

„AZ INTERNETES BANKI, BIZTOSÍTÁSI ÉS BEFEKTETÉSI SZOLGÁLTATÁSOK IGÉNYBEVÉTELÉRE A SZOLGÁLTATÓVAL SZERZŐDÉST KELL KÖTNI.”

„JEGYEZD MEG: A BANK SOHA NEM KÉRI EL AZ ÜGYFÉL TITKOS ADATAIT E-MAILBEN!”

A rovat a



PÉNZÜGYI SZERVEZETEK
ÁLLAMI FELÜGYELETE

támogatásával készült

Irány az internetbank!

ÜGYE A SORBANÁLLÁS BENNE VAN ABBAN AZ ÖT DOLOGBAN, AMIT A LEGJOBBAN UTÁLSZ? MIÉRT PONT A BANKI ÜGYINTÉZÉS MIATT FECSÉRELNÉD AZ IDŐDÉT VÁRAKOZÁSSAL, MIKÖZBEN A BANKSZÁMLÁKHOZ KAPCSOLÓDÓ ELEKTRONIKUS ÉS TELEFONOS SZOLGÁLTATÁSOK SEGÍTSÉGÉVEL SZINTE MINDEN BANKI ÜGYEDET ELINTÉZHETSZ, AMIT NAP, MINT NAP HASZNÁLSZ. KIVÉTELT CSAK A KÉSZPÉNZES TRANZAKCIÓK JELENTENEK.

A szolgáltatásokról

Az internetbanki szolgáltatások lehetőséget nyújtanak a számlaegyenleged lekérdezésére, átutalásra, betétlekötésre, vagy betétfelbontásra, bankkártyához kapcsolódó limitek módosítására, bankkártya vagy hitel igénylésére, mobiltelefonod feltöltésére és befektetések kezelésére, valamint vásárlásra és számos más banki szolgáltatásra. Ezekről tájékozódhatsz a PSZÁF fogyasztóknak szóló honlapján www.pszaf.hu és az egyes szolgáltatóknál is. Az internetes banki, biztosítási és befektetési szolgáltatások igénybevételére a szolgáltatóval szerződést kell kötni. Ha ez megtörtént, a legtöbb banki szolgáltatást bárhol, bármikor intézheted, a bank a beküldött megbízásokat úgy kezeli, mintha személyesen adtad volna le, csak például átutalások esetén általában kisebb díjat számol fel.

A netbank biztonságos?

Az internet, mint pénzügyi szolgáltatási csatorna jól működik, de sokakat elbizonytalanítanak az adatmólosról, adathalásztól származó hírek. Az elektronikus banki szolgáltatások biztonsága érdekében a szolgáltatók folyamatosan fejlesztenek, és többszintű védelmi rendszereket építenek ki. Az alább bemutatjuk a leggyakrabban használt és rendszerint egymással kombinált biztonsági megoldásokat. **Az SSL (Secure Socket Layer):** biztonsági protokoll, melynek segítségével titko-

sított csatornán keresztül biztonságos összeköttetés teremthető a kommunikációban résztvevő számítógépek (a te géped és a bank rendszere) között. Az SSL csak az átviteli csatorna biztonságáról gondoskodik, a felek azonosításáról azonban nem. **A többszintű azonosítási rendszer:** meg kell adnod külön a felhasználó nevedet, a jelszavad, a bankszámlaszámot és további biztonsági kódot, amelyek mindegyike egy-egy szintet jelent. **Többcsatornás rendszer:** a biztonság magasabb foka, ahol nem csak a számítógépen,

számra. A token a számítógéptől teljesen független, véletlen számgeneráló szerkezet, amelyet külön PIN-kód véd. Ennek beírását követően tudod meg az internetes belépéshez szükséges, aktuális azonosító számot.) A bank figyeli az azonosítási, illetve belépési próbálkozások számát, és meghatározott sikertelen próbálkozás – általában 3-5 – után kitiltja a felhasználót a rendszerből. Ez nem csak az illetéktelen behatolókra vonatkozik, hanem akár téged is kitilthat a rendszerből, ha az azonosítót véletlenül többször is elírod).

„AZ ELEKTRONIKUS BANKI SZOLGÁLTATÁSOK BIZTOSÁGA ÉRDEKÉBEN A SZOLGÁLTATÓK FOLYAMATOSAN FEJLESZTENEK, ÉS TÖBBSZINTŰ VEDELMI RENDSZEREKET ÉPÍTENEK KI.”

hanem egy másik eszközön is azonosítanod kell magad. (Ilyen az SMS értesítés; vagy az időablak funkció, amelyben egy előre megadott mobiltelefonszámról indított hívással 5-10-15 percig engedélyezi az aktív műveleteket a rendszeren belül, utána letilt. Bizonyos bankok egyszer használatos kódot küldenek egy előre egyeztetett mobiltelefon

Webkártya hasznos eszköz?

