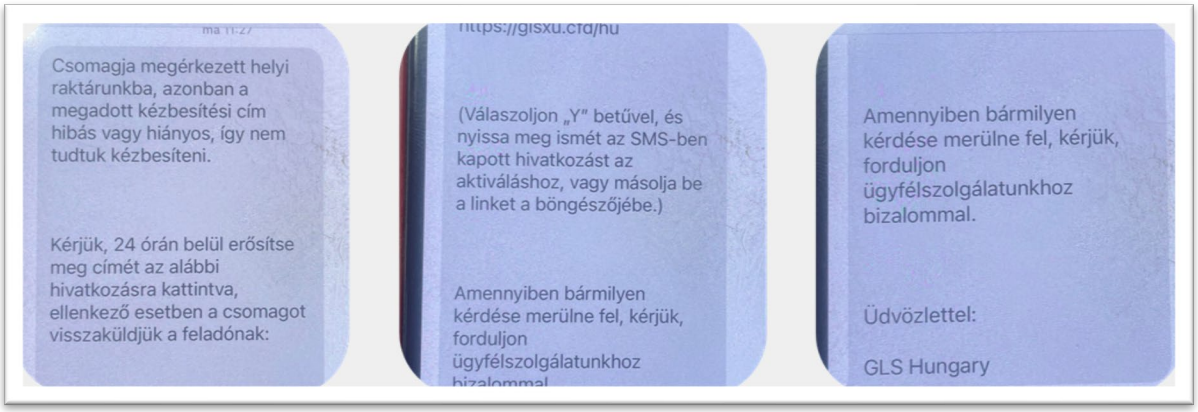
Telefonos és SMS-alapú csalások (vishing, smishing)

A csalók banki ügyintézőnek, futárnak, hatóságnak vagy más olyan személynek adják ki magukat, akinek reális oka lehet adatokat ellenőrizni. Gyakran hamisítják a hívószámot. Céljuk, hogy a sértett banki vagy személyes adatokat adjon meg, távoli elérést biztosító alkalmazást telepítsen, vagy pénzt utaljon. A kommunikáció sürgető hangvételű, és az SMS-ek gyakran adathalász linket tartalmaznak.

Online piactéri és hamis webáruházas csalások

A hamis webshopok és piactéri átverések jellemzően irreálisan olcsó termékekkel vagy sürgető ajánlatokkal csábítanak. A csalók hamis fizetési vagy futárszolgálati oldalra irányítják az áldozatot, vagy fizetés után eltűnnek.

A próbavásárlások során is találkoztunk több ilyen esettel:



Mystery Visit kutatás 2025

Befektetési és kripto-csalások

Magas hozamot ígérő, valós platformokat utánzó weboldalak és hirdetések, gyakran influencerek vagy ismert személyek arcával visszaélve igyekeznek bizalmat kelteni. A bejelentett kripto-befektetési csalások száma 2024-ben megduplázódott, több mint 5 milliárd forintos kárt okozva.

Ártó applikáció, szoftver vagy kód telepítésén alapuló csalások

Hamis banki vagy technikai támogatói hívásokkal veszik rá az áldozatot távvezérlő szoftverek telepítésére, majd így férnek hozzá a számlához. Az ilyen támadások aránya gyorsan nő, 2025 első negyedévében már a pénzforgalmi csalások mintegy 8%-át tették ki.

Romantikus vagy „nigériai" csalások

Hosszú távú bizalmi és érzelmi kapcsolat kiépítésével, akár „külföldi katona" vagy „orvos" szerepével visszaélve kérnek egyre nagyobb összegeket szállítási, vám- vagy egészségügyi költségre. Másik típusa, ha gazdag, de váratlan kalandba keveredett emberként próbálják rávenni az áldozatot pénz utalására vagy „befektetésére". Magyar esetekben több tízmilliós kár is előfordult.

