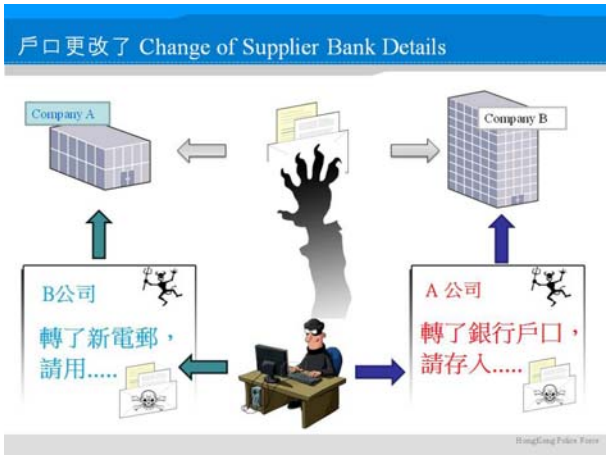
香 港 警 務 處
Hong Kong Police Force

商 業 罪 案 調 查 科
科 技 罪 案 組
Commercial Crime Bureau
Technology Crime Division

# 電郵騙案

電郵於現今社會是一種普遍的溝通方式，很多人會用以聯絡親友以及商業上的伙伴。有些不法分子會利用駭客技術入侵電郵戶口，以各種方法騙取受害人匯款。而有些受害人亦因此受騙，蒙受鉅額金錢損失。以下爲一些常見的案例：




**案例一（企業電郵）:「銀行戶口更改」**

騙徒根據盜取得來的電郵，得知 A 公司(賣方、付貨公司)與 B 公司(買方、應付款公司)的業務往來情況。其後，騙徒假扮 A 公司發假電郵(真假電郵極爲相似)予 B 公司，訛稱電郵地址及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。其後 B 公司以電話聯絡 A 公司，才知道被假電郵欺騙，蒙受金錢及商譽損失。

**案例二（個人電郵）:「親友於外地急需用錢」**

騙徒在利用駭客技術入侵私人電郵戶口後，會發放電郵給該電郵中聯絡名單上的親友。騙徒會在電郵中訛稱自己在外地遇到意外，急需要用錢，要求受害人匯款到騙徒的戶口。有些受害人在並無確定的情況下就忽忙匯款, 之後和該親友聯絡，才發覺受騙。

**警方呼籲**

警方呼籲各各位市民加緊留意可疑電郵，提高對此類騙案的防範意識，包括匯款前主動前以電話、傳真或其他方式確認對方真正身份或該項要求的真確性，以防止此類案件的發生。

防範黑客入侵電腦保安貼士：

| 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，以免被不法之徒盜用；<br>● 不要使用公眾場所的電腦登入個人電郵信箱、使用即時通訊軟件、網上銀行或進行其他涉及敏感資料的操作；<br>● 使用妥當的密碼，並定期更改；<br>● 不要隨意開啓來歷不明的電郵；<br>● 不要下載來源/性質可疑的附件；<br>● 開啓附件前用防毒軟件掃描病毒。 | ● 使用正版軟件；<br>● 更新軟體研發商的修補程式；<br>● 安裝和開啓防火牆、入侵偵測系統；<br>● 更新病毒及間諜軟體定義檔；<br>● 定期用防毒軟體掃描電腦；<br>● 不要下載來源/性質可疑的軟件；<br>● 保護無線網路。 |