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.

3. Communicate with your business partners via secure methods, such as using encoded attachments, using electronic signatures, etc.

4. Adopt security measures such as introducing anti-virus tools to PCs used for foreign remittance and related communications.

5. Alert internally and share information, not only with the staff/divisions dealing with remittances, but also among the staff/divisions sending/receiving e-mails.