

Bankkártyás csalások: ismert szolgáltatók partnereinél is célszerű az óvatosság

Ismert utaztatási társaságok külföldi autókölcsönzési vagy szállásadói partnereihez kötődő ügyleteknél fordulhattak elő digitális bankkártya-csalási kísérletek. A támadások nem a biztonságosan működő magyar bankoknál, hanem kereskedelmi szolgáltatók kapcsán indultak. Vásárlási limitbeállítás, tranzakciós értesítések, végső esetben azonnali kártyaletiltás segíthet a védekezésben.

A Magyar Nemzeti Bankhoz (MNB) több ügyféljelzés érkezett arról, hogy az ismert utaztatási társaságok (pl: légitársaság, szállásfoglalási rendszer) által harmadik fél (pl: autóbérlő cégek, privát szállásadók, hotelek) felé közvetített szolgáltatásoknál észleltek digitális bankkártyacsalási kísérleteket. Az MNB Pénzügyi Navigátor fogyasztóvédelmi honlapján tavaly [felhívta a figyelmet](#): az interneten csak megbízható kereskedelmi szolgáltatók oldalán célszerű megadni bankkártya-adatainkat. Interneten vásárlásnál a bankkártya PIN-kódját még kérésre sem szabad megadni, hiszen arra csak az ATM-eknél, POS-termináloknál van szükség.

A mostani esetek – amelyek nem a biztonságosan működő hazai bankokat, hanem egyéb szereplőket érintenek – azt jelzik: a fogyasztóknak még az ismert társaságok kapcsán is elővigyázatosságnak kell lenniük. A bankkártyás csalások kapcsán elszemvedett ügyfélkárók összegét befolyásolhatja, hogy a (külföldi) autókölcsönzéshez, szállásfoglaláshoz (de akár egy automata benzinkút használatához is) a harmadik fél szolgáltatók – részükről méltányolható üzleti-elővigyázatossági okokból – nem csak a szolgáltatási költséget vonják le, de ezen felül letétet is felszámítanak.

Ha az ügyfél a szolgáltatás igénybevétele során nem okozott kárt (pl. nem sérült az autó vagy a szállodai szoba), a letétet utólag visszatérítik. Előfordulhat az is, hogy már a foglalás után a szolgáltató legálisan egy kis összegű „próbalevonást” végez az ügyfélkártyáról – így ellenőrizve, hogy az tényleg létezik –, amelyet aztán azonnal visszatérít. Akadnak olyan szolgáltatók is, akik a letét teljesítéséhez készpénzt, esetleg betéti bankkártyát nem, csak hitelkártyát fogadnak el.

Egyes ügyfelek jelzésük szerint kizárólag a jól ismert szolgáltatók felületén adták meg a közvetített szolgáltató harmadik fél (pl. autókölcsönző) kifizetéshez szükséges adataikat (név, kártyaszám, lejárat dátum, CVC-kód). Ennek ellenére utólagosan – akár a szolgáltatás sikeres igénybevétele után, pl. külföldi utazásukról hazatérve – az tapasztalták, hogy további nagy összegeket próbáltak leemelni kártyaszámlájukról.

Más esetekben bűnözői körök szerezhették meg nagy tömegben a szállásfoglaló/autóbérlő ügyfelek email címeit (vagy az ismert utazási szolgáltató vagy a harmadik fél partner informatikai rendszerének feltörésével). Ezek ismeretében az ismert szállásközvetítő vagy egyéb céghez látszólag hasonló email címről követelték, hogy a fogyasztók adják meg banki adataikat „megerősíteni azonosításukat” vagy mert „bankkártyájukkal problémák merültek fel”, különben visszatérítés nélkül törlik szállás/autófoglalásaikat.

E kibertámadások ellen célszerű korlátozni (főképp egy külföldi útról való visszatérésünk után) bankkártyánk vásárlási, készpénzfelvételi limitjeit. Mindenkor érdemes igénybe venni a kártyás tranzakciókról azonnali jelzést küldő felugró ablakos vagy sms-értesítési szolgáltatást. Jóvá nem hagyott tranzakcióról értesülve haladéktalanul le kell tiltani bankunknál kártyánkat, s ehhez – különösen utazásnál – érdemes előkészítve tartanunk az erre szolgáló telefonbanki elérhetőségeket. Ha külföldön járunk, hasznos lehet némi készpénzt vagy egy második fizetési kártyát is magunknál tartani támadás esetére.

Sajtókapcsolat:

- +36 1 428 2600
- sajt@mn.b.hu

Eredeti tartalom: Magyar Nemzeti Bank

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:

<https://hellosajto.hu/10898/bankkartyas-csalasok-ismert-szolgaltatok-partnereinel-is-celszeru-az-ovatosag/>