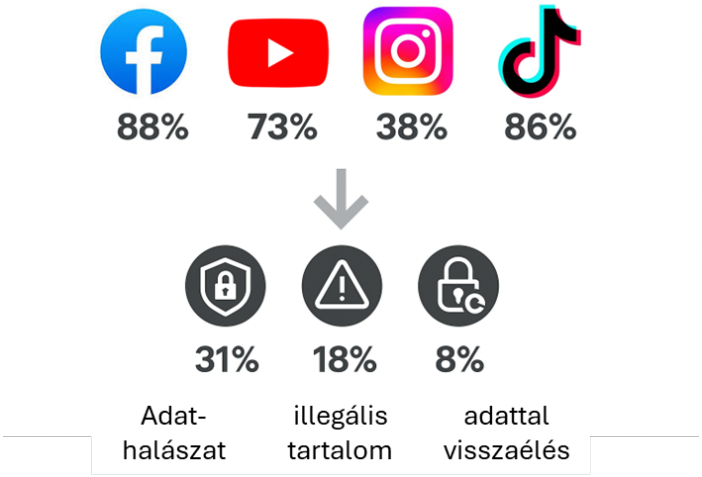
A szégyenérzet és a bizalmatlanság miatt számos áldozat nem él a feljelentés lehetőségével.

Wangiri vagy visszahívásos csalások

Rövid külföldi vagy emelt díjas számról „megcsörgetve" az áldozatot próbálnak visszahívást elérni. A visszahívás magas percdíjjal jár, amelyből részesednek a csalók. A technikájukat fejlesztő csalók legújabb módszere, hogy már SMS-sel vagy robothívással sürgetik a visszahívást.

Magyarországi trendek és jellemzők

A magyar internetezők több mint négyötöde használja rendszeresen a közösségi médiát, és mintegy kétharmaduk találkozott már valamilyen problémával, köztük adathalászattal vagy csalási kísérlettel. A magyar felhasználók különösen érzékenyek a hivatalosnak tűnő, nyelvileg kifogástalan üzenetekre, amelyeket egyre gyakrabban mesterséges intelligenciával készítenek. A károk többsége adathalászathoz, befektetési csalásokhoz és piactéri átverésekhez köthető.



Magyar felnőttek közösségi médiahasználata és a tapasztalt problémák (Impetus Research, 2024)

A platformok védekezési eszközei és módszerei

Bankok és pénzügyi szolgáltatók

Az MNB szabályozói és felügyeleti eszközökkel ösztönzi a bankokat fejlett csalásszűrő rendszerek használatára, és bizonyos esetekben az első veszteség viselésére. A bankok kétfaktoros azonosítást, tranzakciós limiteket, viselkedéselemző algoritmusokat és kockázatalapú riasztásokat alkalmaznak. A bankok aktív csalások felismerésére irányuló edukációs kampányt is folytatnak ügyfeleik körében, mint például:

Az NKI riasztásokkal és tájékoztató anyagokkal támogatja a megelőzést. A Revolut digitális jellege miatt agresszíven épít csalásmegelőző funkciókat az alkalmazásba, amelyek jó példaként szolgálhatnak.

Ár-összehasonlító oldalak

Az ár-összehasonlító oldalak fontos fogyasztóvédelmi funkciót töltenek be, de ezek ellen is előfordulnak csalási kísérletek. Ennek egyik példája egy hamis mobilalkalmazás volt, amelyet a GVH eltávolíttatott.

Közösségi és kommunikációs platformok: automatikus szűrés és bejelentés

A nagy platformok gépi tanuláson alapuló szűrőkkel igyekeznek kiszűrni a gyanús tartalmakat, de a rendszerek pontatlanok lehetnek, és a felhasználói jelentések továbbra is kulcsszerepet játszanak.

Jelentési csatornák, szabályozási környezet, felhasználói tapasztalat

A felhasználók több csatornán (platformokon belül, az Internet Hotline-on, az NKI-n vagy a rendőrségen keresztül) tehetnek bejelentést, de sokan nem ismerik ezeket, vagy elégedetlenek a visszajelzés gyorsaságával.

