中国银行（中东欧）有限公司
BANK OF CHINA (CENTRAL AND EASTERN EUROPE) LIMITED

TÁJÉKOZTATÓ A MEGHATALMAZOTTI HOZZÁFÉRÉSEKHEZ KAPCSOLÓDÓ VISSZAÉLÉSEK MEGELŐZÉSÉRŐL

A pénzügyek rendezése mindinkább digitális útra terelődik, a visszaéléseknek pedig számos új formája jelent meg a digitális térben, így például a személyes hitelesítési és érzékeny fizetési adatok megszerzésén, majd ezek alapján fizetési megbízások jogosulatlan kezdeményezésén alapuló visszaélések, a megtévesztésen és pszichológiai manipuláción alapuló visszaélések – melyek során a fizető felet igyekeznek rábírni a fizetési megbízás kezdeményezésére, illetve a visszaélést elkövetők által kezdeményezett fizetési megbízások jóváhagyására –, valamint a fizető fél birtokában lévő készpénz-helyettesítő fizetési eszközhöz, például fizetési kártyához, mobilbankhoz vagy internetbankhoz történő közvetlen hozzáférésen alapuló visszaélések.

Az említett visszaélések járulékos kockázata, amikor az érintett ügyfél (meghatalmazott) elektronikus hozzáférésén, online felületein (például internetbank, mobilbank) keresztül további ügyfelek (meghatalmazó) fizetési számláihoz is hozzáférhetnek a csalók!

A csalók a kicsalt adatokkal olyan visszaéléseket követnek el, amellyel **könnyen jelentős anyagi károkat is okozhatnak áldozatuknak**. A csalások elkövetői egyre változatosabb és egyre nehezebben felismerhető módszereket találnak ki, ezért nagyon fontos **a legapróbb gyanús jelek felismerése** és a körültekintő viselkedés.

A fenti kockázatok megelőzésére és csökkentésére a Bank az alábbiakat javasolja az ügyfeleinek, ideértve a bankszámlák feletti meghatalmazottakat is:

- semmilyen esetben se telepítsenek olyan szoftvereket és applikációkat, amelyek az eszköz (telefon, tablet, számítógép) távoli irányítását teszik lehetővé.
- soha ne adjanak távoli hozzáférést a napi pénzügyekhez, bankolásra használt eszközeikhez.

INFORMATION GUIDE ON THE PREVENTION OF MISUSE OF PROXY ACCESS

As financial transactions are increasingly going digital, many new forms of fraud have emerged in the digital space, such as fraud based on obtaining personal authentication and sensitive payment data and then using these data to initiate unauthorised payment orders, fraud based on deception and psychological manipulation, whereby the payer is persuaded to initiate a payment order or to approve payment orders initiated by the perpetrators of the fraud, and fraud based on direct access to a cash substitute payment instrument in the payer's possession, such as a payment card, mobile bank or internet bank.

An additional risk of these abuses is that fraudsters may gain access to the payment accounts of other customers (authorised persons) via the electronic access or online interfaces (for example internet bank, mobile bank) of the customer (authorised representative) concerned!

Fraudsters use fraudulent data to commit abuses that can **easily cause significant financial damage** to their victims. The methods used by fraudsters are becoming **increasingly varied and difficult to detect**, so it is important to be aware of the smallest suspicious signs and to act with caution.

To prevent and mitigate the above risks, the Bank suggests the following to its customers, including the authorized persons over the bank accounts:

- never install software or applications that allow remote control of the device (phone, tablet, computer).
- never give remote access to your daily finances and banking devices.
- always install the latest available software updates immediately and take extra care to

