

SAJTÓKÖZLEMÉNY

Aki bedől az AI tartalomnak, háromszor nagyobb eséllyel válik csalás célpontjává – figyelmeztet a Visa

A KiberPajzzsal közös sajtótájékoztatóján a Visa bemutatta legfrissebb kutatásának eredményeit. Ebből többek között az is kiderül, hogy a „digitális tájékozatlanság” közvetlenül növeli a sebezhetőséget: aki a közösségi médiában valódinak hiszi a mesterséges intelligencia által generált hamis tartalmakat, háromszor sebezhetőbbé válik a csalásokkal szemben.

A KiberPajzs program kiemelt szerepet játszik abban, hogy a lakosság és a pénzügyi szektor szereplői időben felismerjék a kiberfenyegetéseket, és egységes, naprakész ismeretekre támaszkodhassanak. A program a megelőzés, az edukáció és az összehangolt szakmai fellépés révén nyújt segítséget a digitális csalások visszaszorításában. Ezek egyik legújabb és legveszélyesebb területe a hamis hirdetések és a mesterséges intelligencia által generált átverések, amelyek mértéke és kifinomultsága rohamosan növekszik a közösségi médiában – így a felhasználók számára minden eddiginél nehezebb megkülönböztetni, mi valódi és mi hamis.

Ennek kapcsán készített a Visa egy kutatást tizenegy európai országban 9500 felnőtt bevonásával, többek között azt vizsgálva, hogyan hatnak a felhasználókra a social media felületeken a mesterséges intelligencia segítségével előállított tartalmak. Az eredmények azt mutatják, hogy a mindennapi online szokások új sebezhetőségi pontokat teremtenek, amelyeket a csalók gyorsan kihasználnak. A magyarok közel negyede (24%) osztott már meg bejegyzést anélkül, hogy ellenőrizte volna annak hitelességét. Közel egyharmaduk (31%) ritkán olvas tovább a főcímnél a közösségi médiában vagy hírportálokon, mielőtt véleményt formálna, és a közösségi média felhasználók közel 8%-a bevallotta, hogy semmilyen lépést nem tesz online biztonsága érdekében.

A hatás pedig túlmutat a pénzügyi veszteségen: érzelmi stresszt, fokozott szorongást és csökkent hatékonyságot okoz. Erről az érintettek 20%-a számolt be, az áldozatok harmada ráadásul több mint három munkanapot tölt a visszaélések rendezésével.

Ahogy az online csalások egyre kifinomultabbá és elterjedtebbé válnak, a fogyasztói magatartás változása kézzelfogható hatást gyakorol a tágabb gazdaságra. Becslések szerint 2,6 millió magyar változtatott online vásárlási szokásain, miután átverték vagy csalás célpontja lett: 40%-uk azt állítja, hogy kevesebbet vásárol online, illetve kerüli a kisebb vagy ismeretlen márkákat.

„A mesterséges intelligencia jelentős szerepet játszik abban, ahogyan élünk és dolgozunk, a személyre szabott élményektől a működési hatékonyságig, de új kockázatokat is hordoz – mondta Sármy Bence, a Visa Magyarországért felelős vezetője. – A csalók ezeket az eszközöket megtévesztésre használják, aláásva az online csatornába vetett bizalmat. Egyre könnyebb összetéveszteni a hamisít a valódival, aminek kézzelfogható következménye a pénz-, idő- és bizalomvesztés. Ezért fektetünk mesterséges intelligencia-alapú innovációba, működünk együtt iparági partnereinkkel és látjuk el a fogyasztókat a biztonsághoz szükséges eszközökkel és tudással, hiszen együtt egy biztonságosabb digitális jövőt építhetünk mindenki számára.”

Számos előnye mellett a mesterséges intelligencia a kiberbiztonság teljes ökoszisztémáját is képes átalakítani, ezért a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete (NBSZ NKI) számára is stratégiai területet jelent. Bár a mesterséges intelligencia térnyerésével új típusú fenyegetések

és támadási formák jelentek meg, a technológia egyúttal innovatív védekezési lehetőségeket is kínál. Az AI így egyszerre hordoz kockázatot és kulcsfontosságú erőforrást; a jövő kiberbiztonsági stratégiái pedig csak akkor lehetnek eredményesek, ha a vállalkozások felkészülten, tudatosan és felelősen építik be a mesterséges intelligenciát mindennapi működésükbe.

„A mesterséges intelligencia mára a kiberbiztonság meghatározó alappilléreivé vált: olyan erőforrássá, amely nélkülözhetetlen a modern fenyegetésekkel szembeni hatékony fellépéshez – fogalmazott Szabó Lajos, az NBSZ NKI igazgatója. – Az automatizált elemzési rendszerektől a prediktív technológiákig számos területen támogatja a vállalkozásokat abban, hogy tudatosan, magabiztosan és felkészülten működjenek egy egyre összetettebb digitális környezetben.”

Az elmúlt években globálisan és így Magyarországon is meredeken nőtt a digitális csalások száma és aránya. A folyamatosan változó kibertérben a megelőzés, valamint a bűnüldözés támogatása csak akkor lehet eredményes, ha a pénzügyi, szabályozói, kormányzati és bűnüldözői szereplők összehangoltan és proaktívan lépnek fel. Ezt a munkát erősíti Kovács Levente és Terták Elemér „Kiberbiztonság – kibertér” című új szakkönyve, amelyet a sajtótájékoztatón mutatott be a Magyar Bankszövetség.