Magyarországon használt online piacterek és a csalásfelderítés sajátosságai

Magyarországon az online piacterek, mint Jófogás, Vatera, Vinted, Facebook Marketplace egyre népszerűbbek, ám ezzel együtt nő a csalások kockázata is. A platformok vevővédelmi rendszerekkel, automatizált szűrésekkel és jelentési csatornákkal védekeznek, de az off-platform tranzakciók és az emberi viselkedésre pszichológiára építő csalások továbbra is komoly problémát jelentenek.
A korábban ismertetett csalástípusok rendszeresen megjelennek ezeken a felületeken a magyar felhasználókat célozva. Gyakran professzionális, stockfotókkal illusztrált hirdetéseket használnak, a piacinál jelentősen alacsonyabb árral.

Próbavásárlásos kutatás: friss tapasztalatok (2025. október-november)

Az NMHH megbízásából próbavásárlásos kutatás készült, hogy valós interakciók során példázza az online piacterekhez (apróhirdetéses felületekhez) és webshopos vásárlásokhoz kapcsolódó csalási kísérleteket, amelyek sajnálatos módon az online vásárlások állandó kockázataivá váltak. A Mystery Visit kutatás célja az volt, hogy valós tranzakciós helyzetekben tárja fel azokat a csalási mintázatokat, amelyekkel a magyar felhasználók ténylegesen találkoznak. A módszer előnye, hogy nem önbevallásra, hanem tényleges tranzakciókra épít.

A terepmunka 2025. október-novemberben zajlott. Összesen 50 darab, 3 eladási és 47 vételi próbavásárlás történt, Facebook Marketplace-en, Jófogáson, Vaterán, továbbá Google Search Ads-ből elért webshopokon és Facebook-csoportokban. A minta szándékosan a csalásgyanús

hirdetésekre koncentrált, így alkalmas a kockázatot jelentő mintázatok bemutatására, nem reprezentatív.

Az eladási próbavásárlások tapasztalatai

A három eladási kísérlet mindegyike piactéren zajlott. Egy esetben azonosítottak egyértelmű csalási kísérletet: a „vevő” külső futárszolgálati linket küldött, banki belépési adatokat kért „pénz fogadásához”, sürgette a folyamatot és kommunikációs csatornaváltást javasolt. A legitim érdeklődők ezzel szemben nem kértek indokolatlan adatot, nem küldtek külső linket, és nem gyakoroltak nyomást.

A vételi próbavásárlások tapasztalatai

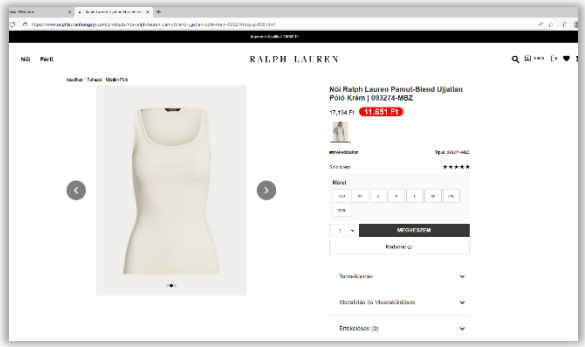
A 47 vételi próbavásárlás közül 7 eset (15%) minősült nagy valószínűséggel vagy egyértelműen csalásnak.

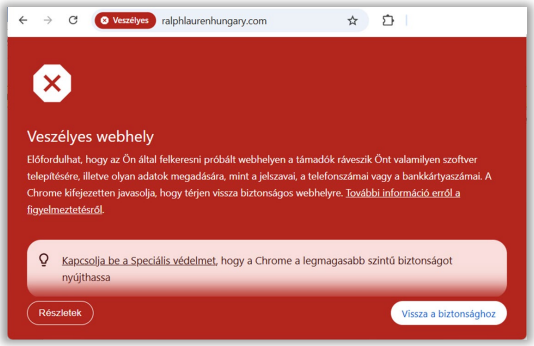
A kutatók azt tapasztalták, hogy a csalások főként Google Search Ads-ben megjelenő ajánlatokhoz és webshopokhoz kötődtek, az online apróhirdetési felületeken ez ritkább volt.

