

KIBERBŰNÖZÉS KORA – MINDEN MÁSODIK MAGYAR ÉRINTETT

A Mastercard „Age of Cybercrime 2025” kutatása szerint Magyarországon is egyre több az online csalás, amely – ha sikerrel jár – akár egy vállalkozás végét is jelentheti. A Mastercard szakértői szerint a növekvő kiberbűnözés ellen csak az iparági szereplők összefogásával, oktatással és a mesterséges intelligencia még intenzívebb használatával lehet eredményesen fellépni.

AJÁNLO

Olvassa el a Kiberbűnözés kora című tanulmányt teljes terjedelmében: [A kiberbűnözés kora 2025](#)

Több tízmilliárdos károk, több millió érintett

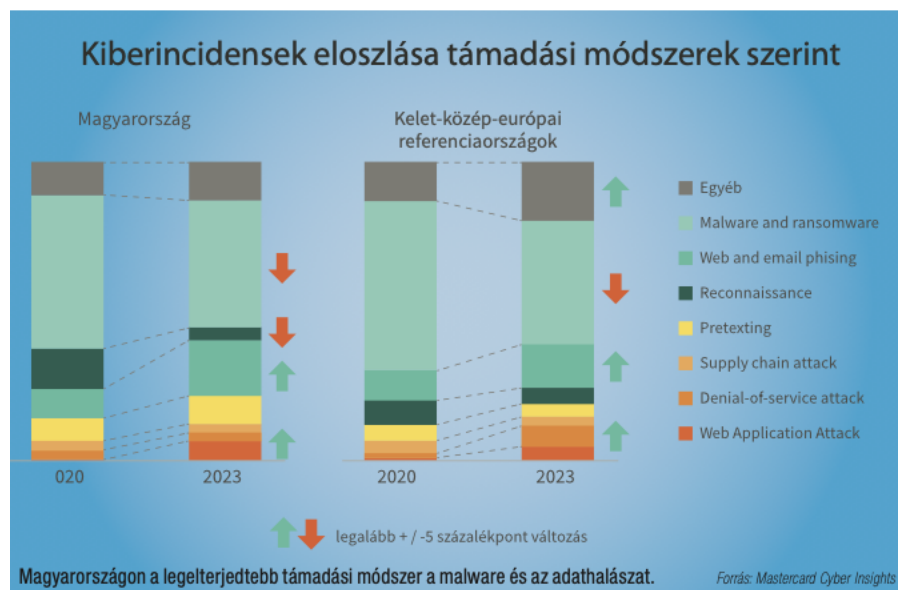
A kiberbűnözés napi valóság Magyarországon. A Magyar Nemzeti Bank adatai szerint 2024-ben 41,9 milliárd forintnyi kárt okoztak a digitális csalások, összesen 220 ezer tranzakciót érintve. A Mastercard friss kutatása szerint a magyarok 48 százaléka tapasztalt már valamilyen online bűncselekményt a környezetében. Vagyis minden második magyar találkozott már például hamis csomagküldéses SMS-sel, adathalász e-maillal vagy fogadott telefonhívásokat csalóktól.

A kisvállalkozások vannak a legnagyobb veszélyben

A „Kiberbűnözés kora 2025” jelentés egyik legaggasztóbb adata, hogy a kibertámadást elszenvedő KKV-k 60 százaléka fél éven belül megszűnik. A kiberbűnözés tehát nemcsak az egyes emberek pénztárcáját, hanem a magyar gazdaság stabilitását is fenyegeti. A legelterjedtebb támadási módszerek a malware és az adathalászat, amelyek gyakran pszichológiai manipulációra építenek, a felhasználók bizalmát kihasználva.

A mesterséges intelligencia hajtja a csalásgyárat

A Mastercard kutatása szerint a kiberbűnözés ma már szervezett iparág, amely nagyban alkalmazza a mesterséges intelligenciát és az automatizációt. „Az új technológiák csúcsra járatják a csalásokat, növelve az alacsony költségű deepfake-ek létrehozásának és telepítésének lehetőségét” – figyelmeztet Wittinghoff Dániel, a Mastercard kibervédelmi üzletfejlesztési igazgatója. A mesterséges intelligenciával működtetett botok valós időben gyűjtenek adatokat, hamis identitásokat hoznak létre, és összehangolt kibertámadásokat hajtanak végre. Ez már nem egyedi hackerakció, hanem iparszerű csalásgyár.



Ezt ellensúlyozza a Mastercard a legújabb technológiák hadrendbe állításával: az elmúlt hat évben a vállalat 10,7 milliárd dollárt fektetett be kiberbiztonsági és csalásmegelőzési technológiákba világszerte. A Mastercard fejlett AI-alapú adatelemzési rendszerei képesek felismerni a gyanús tranzakciókat és valós időben reagálni a fenyegetésekre, ezzel segítve a bankokat, fintechcégeket és kereskedőket.

