

陸、測試信件樣本

一、信件範本一

親愛的消費者您好：

恭喜您於114年1-2月期別索取的雲端發票有1筆中獎！

感謝您選擇財政部電子發票整合服務。但由於載具設定有誤，您的中獎金額無法自動匯款，請依以下步驟更新您的資料。

1. 請點擊載具歸戶[更新頁面](#)，打開更新操作界面。
2. 輸入您的手機號碼和驗證密碼。
3. 選擇“更新載具歸戶”並完成操作。

※請注意以下可能導致匯款失敗的情況：

1. 您所提供之身分證字號須與金融帳戶所有人之個人資料一致，否則將造成匯款作業失敗。
2. 如匯款失敗將以電子郵件通知您，請依郵件內容於指定日期前至整合服務平台確認及修改領獎資料，以利中獎獎金匯入。
3. 請立即將悠遊卡、一卡通及信用卡等歸戶至手機條碼，即享有自動對獎、中獎主動通知及獎金自動匯入等服務。

感謝您使用雲端發票，敬祝愉快。

如您有其他問題，請與我們聯繫：

整合服務平台客服專線：0800-521-988

整合服務平台客服信箱：[請聯絡我](#)

整合服務平台智慧客服：robot.einvoice.nat.gov.tw

兌獎客服專線：4128282(手機請撥：02-4128282)

兌獎單位客服信箱：invoice@mail.fisc.com.tw

※此封信件僅供中獎通知，非領獎證明，中獎發票兌領方式依據您開獎前實際設定為準。

圖 15：信件範本一

二、 信件範本二

 盡快回覆此活動

☒ 傳送電子郵件給召集人

新增郵件 (選用)

✓ 接受

✗ 拒絕

 關注

...

mis-windows@gmail.com 邀請您加入排定的 Webex 會議。

由 Eson Huang 主持

2025年1月19日

上午 9:10 | (UTC+08:00) 台北 | 2 小時

加入會議

更多加入方式：

從會議鏈結加入

<https://mis-window.webex.com/tia-window-tc/j.php?MTID=m28e87883e80zp8e83847e5db4ax57198>

透過會議號加入

會議號 (存取碼)：2471 411 3755

會議密碼：saQf9BpQm43

透過電話加入

僅使用 VoIP

從視訊系統或應用程式加入

撥打 24409162152@mis-window.webex.com

您也可以撥打 221.5.298.7 並輸入您的會議號。



圖 16：信件範本二

三、 信件範本三



你的 Facebook 安全驗證碼

你好，
你的安全驗證碼為：

3 2 9 3 7 5 4 2

我們必須驗證你的電子郵件地址，以便在 Facebook 確認你的身分。請在瀏覽器中貼上這組驗證碼，且該驗證碼只能使用一次。

如果你並未索取驗證碼，那麼可能有人正在嘗試登入你的帳號。[你可以更改密碼，以確保帳號安全。](#)

謝謝！
Facebook 帳號安全團隊

來自



© Facebook, Meta Platforms, Inc., Attention: Community Support, 1 Meta Way, Menlo Park, CA 94025

這是寄送到 doome00929@gmail.com 的訊息。

為了保護你的帳號安全，請勿轉寄這封電子郵件。瞭解詳情

圖 17：信件範本三

四、信件範本四



臺灣銀行
BANK OF TAIWAN

網路銀行首頁 | 臺灣銀行首頁

「臺銀行動+」交易通知

貴用戶 已於 2025/06/13 01:35:05

完成 - 臺銀支付申請

申請日期：2025/06/13

注意事項：

- 1.您必須設定完成「臺銀支付」密碼後，始可啟用。
- 2.您必須申請本行「簡訊動態密碼服務」或「行動推播動態密碼服務」方可以「臺銀支付」功能進行帳單支付。
- 3.若您尚未申請本行「簡訊動態密碼服務」或「行動推播動態密碼服務」，請先備妥讀卡機及晶片金融卡後，於網路銀行申請「簡訊動態密碼服務」或「行動推播動態密碼服務」。

網路銀行交易安全公告事項

- 為保護您不連結至偽造網站，建議您直接鍵入本行網路銀行網址 <https://ebank.bot.com.tw/>，於連結成功後再設定此網址為我的最愛，請勿從其他搜尋引擎或線上廣告連結到本網站。
- 請勿隨意下載來路不明的程式或電子郵件，及使用公共場所之電腦（如：網咖）登入網路銀行，以防他人竊取您的使用者代碼或密碼；勿隨意洩漏您的帳戶資料或個人資料（如個人身分證字號、提款卡卡號、信用卡卡號、生日等）。
- 為了預防您離開電腦過久，以至遭他人竊用，若您欲離開本行網路銀行，敬請務必執行簽出，以保障您的權益及帳戶安全。
- 若您需要變更電子郵件，請隨時利用 臺灣銀行網路銀行 進行變更。

本訊息由 臺灣銀行 提供
若您對以上通知有任何問題，歡迎來電(02)21910025 或 0800-025-168(限市話)。謝謝!

隱私權聲明 | 資料保密 | 資訊說明 | 資安政策

營業時間：週一至週五 9:00至15:30；延長營業時間之分行，請參考 [服務據點 說明](#)
電話：(02)2349-3456 客服中心：0800-025-168 (限市話) | (02) 2191-0025

圖 18：信件範本四

柒、改善與建議

建議對於內部同仁應定期執行電子郵件警覺性測試，以及定期宣導社交工程之資安相關知識，以提升同仁對於社交郵件的資安意識。最佳防範這類社交工程型態攻擊的方法，就是要隨時提醒使用者要有資安警覺，不要點選來路不明的電子郵件。

對於防範電子郵件社交工程，一般使用者可多注意以下細節。

郵件讀取：

1. 檢查確認寄件者(是否為認識的人或業務需要)。
2. 檢查確認郵件主旨(是否為奇怪的主旨或與寄件者不搭配)。
3. 不輕易開啟郵件中的超連結以及附件。
4. 重要檔案可雙方約定密碼，並對檔案加密後傳送。
5. 開啟超連結或檔案前，確認對應軟體(如 Windows、IE、Office)都保持在最新的修補狀態。
6. 檢查是否有必要提供個人資訊。
7. 若懷疑郵件來源，透過電話或其它方式向寄件人於開啟前確認。

轉信或寄信：

1. 未經查證之訊息，不要轉寄。
2. 轉寄郵件前先將他人郵件地址刪除，避免別人郵件地址轉寄出去。
3. 寄送郵件給群體收件者時，應將收件者列在密件副件，以免收件人資訊外洩。
4. 勿將公務信件轉寄私人電子信箱地址。

變更收信軟體的設定，也可以提高安全性。

1. 不要自動下載圖檔。
2. 關閉郵件預覽功能。
3. 以純文字開啟郵件。