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!

123-123-123457
?

收款人銀行戶口號碼突然改變？

Sudden change of recipient's bank account number?

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
Hong Kong Police Force

防 止 罪 案 科
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.

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

攜手同心防罪行 Join Hands, Prevent Crime

『戶口更改』騙案

香港的中小企業往往倚賴電郵作為與顧客的主要溝通渠道，而專門欺詐中小企的「戶口更改」電郵詐騙案在本港及世界各地冒起。

【舉例】： 假設 A 公司為售貨公司，
而 B 公司為應付款公司。
騙徒盜取電郵資訊，得知 A 與 B 公司業務往來。
騙徒假扮 A 公司發假電郵予 B 公司，訛稱收款銀行戶口號碼已更改，要求 B 公司將應付的款項存入指定戶口。
為了阻礙兩間公司溝通，騙徒更會假扮 B 公司，發假電郵予 A 公司，聲稱電郵地址也更改。
最後，當 B 公司聯絡 A 公司時才知道被假電郵欺騙，蒙受金錢及商譽損失。

警方呼籲

各中小企業負責人應加緊留意可疑電郵，提高對此類犯罪的防範意識，包括：-
主動提醒交易夥伴在匯款前，先以電話、傳真或其他方式確認收款人身份，以防被騙。

電郵及密碼保安	電腦系統保安
● 要小心保管個人資料，包括個人及商務電子郵件戶口； ● 不要使用公眾場所的電腦登入個人電郵、網上銀行或進行其他涉及敏感資料的操作； ● 使用妥當的密碼，並定期更改； ● 不要隨意開啟來歷不明的電郵； ● 不要下載來源/性質可疑的附件； ● 開啟附件前用防毒軟件掃描病毒。	● 使用正版軟件； ● 更新軟體研發商的修補程式； ● 安裝和開啟防火牆、入侵偵測系統； ● 更新病毒及間諜軟體定義檔； ● 定期用防毒軟體掃描電腦； ● 保護(WIFI)無線網路。