

Kepada Nasabah Yang Terhormat,

Seiring dengan semakin maraknya laporan terjadinya tindak kejahatan pada sektor keuangan dengan apa yang disebut sebagai **Business Email Compromise ("BEC")**, dimana pelaku tindak kejahatan menyamar sebagai pejabat eksekutif atau yang berwenang pada perusahaan atau sebagai supplier di luar negeri yang meminta pengiriman uang pembayaran dan akhirnya mencuri uang tersebut.

Untuk melindungi diri anda dari tindak kejahatan BEC, dimohon untuk melakukan pengecekan kembali apabila ada sesuatu hal yang patut dicurigai sebelum anda melakukan pengiriman uang ke luar negeri. Kami, PT. Bank Mizuho Indonesia (BMI) menyarankan kepada seluruh nasabah, untuk melakukan beberapa tindakan pencegahan terkait hal tersebut diatas sehingga akun dan transaksi anda tetap aman dari tindakan kejahatan.

Di bawah ini kami sampaikan beberapa informasi yang dapat dijadikan sebagai pedoman.

(1) Definisi BEC

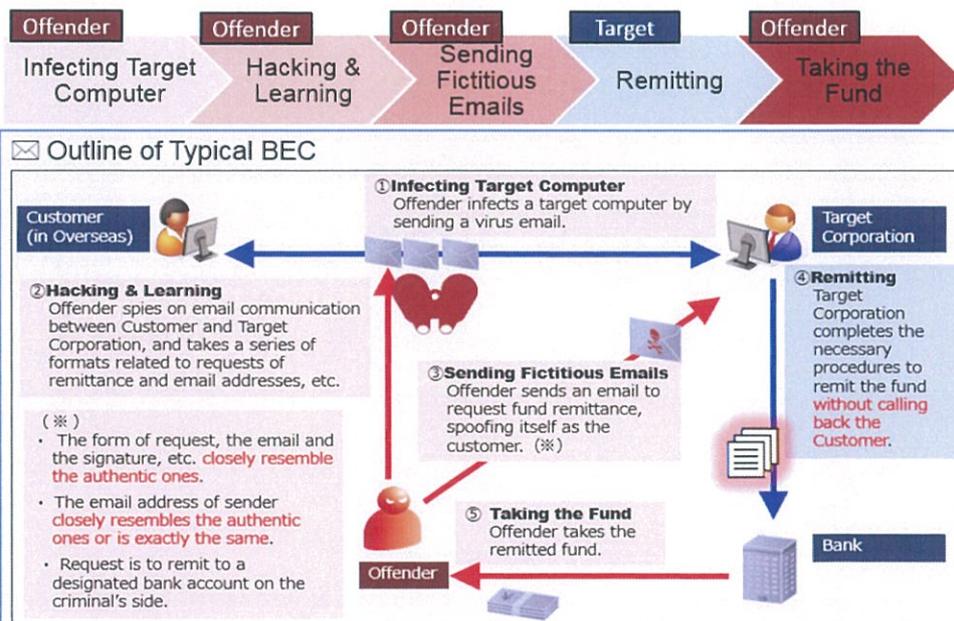
Business Email Compromise di definisikan sebagai tindak kejahatan melalui penipuan yang cukup canggih, dimana target merupakan pelaku bisnis yang berhubungan dengan supplier di luar negeri atau pelaku bisnis yang sering melakukan pembayaran atau pengiriman dana melalui transfer ke luar negeri. Jika anda sering melakukan pembayaran atau pengiriman dana berdasarkan komunikasi dengan *counterparty* anda di luar negeri melalui email, maka besar kemungkinan anda dijadikan target atau sasaran dari pelaku tindak kejahatan BEC tersebut.

(2) Tipikal BEC



Pelaku tindak kejahatan BEC meretas (hacking) email komunikasi anda sebagai "Target Korporasi" dengan nasabahnya atau counterparty dengan melakukan penyebaran virus pada komputer anda.

⇒ Selanjutnya, pelaku tindak kejahatan mengirimkan email fiktif (biasanya dalam bahasa Inggris) yang meminta pembayaran regular dengan mengutip nomor invoice serta besaran jumlahnya sesuai dengan aslinya (*valid invoice information*).



- ⇒ Cara yang lebih canggih adalah di mana alamat email pengirim sudah tampak benar di layar, tetapi pada saat kita klik dua kali, ternyata alamat email si pengirim berbeda dengan yang awal!

