MIZUHO

PT Bank Mizuho Indonesia
Sinar Mas Land Plaza - Menara 2, 24th Floor
Jl. M.H. Thamrin No. 51 Jakarta 10350 - Indonesia
Tel : 62-21 392 5222 (hunting)
Fax. : 62-21-3926354
SWIFT : MHCCIDJA

12 August 2019

Dear Valued Client,

Recently, there have been reports on the occurrence of financial crimes called Business Email Compromise ("BEC"), where an offender who falsely represents himself/herself as an executive officer of a corporation or an overseas supplier requests funds to be remitted and ultimately defrauds the funds.

In order **to protect yourself from BEC**, please take due care and check that there are no suspicious elements when you conduct overseas remittance. PT. Bank Mizuho Indonesia ("BMI") advice our valued client to follow some of precautions or preventive measures to keep your accounts and transactions safe.

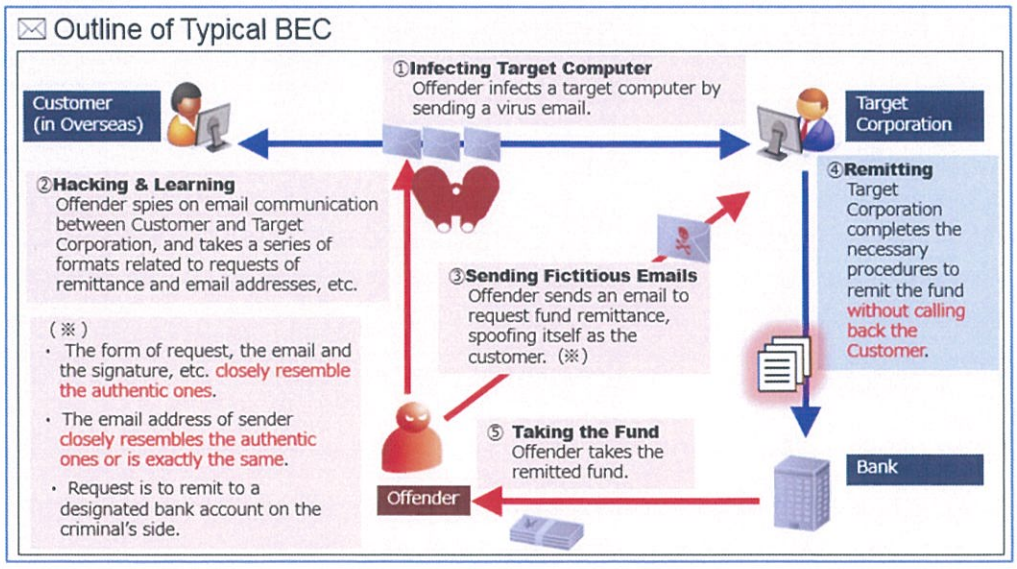
Below details information that we can share for your references.

(1) What is BEC

Business E-mail Compromise is defined as a **sophisticated scam targeting businesses working** with foreign suppliers and/or businesses that regularly perform wire transfer payments.
If you regularly perform wire transfer payments based on emails, there is a possibility that you might be a target of BEC.

(2) Typical BEC

- Offenders **hack into daily email communication** between the target corporation and its customers by infecting the personal computer of Target Corporation or its customers, etc.
  - ⇨ Following that, the offenders send fictitious emails (usually in English) that requests to send money, imitating the sender, the subject and the text field of the hacked emails.



- ⇨ **The more advance way has occurred where the email address has perfectly appeared on screen, but when it is doubled clicked, the real fake address will appear!**
  For example:

Legitimate email address: Bankmizuho@mizuho.co.id
On screen, it will appear as it is, but when it is double clicked, the real fake one will appear, i.e. Bank.mizuho@mizuho.co.id

(3) How to Protect Yourself from BEC

Protect your computer system from being hacked.
Please keep your software updated. Targets are:

- Operation systems ; Application software ; Antivirus software

The attached files are to be encrypted with difficult passwords when you communicate with external counterparties by email.

Notes:

⇨ Current email scams to be aware in 2019 (source: globalsign.com)

1. Netflix wants you to update your payment details
2. Lottery company wants you to know you've won
3. Apple wants to confirm your recent applications purchase
4. Australia wants you to bid on commercial projects

Check the received email. Employees and executive officers who might receive emails requesting to send funds should make sure to check the received emails.

Double-check the sender's email address. A spoofed email address often has an extension similar to the legitimate email address. For example, a fraudulent bastian@abc_company.com instead of the legitimate bastian@abc-company.com.

Double confirmation and verify before sending money to your supplier or beneficiary. Not only receive email confirmation but also confirm through a phone call using previously known numbers, not phone numbers provided in the email to avoid fraud.

Also confirm the request when receiving a suspicious email. Check that the email is legitimate by means other than using email, by making a telephone call or conducting a facsimile transmission. If you have to use an email to confirm the details of received email, do not REPLY but FORWARD the email by entering the correct email address manually.

Never open attachments or click on any links from suspicious emails. Don't open any email from unknown parties. If you do, do not click on links or open attachments as these often contain malware that accesses your computer system.

Know your customer's and vendors habits. If there's a sudden change in business practices, for instance, change of beneficiary and bank in other country. Please be aware of it, the request could be a fraudulent action!

Even with any reason provided related to existing account, such as the account is being frozen by the regulator or for tax payment obligation. Do not easily trust anybody who requests to change the instruction related with the beneficiary account. You need to verify and confirm the request through a different source such as calling by phone to the registered office fixed line.

MIZUHO

IMPORTANT

NB: PLEASE SHARE THIS INFORMATION TO ALL STAFFS (ESPECIALLY WHO HANDLE PAYMENT TRANSACTIONS AND RELATED VENDORS)

Please visit https://www.mizuhobank.co.id/ for more information regarding our latest announcement and financial information or see Public Service Announcement from Federal Bureau of Investigation of the US (URL: https://www.ic3.gov/media/2018/180712.aspx).

Thank you