Hogyan bankoljunk biztonságosan az interneten?

A Takarékbank vigyáz ügyfeleire, ezért számos biztonsági intézkedést hajt végre annak érdekében, hogy Ön nyugodtan használhassa elektronikus csatornáinkat. Annak érdekében, hogy a kockázatokat minimálisra csökkentsük Önre is szükség van!

Az alábbiakban összegyűjtöttük azokat a legfontosabb tanácsokat, amelyek betartásával jelentősen csökkenthetők az elektronikus bankolás kiberbiztonsági kockázatai.

1. Biztonságos jelszókezelés
- Belépéshez szükséges jelszavát soha ne ossza meg senkivel!
- Semmilyen formában ne jegyezze fel (pl.: post-it)!
- Rendeszeresen változtassa meg jelszavát!
- Jelszava ne legyen személyéhez kötött vagy könnyen kitalálható. Lehetőleg min. 12 karakterből álljon és tartalmazzon különböző speciális karaktereket (@&!), számokat (123), valamint nagy betűket (ABC) is!

2. Internetes bankolás
- Ne használjon nyilvánosan elérhető wifi hálózatot bankolásra még akkor sem, ha a wifi hálózat titkosított.
- Internet banki alkalmazásának linkjét mentse el böngészőjének kedvencei közé és mindig onnan nyissa meg.
- Bejelentkezéskor sose engedélyezze a böngészőnek, hogy megjegyezze a beírt azonosítót, számlaszámot és jelszót!
- Állítsa be, hogy minden egyes tranzakció végrehajtását jelszóval kelljen megerősíteni!
- Ha befejezte az internetbank használatát, akkor használja az internetbank menüjében található „Kilépés” funkciót, a böngésző ablakát csak ezután zárja be!

3. Informatikai eszközeinek védelme
- Engedje, hogy eszközei automatikusan frissítsék magukat! Amennyiben a frissítés nem automatikus, a program utasításait követve végezze el a frissítést.
- Vírusfertőzésekkel és betörési kísérletekkel szemben védje meg magát és számítógépét tűzfalakkal és víruskeresőkkel. Alkalmazzon mobiltelefonjára is védelmi megoldásokat.
- Bizalmas adatokat (belépési jelszó, azonosító, bankszámlaszám) ne tároljon informatikai eszközén!
- Ha eszközét ellopták vagy elveszítette, mielőbb változtassa meg az internetbank belépéséhez használt jelszavát!
- A Banktól érkezett SMS-eket olvasás után törölje mobiltelefonjáról!

4. Videobankolás információbiztonsági szempontból
- Videóhívás esetén fokozottan ügyeljen, hogy az elhangzott információk és a készüléken látható információk ne juthassanak illetéktelen személyek tudomására.
- Videóhívás esetén saját informatikai eszközeit használja (pl.: mobiltelefon, laptop).
- Javasoljuk, hogy a videobank linkjét (www.videobank.takarekbank.hu) mentse el böngészője kedvencei közé és mindig onnan nyissa meg.