Email Threats Sample Report
Q4 2012

Openfind™

垃圾信來源

根據 Openfind 電子郵件威脅實驗室於 2012 年 Q4 針對全球垃圾郵件來源 IP 觀察研究，垃圾信來源國家的前三名分別為中國、澳洲與美國，依序佔整體垃圾信的 28 % 、9% 與 6%。 如同前季結果，中國仍為全球主要垃圾郵件來源，並比第二名高出近 20%。其後的順位則從第三季的印度、日本，換為澳洲、美國，並皆不到 10%。

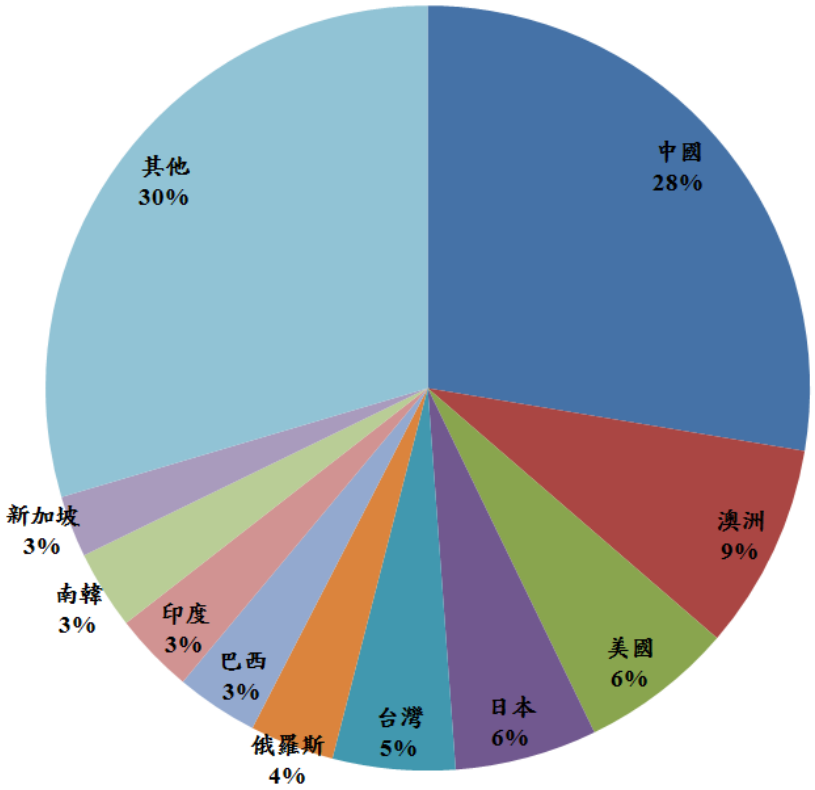

圖 1. 2012 年第四季垃圾信來源國家分布

細部觀察 10 月、11 月及 12 月來源比例，可發現澳洲在 11 月時，突然冒出高於中國的垃圾信件量，在 12 月時又降至 1.8 %，推測可能跟第四季時部分業者透過大量發送廣告信件之方式明顯提升業績，同業一起跟進，造成垃圾郵件量衝高，後又因主關單位對業者開罰後產生殺雞儆猴之效，垃圾郵件量又再度降低。在上一季中較美國高出一個名次的日本，在本季出現反轉，觀看三個月份的垃圾信件量發現，美國每月垃圾信量不低於日本， 2013 年第一季可持續觀察美國與日本的拉鋸戰。

表 1. 2012 年第四季垃圾信來源國家比例

國家	10 月	11 月	12 月	季平均	季排名
中國	28.5%	20.3%	35.1%	27.6%	1
澳洲	0.1%	23.5%	1.8%	8.7%	2

美國	7.9%	5.3%	6.2%	6.5%	3
日本	7.5%	4.4%	6.2%	6.0%	4
台灣	4.8%	2.6%	8.6%	5.2%	5
俄羅斯	3.8%	3.5%	3.4%	3.6%	6
巴西	5.4%	2.6%	2.3%	3.5%	7
印度	4.0%	3.3%	2.7%	3.4%	8
南韓	3.9%	1.8%	4.4%	3.3%	9
新加坡	2.3%	0.9%	4.8%	2.6%	10
其他	31.8%	31.8%	24.4%	29.6%	

