PT. Bank Mizuho Indonesia
Sinar Mas Land Plaza - Menara 2,24th floor
Jl. M.H. Thamrin No.51 Jakarta 10350 - Indonesia
Tel : 62-21 3925222 (hunting)
Fax : 62-21 3926354
SWIFT : MHCCIDJA

Friday, 02 November 2018

Dear Valued Customers,

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 customers 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.

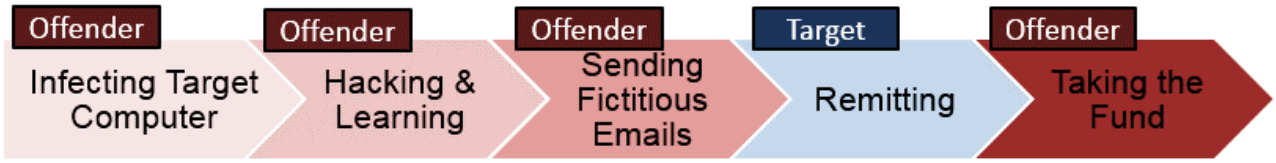
(1) What is BEC

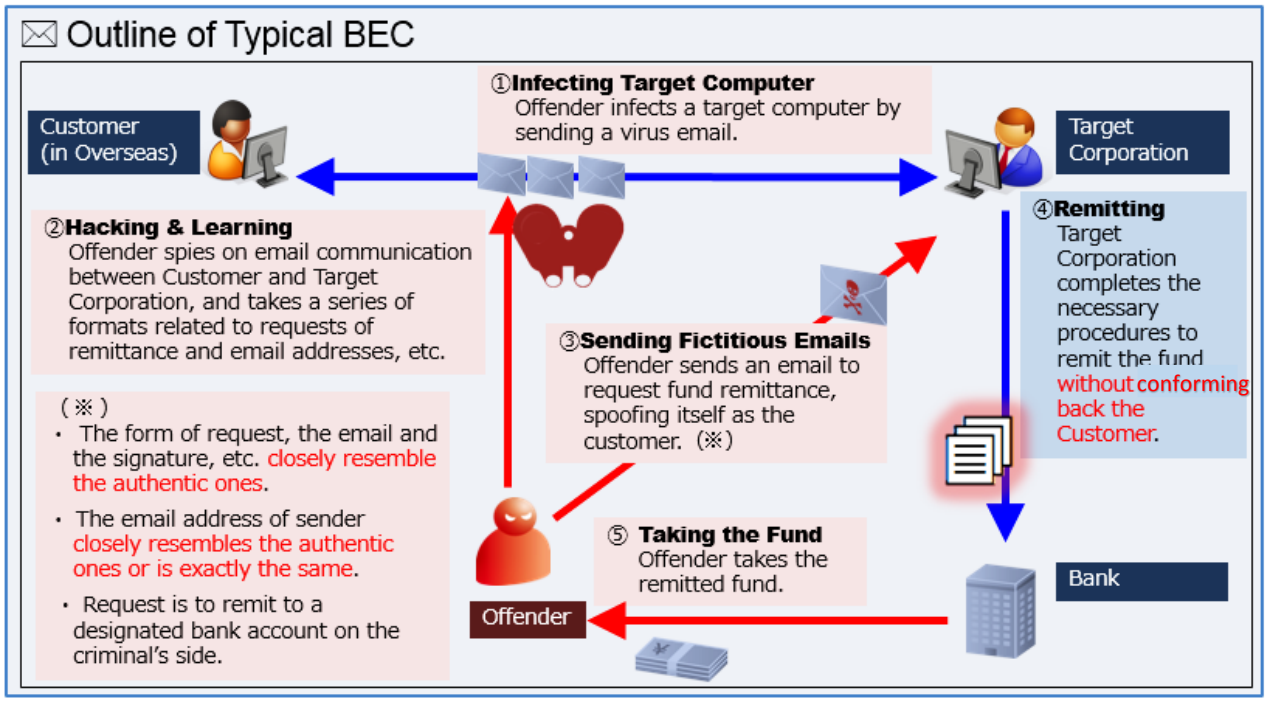
Business E-mail Compromise is defined as a **sophisticated scam targeting businesses working** with foreign suppliers and/or businesses that regularly perform wire transfer payments.
If you regularly perform wire transfer payments based on email communication with your suppliers or buyers, there is a 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) pretending to be the usual counterparties (by imitating the real sender with usual subject and text field), and requests to send regular payment by quoting valid invoice numbers, etc..





How to Protect Yourself from BEC

Protect your computer system from being hacked.

Please keep your software updated. Targets are:

- Operating systems ; Application software ; Antivirus software
- Important information shall be kept in a separate file and attached to your email.

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

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 name@abc_company.com instead of the legitimate name@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 telephone 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. Do not 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 customers and vendors habits. If there is a sudden change in business practices, such as instruction to different banks or different beneficiary, please be aware. The request from beneficiary and bank in other country could be fraudulent. You need to verify and confirm the request through a different source before sending the money (recommended media is through telephone call to authorized person).

Please visit https://www.mizuhobank.co.id/ for more information regarding our latest announcement and financial information.

This information is provided as reference only, and is not intended to be relied upon by any party as the source for making any transactions or decisions. BMI would not be responsible for any claims and all consequences by law, any future losses, damages, claim, suit, and any kind of protest from any party, which may arise as result of this information.

Thank you.