ONLINE CSALÁSOK ELLENI KÜZDELEM

- **A csalás szándékos megtévesztés, amelynek célja haszonszerzés vagy másnak veszteség okozása (EU 2017/1371 irányelve).**
- **Az online csalás az interneten vagy digitális platformokon történik.**
- **Az online csalások főbb típusai:**
  - **túlterheléses (DoS-)támadás;**
  - **pszichológiai manipuláció (social engineering), melynek egyik jellemző példája az adathalászat (phishing);**
  - **adatok elleni fenyegetés;**
  - **zsaroló programok (ransomware);**
  - **rosszindulatú programok (malware)**
  - **elérhetőség elleni fenyegetések (szolgáltatás-megtagadás, internetes fenyegetések).**
- **Statisztikai adatok azt mutatják, hogy az online csalások száma és értéke folyamatosan növekszik. Ez utóbbi részben az elektronikus pénzforgalom növekedésének következménye.**
- **A digitális pénzügyi csalások megelőzésében nagy szerepe van a lakossági tudatosságnak, melynek segítségével beazonosíthatóak a csalási kísérletek.**

A Képviselői Információs Szolgálat Infojegyzete a kormány T/11917. számú törvényjavaslatához kapcsolódóan bemutatja az online csalások típusait és elterjedését, valamint az ellene való küzdelem hazai és európai törekvéseit.

A csalás olyan szándékos megtévesztés, amelynek célja a személyes haszonszerzés vagy egy másik félnek veszteség okozása ((EU) 2017/1371 irányelve 3. cikk (2)). Az online csalások közös vonása, hogy azok az interneten vagy más digitális platformokon elkövetett bűncselekmények, egy incidens azonban egynél több veszélykategóriába is besorolható. Az elsődleges kategória lehet pszichológiai befolyásolás (social engineering), zsarolóvírus (ransomware), malware, adatok elleni fenyegetés, hozzáférés elleni fenyegetés (DoS-támadások), csalás (fraud), és az ellátási lánc elleni támadás (ENISA Threat Landscape: Finance Sector 2024).

A Microsoft legfrissebb Digital Defence Report (2024) jelentése szerint az online csalások száma négyszeresére emelkedett 2022 óta. Az úgynevezett tech scam-ek, vagyis a technikai támogatást imitáló csalások napi előfordulása a jelentés szerint 2023 óta egy év alatt majdnem tizenötszörösére emelkedett.

AZ ONLINE CSALÁSOK TÍPUSAI

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) által készített elemzés az európai pénzügyi ágazat kiberfenyegetettségéről (ENISA Threat Landscape: Finance Sector 2024) megállapítja, hogy a kibertámadások többségét pénzintézetek ellen követik el (46 százalék). A második leggyakoribb célpontok a kormányzati szervek (13 százalék), majd a magánszemélyek (10 százalék) következtek. Az elemzés hasonló tendenciát állapít meg az Európán kívül megfigyelt incidensek esetében is.

Magyarországon az elektronikus pénzforgalom adatai dinamikus növekedést mutatnak (Flór 2023, Digitális Fizetési Index 2023), ezzel párhuzamosan a kitettség is nő. Felmérések szerint a **pénzügyi csalások** száma és értéke hazánkban és a világszerte is emelkedik (ENISA Threat Landscape: Finance Sector 2024). Hazánkban a sikeres elektronikus pénzforgalomhoz kapcsolódó visszaélések jelentős mértékben emelkedtek ugyan (a 2020. évi 3. negyedéves 1 milliárdról 2023 2. negyedévére közel 5 milliárd forintra) az okozott kár aránya a kártyakibocsátó bankok oldalán az összes fizetési kártyás forgalomhoz viszonyítva csak alig 0,016 %-ot tett ki (Flór 2023). Egy közelmúltban végzett felmérés szerint Magyarországon a megkérdezettek több mint fele tapasztalt már e-mailes vagy SMS-es csalási megkeresést. A magas arány azt mutatja, hogy sokan képesek azonosítani csalási kísérleteket, magas a digitális pénzhasználat tudatossága, ami a biztonságos kiberhasználat egyik alappillére (Digitális Fizetési Index 2023).

