

香港金融管理局
解構偽冒電郵 - 動畫

金大使為你拆解網上騙局

熒幕蓋字： 金大使為你拆解網上騙局

金大使： 金大使為你拆解網上騙局

熒幕蓋字： 絕對不會被騙之男
醒目仔

醒目仔： 銀行電郵？

熒幕蓋字： 一定騙到你之達人
釣魚大郎

釣魚大郎： 親愛的顧客
為加強網上銀行的安全措施
請進入以下網址啟動你的多重認證
如未有啟動多重認證的網上銀行賬戶
將被暫停網上轉賬服務

醒目仔： 停了便麻煩了！
要立刻處理！

金大使： 慢著！
這封電郵很可疑啊！

熒幕蓋字： 網絡安全大使
金大使

醒目仔： 很明顯是銀行寄給我的
有甚麼問題呢？
我反而覺得你更可疑……

- 金大使： 少年，你太年輕了！
由於電郵本身疑點重重
即使發件人名稱和超連結與你的銀行一模一樣
都有可能是騙徒偽造出來的釣！魚！電！郵！
- 熒幕蓋字： 釣魚電郵
- 金大使： 釣魚電郵一般會用看似合理的原因去欺騙收件人
點擊電郵裡的超連結或附件
- 熒幕蓋字： 大額資金轉賬交易通知
要求啟用新安全功能
- 金大使： 例如通知你「有大額資金轉賬的交易」
或是要求你「啟用新的安全功能，否則會暫停你的網上銀行
服務」
這些都是騙徒常用的手法
- 醒目仔： 即是好像我這個嗎？
- 金大使： 全對！
- 醒目仔： 噢！原來你想欺騙我！
- 釣魚大郎： 不是呀！不是呀！
- 金大使： 好像這條超連結
看似和真的一樣
但實際是連接到欺詐銀行網站
然後盜取你網上銀行用戶名稱和密碼等的個人資料
- 熒幕蓋字： 開啟附件時將電腦病毒植入電腦或手機
- 金大使： 騙徒又會哄你打開電郵附件
將電腦病毒植入你的電腦或手機
這些病毒程式可以記錄你在電腦或手機輸入的個人資料

釣魚大郎： 到時候你的錢便是我的錢了
哈！哈！哈！

醒目仔： 那可以怎樣防範呢？

金大使： 一般來說
銀行很少會主動向客戶查詢個人資料
或透過電郵內的超連結要求你登入網上銀行或更新資料
如果有懷疑
千萬不要開啟任何附件或超連結

熒幕蓋字： 聯絡客戶服務熱線
確認電郵真偽

金大使： 你可以聯絡客戶服務熱線
向相關銀行確認電郵的真偽
這樣騙徒便無所遁形了

金大使： 記著！記著！記著！

熒幕蓋字： 釣魚電郵可亂真 附件連結要小心

金大使： 釣魚電郵可亂真 附件連結要小心

熒幕蓋字： 
www.hkma.gov.hk/cybersecurity