類別：資訊保護

【案號：*S980407*】

購物網站標錯價 疑遭駭客入侵

【資料來源：中央社 *98/09/28*】

焦點話題

○○家具連鎖店的購物網站傳出標錯價事件，千元禮券錯標成 *0* 元，估計 *10* 小時內湧進的訂單共計 *64* 億筆，涉及禮券總金額達新台幣 *6.4* 兆元。

消保官表示，○○公司代表至消保會說明，並澄清此次事件並非是標錯價格，因為網站上根本沒有賣禮券，禮券是消費者以 *20* 元積 *1* 點，累積 *3000* 點就贈送 *1* 張 *1000* 元的禮券，因為是贈送品，在內部電腦資料上價格是「*0* 元」。

○○公司說明，屬於內部電腦資料的禮券並沒有貼在公開的網站上，但有駭客入侵轉貼在公開的網站上，並破解公司每 *1* 種商品限制售出 *50* 件以內的程式，導致後來有 *4000* 多筆訂單，合計消費額達到 *6.4* 兆元，

○○公司強調第一時間已關閉主機，消保會也對○○公司提出 *3* 項要求，首先是關閉主機；其次是在 *30* 日提出遭駭客入侵的證明及有適當的解決方案；顧客的資料除提供警方偵查外，不做其它使用。

重點摘要

1. 網路購物網站應該加強網站資訊安全的維持，避免因遭駭客入侵或系統出問題，導致衍生消費爭議。
2. 若網路購物網站標錯價時，在證明對於標價錯誤沒有過失時，可以撤銷標錯的價格。

法律觀點

網路購物是現在時興的消費方式，消費者可以在任何地方透過網路完成交易，為民眾帶來很大的方便，資策會產業情報研究所預估，*2009* 年台灣網路購物市場規模將達到新台幣 *3,116* 億元，較去年成長 *30.4%*[1]，可見網路購物市場發展的潛力不容小覷。

本案例○○公司表示禮券是點數兌換贈品，因此在公司內部網站裡標示為 *0* 元，但有駭客入侵而將此標價貼在公開網頁上。駭客入侵○○公司內部網站的行為，會構成刑法第 *358* 條無故入侵他人電腦罪[2]。至於駭客將○○公司於內部電腦將禮券標示為 *0* 元的資訊變更成在網站上的公開資訊，也會構成刑法第 *359* 條無故變更他人電腦電磁紀錄罪[3]。此外，○○公司因此侵入行為所造成的損害，也可以對駭客請求民事的損害賠償。

至於○○公司對於消費者的責任，除非○○公司有預先保留決定接單與否的權利，否則依照民法第 *154* 條第 *2* 項規定，貨物標定價格陳列時，視為要約[4]，因此網友進行下單時，雙方即對買賣契約產生合意，雙方都必須受到契約的拘束。但因為禮券標示的價格並不是○○公司的意思，依照民法第 *88* 條[5]的規定，○○公司對於標價錯誤沒有過失時，可以撤銷標錯的價格。因此，○○公司恐怕必須證明對於網站的維護沒有過失，才能夠以駭客入侵為由，撤銷標錯的價格，但依民法第 *91* 條[6]的規定，對於信賴標錯價格的消費者因此遭受的損害，仍有民事損害賠償責任。然而，對於明明知道是網站標錯價格卻下單的網友，○○公司並無民事賠償責任。

因此，網路購物業者應該要謹慎維護網站資訊安全，避免遭駭客入侵，且在產品資訊公開於網站前，也要再三確認標示的資訊是否正確，否則一旦

---

[1] 資料來源 http://mic.iii.org.tw/intelligence/pressroom/pop_pressfull.asp?sno=173&type1=2。

[2] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[3] 刑法第 359 條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

[4] 民法第 154 條第 2 項：「貨物標定賣價陳列者，視為要約。但價目表之寄送，不視為要約。」

[5] 民法第 88 條第 1 項：「意思表示之內容有錯誤，或表意人若知其事情即不為意思表示者，表意人得將其意思表示撤銷之。但以其錯誤或不知事情，非由表意人自己之過失者為限。」

[6] 民法第 91 條：「依第八十八條及第八十九條之規定撤銷意思表示時，表意人對於信其意思表示為有效而受損害之相對人或第三人，應負賠償責任。但其撤銷之原因，受害人明知或可得而知者，不在此限。」

標示價格展示產品後，即會構成民法上的要約，網友下單後，契約即為成立有效，負有履約責任。更重要的是，此種事件可能會影響到公司的商譽，造成的損害恐怕不是金錢可以客觀衡量的。

管理 *Tips*

就本案例而言，最主要之關鍵點在於標錯價格是否為○○公司之過失，是以對○○公司來說，可從為○○公司過失及非○○公司過失 2 方面分別探討其管理之需求，如為○○公司過失，則應再從網站資訊的管理再行加強，包含線上資料更新的適當核可、資料更新後的確認等環節，確認其控管之完整性，如為非○○公司過失，則應從網站的防護機制再行加強，包含：網站伺服主機之防護機制(防毒、防駭-修補程式更新、弱點掃瞄)、網路的防護機制(防火牆、入侵偵測/防禦系統的設置)及應用程式的防護(避免後門程式- Code review)等機制。

另外公司也應考量在相關的控管程序、授權機制及防護機制是否有留存適當的控管紀錄，足資可在法律上證明已盡良善管理之責任，避免相關法律權責。

相關標準

A.10.4.1 對抗惡意碼的控制措施

應實作防範惡意碼的偵測、預防及復原控制措施以及適切的使用者認知程序。

A.10.6.1 網路控制措施

網路應適切地加以管理與控制，使其不受威脅，並且維護使用網路的系統與應用程式的安全，包括輸送中資訊。

A.10.9.1 電子商務

應保護在公眾網路上傳輸而涉及電子商務的資訊，使不受詐欺行為、契約爭議及未經授權的揭露與修改。

A.10.9.2 線上交易

應保護涉及線上交易的資訊，以防止不完整的傳輸、誤選路

(*mis-routing*)、未經授權的訊息修改，未經授權的揭露，未經授權的訊息複製或重演。

A.10.9.3 公眾可用的資訊

應保護公眾可用系統上可取得資訊的完整性，以防止未經授權的修改。

A.10.10.1 稽核存錄

稽核日誌係記錄使用者活動、異常及資訊安全事件，宜產生與保留一段議定的期間，以協助未來的調查與存取控制監視。

A.10.10.4 管理者與操作者日誌

系統管理者與操作者的活動應加以存錄。

A.12.6.1 技術脆弱性控制

應取得關於使用中資訊系統之技術脆弱性的及時資訊、評估組織對此等脆弱性的暴露，以及採取適當的措施以因應相關的風險。

A.13.2.3 證據的收集

在涉及法律行動(民事或刑事)的資訊安全事故後，對人員或組織的跟催措施，應收集、保存及呈現證據，以符合在相關審判時提出證據的規則。

A.15.1.3 組織紀錄的保護

應依據法令、法規、契約及營運要求，保護重要紀錄，免於遺失、毀損及偽造。