反詐騙教育宣導～進修部提醒您

反詐騙宣導(資料來源：內政部警政署-釣魚簡訊防制宣導)

001.一點就詐!小心釣魚簡訊讓手機中毒!

詐騙集團會利用發送簡訊，以「貨運單號查詢」訊息誘騙民眾點擊釣魚連結。點擊後被導引至假冒之貨運業者網頁（例如 黑貓宅急便)，並要求下載有毒之檔案: 在 Android 系統稱為 應用程式套件(apk.)；iOS 系統稱為 設定描述檔(ipa.) 。

民眾不疑有他下載後，手機就有可能被詐騙集團控制，利用您的手機再繼續發送詐騙簡訊給更多的人。

提醒您，可疑網址不要點，切勿隨意安裝來路不明的程式，避免手機中毒!

002.安卓用戶照過來 165教您 開啟垃圾訊息阻擋功能阻擋詐騙簡訊

安卓的用戶，手機請開啟垃圾訊息阻擋功能

開啟【垃圾訊息阻擋】

【垃圾訊息阻擋】

【啟用】垃圾訊息阻擋功能

內政部警政署 刑事警察局
CRIMINAL INVESTIGATION BUREAU
165 Anti-fraud Hotline Service

標榜高額獲利、穩賺不賠
獲利來源不明或
獲利率顯不合理之情形
應避免投資

請勿輕信網友介紹
來路不明之投資管道

小心求證為防詐之不二法門

003. iPhone 用戶照過來 165 教您阻絕透過 iMessage 發送的詐騙簡訊

不斷收到惱人的投資或借貸簡訊?　　165 專線提供 4 種方法給您參考

透過關閉 iMessage 功能 阻絕詐騙簡訊

1、單則簡訊封鎖、刪除與回報

2、設定【不使用電子信箱接收 iMessage 】

3、開啟【過濾未知的寄件人】功能

4、關閉 iMessage 服務

♦若您並無使用 iMessage 進行通訊，建議可直接關閉此項功能。

♦若您有在使用 iMessage 通訊，則可參考前 3 種作法。

最重要的，還是要認明簡訊內容及詐騙話術喔!