台灣目前在季排名位居第五，垃圾郵件來源比例不低，值得重視，甚至在 12 月時出現了 8.6 %的高峰，當月僅次於中國，中國與台灣的垃圾郵件來源高低曲線具有相似趨勢，最低點皆出現在 11 月，而中國在 12 月的反彈力道較大。Openfind 電子郵件威脅實驗室會持續觀察與監控全球各國垃圾郵件發布狀況，掌握威脅趨勢，透過雲端防護技術，第一時間有效讓 MailGates 的用戶免除垃圾郵件困擾。

URL 內容解析

Openfind 電子郵件威脅實驗室與鴻璟科技共同合作深入觀察垃圾郵件內含之 URL 網頁內容，並將網頁進行分類，下表為本季網頁內容分類狀況。最多的網頁主題為購物相關類別，顯示約有 24 % 的垃圾郵件網址會導引收件人前往購買物品之網頁，多為商品廣告、EDM 、商品目錄等等購物訊息。

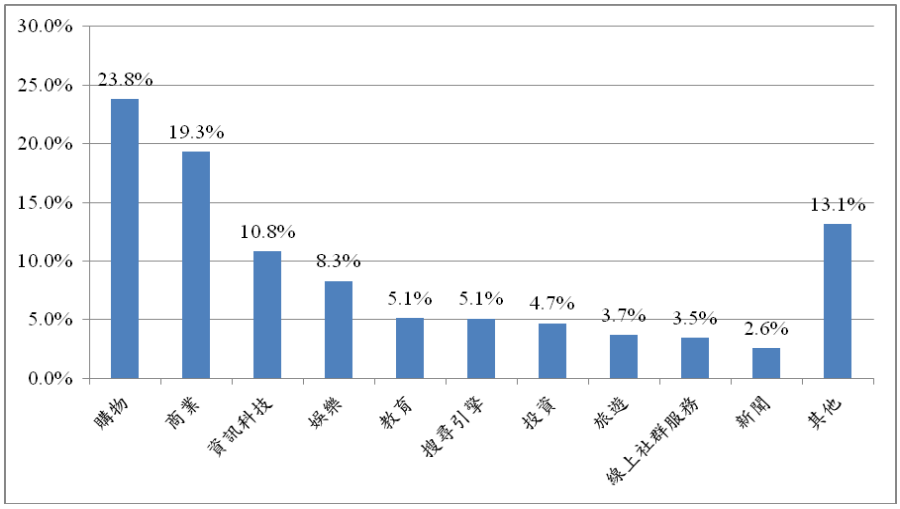

圖 2. 2012 年第四季垃圾信 URL 網頁內容分類

除了滿足現代人快速的購物需求外，網路使用者在財務方面對於商業訊息、投資快訊也常有眾多接觸，在休閒議題上面，演藝娛樂、旅遊景點、或社群網路服務也都榜上有名，皆貼近民眾生活，顯示垃圾郵件所含之 URL 亦可表達出部分網路使用者之潛在關心議題。

表 2. 2012 年第四季與第三季 URL 網頁內容分類比較

	第三季		第四季	
排名	類別	比例	類別	比例
1	購物	24.4%	購物	23.8%
2	商業	20.3%	商業	19.3%
3	資訊科技	9.0%	資訊科技	10.8%
4	娛樂	6.6%	娛樂	8.3%
5	投資	5.7%	教育	5.1%
6	搜尋引擎	5.3%	搜尋引擎	5.1%
7	線上社群服務	4.5%	投資	4.7%
8	教育	4.0%	旅遊	3.7%
9	旅遊	3.5%	線上社群服務	3.5%
10	新聞	2.5%	新聞	2.6%

觀察第三季與第四季 URL 網頁內容，可發現兩季前十大排名主題大同小異，甚至前三大類別購物、商業、資訊科技的排名相同且比例相似，近期若要著手處理垃圾郵件防護過濾困擾時，可以先從購物、商業及 IT 相關議題進行處理，設定特殊關鍵字或進行樣本訓練，可有效預防大多數垃圾郵件問題。Openfind 電子郵件威脅實驗室將持續研究垃圾郵件網頁分類趨勢，以期達成對症下藥，有效屏除垃圾郵件所帶來的種種威脅。

