

BIZTONSÁGI TÁJÉKOZTATÓ ELEKTRONIKUS BANKI SZOLGÁLTATÁSOK HASZNÁLATÁHOZ

A Bakonyvidéke Takarékszövetkezet (továbbiakban: Takarékszövetkezet) által ügyfelei részére a számlavezetési szolgáltatások kiegészítéseként nyújtott internetes banki szolgáltatások (a továbbiakban szolgáltatások) tekintetében az alábbi biztonsági tájékoztatást nyújtja:

I. Alapvető információk

1. Az interneten keresztül, informatikai eszközök segítségével igénybe vett banki, pénzügyi szolgáltatások a technológiából adódóan olyan speciális, a hagyományos banki szolgáltatások esetén ismeretlen kockázatokkal és veszélyekkel jár, amikre mind a szolgáltatónak (jelen esetben a Takarékszövetkezetnek) mind pedig a szolgáltatás felhasználójának (tehát Önnek) fel kell készülni.
2. A szükséges biztonsági intézkedések rá háruló részét a Takarékszövetkezet a saját hatáskörében megteszi, minden ésszerű technikai és adminisztratív védelmi eszközt felhasználva.
3. A szolgáltatás biztonságos használatához azonban Önnek, mint a szolgáltatás felhasználójának is be kell tartania néhány alapvető szabályt.

II. Azonosítók és jelszavak kezelése

1. A szolgáltatás használatát lehetővé tévő jelszavát Önnek titkosan kell kezelnie.
2. A kezdeti jelszót (amit a Takarékszövetkezet állít be) az első bejelentkezés után meg kell változtatnia, ettől a ponttól kezdve a jelszót csak Ön ismerheti.
3. A jelszóval kapcsolatban minden körülmények között tartsa be az alábbi előírásokat:
 - a. NE írja fel sehová
 - b. NE árulja el másnak
4. Az Ön jelszavát még a Takarékszövetkezet dolgozói sem ismerhetik meg: a Takarékszövetkezet dolgozóinak még hibaelhárítás céljából sincs szüksége az Ön jelszavára, ezért ne árulja el a jelszót senkinek, aki esetleg a Takarékszövetkezet (vagy valamely informatikai szolgáltatója) nevében azt Öntől kéri.

III. A szolgáltatás használata

1. A szolgáltatást a Takarékszövetkezet a mindenkor érvényes internetes banki szolgáltatásokról szóló hirdetményében meghatározott internetes címen nyújtja.
2. Ügyeljen arra, hogy minden esetben pontosan ezen az internetes címen keresse a szolgáltatást. Ennek érdekében javasoljuk, hogy azon a számítógépen, amin a szolgáltatást szokásosan igénybe veszi, mentse el a böngészőprogramjának „Könyvjelző” funkciójával, és onnan használja.
3. Gondoskodjon arról, hogy a számítógépén folyamatosan fussanak azok a védelmi programok, amelyek együttesen alkalmasak arra, hogy számítógépét megvédjék mindazoktól a támadásoktól (vírusok, billentyűzet-figyelő és egyéb kártékony

programok, hackerek), amelyekkel illetéktelenek megszerezhetik a bankszámla feletti hozzáférést.

4. A szükséges védelmi programok:
 - a. vírusvédelmi rendszer
 - b. tűzfal
5. Gondoskodnia kell arról is, hogy a védelmi programoknak mindig a legfrissebb verziója, továbbá a legfrissebb védelmi adatbázisa legyen a számítógépen, ellenkező esetben a számítógép védtelen marad a napi gyakorisággal megjelenő legújabb vírusokkal, illetve támadási módokkal szemben.
6. Ne használja a szolgáltatást olyan idegen számítógépen, amellyel kapcsolatban a legkisebb gyanú is felmerül, hogy esetleg nem rendelkezik az előbbieken ismertetett védelmi funkciókkal.
7. Ilyen „megbízhatatlan” számítógépnek kell tekinteni különösen a nyilvános internet hozzáférési pontokat, internet kávézókat. Ezek használata mindenképpen kerülendő.
8. Még a saját számítógépen indított böngészőben is tiltsa le a jelszavak megjegyzésének funkcióját.

IV. Tipikus veszélyek és megelőzésük

1. A visszaélés kísérletek mindegyike valamilyen úton-módon arra törekszik, hogy az Ön hozzáférési lehetőségét (azonosító, jelszó, SMS-kód) megszerezze. Ennek többféle módja van.
2. Az egyik lehetséges módszer szerint a védtelen számítógépen észrevétlenül futó program „megjegyzi” az Ön által felkeresett internetes oldalak (így az internetes banki szolgáltatás) internetes címét, továbbá minden egyes leütött billentyűt, majd ezeket – szintén észrevétlenül – interneten keresztül a csalókhoz továbbítja. Erre a problémára adnak megoldást az előbbi fejezet szerinti védelmi programok.
3. Egy másik tipikus visszaélési módszer, hogy a csalók – például a „phising”, azaz „adathalászat” néven ismert félrevezető e-mailt, illetve az abban található hamis linket használva – egy másik, hamisított internetes oldalra irányítják a felhasználót. Az ilyen hamisított oldalak a megtévesztésig hasonlítanak a Takarékszövetkezet által működtetett valódi oldalhoz, de csak a nyitóoldalon: egyetlen céljuk ugyanis, hogy az odacsalt felhasználó ott adja meg felhasználói azonosítóját és jelszavát, ami ezzel a csalók kezébe kerül.
4. Az adathalászok, illetve általában a hamisított internetes oldal ellen az alábbi szabályok betartásával tud hatékonyan védekezni:
 - a. a szolgáltatást mindig a böngésző „Könyvjelző” funkciójával mentett internetes címen használja
 - b. semmilyen körülmények között nem indítja el a szolgáltatást email üzenetben kapott linkre kattintva.
5. Nagyon fontos, hogy Ön tisztában legyen vele: a Takarékszövetkezet soha nem fog ilyen tartalmú e-mailt küldeni Önnek. Ha mégis ilyen e-mailt kap, az akkor is hamisított (és csalási kísérlet), ha az minden látható részletében a Takarékszövetkezettől származó e-mailnek tűnik.

6. Semmilyen technikai védelmi funkció nem véd azonban az emberi fegyelmezetlenségből eredő veszélyektől. Egyetlen perc alatt is visszafordíthatatlan visszaélésre ad Ön alkalmat, ha például a jelszót monitorra ragasztott cetlin „tárolja” és a mobilját az íróasztalon felejtve kiugrik egy cigarettára, egy kávéra, a mosdóba ... Mire visszajön a helyére, akár a számlán lévő összes pénzt is átutalták, mégpedig az Ön „nevében”, tehát az Ön felelősségére.
7. Ne tegye lehetővé, hogy csalás áldozatává váljon! Tartsa be ezeket a szabályokat, hogy biztonságosan tudja használni az internetes banki szolgáltatásokat!
8. Ha bármilyen visszaélési, csalási kísérletre gyanakszik, vagy „adathalász” e-mailt kapott, értesítse a Takarékszövetkezetet!

Bakonyvidéke Takarékszövetkezet