A **webkártyákat** kifejezetten online vásárlásra fejlesztettek ki. A vásárlás lebonyolítását megelőzően a webkártyát – amelyhez elkülönült kártyaszám tartozik – csak anynyi pénzzel szükséges és érdemes feltölteni, amennyit az online vásárláskor el kívánsz költeni. A webkártyával bonyolított vásárláskor kiküszöbölhető, hogy a bankkártya-számmal esetleg visszaéljenek. Erre a nap 24 órájában át tudsz tenni egy bizonyos összeget – praktikus, ha előbb megnézed, mennyi pénzt is szeretnél így elkölteni, és csak utána utalsz –, így amikor nem használod, nem kell rajta pénzt tartanod.

A te felelősséged is!

A biztonságos internet-bankolás részben a te felelősséged is, ezért neked is gondoskodnod kell bizonyos feltételekről. Fontos, hogy a számítógépeden legyen aktív tűzfal. A tűzfal az illetéktelen hálózati hozzáféréseket megakadályozó szoftveres vagy hardveres eszköz, amely a kommuni-



részéről küldött telefonos vagy e-mailes megkeresésben. Ez így kicsalt azonosítóval aztán belépnek az ügyfél internetbankjába, és onnan előre megszervezett számlákra utalják az ügyfél pénzt. **Jegyezd meg: a bank SOHA nem kéri el az ügyfél titkos adatait e-mailben!**

kor emelsz fel, ha szükség van rá! Növeli a biztonságot az SMS-szolgáltatás, s talán mondanunk sem kell: soha ne tartsd felírva a kódjaidat, azonosítót!

A telebank és a mobilbank

A pénzintézetek nemcsak az interneten, hanem telefonon és mobilon keresztül is fogadják a megkereséseket automata telefonszolgálat, illetve ügyintézők segítségével. Itt kérhetsz általános tájékoztatást, lekérheted a számlaegyenlegedet és a tranzakciókat, de különböző megbízásokat is adhatsz. A telefonon történő megbízás egyedi tranzakciós kód alapján történik, ez az ügyletet biztonságossá teszi, illetve annak hitelességét igazolja. Ügyfelei számára a legtöbb pénzintézet magát a telebanking szolgáltatást díjtalanul nyújtja, de természetesen az ezen keresztül végzett ügyletekre vonatkozóan a bank díjat számol fel. A mobilbanki alkalmazások Európa-szerte nem túl elterjedtek, ugyanakkor a mobilod komoly biztonsági eszközként működhet. Kérhetsz rá egyenleget tartalmazó SMS-t, és a vásárlásokról is kaphatsz külön üzenetet.

káció folyamatába beépülve figyeli és szabályozza az átáramló forgalmat. Fontos, hogy a gépedre vírusirtó program is legyen telepítve. A vírusirtó vagy antivírus program célja annak biztosítása, hogy a hálózatba vagy egy adott számítógépbe ne juthasson be olyan állomány, mely károkozást, illetéktelen adatgyűjtést, vagy olyan műveletet hajt végre, amely veszélyezteti az internetes banki alkalmazások biztonságát. A vírusirtó programok ma már nem drágák, sőt sok ingyenesen használható is letölthető a netről. És a biztonságos bankoláson kívül is hasznosak a mindennapi számítógép-használat során. Az illetéktelen behatolókkal szemben védelmet jelenthet, ha számítógépedhez belépéshez jelszót használsz, amit időként megváltoztatatsz.

„FONTOS, HOGY A GÉPEDE VÍRUSIRTÓ PROGRAM IS LEGYEN TELEPÍTVE.”

Más csalogó olyan weblapokat készítenek, amelyek megszólalásig hasonlítanak a bankéra, és ott kérik a jelszavakat. Ezért, ha netbankolni szeretnél, sose kövess maillben kapott linket, hanem közvetlenül keresd fel a bank weboldalát!

Bárhon, bármikor – biztonságosan

Az internetbanki szolgáltatások nagy előnye, hogy nem csak otthon használhatod őket: akár egy vizsga után is lekérdezheted az egyenlegedet az egyetem számítógép-termében. Ha épp vakáció közben derül ki, hogy nem fizetted be egy számlát, akkor azt akár egy külföldi városból is megteheted. Egyes bankok chipkártyás azonosítással teszik biztonságosabbá a rendszert, ha neked is ilyen van és elutazásod alatt is bankolni szeretnél, akkor a kártyaolvasót is csomagoldd be. Vigyázz, hogy amikor nyilvános helyen be-

lépsz, senki ne láthassa a jelszavadat! Ügyelj arra is, hogy a gép, amin használod, ne futtasson adathalász programokat. Internet-kávézóban például mindig indítsd újra a gépet, mielőtt belépsz az internetbankba. Ha sokat használod a netes szolgáltatásokat nyilvános helyről, állíts be alacsony limitet, amelyet csak ak-

