

## 防範釣魚網站宣導

### 壹、慎防網路釣魚 (Phishing)

網路釣魚為網路詐騙手法，歹徒會利用偽造的電子郵件或網站，騙取使用者的個人私密資料(例如:身分證號碼、銀行帳號、信用卡號或密碼等)，並進行犯罪行為。和安保險代理人股份有限公司(後稱本公司)不會寄發電子郵件要求客戶輸入身分證號或密碼等資訊，若您收到以本公司名義寄發的可疑郵件，難以辨識真偽時，請不要回覆此封電子郵件，若有任何問題請隨時與我們聯繫。

為了保障您使用本公司網站各項服務的安全，當您透過電子郵件或是其他網站點選連結本公司網頁時，請務必仔細核對瀏覽器的網址列，應顯示本公司之正確網址。

網路釣魚主要是利用人類信任或好奇的心理，誘騙受害者掉入詐騙圈套。

### 貳、常見的三種釣魚手法

- 一、透過 E-mail 或是其他即時通訊軟體，發送金融機構或是入口網站假連結 (例如 [www.google.com](http://www.google.com) 變成 [www.gooogle.com](http://www.gooogle.com))，通知用戶需要登入網站與修改資料等訊息，點擊後就會下載惡意軟體或是利用跟原本網站類似的表單騙取相關資料。
- 二、假冒成活動優惠或抽獎網站，通常會使用「優惠」、「免費」或「限量」等字句來吸引人點擊連結，當用戶點入這個偽裝的活動網站，填入相關資料，就讓詐騙者有機會利用這些資料去進行不當行為。
- 三、歹徒利用社群網站向用戶傳遞「問候」並「請求幫忙」的詐騙訊息，通常會使用盜取得手的帳號，偽裝身分傳訊息給帳號中的親友，要求你幫忙購買遊戲點數或借手機號碼進行小額付款。面對來自網路上各方親友突然的請求訊息時務必冷靜確認，可先詢問對方只有雙方才知道的私事，以確認對方的身分。

### 參、「釣魚信件」的防範之道

- 一、點選信件中的網站連結前，移動滑鼠檢查真實連結網址。
- 二、確認信件來源，切勿輕易下載附加檔案。
- 三、收到要求提供個人資料的電子信件要小心。
- 四、檢查信件內是否有拼寫錯誤和語法錯誤。
- 五、自行連線至官方網站再輸入資料。
- 六、安裝具有防範網路釣魚技術的資安軟體。

#### 肆、本公司官方網站、網路投保網站之正式網址

- 一、和安保險代理人(股)公司官網：<https://www.hoan.com.tw/>
- 二、和安保險代理人網路投保：<https://mi.hoan.com.tw/HoanB2CWeb>

#### 伍、消費者保護相關資訊連結

- 一、行政院消費者保護會：<https://cpc.ey.gov.tw/>
- 二、金融監督管理委員會保險局：<https://www.ib.gov.tw/>