A következőkben tájékoztatni szeretnénk Tisztelt Ügyfeleinket a manapság gyakran Magyarországon és külföldön is előforduló **adathasználat** veszélyeiről, formáiról.

Ügyfeleink adatainak biztonsága, illetve azok védelme különösen fontos számunkra, ezért szeretnénk figyelmeztetni, hogy manapság egyre többen esnek az adathalász e-mailek csapdájába, ami bizalmas személyes-, illetve kártya adatok illetéktelen kezekbe kerülését eredményezheti.

Habár ezek az adathalászok egyre kifinomultabb módszerekkel próbálják adatainkat kicsalni, az alábbi jelekre való odafigyeléssel ez megelőzhető:

- Ezen e-mailek domainje (a "@" és a "." közötti szöveg), és/vagy kiterjesztése (a "." jelet követő néhány karakter) általában hasonlít, de soha sem egyezik a szolgáltató eredeti e-mail címével. Ilyen megtévesztő hamis e-mail cím lehet például: noreply@sberbanc.com
  A Sberbank Magyarország kizárólag a sberbank.hu domaint használja ügyfél kapcsolattartásra!
- Az ilyen adathalász levelekben az ügyfél gyakran nincs név szerint megszólítva. Ha viszont hivatalos, szolgáltatótól származó levelet kap, abban mindig a szolgáltató adatbázisában szereplő valós nevét fogja látni.
- A csalók többféle módon próbálhatják megszerezni a számukra fontos információkat, ennek egyik leggyakoribb formája, hogy egy általuk üzemeltetett, az eredetihez külsőleg nagyon hasonló, de hamis weboldalra irányítják át a címzettet, ahol adategyeztetés címén kérik el Öntől személyes- vagy kártya adatait. Ebben az esetben a kapott üzenetben megjelenik egy hivatkozás, mely az említett weboldalra mutat. Ha egerét a link fölé húzza, a legtöbb böngésző kattintás nélkül, az ablak bal alsó sarkában megjeleníti a meglátogatni kívánt oldal elérhetőségét. Amennyiben az így kijelzett cím nem egyezik a szolgáltató weboldalával, semmilyen körülmények között ne látogassa meg azt!
- A szolgáltatók soha, semmilyen esetben nem kérik ügyfeleik jelszavait, azonosítóit, azok módosítását kizárólag az ügyfelek kezdeményezik. Valamint, a szolgáltatók soha nem kérnek az ügyfelek vásárlási szándéka nélkül bankkártya adatokat sem (például lejárati idő, CVC/CVV kód), így amennyiben Ön nem kíván fizetni a kártyájával, annak adatait semmilyen esetben ne adja ki.
- Amennyiben gyanús e-mail érkezik fiókjába, kérjük, vegye fel a kapcsolatot azzal a szolgáltatóval, akinek a nevében az üzenet érkezett hivatalos honlapján keresztül.
- Ha a Sberbank csoport nevében érkezne az Ön részére hasonló levél, kérjük, azt továbbítsa részünkre az info@sberbank.hu címre.

Sberbank Magyarország Zrt.

2018. február 13.

We would like to kindly inform our clients about the dangers and forms of **phishing,** which became a common issue nowadays both in Hungary and abroad.

The safety of our clients' personal data is a top priority for us, and that is why we would like to warn everyone about the increasing number of phishing victims. Believing these harmful e-mails may result in information about the client and details of his/her debit card getting into the wrong hands.

Although these swindlers are using more and more sophisticated ways to get their hands on our private data, paying attention to the details below can help us prevent their success:

- The domain of these e-mails (the text between the "@" and "." signs), and/or their extension (the characters following the "." sign) are usually similar, but never exactly the same as in the official e-mail address of the service provider. Such fake address could be: noreply@sberbanc.com
  Sberbank Magyarország uses only the sberbank.hu domain to keep in touch with the clients.
- You cannot see your full real name in these phishing e-mails. When you get an official letter from your true service provider however, your name as it is in their database, will always appear in the text.
- These criminals will most likely try more than one way to get your private information, and a common way of doing this is by redirecting you to one of their websites, which looks much like the original webpage of your service provider. There they will ask for your personal information or for the details of your card. In these e-mails there is always a URL link to their website. If you hover your mouse over this URL, most browsers will show you the real address of that page in the bottom left corner. If that address does not match the original one of your service provider, do NOT visit that website!
- A real service provider will never ask for passwords or account IDs, and modifying these can only be initiated by the client. Furthermore, they never ask for the details of the client's card (e.g. expiry date, CVC/CVV code), unless the client wants to purchase something with it. So if you do not intend to buy anything, do not provide the details of your card.
- If you were to receive a suspicious e-mail, please contact the service provider, whose name was used in that e-mail.
- If you were to receive such an e-mail in the name of the Sberbank group, please contact us at info@sberbank.hu

Sberbank Magyarország Zrt.

13 February 2018