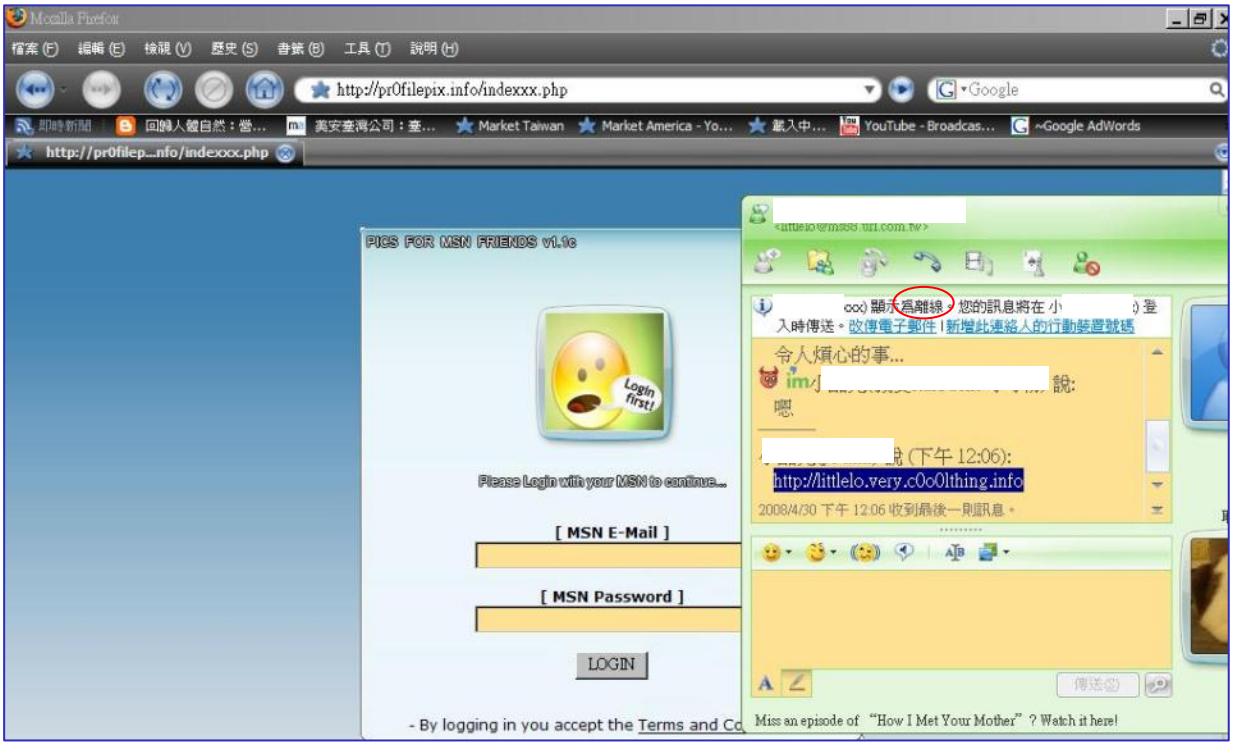
即時通訊 IM，Instant Message

前言：

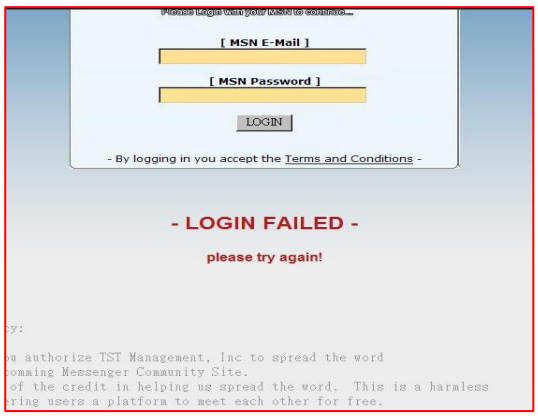
一打開電腦，上網、打開 MSN 似乎已經變成了開機的標準程序了，收發 email 也變成了所謂官方標準流程；MSN、Yahoo! Messenger、Skype、QQ、ICQ 這一類的即時訊息（IM，Instant Message）已經進乎取代了 email，成為最受歡迎的溝通工具。透過即時訊息，使用者可以經由文字、繪圖與表情符號，來互傳訊息、資訊與心情，甚至可以傳送更加即時性的影像、聲音及檔案。不管同不同意，IM 軟體〈MSN、Yahoo! Messenger、Skype、QQ、ICQ〉已經走入你我的生活，不僅是大家聊天時所使用的工具，更漸漸演變為員工與客戶互通訊息之最主要媒介，當然相對的這一類的軟體自然也就衍生出不少的資安漏洞。而這些資安的問題到底有哪些？到底會引發出什麼樣的後果？以下舉個案例來看看最常發生的事件。

案例：

相信有用 MSN 都會收過下面這樣的訊息，一個離線的朋友突然傳送一個網址給你。



類似這樣的訊息前面通常都會有「查詢你的 MSN 有誰加入你」，因為是朋友傳送的，也不疑有他就點下去開啟一個網頁（釣魚網站*），也就因為好奇想知道我有被誰加入就打入自己的帳號密碼(社交工程*)，當然神奇的事情出現了。



神奇的是告訴你登入失敗，相對的你的帳號密碼也被拿走了，你也成為受害者之一，反正知道帳密就可以知道你的通訊錄中朋友的聯絡方式，隔沒多久你的朋友也會收到類似的訊息，就這樣，所謂的駭客，就從此過著幸福快樂的日子（持續收集有用資訊：個資、機密文檔）。

建議：