- minden esetben azonnal telepítsék az újonnan elérhető, legújabb szoftverfrissítéseket, továbbá fokozott figyelemmel gondoskodjanak a kártékony kódok elleni védelem (vírusvédelem) telepítéséről.
- a Bank Mobile Banking applikációját minden esetben hivatalos webáruházból töltsék le. E-mailben kapott linken keresztül soha ne töltsék le a Bank applikációját!
- a Netbankot minden esetben a Bank hivatalos weboldaláról nyissák meg! E-mailben kapott linken keresztül soha ne lépjenek be a Netbankba!
- szoftvereket, illetve applikációkat csak megbízható helyről telepítsenek, ismeretlen vagy gyanús szoftverek telepítését minden esetben kerüljék!
- javasoljuk a napi munkához és a privát szférához használt eszközök (telefonok, tabletek, asztali gépek, etc.) elkülönítését.
- soha ne hagyják a Bank online felületeihez történő belépéshez szükséges E-token-t nem biztonságos helyen, és ne adják át azt harmadik, jogosulatlan személyek részére.
- figyelmesen olvassák el a banki SMS és push üzeneteket, az azokban megküldött kódokat senkinek ne adják ki!
- minden esetben gondoskodjanak az eszközön a vezeték nélküli hálózatok (Wi-Fi) biztonságáról. Javasoljuk Ügyfeleinknek, hogy kerüljék a nyilvános Wi-Fi hálózatokat, különösen akkor, ha az adott eszközt (telefon, tablet, stb.) napi bankoláshoz is, illetve bankoláskor használják.
- ne használjanak feltört operációs rendszert futtató mobilkészüléket (jailbreakelt vagy rootolt), mert a feltört operációs rendszer számos beépített biztonsági funkciót kiiktathat!
- ellenőrizzék rendszeresen az online fiókjaikat!
- ellenőrizzék rendszeresen bankszámlát és a bankszámlakivonatot, és a gyanús tevékenységekről haladéktalanul tegyenek bejelentést a Banknál.
- az interneten csak biztonságos webhelyeken fizessenek! Ellenőrizzék, hogy a webhely címének beírására szolgáló mezőben látható-e a ”lakat”, illetve figyeljenek arra, hogy a webcím eleje *https* legyen, és csak biztonságos kapcsolatot használjanak!
- figyeljenek arra, hogy a Bank soha nem kérdez olyan bizalmas információkat telefonon vagy e-mailben, mint az online fiók hitelesítő adatai

- install protection against malicious code (virus protection).
- always download the Bank's Mobile Banking Application from the official web store. Never download the Bank's Mobile Application via a link received by e-mail.
- always open Netbank from the official Bank website. Never access the Netbank via a link received by e-mail.
- software and applications should only be installed from trusted sources, and unknown or suspicious software should always be avoided.
- we suggest the separation of devices (phones, tablets, desktops, etc.) used for daily work and private use.
- never leave your E-token for accessing the Bank's online services in an unsecured place or give it to unauthorised third parties.
- carefully read the SMS and push messages sent by the Bank and do not give out the codes sent in them to anyone!
- always ensure that the wireless networks (Wi-Fi) on your device are secure. We advise our customers to avoid using public Wi-Fi networks, especially if the device (phone, tablet, etc.) is used for daily banking or when banking.
- software or applications should only be installed from trusted locations, and unknown or suspicious software should be avoided at all costs.
- do not use mobile devices running a hacked operating system (jailbroken or rooted), as a hacked operating system can disable many built-in security features!
- check your online accounts regularly!
- regularly check your bank account and bank statement and report suspicious activity to the Bank immediately.
- pay online only on secure sites! Make sure that the "padlock" is visible in the field for entering the website address, that the web address starts with https and that only secure connections are used.
- please note that the Bank will never ask for confidential information such as your online account credentials (username, password) by phone or e-mail. If you receive such a request, be suspicious and report it to the Bank as soon as possible.

(felhasználónév, jelszó). Ha ilyen jellegű felszólítást vagy kérést kapnak, gyanakodjanak, és mielőbb jelentsék azt a Banknak!

- ha azt gyanítják, hogy a fiók adatait csalónak adták meg, azonnal vegyék fel a kapcsolatot a Bankkal!
- ha megpróbálták megkárosítani, minden esetben tegyenek bejelentést a Banknál és a rendőrségen, még akkor is, ha a csalási kísérlet nem volt sikeres!

- if you suspect that your account details have been given to a fraudster, contact the Bank immediately!
- if an attempt has been made to defraud you, always report it to the Bank and the police, even if the attempt to defraud was not successful!

Amennyiben a fentiekkel kapcsolatosan bármilyen további kérdésük lenne, bizalommal forduljanak Bankunkhoz!

If you have any further questions regarding the above, please do not hesitate to contact our Bank.

Budapest, 2024. május 15.

Bank of China (CEE) Zrt.

Budapest, 15 May 2024

Bank of China (CEE) Ltd.