請勿輕信網友介紹來路不明之 高額獲利投資管道 或 超低利率貸款

內政部警政署 刑事警察局 CRIMINAL INVESTIGATION BUREAU 165 Anti-fraud Hotline Service

Quick TIPS 單則簡訊封鎖、刪除與回報

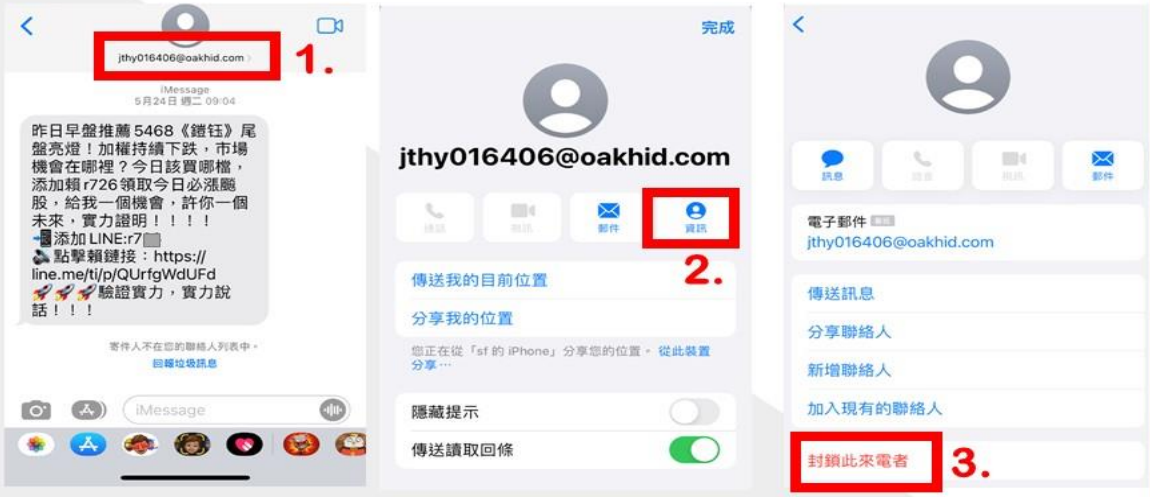
Quick TIPS 設定【不使用電子信箱接收iMessage】

Quick TIPS 開啟【過濾未知的寄件人】功能

Quick TIPS 關閉 iMessage 服務

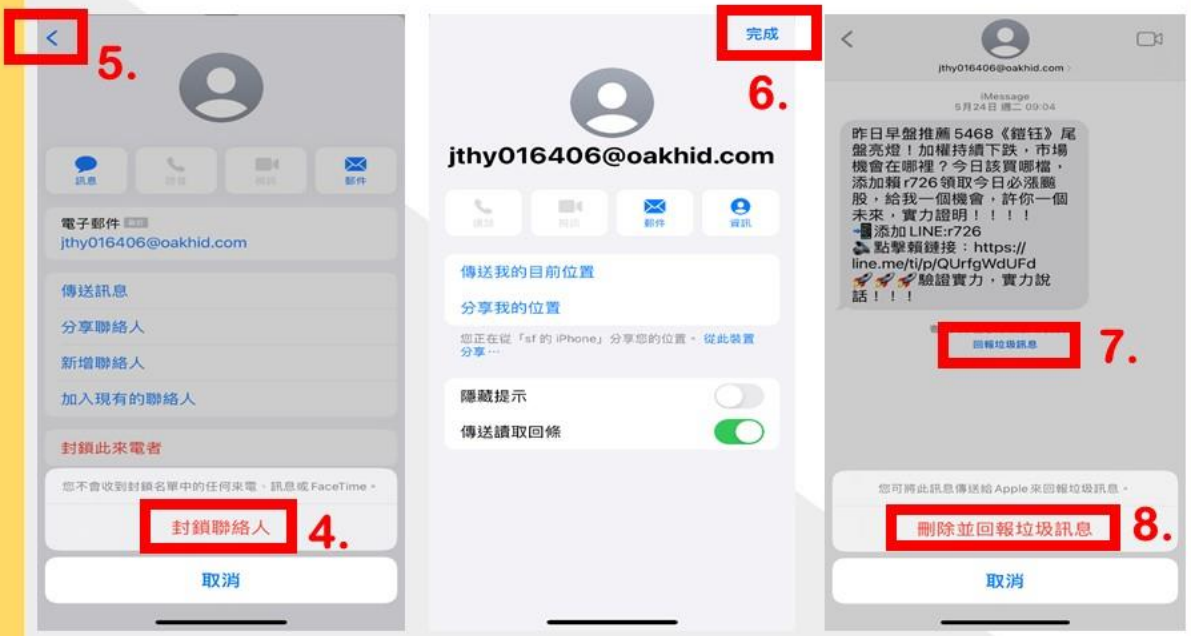
阻絕惱人詐騙簡訊 一勞永逸

單則簡訊封鎖、刪除與回報



點擊【郵件>】 ➡ 點擊【資訊】 ➡ 封鎖此來電者

單則簡訊封鎖、刪除與回報



【封鎖聯絡人】回上一頁 ➡ 點擊【完成】➡ 回報垃圾訊息 刪除並回報垃圾訊息

設定【不使用電子信箱接收iMessage】

點擊【設定】➡ 點擊【訊息】

設定【不使用電子信箱接收iMessage】

【傳送與接收】 取消勾選電子郵件

開啟【過濾未知的寄件人】功能

點擊【設定】 點擊【訊息】

開啟【過濾未知的寄件人】功能

【訊息過濾】 ➡ 開啟【過濾未知的寄件人】

關閉 iMessage 服務

點擊【設定】 ➡ 點擊【訊息】 ➡ 關閉【iMessage】

004.防制詐騙簡訊全民一起來，165系統再升級民眾檢舉更便利

你是否曾經收過類似的詐騙簡訊?「我是你的服務顧問林XX，麻煩聯絡我一下：fraud777」、「疫情紓困專案，點https：//bit.ly/*626****」或是「您的貨運單號是70****76，透過https：//qw*r.t*ui.com查詢」。

