

網上交易安全你要知!

皇仁舊生會中學 - 黎燕兵，陳嘉偉



在香港,網上交易(例如：拍賣或付款)非常普遍。-亦因為此，有很多人就在進行網上交易時被騙。

網上交易安全例子



<--某大銀行網頁

有一日，小明因在拍賣網購物，故需要透過網上理財轉帳給賣家。由於這是他第一次使用網上理財，所以他從未瀏覽某大銀行網上理財的網站。於是，他利用搜尋器找到數個某大銀行的網站。

他隨即登入了此網站,可是並沒有核對該網站的可信性，便利用該網站的網上理財系統。

偽裝銀行網頁與某大銀行的真正版面是極之相似的，其實真正的銀行網頁是這樣的:



小明毫不猶豫地把自己在某大銀行的戶口號碼及密碼輸入該系統，可是他的戶口資料已立即被傳送到偽裝網站的伺服器中，並存貯於硬碟。



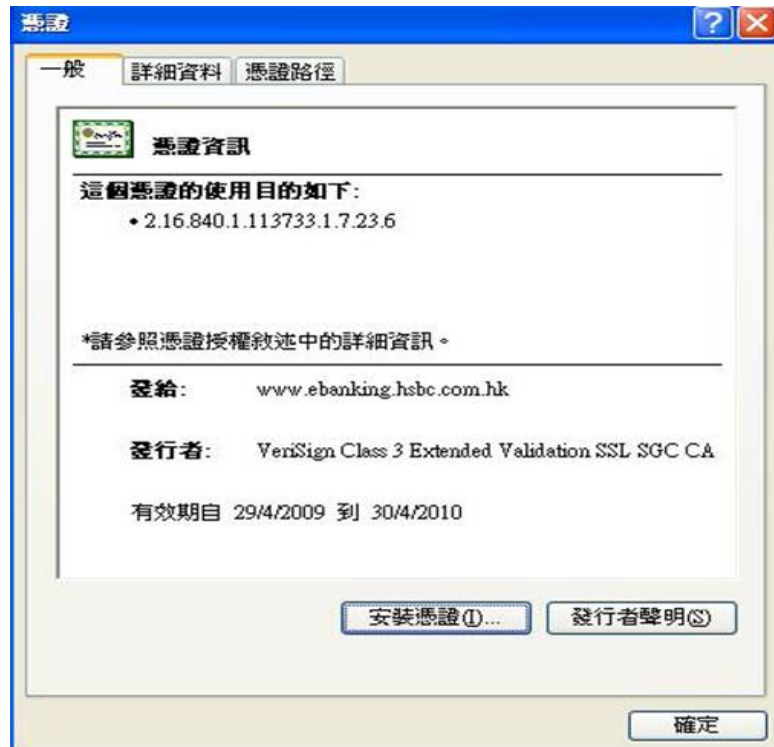
<--網上理財登入介面



不法份子利用戶口資料

當不法份子從該釣魚網站獲取這些資料後，他們便利用這些資料登入真正的銀行，並且把戶口內的金錢轉帳到自己的銀行戶口。

如何避免造成損失?



<--憑證介面

1. 一般銀行月結單內都提供銀行的網址，可信性比搜尋器找到的網頁更高。
2. 不要隨便輕易提供自己個人戶口和密碼。
3. 只登入有安全憑證的網站(Https)*

頁面資訊 - https://kd.gamania.co.jp/index2.asp

一般 媒體 權限 安全

網站身分

網站: **kd.gamania.co.jp**
擁有者: **這個網站沒有提供擁有者資訊。**
驗證機構: **Betrusted Japan Co., Ltd.**

檢視憑證 (Y)

隱私及瀏覽記錄

我以前有瀏覽過這個網站嗎? 是, 來過 4 次
此網站有在我的電腦中儲存資訊 (Cookie) 嗎? 是
我有在此網站儲存任何密碼嗎? 否

檢視 Cookie (K)
檢視已存密碼 (W)

技術細節

連線已加密: 高等級加密 (RC4 128 位元)
您正在瀏覽的網頁在傳送前有經過加密。
加密使得未經許可的人非常難以破解以取得電腦間的通訊。所以幾乎不大有人可以截取到您在網路上傳送與接收的資訊。

*註釋:Https 即把重要的傳輸資料加密是一個比較安全的方法，比如網址開頭是「Https」的網站所使用的資料都是經過加密處理的，比起一般的「Http」網址的網站更安全，一般銀行或是網路交易公司也是使用這種網站。(註: 如果是 Https 的，在 Browser URL 的旁邊會出現一個小小的鎖，表示資料已加密)

參考資料

[HTTPS 維基百科，自由的百科全書](#)

HTTPS 以保密為目標研發，簡單講是 [HTTP](#) 的安全版。其安全基礎是 SSL 協議，因此加密的詳細內容請看 [SSL](#)。全稱 Hypertext Transfer Protocol over Secure Socket Layer。

它是一個 [URI](#) scheme，句法類同 [http](#):體系。它使用了 HTTP，但 HTTPS 存在不同於 HTTP 的默認[端口](#)及一個加密／身份驗證層（在 [HTTP](#) 與 [TCP](#) 之間）。這個協議的最初研發由[網景公司](#)進行，提供了[身份驗證與加密](#)通訊方法，現在它被廣泛用於[互聯網](#)上安全敏感的通訊，例如交易支付方面。

詳細資料:<http://zh.wikipedia.org/zh-hk/HTTPS>

參考資料:[匯豐銀行網頁](#),[維基百科](#)