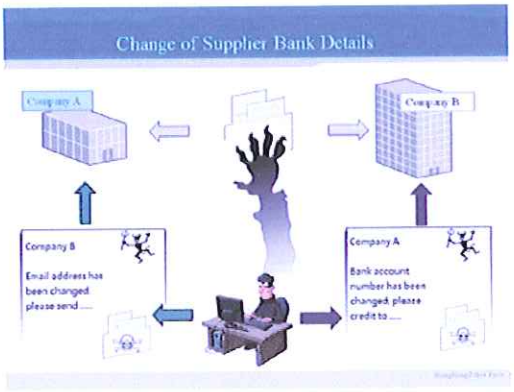
香 港 警 務 處
Hong Kong Police Force

商業罪案調查科
科技罪案組
Commercial Crime Bureau
Technology Crime Division

Email Scam

Email is one of the main communication channels for both personal and commercial dealings. Nowadays, fraudsters would hack email accounts, and cheat recipients by all possible means to make remittances. Some victims have suffered significant amount of losses in some cases. Here are the common scenarios:



Example 1 (Corporate Level) - "Change of Supplier Bank Details":
Fraudsters knew from stolen emails about the transactions of Company A (the seller, the consignor) and Company B (the buyer, the paying company). Later, fraudsters, pretending to be Company A, sent fictitious emails (which are very similar to genuine emails) to Company B, claiming that the email address and payment receiving bank account number have changed, and requesting Company B to credit the amount payable to the designated account. Afterwards, when contacting Company A by phone, Company B found out that it had been deceived by fictitious emails and suffered losses both in money and business reputation.

Example 2 (Personal Level) - "Overseas Relatives/Friends need immediate money remittance":
After hacking into a personal e-mail account, fraudsters sent out deceptive e-mails to all persons on the contact list. The email depicted the sender had encountered an accident overseas and requested a transfer money as a matter of emergency. Some recipients made the remittance without further verification.

Police Appeal:
The Police call on all email users 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.

IT security tips to mitigate the risk of hacking:

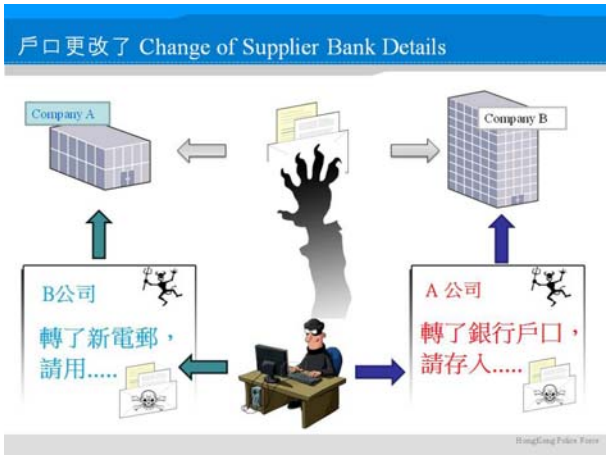
Email and password security	Computer system security
● safeguard personal data, including personal and commercial email accounts to prevent from being stolen by culprits; ● do not use computers in public places to access personal email box, using instant messaging software, e-banking or doing other operations involving sensitive data; ● use proper passwords and change them regularly; ● do not open emails of dubious origins; ● do not download attachments of suspicious origin / 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

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； ● 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； ● 使用妥當的密碼，並定期更改； ● 不要隨意開啓來歷不明的電郵； ● 不要下載來源/性質可疑的附件； ● 開啓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； ● 安裝和開啓防火牆、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； ● 不要下載來源/性質可疑的軟件； ● 保護無線網路。