詐騙集團以假冒金融機構、股票投顧、投資理財、政府部門或郵政、快遞公司等名義傳遞詐騙簡訊，透過各種管道發送訊息將詐騙的觸手伸至每一部手機、電腦及行動裝置。刑事警察局觀察，以投資詐騙簡訊為例，以往詐騙集團會以「飆股、報明牌」等用詞發送簡訊，近來更演變為「有急事找你、找你好久了」等讓人疑惑的裝熟用詞發送詐騙Line ID至民眾手機，誘使民眾好奇加入；另外以紓困貸款詐騙簡訊為例，詐騙集團常以「你的申請已核准」或於簡訊內容夾帶詐騙網址，誘使民眾點擊進入網頁，騙取個資。

其實不難發現，詐騙集團可能透過SMS簡訊或是iOS特有的iMessage以及個人電子郵件等管道讓民眾接收詐騙訊息，刑事警察局提醒民眾，收到不明來源之簡訊或郵件邀請民眾加Line或提供詐騙網址，要求您輸入個資，都應該提高警覺。請多加查證，勿隨意上傳個人證件或提供帳號、信用卡資料，避免讓詐騙集團綁定電子支付設定轉帳或盜刷信用卡。

另為便利民眾檢舉詐騙簡訊並提升檢舉意願，刑事警察局已簡化165全民防騙官網及警政服務App「網路檢舉」功能，呼籲民眾如有收到詐騙訊息，僅須透過「165全民防騙官網或警政服務App」，填入「姓名、聯絡電話、註解說明(將訊息複製貼上)及驗證碼」等資訊，再將訊息內容截圖上傳後送出，即可快速完成詐騙訊息的檢舉，期待能透過簡化檢舉詐騙的程序，讓民眾更有意願一起來防制詐騙。

公 告

165全民防騙官網

內政部警政署165全民防騙網
National Police Agency,Ministry of the Interior
165反詐騙諮詢專線
我要報案 我要檢舉

