Tájékoztató a bankkártyák biztonságos használatáról

Tartalomjegyzék

1. Általános tudnivalók a bankkártya használattal kapcsolatban: 2
2. Tanácsok az egyes visszaélés típusok megelőzéséhez: 2
   a. ATM készpénz felvétel során 2
   b. Személyes vásárlás esetén 3
   c. Internetes vásárlás esetén 3
3. Adathalászat 3
4. További fontos információk 4

A következőkben a bankkártyák biztonságos használatával kapcsolatban szeretnénk néhány tanácsot adni Tisztelt Ügyfeleink részére.

1. Általános tudnivalók a bankkártya használattal kapcsolatban

- A bankkártya a bank tulajdonát képezi, melyet a kártyabirtokos nevére állít ki, ezért annak használatát kizárólag ő gyakorolhatja. Amennyiben valamely családtag is szeretné használni az ön nevére kiállított fizetési eszközt, az ő részére társkártya igényelhető az ön számlájához kulcsolva.
  A bankkártya azonosító adatait (CVC kód, PIN kód), beleértve a kártya számát és a lejárati dátumát, harmadik féllel megosztani tilos. Az említett adatok ismeretében bárki képes internetes tranzakció, vagy a bankkártya birtokában bármely más elektronikus terminálnál vásárlási vagy készpénz felvételi tranzakciót kezdeményezni.
- A PIN kódot lehetőleg tartsuk fejben, és ne jegyezzük fel.
  Amennyiben mégis szeretnénk a PIN kódot tartalmazó papírt megtartani, azt biztonságos helyen, a kártyától elzárva tároljuk, hogy lopás esetén ne lehessen felhasználni.
- A bankkártya helyéről mindig legyen tudomása.
  Vesztett kártyák használatából eredő veszteségekért a bank nem vállal felelősséget. Fontos még ezen kívül, hogy a bankkártyát ne tévesszük szem elől, ne hagyjuk mások által hozzáférhető helyen, beleértve vásárlás után a pénztár vagy ATM melletti pulton, avagy gépjárműben.
- Javasoljuk a költési szokásoknak megfelelő napi vásárlási és készpénzfelvételi limitek beállítását, összeg és tranzakció darabszám vonatkozásában is.
  A kártyavisszaélések elleni első védvonal a reális napi limitek megfelelő beállítása. A gyors, akár két-három percen belül végrehajtott készpénz felvételi tranzakciók, vagy internetes vásárlások ellen a legjobb megoldás az ésszerű kártyalimitek megadása, melyet alkalmanként lehetőség van egy telefonhívással, akár időlegesen is módosítani.
- A számlakivonatokat rendszeresen ellenőrizze.
  A kártyás visszaélések körében egyre gyakoribbak a kis összegű, nem feltűnő költések, melyek gyakran elbújnak a folyamatos kártyahasználat által generált tranzakciós tömegben. A számlakivonat mellett ezért javasoljuk ügyfeleink számára SMS szolgáltatás beállítását is a kártyához, hogy azonnal értesülhessenek a csalárd tranzakciókról.
- A vásárlás során kapott nyomtatott bizonylatot mindig őrizze meg legalább 15 napig, hogy az esetleges dupla, vagy téves elszámolásokból eredő reklamációkat gyorsan le tudják a bankok kezelni.

2. Tanácsok az egyes visszaélés típusok megelőzéséhez

a. ATM készpénz felvétel során

- Ügyeljen arra, hogy a PIN kód beütéskor mindig takarva legyen, ne csak az ön mögött sorban állók elől, hanem az esetlegesen ATM-re szerelt kamera elől is.
- Harmadik fél segítségét ne fogadja el készpénz felvételhez.
  A kártyát ne adja ki ismeretlennek, ne felejtse, hogy tranzakció lebonyolításához mindössze a kártyán lévő három azonosító adatra van szükség.
- Amennyiben az ATM-en a kártyanyílás környékén, az ATM terület beléptetőjénél, vagy bárhol máshol mozgó, laza alkatrészt vél fölfedezni, kérjük, jelezze az üzemeltető banknak, és

ne használja az automatát, mert előfordulhat, hogy kártyamásoló fölszerelésének következményével van dolga.

b. Személyes vásárlás esetén

- A PIN kódot mindig takarja beütéskor.
- A kártya sose kerüljön ki a látóköréből.
  Éttermi, szállodai, egyéb vásárlások esetén a kiszolgáló nem viheti el a kártyát hátsó helyiségbe, a legtöbb kereskedő ezt a helyzetet mobil terminál használatával orvosolja.
- A bankkártya terminálnak mindig összeköttetésben kell lennie pénztárgéppel, és PIN kódos vásárlás esetén azonnal bizonylatot kell nyomtatnia, egyéb esetben a tranzakció nem jön létre.