Ebben minden bizonnyal szerepet játszott az is, hogy a keresőhirdetések és az önálló webshopok esetében a csalási kísérletek könnyebben voltak azonosíthatók és elérhetők a kutatási design keretein belül. Az eredmények értelmezésénél fontos szem előtt tartani, hogy a vizsgálat nem reprezentatív, kifejezetten a csalásgyanús hirdetésekre koncentrált. A megfigyelések így elsősorban arra világítanak rá, hogy a különböző csatornák eltérő módon és mértékben teszik lehetővé a csalásgyanús helyzetek kialakulását és felismerését, nem pedig arra, hogy tényleges kockázati rangsort állítsanak fel az online értékesítési felületek között.

A feltárt csalások egy része nem „nyilvánvaló” módon működött. A próbavásárlások során megjelentek olyan hamis webshopok is, amelyek vizuálisan igényesek voltak, részletes termékleírást tartalmaztak, és első ránézésre nem tértek el élesen a legitim kereskedelmi felületektől.

Példa egy nem sokkal a próbavásárlás után már veszélyessé nyilvánított hamis webshopra:





Ez azt jelzi, hogy a csalások egy része már professzionális eszköztárral dolgozik, és nem feltétlenül azonosítható kizárólag egyszerű, felszíni jelek alapján.

Ugyanakkor több, kockázatot jelző mintázat visszatérően megjelent. A tipikus figyelmeztető jelek: stockfotók és gyenge minőségű, magyartalan hirdetésszöveg, a piaci árnál lényegesen alacsonyabb ajánlat, indokolatlan adatbekérés, külső linkek (futár vagy fizetési oldal), gyanús domain és hiányzó ÁSZF, illetve fizetéskori csalások (többszöri terhelés, a hirdetettől magasabb összeg levonása). A kommunikáció során esetenként megjelent indokolatlan adatbekérés, különösen bankkártyaadatok kérése.

A fizetési és szállítási gyakorlatok szintén jól elkülönítették a legitim és a csalásgyanús eseteket. A csalási kísérletek során a bankkártyás fizetés preferálása, a kétfaktoros hitelesítés hiánya és a kizárólag futárszolgálatra épülő szállítási narratíva volt jellemző, míg a legitim tranzakcióknál választható alternatíva volt a banki átutalás és a csomagautomatás átvétel. Pénzügyi veszteség kizárólag a csalási kísérletekhez kapcsolódott.

Összességében a Mystery Visit kutatás is azt mutatja, hogy az online csalások jól azonosítható mintázatok mentén működnek, ezek a minták azonban nem minden esetben szűrődnek ki időben sem a platformok automatikus védelmi rendszerein, sem a felhasználói döntéshozatal során. A csalások jelentős része nem technológiai hiányosságokra, hanem a felhasználók bizalmára és figyelmére épít.

A próbavásárlásos eredmények alapján az online csalások kezelése nem kizárólag egyéni tudatossági kérdés. Bár a felhasználói figyelem és óvatosság kulcsszerepet játszik, a kockázatok rendszerszintűek, és a digitális kereskedelmi környezet működéséből fakadnak.

Javaslatok, megállapítások

Online csalások és védekezés Magyarországon

A hazai online csalások egyre változatosabbak, a klasszikus adathalászattól az AI-alapú megtévesztésekig. A pénzügyi szektor technikailag felkészült, de a csalások nagy része a felhasználói hibákból ered. A platformok védelmi rendszerei nem mindig elégségesek, a felhasználói tudatosság kulcsfontosságú. A próbavásárlási kutatás szerint a csalásmintázatok jól azonosíthatók, de gyakran nem szűri ki őket a rendszer. Javasolt a minimumszabályozás bevezetése lehetőleg európai együttműködés keretében, hiszen a csalások és a digitális felületek is határokon átívelőek, valamint a szektorok közti együttműködés, célzott edukáció további erősítése és a platformok rendszeres tesztelése.