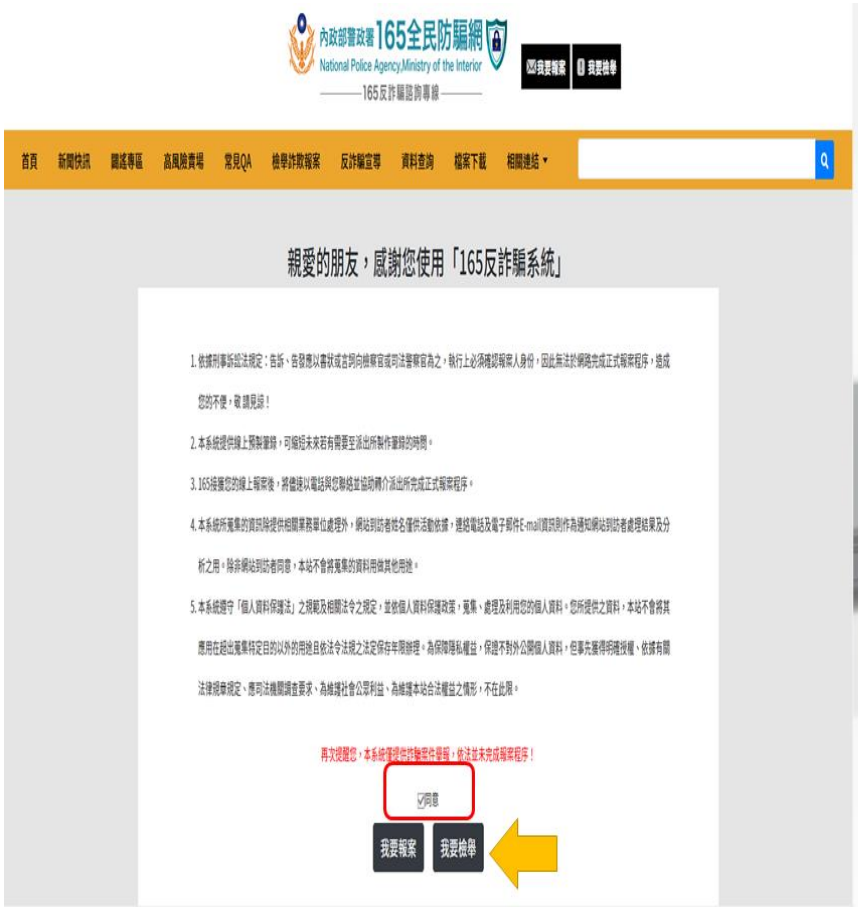
檢舉功能更新

1

進入官網首頁
點擊上方**我要檢舉**
或
檢舉詐欺報案分頁

跳轉進入報案檢舉頁面

內政部警政署 刑事警察局
CRIMINAL INVESTIGATION BUREAU
165 Anti-fraud Hotline Service



2

進入報案檢舉頁面

閱覽完文字說明後

點選同意

點擊我要檢舉

3

僅需輸入必填欄位

姓名
聯絡電話
註解說明
驗證碼

+新增詐騙簡訊截圖

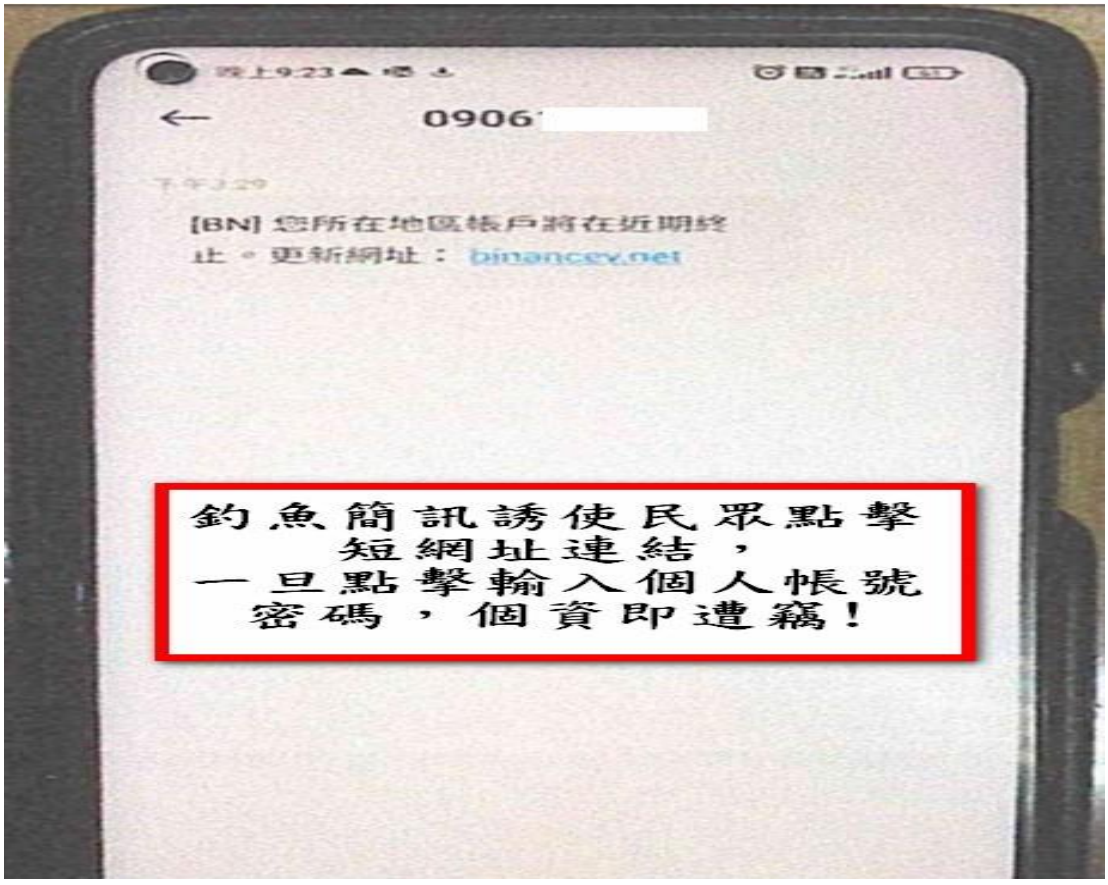
點擊「送出」

005. 手機簡訊附釣魚網站 帳號密碼全數親手交出

網路釣魚是最廣泛和最常見的網路攻擊技術，提醒用戶對於個人電腦設備、電子郵件以及帳戶資料應自行妥善保管。在這個網路時代帶來生活便利的同時，也隱藏著相當的風險，各種資訊都有可能會從民眾自己的手中被惡意獲取及利用。

165 反詐騙諮詢專線提醒您，收到各類資訊、通訊內容時，先保持「零信任」態度，因歹徒常利用似是而非的拼音混淆視聽，若收到可疑簡訊，切勿直接點擊，請先比對發送簡訊內容、短網址連結等是否為官方資訊；若無法立即辨識，可透過公司客服專線、電子郵件或官方 LINE 帳號確認真偽，亦可撥打 165 反詐騙諮詢專線或 110 報案專線諮詢、查證，避免遭受詐騙!

