2021年1月25日

オー・エム・シー株式会社
代表取締役　渡辺　信次

【重要なお知らせ】

弊社社名、銀行口座等を騙った詐欺メールにご注意下さい

弊社の社名、役職員の氏名を含むメールアドレス等を詐称した「なりすましメール」が発信されている可能性があります。これらの「なりすましメール」は弊社とは一切関係がありません。

【手口】

弊社のドメイン（jomc.co.jp）に似たドメインから弊社社員になりすまし、従来から弊社が指定している銀行口座とは異なる銀行口座へ代金を振り込むよう依頼する。

【対応】

弊社は、メールのみで振込先銀行口座変更のお知らせをすることはございません。
こうしたメールがあった場合は、削除・無視していただきますようお願い致します。
またメールアドレスは弊社のものと酷似している場合がありますので、送信元メールアドレスには十分ご注意いただけますよう、お願いいたします。

不審なメール等に関してご質問・御連絡等を頂く場合は、電話（072-688-8331）でご連絡いただきますようお願い致します。

オー・エム・シー（株）　569-1026 大阪府高槻市緑が丘2丁目3番12号
TEL:072-688-8331 / FAX:072-688-8332
O.M.C. Co., Ltd.2-3-12Midorigaoka, Takatsuki, Osaka 569-1026　E-mail: mail@jomc.co.jp

その送金依頼、ニセモノかもしれません
－ビジネスメール詐欺「BEC」に注意！－

IPA
2018年8月
独立行政法人情報処理推進機構

RE: MA666 - メッセージ (HTML 形式)

[redacted] <[redacted]@[redacted].co.jp>; <[redacted]>

RE: MA666

前回の転送メールにございますように、[redacted] 弁護士の協力で、ある中国企業から
第一回目の支払いとして、銀行国際送金による入金の必要があります。
USドル、ユーロ、もしくはビットコインの決済が可能です。

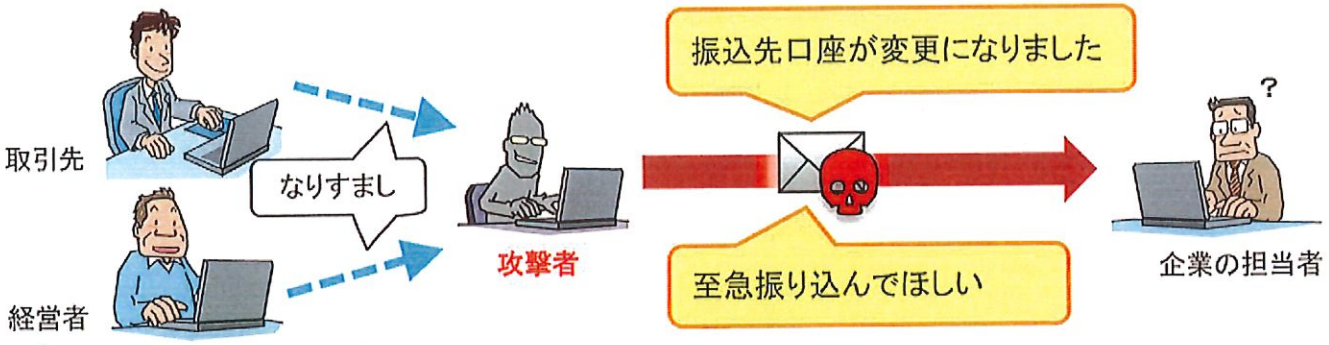
今日、支払い確認の得られる最適な方法を教えていただけませんでしょうか。
また、2018年7月6日までの銀行残金表をいただきたいと存じます。

どうぞよろしくお願い申し上げます。
敬具

取引先からの送金口座の変更・支払い手段の変更を知らせるメール、社長からの至急の送金指示のメールを受信しました。あなたならどうしますか？

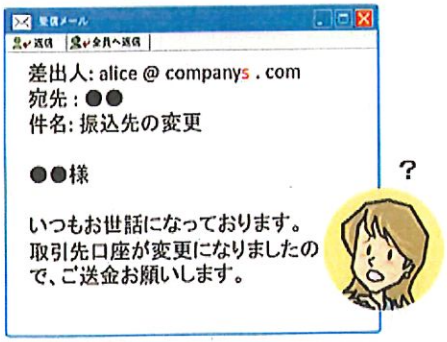
●ビジネスメール詐欺の代表的な手口

◆ 取引先担当者や経営者等へなりすまして偽のメールを送り付け、詐欺を行う



●ビジネスメール詐欺への対策

① 普段と異なるメールは社内で相談・連絡する



② 急な振込先の変更等には電話やFAXで確認する

③ セキュリティソフトを導入し最新の状態にする & 複雑なパスワードを使用する

ビジネスメール詐欺に関する詳しい資料や事例は、次のURLで公開しています。
https://www.ipa.go.jp/security/announce/201808-bec.html

ビジネスメール詐欺の事例を確認した場合など、下記へ情報提供をお願いいたします。

IPA J-CSIP事務局 情報提供宛先
jcsip-info@ipa.go.jp

Please be aware of BEC (Business E-mail Compromise) or fraudulent e-mails posing as trusted sources instructing foreign remittance (foreign remittance fraud)!

There have been a number of cases in which a fraudulent e-mail appearing to be from a trusted external/internal source has requested a foreign remittance be made.
Please be aware of different scenarios/cases and take various preventive measures at your entity.

Actual cases of fraud

In the case of foreign remittance made from business entities in Japan

- Funds were defrauded through the execution of foreign remittances based on a request sent by e-mail to amend the deposit account, or on an invoice attached to an e-mail, from a person pretending to be a business partner, such as a supplier.
- Funds were defrauded via computers which were infected with viruses or through internal e-mails which were hacked.
- Funds were defrauded by an instruction to amend the IBAN, which processed STP numerous times, especially within the EU.
- Funds were defrauded through the execution of a foreign remittance based on an e-mail or phone call from a person pretending to be the parent company's CEO/EFO or another person at the executive level.

In the case of receiving funds from foreign business entities

- Funds were defrauded with remittance instructions such as to amend the deposit account. Those remittance instructions were in e-mail messages or invoices attached to an e-mail.

Examples of Preventive Measures to be taken

1. Confirm facts by means other than e-mail, e.g. phone call or fax, whenever possible, in the following cases;
   - Receiving an e-mail to amend a deposit account or name of account holder, especially an instruction to designate a receiving bank located in a different country than that in which the receiver resides.
   - Receiving an e-mail to change an account from that of the business entity to an individual.
   - Receiving an e-mail to amend a deposit account from a third party such as a middleman.
   - Receiving an e-mail with an e-mail address which is not an official address of that entity.
   - Receiving an e-mail of remittance request with a header of "urgent" or "confidential".

2. Return e-mails by forwarding, not replying to the original message, typing the e-mail address of the correct business partner in order to confirm the legitimacy of receiver.