防範 Phishing 手冊內容

93.09.13

有一種新的網路詐騙手法稱為「phishing」，意為以「願者上勾」方式騙取受害人之個人金融資料，如帳號、密碼、身分證號碼及一些可藉以盜用受害人存款或信用卡等資料。歹徒取得資料後，甚至可使用受害人名義貸款、申用信用卡及駕照等，以致受害人信用破產。若民眾瞭解此種詐騙手法運作方式，便可避免受害。

「Phishing」詐騙方法：

典型案例，受害人收到發自某信用卓著且平日業務上時有來往公司之電子郵件（例如往來銀行），有時也可能冒用政府單位之來函；信上可能警告收信者因發生某些問題，若不立即處理，將可能產生嚴重後果，所用標題可能是「立即處理」或「立即聯絡以解決消費者帳戶問題」等字句，信中常提供網址以引誘收信人連結進入其詐騙網站，該網站與正式公司之網站模仿得唯妙唯肖，令人難以分辨，進入網站後常會跳出另一視窗以收集收信人之個人金融資料。有時候歹徒會要求收信人更改留存銀行之資料，或編造一些理由，要求收信人鍵入個人金融資料以利確認，如帳號、密碼、社會保險號碼及一些足以佐證個人身份之資料（如母親娘家姓氏或出生地等等），一旦回應這些資料，收信人即成為受害人。

如何自我保護：

1. 切勿應不明人士要求提供個人資料予他人，不論經由網路抑或電話，網站或電子郵件皆可被模仿得唯妙唯肖，其至連安全認證皆可能被模仿，爰此，若電子郵件非本人主動發起，切勿提供任何資料予對方。
2. 若相信對方是真正要接觸之對象，請親自確認。網址或電話號碼應由日常來往之帳單或電話簿查詢而得，關鍵在必須主導發動，且應使用已確認過之聯絡方式。
3. 切勿應不明人士要求以電話或其他網路操作方式提供密碼予他人。銀行絕不會要求核對帳戶密碼，只有歹徒才會搜集消費者個人金融資料以詐取存款。
4. 應有檢視個人戶頭內來往紀錄之習慣，以確認每筆紀錄皆為正確。若收到銀行對帳單日期過晚，應立即查明原因，若銀行提供電子查詢帳戶功能，請定期檢查進出紀錄以篩選出可疑之操作。

若不幸成為受害人如何因應：

1. 立即通知往來銀行，並告知已被騙之訊息。
2. 應向財團法人金融聯合徵信中心查詢，電話：23813939 轉 201－209，中心地址：台北市重慶南路一段二號十樓。

3.向各地區警察局報案電話 110。

4.反詐騙諮詢專線 165。

5.內政部警政署刑事警察局電腦犯罪檢舉專線（02）27697403、傳真（02）27644402、網址：http：//www.cib.gov.tw。

消費者防範詐騙之道：

1. 切勿經由網路抑或電話提供個人資料予不明人士，如帳號、密碼、身分證號碼等。
2. 切勿點選不明電子郵件內提供之鏈結，此種鏈結常隱藏有電腦病毒在其中，會破壞消費者電腦的正常運作。
3. 切莫輕易相信電子郵件中之警告，「如若不依其步驟作業即會遭至嚴重後果」等心生恐懼，而按照其指示操作，或提供個人資料以供其確認。
4. 若消費者相信對方是真的有事要處理，務必親自直接輸入網址或由以往曾經使用過之 Book Marked（我的最愛）中取得其網址，而不可使用對方電子郵件內所提供之連結，予以回應。
5. 若不幸成為受害者，請立即行動以求自保：通知來往金融機構、個人信用紀錄檔案標示警訊以及注意帳戶進出情形。