新聞連結 https://news.tvbs.com.tw/local/1774640



006.<收到支付運費電子郵件 請勿輕信填輸信用卡資料>

近日詐騙集團假冒『台灣宅配通』發送電子郵件

內容為👉某貨件(編號)仍在等待您的指示 支付費用後將立即發貨📦

並提供點擊連結跳轉至網頁要求你輸入信用卡💳資料支付運費

#內文很多簡體字

這是詐騙集團亂槍打鳥行騙💢

請民眾注意⚠️⚠️⚠️

收到不明郵件或釣魚簡訊請務必保持警覺🤨、先查證🧐，勿輕信詐騙集團話術填輸信用卡資料，以免信用卡遭盜刷扣款💸

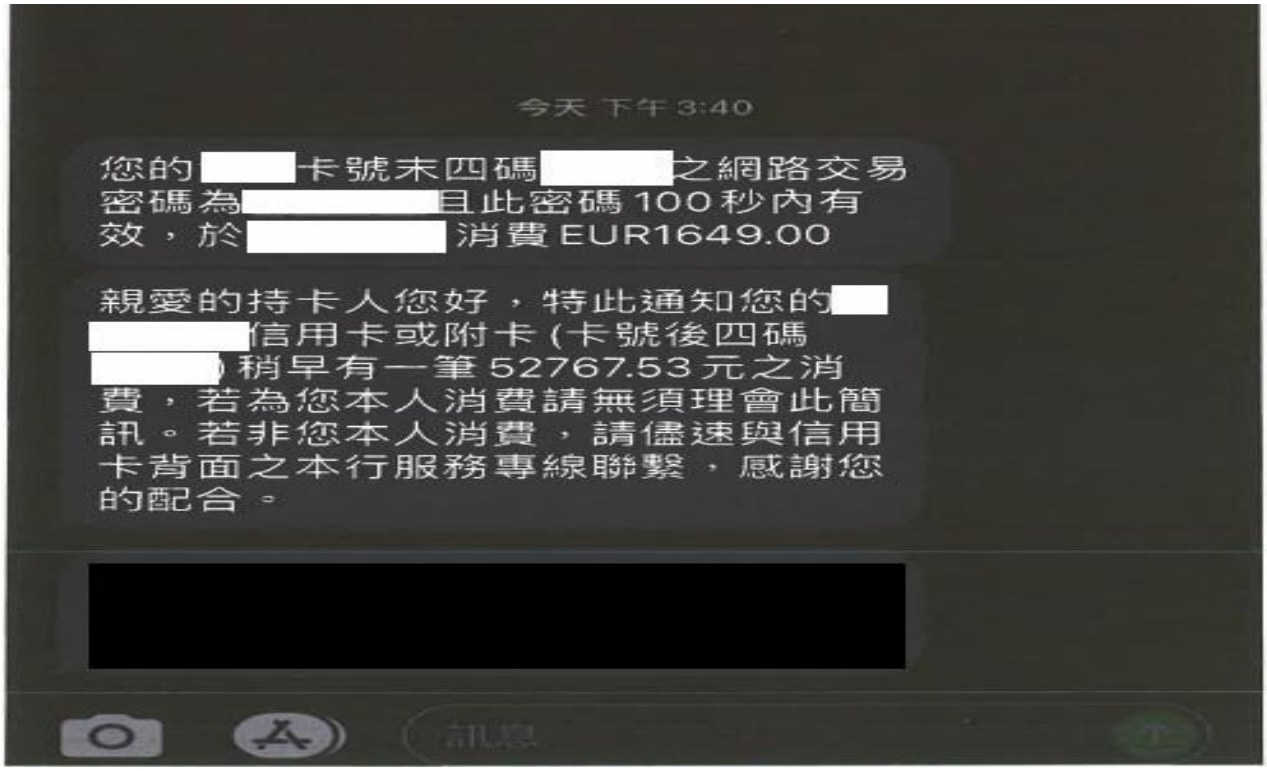
台灣宅配通官網

🔗https://www.e-can.com.tw/news_activityDetail.aspx?id=3.....