1. 或許你已經點過N次的類似網站，不覺得有什麼問題（衍生問題很多），建議趕緊修改密碼，別再用所謂的懶人密碼或個人訊息密碼了，這都會是駭客的密碼字典檔中一定會有的資料，建議建立的密碼可以有英文、數字以及特殊符號的組合，單純只有英文或是數字的密碼，對駭客而言，五分鐘內就可以暴力破解了。修改 MSN的密碼可至下列網址修改 https://account.live.com/ResetPassword.aspx?mkt=ZH-TW
2. 對於離線朋友傳送的訊息不要隨一點開，建議先回傳訊息詢問，如有回應則表示朋友是假裝離線狀態。
3. 來入不明的檔案不要儲存及執行。

名詞解釋：

1. 釣魚網站：以下以某銀行為例子說明，駭客藉由扒站軟體將某銀行的整個網站抓下來，再於網路上申請一個類式的網站名稱，如：www.landbank.com.tw 與www.1andbank.com.tw，上述的兩個網址看起來是一樣的，可是在landbank的英文l部分改為數字 1，相信一定看不出來，當你連上該假網站後輸入你的帳密，很不幸的，你的帳密就送給駭客了，這就是釣魚網站。
2. 社交工程：駭客藉由電子郵件或即時通的方式傳送每個人有興趣的標題，如健康養身、情色、旅遊、公務、政治等各式熱門標題中夾帶開檔木馬或後門程式於正常檔案亦或是知名連結(如 landbank)之方式，藉以騙取您前往該網站進行帳密之輸入行為稱之。

一般而言，社交工程多與釣魚網站同時進行，如此上當的人就可大大增加，在此建議，對於不知名的郵件、網址，先看清楚該郵件之正確寄件人為誰，其郵件帳號是否正確，因駭客可偽裝成貴單位內部之人員發信，寄件人名稱是可偽造的，但寄件人郵件帳號就比較難偽造，故先請確認寄件人之郵件帳後是否屬實，在進行下一步的操作即可。我們將在未來提供更多的觀念給各位。

多一點確認，少一分損失

資料提供：數聯資安（圖片來源）
國立嘉義大學電算中心