Caution on Fraudulent Emails

In view of the recent incidents of fraudulent emails in the market, HKTDC would like to remind our exhibitors to stay vigilant and take extra precautions. We hope that the following tips may help to raise your awareness.

1) Ensure that the email is genuinely from HKTDC
    - Always identify the sender of the email from its domain.

2) Check the HKTDC disclaimer
    - All emails sent from HKTDC will carry the Council's disclaimer at the bottom of the email.

3) Reconfirm bank account number and beneficiary name (Hong Kong Trade Development Council) when making payments.

4) Always use trusted Wi-Fi network
    - There is always security risk when using untrusted public Wi-Fi network to access emails. It is possible that hackers can capture your emails or send fraudulent emails to you on untrusted Wi-fi network.

The above is for reference only. In case of doubt, please contact HKTDC hotline at +852 1830 668 and quote the fair name concerned.

For your further information, please find below a fraudulent email prevention pamphlet from the Hong Kong Police Force Crime Prevention Bureau.

香港警務處 Hong Kong Police Force | 防止罪案科 Crime Prevention Bureau

電郵騙案

電郵騙案

有否認清電郵地址？
真假電郵極為相似
Confirm the genuine email address?
The fraudulent one might be similar!

收款人銀行戶口號碼突然改變？

Sudden change of recipient's bank account number?

123-123-123457
?

必須以電話
核實對方真正要求
Must verify the true identity or the request by "Phone"!

舉報罪案 請致電 999　http://www.police.gov.hk/info/doc/bankdetails_c.pdf　Call 999 to report crime

香 港 警 務 處 | 防 止 罪 案 科
Hong Kong Police Force | Crime Prevention Bureau

攜手同心防罪行 Join Hands, Prevent Crime

"Change of Supplier Bank Details" Scam

Nowadays, SMEs usually depend on email as the main communication channel with customers. "Change of Supplier Bank Details" scam especially targeting SMEs is emerging around the world including Hong Kong.

[Example]:

Fraudsters knew from stolen emails about the transactions of Company A (the seller) and Company B (the buyer). Later, fraudsters, pretending to be Co.A, sent fictitious emails (which are very similar to genuine emails) to Co.B, claiming that the email address and payment receiving bank account number have changed, and requesting Co.B to credit the amount payable to the designated account. Afterwards, when contacting Co.A by phone, Co.B found out that it had been deceived by fictitious emails and suffered losses both in money and business reputation.

Police Appeal

The Police call on SME operators to be alert of suspicious emails and raise their awareness in preventing this kind of scam, such as taking the initiative to confirm the true identities of recipients by telephone, facsimile or other means before remittances so as to prevent such kind of scam.

Email and password security	Computer system security
• safeguard personal data, including personal and commercial email accounts to prevent from being stolen by culprits; • do not use computers in public places to access personal email box, using instant messaging software, e-banking or doing other operations involving sensitive data; • use proper passwords and change them regularly; • do not open emails of dubious origins; • do not download attachments of suspicious nature; • use antivirus software to scan for virus before opening attachments.	• use genuine software; • update software with patches provided by software developers; • install and turn on firewall and intrusion detection system; • update virus and spyware definition files; • use antivirus software to scan computers regularly; • do not download software of suspicious origin / nature; • protect wireless networks.