007.收到簡訊說欠缺資料無法運送包裹？輸入信用卡恐遭盜刷

近期有民眾接獲一封 +46 開頭的手機簡訊，內容為「欠缺資料，我們無法運送您的包裹」，並附上包裹編號及短網址。

由於民眾原本就有網購習慣，便不疑有他點擊簡訊中提供的網址，接著連結到國際快遞網站(近期為假冒 DHL 及 FedEx)，逐步填輸個人資料，登打信用卡號進行網上付款，並自行輸入驗證碼。等收到銀行通知確認刷卡金額為新臺幣幾萬元時，驚覺簡訊、填輸個資的網站全都是假的，信用卡已被盜刷!



經查，此為歹徒透過亂槍打鳥的方式發送簡訊，以包裹正在等待送達、出現問題為由，並附上釣魚短網址誘騙點擊，連結至假冒的國際快遞網站後，要求輸入姓名、信用卡卡號、有效期限、安全碼等個人資料來支付郵資或手續等費用。若不察完整填輸，個人資料立即遭竊取用以盜刷，俟收到銀行通知消費簡訊提醒，始知遭到詐騙。

針對此類手法，DHL 於官網提供詐欺防制意識說明，提供辨別方法，例如簡訊詐騙通常會含有造成混淆的短網址連結，或者發送簡訊電話特殊，例如開頭為 +235、+46 等，您可截下含有可疑電話和簡訊的螢幕畫面，通報至 phishing-dpdhl@dhl.com。

FedEx 亦於官網提供線上詐騙警示說明，提醒用戶若收到可疑郵件、簡訊，請立即刪除，切勿輸入任何個人資訊。這些快遞公司並不會向客戶傳送不請自來的、要求其提供包裹、請款單、帳號、密碼、個人資訊的電子郵件。

165 提醒您，收到各類資訊、通訊內容時，先保持「零信任」態度，先確認簡訊發送電話、點擊後連結網址是否有被混淆。另外當平時有已知的郵局包裹、郵件運送時，需特別提高警覺，與寄送方保持聯繫，亦不隨便點擊釣魚連結、輸入信用卡資料等個資。萬一誤輸入並送出了信用卡資料時，請立即通知發卡銀行啟動停卡，將損失降至最低。

008.假冒高鐵公司寄送電子郵件，稱「填表單領回饋」無影謀?

民眾向高鐵表示 😈接獲疑似台灣高鐵公司相近名稱之英文社交工程詐騙郵件，內容要求點選互動連結後可獲得免費車票/2300 元回饋的真實性😈

台灣高鐵澄清，實無相關活動或郵件寄送，請民眾切勿點選/操作，避免個資外洩或權益受損。

🔗台灣高鐵官網澄清公告連結 https://www.thsrc.com.tw/...../0a78bc6f-5622-420f.....

009.快遞已發，請您查收？假的!請勿點選!!

近期不少網友接獲一則「快遞已發，請您查收」的簡訊，經查這是「釣魚簡訊」，如果收到請不要點擊連結，也不要下載任何程式、輸入帳號密碼(包含 Google 帳號或 Apple ID、信用卡帳號密碼等)，如果點進去連結進宅配業者網站(如黑貓宅急便、宅配通等)，接著出現要求安裝.apk 檔案，這一定是假的，請提高警覺。

黑貓宅急便澄清稿（都說了沒這回事↓，請小心）

公告

提醒各位消費者，若收到簡訊有疑慮可撥打客服或反詐騙電話查證	2019/07/11

由黑貓宅急便發出的簡訊通知皆不會有任何連結，若您收到署名為黑貓宅急便發出的簡訊通知，內容為請您簽收的電子憑證或是網址連結等都可能為詐騙行為，請勿點選網址，如果有疑慮可以撥打黑貓宅急便客服專線412-8888，或是撥打165反詐騙電話諮詢查證，造成不便，敬請原諒。

https://www.t-cat.com.tw/news/BulletinDetail.aspx?BType=100&ID=1303