

## Telefonos csalás

A megtévesztésen alapuló telefonhívások közös jellemzője, hogy az ismeretlen csalók személyes adatokat és/ vagy a számítógéphez, mobiltelefonhoz való hozzáférést próbálnak megszerezni. A csalók általában egy bank vagy szervezet dolgozójának adják ki magukat, és igyekeznek elhíttetni a felhasználóval, hogy valamely pénzügyi tranzakció során hiba lépett fel vagy csalás gyanúja merült fel, emiatt keresik az érintett személyt.

Általában nem rendelkeznek hivatalos ügyféladatbázissal, ezért véletlenszerűen célozzák hívásaikat, amelyek során ismeretlen vagy rejtett telefonszámról bonyolítják a telefonhívásokat. A hívás során a telefonáló „munkatárs” olyan hamis dolgokra hivatkozik, hogy például egy gyanús tranzakciót észlelt a bank, és ezért az ügyfél számláján lévő összeget biztonságba kell helyezni, amihez átmozgatás, egy ún. „biztonsági számlára történő átutalás” szükséges. A megkeresés során gyakran szoftver vagy alkalmazás letöltésére szólítják fel az ügyfelet, ezáltal igyekeznek távoli elérést lehetővé tevő alkalmazást letölteni az ügyféllel (pl. Anydesk, Teamviewer) azzal az indokkal, hogy ez egy biztonsági program. Kérjük, amennyiben idegenek bármilyen program letöltésére vonatkozó felkérésével találkozik akár telefonon, személyesen vagy e-mailben, a kérést hagyja figyelmen kívül.

**A Magyar Államkincstár egyetlen esetben sem kért, és a jövőben sem fog olyat kérni az ügyfeleitől, hogy egyedi programokat telepítsenek a gépükre szóban elhangzott utasítások alapján.**

A Magyar Államkincstár egyetlen esetben sem kér telefonon olyan információkat, melyek az ügyfelek más banknál vezetett számláira, azok egyenlegére vagy konkrét tranzakcióira vonatkoznak. A Kincstár Központi Ügyfélszolgálatának (a továbbiakban: „Call Center”) munkatársai be nem azonosított ügyfelek részére specifikus adatokat, értékpapírtitoknak minősülő információkat (például adott számlára vonatkozó értékpapír-állomány, esedékességfizetések) nem adnak ki, kizárólag általános tájékoztatást nyújthatnak. A Call Center munkatársai személyes adatot, vagy a számlával kapcsolatos információt kizárólag abban az esetben szolgáltatnak ki, amennyiben az ügyfél-azonosítási folyamat teljeskörűen és sikeresen lezajlott. Jelszóval történő azonosítást követően az automata rendszer által szolgáltatott, ügyfélhez kötött információk, illetve tranzakciók is elérhetők. Tájékoztatjuk, hogy a [TeleKincstár szolgáltatás](#) a Kincstár bármely [állampapír-forgalmazó ügyfélszolgálatán](#), egyszeri személyes megjelenés során igényelhető díjmentesen.

Az Ön biztonságát szem előtt tartva és annak érdekében, hogy naprakészen kövesse számláját, javasoljuk az alábbi lépések megtételét:

- a MobilKincstár alkalmazásban engedélyezze az értesítések küldését
- ellenőrizze számlája egyenlegét és tranzakcióit gyakrabban a WebKincstár és MobilKincstár felületen, valamint a letölthető kivonatokon.

Amennyiben úgy ítéli meg, hogy a fentiekben részletezett adathalász kísérlet miatt a jelenlegi jelszó módosítása szükséges, úgy jelszavát a következő módok egyikével változtathatja meg:

- személyesen bármely állampapír-forgalmazó ügyfélszolgálaton,
- személyes megjelenés nélkül a Call Centeren ügyintéző segítségével, TeleKincstáron jogosultság birtokában ,
- valamint a WebKincstár és MobilKincstár bejelentkező ablakában található „Teendők új jelszó igénylése esetén” funkció használatával.

Biztonsága érdekében a WebKincstár és a MobilKincstár felületre történő belépéshez szükséges jelszó több kritériumnak is meg kell felelnie, melyek a kiemelt biztonságot szolgálják:

- Hossza minimum 8, maximum 16 karakter lehet;
- Numerikus és ékezet nélküli kis és nagy alfabetikus karaktereket használhat;
- Tartalmaznia kell legalább egy számjegyet, illetve négy betűt;
- Az új jelszó nem egyezhet meg az utolsó három jelszavával;
- A jelszó nem tartalmazhat speciális karaktereket. (pl. @#./\_)

A számítógépeken és a mobilkészülékeken csak megbízható vezeték nélküli internethálózat használata javasolt. Fontos, hogy a készülékekre csak megbízható helyekről és fejlesztőktől, legálisan történjen az alkalmazások letöltése. Javasoljuk biztonsági szoftverek és szolgáltatások használatát, valamint biztonsági mentések rendszeres készítését. Ezekről a készülék gyártójától, szervizétől vagy a mobilszolgáltatótól van lehetőség információt kérni.