垃圾信散播手法

延續上一季垃圾信發布模式，轉址服務仍為垃圾信散布的主要手法，相關攻擊模式說明如下：

1. **透過轉址服務網站或其它手法間接轉址（Redirect）**
   在本季中，垃圾信發送者慣用的手法仍是在信中的超連結上作文章；為了隱藏帶有威脅的真實網址位置，除了轉址服務或短網址服務網站，有些攻擊者自己也申請網路上的主機名稱，幫助作轉址及隱藏目標網站網址的功能。

2. **大陸地區的偽造 EDM**
   本季許多簡體商業網站垃圾信內容是像 EDM 一樣加入圖片、排版以及『如果您无法阅读此邮件，请点击这里』等連結，較不同的是廣告目標網站中，中國知名拍賣網站的比率明顯提高。

3. **五花八門的釣魚信件攻勢**
   在同是以超連結為主的各式垃圾信中，以釣魚信件對使用者威脅最大，因為其超連結背後便是駭客準備的陷阱，若是一不小心點入超連結，便得面臨各種資安上的威脅，比單純廣告信還嚴重。

垃圾信樣本

和前一季相比，本季中釣魚信比率上升了一些，其中有趣的例子之一便是針對 Openfind Mail2000 線上用戶而來的釣魚信件：

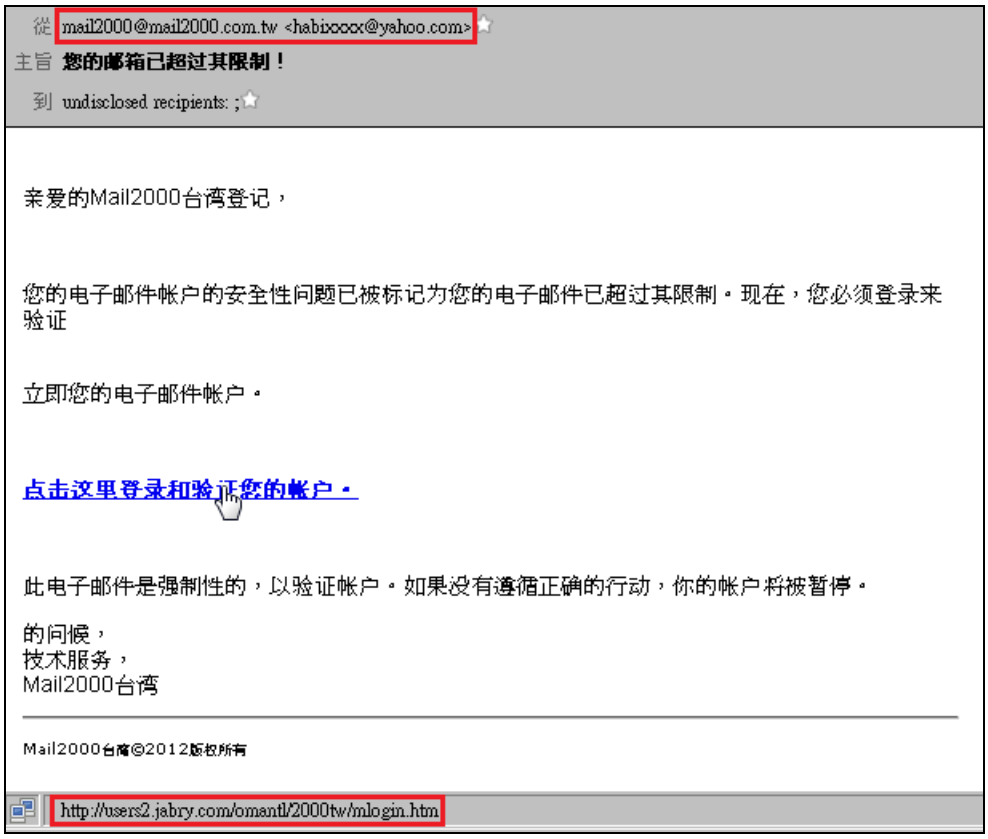

圖 3. 假冒 Mail2000 電子信箱的釣魚信件

在此例中，垃圾郵件發送者以收信者的電子郵件帳戶有安全性問題以及信箱信件超出容量為由，想騙取使用者點選信裡的超連結以進行後續動作，不過使用者打開信件後便可注意到，寄件者的網域同時出現 mail2000.com.tw 及 yahoo.com 不合常理。再者信中的網址仔細觀察後發現其網域 jabry.com 與 Mail2000 沒有關係，而是一家網頁寄存商，且信中語句極不通順，可以想見這封釣魚信應是不諳中文的駭客所寄。

