DG19970003C1

## 三、網際網路用戶慎防詐騙

**01.10.'97 • 高等教育紀事報**

普林斯頓大學研究員提出一份報告，指出由於網際網路結構上的缺失，使得網路竊賊得以輕易地竊取網路用戶的信用卡號碼或其它機密的個人資料。

普大研究員說，利用目前電腦網路軟體技術，電腦竊賊不難侵入知名的網際網頁中，建構一個虛擬的網站，竊取不知情用戶的個人資料。雖然目前爲止，這種情況只是一個理論上可能存在的事實，由於其可能對個人造成很大的損失，網路用戶不得不防患於未然。

舉例來說，網路竊賊可侵入微軟公司的伺服器，改變其網頁中購買微軟產品的網址。欲購買微軟最新出版視窗九五的網路用戶進入微軟網站後，用滑鼠"click"適當的位置，不疑有他地認爲自己正游走於微軟的網頁中，於是輸入基本資料和信用卡號碼，等著產品寄到家中。不知情的用戶還不知道自己進入的是網路竊賊虛擬的網站，竊賊可以藉以窺探用戶的一舉一動，且利用這些竊取的資料從事不法的行爲。

普林斯頓大學電腦系助理教授 Edward W. Felten 說，目前網際網路結構還無法杜絕此類犯罪情形的發生。一個銀行用戶利用網路進入自己的帳戶，輸入密碼和帳號之後，一定不會假設自己有可能進入其它的網址，但根據普林斯頓大學提出的理論來看，這樣的假設是錯誤的。

這份報告提出三點建議以減低網路犯罪的可能性：

第一、取消網路閱覽器的 JavaScript 功能，網路歹徒可利用此功能來掩飾網站網址，以達到虛擬網站的目的。JavaScript 甚至可以製造一個假的視窗，讓使用者誤以爲真，而輸入機密的個人資料。

第二、網路用戶一定要時時注意閱覽器上顯示的網址是否正確，有些用戶爲了要使視窗加大，把螢幕上顯示網址的區域去掉，如此一來，雖有較大視覺空間，但增加了網路犯罪的可能性。

第三、用戶必需慎選欲進入的網站，儘量避免進入一些看起來很可疑的網址，例如“www.microsoft.com”和“www.micros0ft.com”完全不同，用戶必需非常小心

這篇報告的全文可於以下網址上查閱：

http://www.cs.princeton.edu/sip/pub/spoofing.html(附件 3，申玉微摘要)。