K&H: az óvatosság már kevés a csalókkal szemben, többre van szükség

A mesterséges intelligencia megjelenése a pénzügyi csalók eszköztárában odavezetett, hogy a laikusok már nem bízhatnak abban, amit látnak vagy hallanak, mert hamis lehet. A K&H Bank segít, hogy egyszerű módszerekkel felismerhesd a támadásokat.

Folytatódik a harc a csalók ellen, akiknek ma már a mesterséges intelligencia (**MI,** azaz **AI**) is segítséget nyújthat. Erre példa egy idei hongkongi eset, amelyben egy cég alkalmazottja 25 millió dollárt utalt át csalók számlájára, miután vállalatának „pénzügyi igazgatója" egy videóhívásban erre utasította. A képkockákon a háttérben a „kollégáit" látta az illető, ezért fel sem merült benne, hogy csalásról van szó. Ugyanakkor a videóhívásban csak ő szerepelt, a másik felet mesterséges intelligenciával kreálták, a valósághoz teljesen hűen, a valósághoz megszólalásig hasonlító utánzatot – derül ki a K&H korábbi közleményéből, amely a mesterséges intelligencia veszélyeire hívja fel a figyelmet.

A Kiberpajzs is segít a védekezésben

A nemzetközi porondon tényked csalók korábban nehezen birkóztak meg a magyar nyelvvel, ám az AI ebben is segíti őket. Olyannyira, hogy az e-mailek nyelvezete ma már közelít a tökéleteshez. A gyanútlan ügyfelekre nézve ez pedig komoly veszélyt jelent. A csalók a bankok logójától kezdve arculatig mindent pontosan lemásolva igyekeznek átverni az embereket. A legfontosabb tudnivaló, hogy az e-mailben, sms-ben, vagy bármi egyéb írásos csatornán kapott link ellenőrzése még mindig a legbiztosabb módszer a védekezéshez. Érdemes azokat a leveleket, amelyeket nem vártunk, inkább számítógépen megnézni, a telefonokon ugyanis gyakran nem adottak a technikai feltételek például egy link biztonságos ellenőrzéséhez. Az alapszabály az adathalász e-mailekkel kapcsolatban az, hogy minél gyorsabb cselekvésre ösztönzik – például pénzjutalmakkal, vagy szankciókkal – a megcélzott ügyfeleket, annál valószínűbb, hogy átverésről van szó.

Még nem került be a köztudatba, hogy a mesterséges intelligencia segítségével nagyon jó minőségű képek, videók készíthetők, hamisíthatóak hangok, az így készített támadások száma és értéke is rohamosan növekvő tendenciát mutat. Érdemes rászoktatnunk magunkat arra, hogy a telefonhívások esetén kis bevezető fecsegésbe öltöztetett „biztonsági kérdéseket" alkalmazunk, ami azt jelenti, hogy olyan információt kérünk a másik féltől, aminek csak ő lehet birtokában, majd figyeljük a másik fél reakcióját. A hongkongi támadás során, ha az alkalmazott ilyen módon azonosítja a „pénzügyi igazgatót" (pl.: Tényleg ízlett a lányodnak a szülinapi torta?), akkor kisebb eséllyel következhet be a csalás.

A K&H Bank honlapján a látogatók megismerkedhetnek a leggyakoribb banki csalásokkal, az MNB KiberPajzs programja pedig nem csupán a pénzügyi tevékenységet, hanem az egyéb szektorokat érintő csalásokat is bemutatja.

Többszörösére nőhet a lopott pénz összege

A hongkongi példát idéző Deloitte nemzetközi tanácsadó cég becslése szerint a mesterséges intelligencia megjelenése a banki csalásokban óriási növekedést okozhat az ellopott pénz összegében. Az Egyesült Államokban például 2027-re elérheti a 40 milliárd dollárt, szemben a 2023-as 12,3 milliárd dollárral. Ez azt jelenti, hogy ebben az időszakban évente 32 százalékos tempóban nőhet a bankok ügyfeleinek vesztesége.

> “A generatív AI végeláthatatlan lehetőségeket kínál a tolvajoknak mind módszereik megválasztásában és variálásában, mind akcióik számának növelésében. A szakértők úgy látják, hogy csak a mindenre elszánt bűnözők képzelőereje szab határt annak, mi mindennel próbálkozhatnak” - mondta Nagy Ádám Péter, a K&H információ-biztonsági vezetője, akit 2023-ban az Év IT-biztonsági vezetőjének választottak.

A Deloitte arra számít, hogy a mesterséges intelligencia alapú banki csalások jelentős részét kitevő e-mail-es átverések a legrosszabb esetben 2027-re akár a 11,5 milliárd dollár veszteséget is okozhatnak. Hiába járnak élen a bankok évtizedek óta a kibercsalások elleni küzdelemben, szakértők szerint az eddig használt kockázatelemző módszerek nem elegendőek az új veszély elhárítására.

A fegyverkezési verseny logikája érvényesül

Az ügyfelek adatait, pénzét nagyon robosztus biztonsági rendszerrel védő pénzügyi szolgáltatók egy része már integrálta a generatív mesterséges intelligenciát rendszereibe annak érdekében, hogy felismerjék a csalások jeleit. Olyan biztos módszer azonban nincs, amivel szembe lehet szállni a legmodernebb fegyverzettel indított kibertámadásokkal. A csalók is folyamatosan „fejlesztenek”, egyre rafináltabb megoldásokkal próbálkoznak. A másik oldalon pedig támaszkodni kell az AI öntanuló képességére, ugyanis a támadó sötét AI ugyanezt teszi. Minden lopási kísérlet kudarcából vagy sikeréből levonja a tanulságokat és módosít a módszerein. Az ügyfelekkel a korábbinál is gyakrabban kell kommunikálni a veszélyekről. A legfontosabb azonban talán még mindig a „hagyományos” intelligenciához kötődik.

Sajtókapcsolat:

- K&H Kommunikációs Igazgatóság
- sajto@kh.hu

Eredeti tartalom: K&H Bank Zrt.

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/15033/kh-az-ovatossag-mar-keves-a-csalokkal-szemben-tobbre-van-szukseg/