„Ma a digitalizációs vívmányok megtartása a tét, hiszen biztonságosan használható kibertér nélkül a vívmányok elvesznek – mondta Kovács Levente főtitkár, egyetemi tanár. – Jelen korunk egyik legnagyobb kihívása a kibertér védelme: ma ugyanis a legnyereségesebb iparág a kiberbűnözés. A kibertér gyors fejlődése miatt a bűnözők technológiailag ma még előnyben vannak, ezért a megelőzés és a védekezés szerepe felértékelődött. Ehhez a munkához a kibertámadások rendszerezése, bemutatása, megértése és előrejelzése szükséges. Ezzel az új szakkönyvvel célunk megadni az elméleti hátteret, amelyre hatékony oktatási, védekezési, szabályozási és bűnüldözési struktúrák épülhetnek.”

A szakértők egyetértenek abban, hogy a mesterséges intelligencia terjedésével a kiberbiztonság többé nem elszigetelt technológiai kérdés, hanem közös nemzetgazdasági érdek és társadalmi felelősség. A vállalkozások, az állami szereplők és a szakmai szervezetek együttműködése – az olyan kezdeményezésekre építve, mint a KiberPajzs program – elengedhetetlen ahhoz, hogy Magyarország továbbra is biztonságos, átlátható és versenyképes digitális környezetet kínáljon.

Megjegyzés:

Az adatok forrása – ha másként nincs jelölve – a Visa megbízásából készült felmérés magyarországi eredményei. A kutatást az Opinium végezte 9500, 18 év feletti felnőtt bevonásával, akik országosan reprezentatív mintát alkottak a következő 11 európai országban: Egyesült Királyság, Franciaország, Németország, Olaszország, Szlovákia, Spanyolország, Lengyelország, Magyarország, Románia, Bulgária és Csehország.

A KiberPajzs Programról

A 2022 novemberében életre hívott **KiberPajzs Program** egy kiberbiztonsági edukációs és kommunikációs kezdeményezés, amelynek célja az online pénzügyi visszaélések megelőzése, a lakossági fogyasztók és vállalati ügyfelek védelme. A KiberPajzs együttműködő partnerei: Igazságügyi Minisztérium, Magyar Államkincstár, Magyar Bankszövetség, Magyar Nemzeti Bank, Mastercard, Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet, Nemzetgazdasági Minisztérium, Nemzeti Média- és Hírközlési Hatóság, Nemzeti Védelmi Szolgálat, Országos Rendőr-főkapitányság, Pénzügyi Békéltető Testület, Szabályozott Tevékenységek Felügyeleti Hatósága, Szerencsejáték Zrt., Visa; kommunikációs partnere a Médiaunió Alapítvány. **További információ: [Kiberpajzs.hu](https://kiberpajzs.hu)**

A Visa tippjei:

Öt okos módszer a biztonság megőrzésére a közösségi médiában

1) Kérdőjelezd meg a forrást

A csalók gyakran hoznak létre az eredetire megtévesztésig hasonlító hamis webshopokat, látványos hirdetésekkel, MI által generált hírességek ajánlásaival és meggyőző személyes üzenetekkel. Ezek a taktikák hihetetlenül valódinak tűnhetnek. Mielőtt kattintanál, állj meg és tedd fel a kérdést: Megbízható ez az oldal? Egy pillanatnyi kétely költséges hibázástól menthet meg.

2) Tarts egy kis szünetet

A sürgetés a csalók egyik leggyakoribb módszere. Az ingyenes ajándékok, hatalmas kedvezmények vagy „korlátozott idejű” ajánlatok célja, hogy elkapkodott döntésre késztesselek. Inkább lassíts le! Ellenőrizd, hogy az ajánlat reális-e, kutass a cég után, olvass véleményeket, és látogass el a márka hivatalos weboldalára, mielőtt bármilyen személyes adatot megosztanál.

3) Ellenőrizd a küldőt – ne csak a profilt

Üzenetet kapsz egy baráttól, influenszertől vagy szervezettől, amely pénzt vagy személyes adatokat kér? Ne feledd: nem biztos, hogy valódi! Ellenőrizd független forrásból: hívd fel az illetőt, használj egy ellenőrzött weboldalt, vagy vedd fel a kapcsolatot közvetlenül a céggel. A csalók gyakran valódi fiókokat törnek fel, hogy hitelesnek tűnjenek.

4) Maradj biztonságban és jelentsd a gyanús tevékenységet

Védd a fiókjaidat extra biztonsági funkciók, például a kétfaktoros (2FA) vagy többfaktoros (MFA) hitelesítés bekapcsolásával, ahol lehetséges. Tartsd naprakészen az alkalmazásaidat, eszközeidet, és rendszeresen ellenőrizd az adatvédelmi beállításaidat. Ha gyanús hirdetést, bejegyzést vagy fiókot látsz, jelentsd a közösségi platformnak – és a bankodnak, ha pénzről van szó.

5) Fizess biztonságosan – vagy sehogy

Soha ne oszd meg a banki adataidat a közösségi médián keresztül. Ha valaki arra kér, hogy banki átutalással küldj pénzt, az valószínűleg csalás. Mindig használj biztonságos fizetési módokat, amelyek vásárlói védelmet nyújtanak. Ha erre nincs lehetőség, inkább ne vásárolj!