c. Internetes vásárlás esetén

- Legfontosabb, hogy megfelelő licenszekkel rendelkező kereskedőnek adja csak meg a kártyaadatait.
- A legtöbb kereskedő fizetéshez erre alkalmas, biztonságos adatforgalmat bonyolító szolgáltató honlapjára irányít el. Ezek közül példa: Bankok titkosított weboldalai, a Paypal fizetési felülete.
- Amennyiben a kártyaadatainkat olyan weboldalon kívánjuk megadni, melyhez eddig nem volt közünk, és nem használ a vásárlás lebonyolításához közvetítőt, vegyük a fáradtságot, hogy 15 perces kutatással bizonyosodjunk meg a kereskedő jóhiszeműségéről.
- Vásárlás előtt mindig olvassa el a kereskedő üzletszabályzatát, hogy elkerülhetőek legyenek az esetleges próbaidős szolgáltatás igénybevétele utáni havi rendszeres levonások a bankkártyáról.
- Kártyaadatainkat ne jegyeztessük meg a böngészőnkkel, valamint ne kezdeményezzünk vásárlást kölcsön számítógépről, vagy nyilvános hálózatról.
- A vásárlás után a kereskedő köteles visszaigazoló elektronikus számlát küldeni, mely az ő részéről is igazolja a tranzakció sikerességét.

3. Adathalászat

Az internetes világban egyre gyakoribbak az ügyfeleket e-mailen keresztül megkereső csalók, akik személyes- vagy bankkártya adatszerzés reményében lépnek kapcsolatba a különböző szolgáltatók ügyfeleivel.
Bár ezek a megkeresések egyre kifinomultabbak, a lent felsorolt, egy vagy több csalásra utaló jel mindegyikben megtalálható:

- A küldő e-mail címének domainje (a "@" jel és a "." között található), kiterjesztése (a "." utáni lezáró karakterek) nem egyezik a szolgáltató által használt formával. Például: no-reply@sberbanca.com.
  A Sberbank Magyarország kizárólag a sberbank.hu domaint használja ügyfél kapcsolattartásra.
- A levélben a címzett ügyfél nincs név szerint megszólítva.
  Amennyiben hivatalos, automata rendszer által létrehozott üzenetünk érkezik, a szolgáltató a saját adatbázisát használva építi föl azt, vagyis a regisztráció során megadott adatainkat – valós nevünket, becenevünket – fogjuk viszont látni.
- A csalók többféle módon próbálhatják kicsikarni belőlünk a megszerezni kívánt információkat, ennek egyik leggyakoribb formája, hogy egy általuk üzemeltetett, az eredetihez külsőleg nagyon hasonló, de hamis weboldalra irányítanak el bennünket, ahol adategyeztetés címén kérik el tőlünk személyes- vagy kártya adatainkat.

Ebben az esetben a kapott üzenetben megjelenik egy hivatkozás, mely az említett weboldalra mutat. Ha egerünket a link fölé húzzuk, a legtöbb böngésző kattintás nélkül, az ablak bal alsó sarkában megjeleníti a meglátogatni kívánt oldal elérhetőségét. Amennyiben az így kijelzett cím nem egyezik a szolgáltató weboldalával, semmilyen körülmények között ne látogassuk meg azt.

- A szolgáltatók soha, semmilyen esetben nem kérik ügyfeleik jelszavait, azonosítóit, azok módosítását kizárólag az ügyfelek kezdeményezik.
  A szolgáltatók ezen kívül soha nem kérnek az ügyfelek vásárlási szándéka nélkül bankkártya adatokat sem, így amennyiben ön nem kíván fizetni a kártyájával, annak adatait semmilyen esetben, sehova ne adja ki.
- Amennyiben gyanús e-mail érkezik fiókjába, kérjük, vegye fel a kapcsolatot azzal a szolgáltatóval, akinek a nevében az üzenet érkezett hivatalos honlapján keresztül.
- Ha a Sberbank csoport nevében érkezne az ön részére hasonló megkeresés, kérjük, azt továbbítsa részünkre az info@sberbank.hu címre.

4. További fontos információk

A bankkártya tiltás ügyfeleink érdeke is, a kártyáját mindig használja felelősséggel és odafigyeléssel. Elmaradt kártyatiltási kérelemből eredő károkért a bank nem vállal felelősséget.

Bankkártyát tiltani a hét minden napján, 0-24 óráig lehetséges, hétköznapokon 8-20 óráig, hétvégén 9-16 óráig a Sberbank Telebankon keresztül a 06 40 41 42 43-as, valamint munkaidőn kívül a SIA Central Europe Zrt. 06 1 421 22 99-es telefonszámát tárcsázva.

A bank semmilyen formában nem fogja kérni ügyfelei azonosító kódjait, beleértve a kártya PIN-t, a CVC kódot, a Sberbank Online Banking bejelentkezési kódot, valamint a négyjegyű (TPIN1) és a nyolcjegyű (TPIN2) Sberbank Telebank azonosítót is.

A bank adatfrissítéseket, személyes adat egyeztetéseket kizárólag bankfiókban végez.

Személyes adatait banktól független elektronikus csatornán ne adja ki.

Ha a bank nevében eljáró ismeretlen személy keresi meg személyes adatait kérve, haladéktalanul lépjen kapcsolatba ügyfélszolgálatunkkal.

Sberbank Magyarország Zrt.

2015. október 7.