AJÁNLÓ

Olvassa el Wittinghoff Dániel LinkedIn bejegyzését a témában:

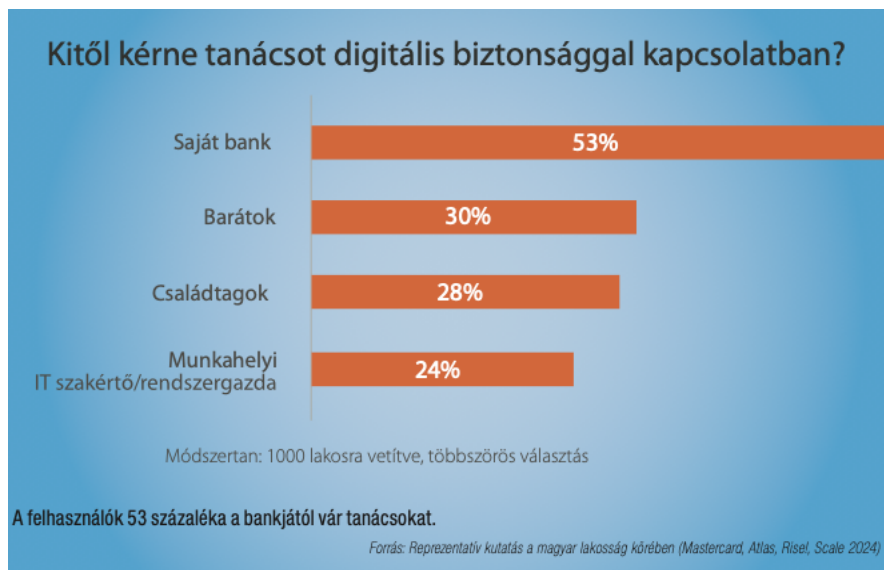
[Mesterséges intelligencia a kibervédelem mindkét oldalán](#)

Költséghatékonyság, a repetitív emberi feladatok átvétele a kreatív munkaerő felszabadítására, fokozottabb ügyfélélmény - többek között ezeken a területeken segít legtöbbet napjainkban a mesterséges intelligencia: az MI-vel megerősített megoldások révén komoly hatékonyságnövekedést ígérnek. Nem véletlen, hogy már a kiberbűnözők is alkalmazzák, ami a védekezésben is új stratégiákat tesz szükségessé.

A magyarok a bankjuktól várnak védelmet

A Mastercard reprezentatív kutatása szerint a magyarok 53 százaléka a bankjától vár tanácsot digitális biztonsági kérdésekben, míg 30 százalék a barátaitól, 28 százalék a családtagoktól, és 24 százalék a munkahelyétől. Ez rávilágít arra, hogy a pénzügyi intézményeknek és a munkáltatóknak kulcsszerepük van az edukációban.

„Az információmegosztás segít felkészülni a támadásokra és növeli a kiberbiztonsági tudatosságot” – erősíti meg Nemes Máté, a Mastercard kiberbiztonsági termékekért felelős igazgatója.



Csak együtt lehetünk ellenállók

A mesterséges intelligencia újraírja a kiberbűnözés ellen folytatott küzdelem szabályait: a nagytömegű és összehangolt kibertámadásokkal szemben nem már nem elegendő a technológiai felkészültség, hatékonyan védekezni csak iparági összefogással, tudatossággal, és közös védelmi stratégiával lehet – vonja le a következtetést a Mastercard tanulmánya. Az ellenállóképesség felépítéséhez elengedhetetlen az ökoszisztémában való gondolkodás, amely megköveteli az állami és a versenypiaci szereplők közötti aktív együttműködést.

A „Kiberbűnözés kora 2025” tanulmány szerint a védekezésnek három kulcsterületre kell összpontosítania:

- **információmegosztás,**
- **technológiai fejlesztés,**
- **folyamatos edukáció.**

A tanulmány pozitív végkicsengésű: ha felhasználók, vállalatok és intézmények összefognak, akkor a „kiberbűnözés kora” helyett a digitális ellenállóképesség kora jöhet el.

ESETTANULMÁNY

Cyber Islands – a magyar összefogás platformja

A Mastercard Magyarországon is aktív szereplője a kibervédelem fejlesztésének. Ezért támogatja a [Cyber Islands](#) nevű kezdeményezést, amely egy nyitott, együttműködésre épülő platform a kiberbiztonság iránt érdeklődő szakemberek, vállalatok, startupok, hallgatók és intézmények számára. A Cyber Islands összekapcsolja az oktatást, az innovációt és a vállalati tudást, és hidat képez a szakmai közösség és az ipar között.

A projekt célja, hogy összekösse a jelenleg elszigetelten működő szereplőket, és előmozdítsa egy nemzeti szintű kibervédelmi ökoszisztéma kialakulását. A Cyber Islands demokratizálja a tudást és a tapasztalatot azzal, hogy azt minden szervezet és szakember számára elérhetővé teszi. A projekt ezen túl nemzetközi együttműködésekre is nyitott, hogy Magyarország a régió egyik vezető kibervédelmi központjává válhasson.

A „digitális szigetcsoportokban” eseményeket, workshopokat és mentorprogramokat szerveznek, ahol a résztvevők valós problémákra keresnek válaszokat – például az AI-alapú csalások felismerésére vagy az adatvédelem megerősítésére.