Az online csalások különösen széles körét foglalja magában a személyekre irányuló pszichológiai manipuláció (**social engineering)**, melynek az emberi tényező a kulcsa: az emberi hibát vagy emberi viselkedést próbálják kihasználni információszerzés céljából (Nemzeti Kibervédelmi Intézet, NKI 2023). A social engineering területén új problémaként jelentkezett a **mesterséges intelligencia** (MI) térhódítása, következésképpen az MI-val támogatott támadások jelentős emelkedésére számítanak (NKI 2023, NKI, 2023. március 9.). Az AuthenticID digitális személyazonosság-hitelesítéssel foglalkozó vállalat globális jelentése szerint az adathalász támadások száma 2024-ben 76 százalékkal nőtt, melynek több mint 90 százaléka pszichológiai megtévesztésen alapult. A jelentés szerint a vállalkozások csaknem fele (46 százalék) tapasztalt növekedést az elmúlt évben az ún. mélyhamisítás (deepfake) technológiával (lásd erről a 2024/20. Infojegyzetet) és a generatív mesterséges intelligenciával elkövetett csalások számában (KnowBe4, 2025. február 4.).

EURÓPAI FELLÉPÉS

Az említett kihívások nem újkeletűek. Az **Európa Tanács** (ET) 2001-ben elfogadta a Számítástechnikai Bűnözésről Szóló Egyezményt, más néven a **Budapesti Egyezményt** (továbbiakban: Egyezmény), amely referenciaként szolgál a kibertér szabályozásában, és iránymutatást ad a csatlakozó államoknak a kiberbűnözés kezeléséhez.

Az **Európai Unió** ugyan formálisan nem részese az Egyezmény aláíróinak, az ET kapcsolódó kiberbiztonságot elősegítő intézményrendszerében és projektjeiben aktív szerepet vállal. A kiberbiztonsággal kapcsolatos európai politikák alakítása, az EU kibervédelmi koncepcióinak, stratégiai dokumentumainak kialakítása közvetlenül támaszkodik az Egyezményében lefektetett fogalmi rendszerre (Krasznay 2021).

Uniós jogalkotási intézkedések

Az uniós vezetők 2018-ben megállapodtak *a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről* szóló **irányelvről** ((EU) 2019/713), amelynek célja a határokon átnyúló együttműködés fokozása és szigorúbb büntetések bevezetése (Európai Unió Tanácsa, sajtóközlemény, 2018. december 11.). Az irányelv vonatkozik a bankkártyára, a csekkre, az elektronikus pénztárcára, a mobilfizetésre és a virtuális fizetőeszközökre mint készpénz-helyettesítő fizetési eszközökre.

A **digitális szolgáltatásokról szóló** jogszabálycsomag tartalmazza a digitális szolgáltatásokról szóló jogszabályt (**Digital Service Act,** DSA, (EU) 2022/2065 rendelete) és a digitális piacokról szóló jogszabályt (**Digital Markets Act**, DMA, (EU) 2022/1925 rendelete). Célja egy biztonságosabb digitális tér létrehozása. A digitális szolgáltatások közé tartozik az online szolgáltatások többsége, köztük azok az **online platformok és keresőmotorok**, amelyek havonta több mint 45 millió felhasználóval rendelkeznek az EU-ban (Európai Bizottság tájékoztatása).

A DMA működési szabályokat és tilalmakat tartalmaz a **kapuőr online platformokra** vonatkozóan. A kapuőrök olyan közvetítő szerepet betöltő nagy online platformok, amelyek különböző mértékben, de jelentős befolyással vannak a felhasználók és az üzleti felhasználók közötti kapcsolatokban. Az EB által első alkalommal kapuőrnek nyilvánított hat vállalat: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft (EB sajtó-közlemény, 2023. szeptember 6.). A Booking hetedikként 2024-ben került fel a listára (EB sajtóközlemény, 2024. május 13.).

Felvilágosítás és együttműködés:

Az **Európai Bizottság** (EB) az eEurope 2005 cselekvési tervének általános célkitűzése volt a biztonságos internet-használat. A cselekvési terv részeként, az EU által finanszírozott **SafeBorders** projekt egyik kezdeményezéseként indul el a Biztonságosabb Internet Napja, melyet minden év februárjában ünnepelnek, mostanra 190 országban. Az esemény különös figyelmet

fordít a kiskorúak online védelmére (Better Internet for Kids honlapja).

Az EB olyan szervezeteken keresztül, mint az **Európai Csalás Elleni Hivatal** (OLAF), nemcsak felületet biztosít a gyanús esetek bejelentésére, de hasznos információkkal szolgál a fogyasztók számára a gyakori csalási taktikákról.

