Business E-mail Compromise: A Growing Online Security Threat

August 2017

A business e-mail compromise happens when a fraudster sends an e-mail to your company's payments team impersonating a contractor, supplier, creditor or even someone in your senior management. For instance, the payments team may receive:

- An e-mail appearing to be from the CEO asking that an urgent payment be made. This is often accompanied by a request for secrecy, directing the recipient not to discuss the matter with anyone else.

- An e-mail from a supplier advising that their account numbers have changed, and instructing all future payments be sent to the new account.

In either case, it can be difficult to detect this type of fraud since cybercriminals make the sender's e-mail address appear to be the same as a known e-mail address. Fraudsters may even hack into the actual e-mail account of a particular user and send the e-mail directly from there.

How You Can Take Action

Start by making your payments team and/or relevant staff aware of this type of fraud so they can be looking out for it. In addition to this:

- Implement payments security that includes a two-step verification process, which involves contacting the sender via an alternative method (e.g., phone, instant message)

- Always use known contact details to follow up
  - Don't reply directly to the e-mail
  - Don't use any phone numbers or other contact information included in the e-mail

If you suspect you've been a victim of a business e-mail compromise fraud, please contact your remittance bank immediately.

If you have any questions, please contact us at:
The Hongkong and Shanghai Banking Corporation Limited, Global Payment and Cash Management
Tel: 03-5203-3247
E-mail: jcsc@hsbc.co.jp