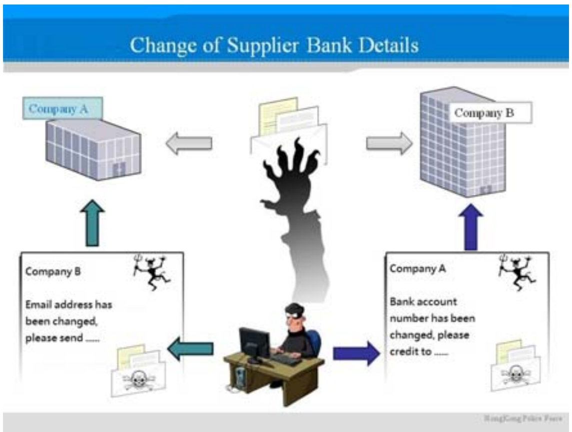
香港警務處
Hong Kong Police Force

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:


Change of Supplier Bank Details
Company A
Company B
Company B
Email address has been changed, please send ......
Company A
Bank account number has been changed, please credit to ......
HongKong Police Force

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:

<u>Email and password security</u>	<u>Computer system security</u>
● 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.