Az **uniós kiberbiztonsági stratégia** (JOIN(2020) 18 final) szintén azzal a célkitűzéssel született, hogy az európai polgárok biztonsága és alapvető jogai ne sérüljenek az online térben. A stratégia hangsúlyozza az együttes fellépést és szorgalmazza a tagállamok közötti kooperációt a kiberbűnözés megelőzése és felderítése érdekében. A csalások elleni közös fellépést segítik elő az olyan európai hatóságok, mint az Europol és az Eurojust. A SIRIUS Terv jól példázza az együttműködési erőfeszítéseket. A projekt az elektronikus bizonyítékokhoz való határokon átnyúló hozzáféréssel kapcsolatos tudásmegosztás központi referenciapontja az EU-ban. Számos szolgáltatást kínál, például iránymutatásokat, képzéseket és eszközöket (Common Challenges in Cybercrime, Europol-Eurojust, 2024).

Hazai fellépés

Jogi szabályozás

2025. január 1-étől megújult a kiberbiztonság védelmét megalapozó jogi szabályozás az új, **Magyarország kiberbiztonságáról szóló** 2024. évi LXIX. törvény (a továbbiakban: törvény) hatályba lépésével. A törvény újraszabja az állam biztonságos működése szempontjából jelentőséggel bíró szervezetek feladatainak és kötelezettségeinek körét; és megújítja a reagáló képességüket az általuk használt elektronikus információs rendszerek kibervédelmének biztosítása érdekében.

A törvény értelmében a kiberbiztonsági hatósági feladatok **négy felügyeleti szerve**:

- a közigazgatási ágazat vonatkozásában, valamint az állami működés szempontjából kiemelt jelentőséggel bíró szervezetek vonatkozásában a **nemzeti kiberbiztonsági hatóság** (Nemzeti Kibervédelmi Intézet);
- a honvédelmi célú elektronikus információs rendszerek tekintetében a **honvédelmi kiberbiztonsági hatóság** (a honvédelmért felelős miniszter);
- a banki szolgáltatások és pénzügyi piaci infrastruktúrák, valamint a közigazgatási ágazat kivételével a NIS 2 ((EU) 2022/2555) irányelv 1. és 2. melléklete szerinti kritikus vagy kiemeltem kritikus ágazatokban a **Szabályozott Tevékenységek Felügyeleti Hatósága** (SZTFH);
- a banki szolgáltatások és pénzügyi piaci infrastruktúrák vonatkozásában (DORA rendelet – lásd erről a 2024/4. Infojegyzetet) a **Magyar Nemzeti Bank** (MNB).

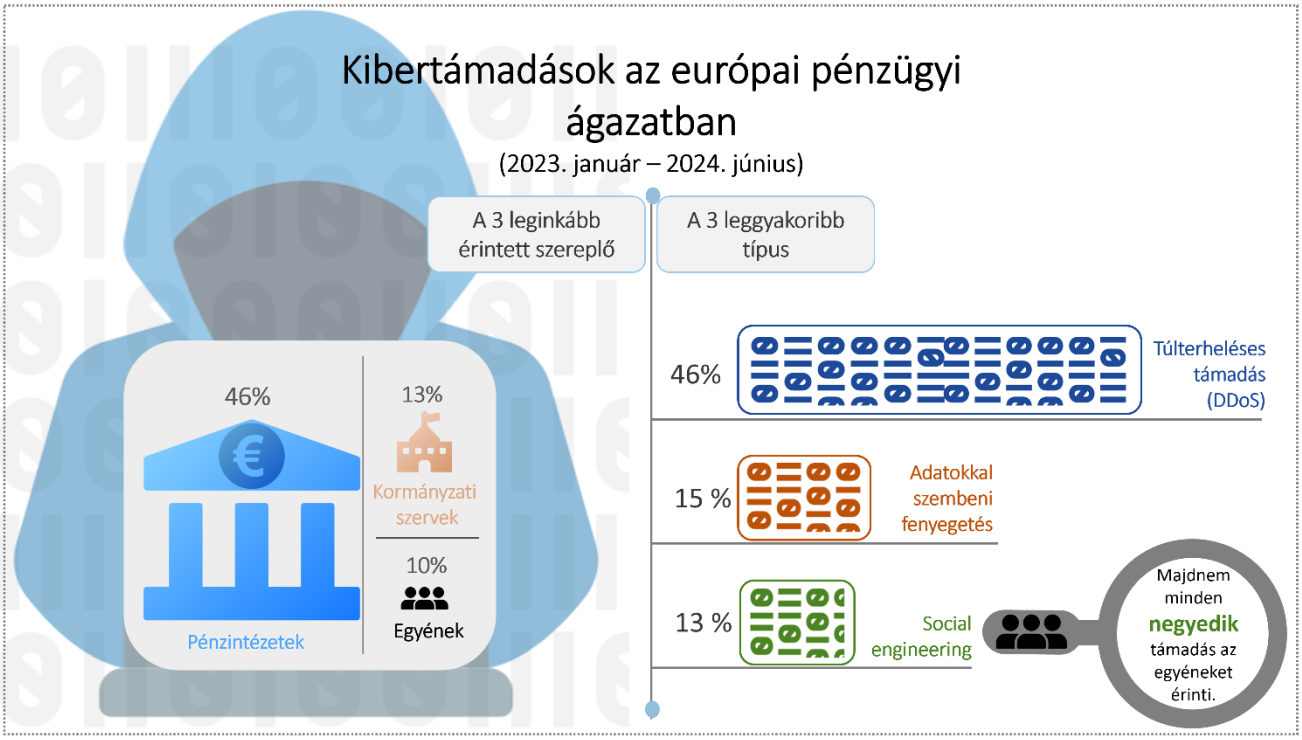
Pénzintézetek és hatóságok közötti együttműködés