Sebagai contoh :

Alamat email yang sah : Bankmizuho@mizuho.co.id

Di layar akan muncul apa adanya, tetapi pada saat di klik dua kali email tersebut akan berubah menjadi Bank.mizuho@mizuho.co.id.

(3) Cara menjaga diri anda dari serangan BEC

Jagalah Komputer Anda jangan sampai diretas oleh hacker.



Selalu perbaharui atau *update* system software pada computer anda. Target dari *hacker*:

- *Operation systems (OS)* ; *Aplikasi software* ; *Antivirus software*

Lampiran file dalam email anda harus dienkripsi (*to be encrypted*) dengan menggunakan kata sandi (*password*) yang tidak mudah ditebak ketika anda berkomunikasi dengan nasabah anda atau pihak *counterparty*.

Catatan :

- ⇒ Penipuan melalui email yang harus di perhatikan di 2019 (sumber: globalsign.com)
1. Netflix ingin ada untuk memperbarui detail pembayaran anda
 2. Perusahaan Lotere menginformasikan bahwa anda telah menang
 3. Apple ingin mengkonfirmasi pembelian aplikasi terbaru anda
 4. Perusahaan dari Australia menawarkan proyek komersial



Melakukan pengecekan terhadap email masuk. Karyawan dan pejabat eksekutif yang dimungkinkan akan menerima email terkait permintaan pengiriman pembayaran atau pengiriman dana, harus mengecek kebenaran isi email tersebut.

Lakukan pengecekan ulang terhadap si pengirim email (*sender*). Sebuah alamat email palsu seringkali memiliki extension yang sangat mirip dengan alamat email aslinya. Sebagai contoh: sebuah alamat email palsu bastian@abc_company.com sangat mirip dengan alamat email aslinya yaitu bastian@abc-company.com.



Konfirmasi ulang dan lakukan verifikasi sebelum mengirim uang anda kepada *supplier* atau *beneficiary* yang dituju. Tidak cukup hanya melakukan konfirmasi melalui email saja, tetapi juga lakukan konfirmasi melalui telepon dengan menggunakan nomor telepon yang sudah terdaftar sebelumnya, bukan nomor telepon yang mungkin tersedia di email untuk menghindari penipuan.

Pastikan melakukan konfirmasi terhadap isi permintaan email yang terlihat mencurigakan. Pastikan bahwa email itu asli dengan dengan melakukan pengecekan melalui telepon atau melakukan pengiriman faksimili. Namun, jika anda harus menggunakan email untuk mengkonfirmasi rincian email yang anda terima, **jangan ME-REPLY namun ,FORWARD** email dengan mengetik alamat email secara manual sesuai email nasabah anda atau *supplier* anda yang anda ketahui.



Jangan pernah membuka lampiran atau melakukan klik link apa pun dari email yang mencurigakan. Jangan buka email apa pun dari pihak yang tidak dikenal. Jika Anda melakukannya, jangan klik link

nya atau membuka lampiran karena sering kali berisi virus atau *malware* yang bisa meretas sistem komputer anda.



Pelajari kebiasaan dari nasabah atau vendor Anda. Jika terjadi perubahan yang tidak biasa dalam praktik bisnisnya, seperti perubahan instruksi pengiriman pembayaran atau dana ke penerima (beneficiary) dan Bank yang berbeda di negara lain. Harap berhati-hati, karena bisa jadi hal tersebut adalah penipuan!

Bahkan jika mereka menggunakan alasan apapun terkait dengan akun yang ada, seperti misalkan terjadi pembekuan rekening oleh pihak regulator ataupun untuk keperluan pajak.

Jangan mudah percaya kepada siapapun yang meminta untuk mengubah instruksi terkait dengan akun si penerima. Anda perlu melakukan verifikasi dan konfirmasi permintaan tersebut melalui sumber yang lain seperti menghubungi lewat telepon ke nomor *fixed line* kantor sesuai yang didaftarkan secara resmi.

IMPORTANT

Catatan : HARAP TERUSKAN INFORMASI INI KEPADA SEMUA KARYAWAN (TERUTAMA KEPADA MEREKA YANG BERTANGGUNG JAWAB ATAS PEMBAYARAN DAN JUGA SUPLIER TERKAIT)

Silakan kunjungi website <https://www.mizuhobank.co.id/> untuk informasi lebih lanjut mengenai pengumuman terbaru dan informasi keuangan kami atau Pengumuman Layanan Publik dari Federal Bureau of Investigation of the US (URL: <https://www.ic3.gov/media/2018/180712.aspx>)..

Terima Kasih