forrás: https://kiberpajzs.hu/ kép internet

HAMIS TRANZAKCIÓK JÓVÁHAGYÁSA

A bankok az online belépéshez és a tranzakciók jóváhagyásához kétlépcsős hitelesítést követelnek meg, az ügyfélnek a jelszón kívül egy másik módon is azonosítani kell magát. Ez az azonosítás történhet az ügyfél birtokában lévő kódgenerátorral, az ún. tokennel, amely a sorozatszámától és a használat időpontjától függően egy egyszer felhasználható, rövid ideig (1-2 perc) érvényes kódot szolgáltat, vagy az ügyfél által megadott telefonszámra érkező SMS-ben szereplő szám megadásával. Előfordulhat azonban olyan eset is, amikor a másodlagos hitelesítéshez elégséges csak a telefonon megjelenő felugró gombot megnyomni, vagy az ujjlenyomat-olvasóhoz hozzáilleszteni az ujjat. Ezek a jóváhagyási kérelmek megjelenhetnek az ügyfél telefonján akkor is, ha nem személyesen maga az ügyfél, hanem a bankszámlája felett rendelkező más személy kezdeményezte a belépést vagy a tranzakciót. Ha egy csaló próbál belépni vagy hamis tranzakciót indítani, az ügyfélnek ugyanúgy meg kell adnia a másodlagos hitelesítési adatokat ahhoz, hogy a belépés vagy a tranzakció sikeres legyen.

Mit tegyen, ha hamis azonosítási folyamatot észlel?

- Mindig ellenőrizze, hogy a belépési kísérletet vagy a tranzakciót, melyet jóvá akar hagyni, valóban Ön, vagy az Ön által megbízott személy kezdeményezte! Sose hagyjon jóvá ismertlen kérést!
- A kapott jóváhagyó SMS-ben ellenőrizze a jóváhagyásra váró műveletet, az összeget és a címzettet, ha szerepel benne!
- A banki műveletek jóváhagyásához használt tokent sose hagyja felügyelet nélkül!
- Használjon a mobiltelefonján képernyőzárat!
- Csak saját ujjlenyomatait regisztrálja a telefonjába!
- Állítsa be úgy a mobiltelefonját, hogy az SMS-ben kapott üzenetek tartalma csak a képernyőzár feloldása után legyen látható!