A kiberbűnözés elleni hatékony fellépés érdekében az Országos Rendőr-főkapitányság (ORFK) egy önálló szervezeti egység, a Mátrix Projekt keretében kiemelt figyelmet fordít az online csalások felderítésére. Az egység munkáját a rendőrség teljes kibervédelmi tevékenységét ellátó, az ORFK bűnügyi főosztályának kiberstratégiai osztálya koordinálja. A projekt részeként, elsősorban a banki csalások megfékezésére, a rendőrség együttműködési megállapodást kötött az OTP Bankkal és a CIB Bankkal a gyors információáramlás és az azonnali intézkedések érdekében (police.hu, 2023. november 17.; police.hu, 2025. január 8.). A projekt eredményeiről külön kiadványban számolnak be.

Tájékoztatás

Az ügyfelek megfelelő digitális pénzügyi ismeretek és tudatosság birtokában felkészültebbek lehetnek az online térben megjelenő veszélyekkel kapcsolatban. 2022-ben KiberPajzs néven a Magyar Nemzeti Bank, a Magyar Bankszövetség (mint a hazai bankok érdekképviseleti szerve), az Országos Rendőrfőkapitányság, a Nemzetbiztonsági Szakszolgálat, a Nemzeti Kibervédelmi Intézet, valamint a Nemzeti Média- és

Hírközlési Hatóság **közös kommunikációs és edukációs kampány**t indított, amelyhez később csatlakozott az Igazságügyi Minisztérium, a Szabályozott Tevékenységek Felügyeleti Hatósága, a Magyar Államkincstár, a Nemzetgazdasági Minisztérium és a Nemzeti Védelmi Szolgálat is. Az MNB konkrét tanácsokkal segít a kibercsalások kivédésében, továbbá honlapján ismerteti az adathalász csalások leggyakoribb típusait, valamint segítséget nyújt abban is, hogyan védhető ki az adott támadás és csökkenthető az általa okozott kár.



Forrás: Infoszolg/ENISA Threat Landscape: Finance Sector 2024

Források:

- Digitális Fizetési Index Magyarország 2023.
- ENISA Threat Landscape: Finance Sector 2024
- Európa Tanács Számítástechnikai Bűnözésről Szóló Egyezménye
- Éves kiberbiztonsági jelentés 2024.
- Flór Nándor László: A hazai elektronikus pénzforgalom egyre dinamikusabban fejlődik. Oeconomus elemzések. 2023.
- Krasznay, Csaba: Húsz év a globális kiberbűnözés elleni küzdelemben - A Budapesti Egyezmény értékelése. Külügyi Szemle, vol. 2021, no. 1, pp. 191–214.
- Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény
- Microsoft Digital Defence Report 2024
- Pénzforgalom 2030

Készítette: Soltész Katalin
Képviselői Információs Szolgálat
E-mail: infoszolg@parlament.hu

infoszolg

Internet: www.parlament.hu/infoszolg
Intranet: intra.parlament.hu/infoszolg/
Telefon: (1) 441-6486