圖 4. 偽造 Mail2000 電子信箱的釣魚頁面

圖 5. 實際的 Mail2000 電子信箱頁面

連結到其網址 (http://users2.jabry.com/omantl/2000tw/mlogin.htm) 後，如圖 3，瀏覽器並未轉址到 Mail2000 相關網址，而是在原網址，發現頁面有部份亂碼文字及排版走位，此外其它部分和圖 4 的正牌 Mail2000 頁面沒什麼差別；而檢查此頁面的 html code 時找到頁面中的登入表格如下：

```
<form name="form1" onsubmit="return do_submit()" action="http://loganbnksa.freeserver.me/mailtw/olb.php" method="post">
```

可發現其目標網站也和 Mail2000 沒有關係。接著嘗試由此釣魚頁面的表格登入：

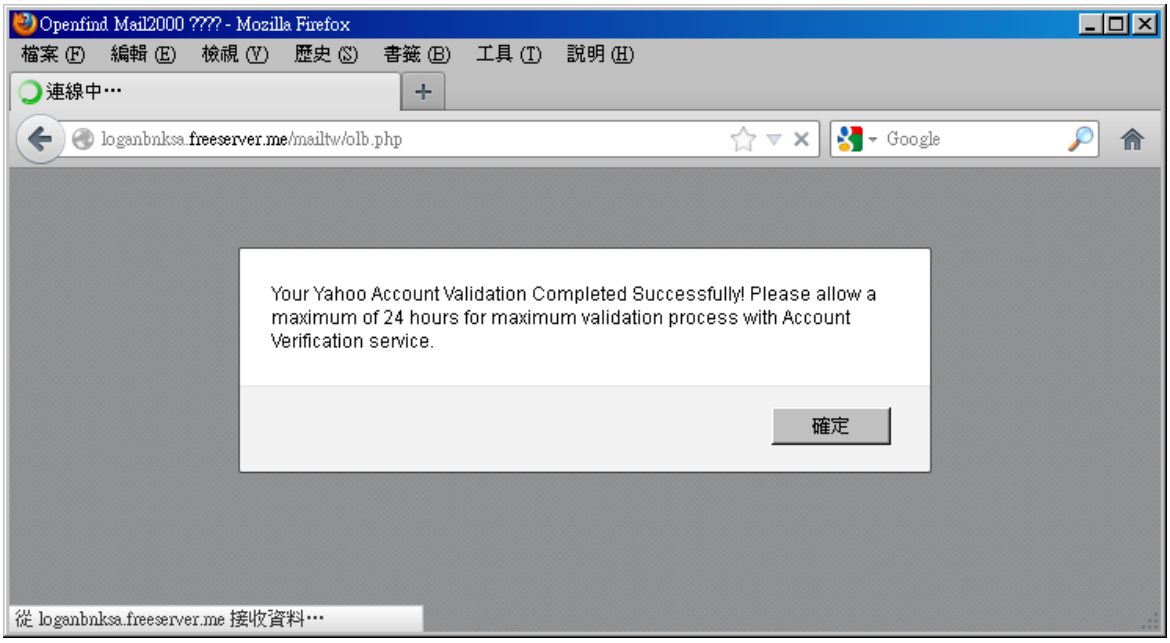

圖 6. 由釣魚頁面登入後的提示頁面

在不輸入帳號及密碼的情況下，直接按釣魚網頁上的登入按鈕後，頁面上以英文秀出帳號確認成功的對話視窗，接著瀏覽器便轉址到真正的 Mail2000 電子信箱網址，顯示駭客主要的目的即在竊取使用者帳密。

除了針對一般電子郵件使用者帳戶進行攻擊外，銀行、投資管理、基金金融公司網站也易成為駭客攻擊目標，以下為針對從澳大利亞起家的麥格理銀行 (www.macquarie.com.au) 客戶的釣魚信件範例：

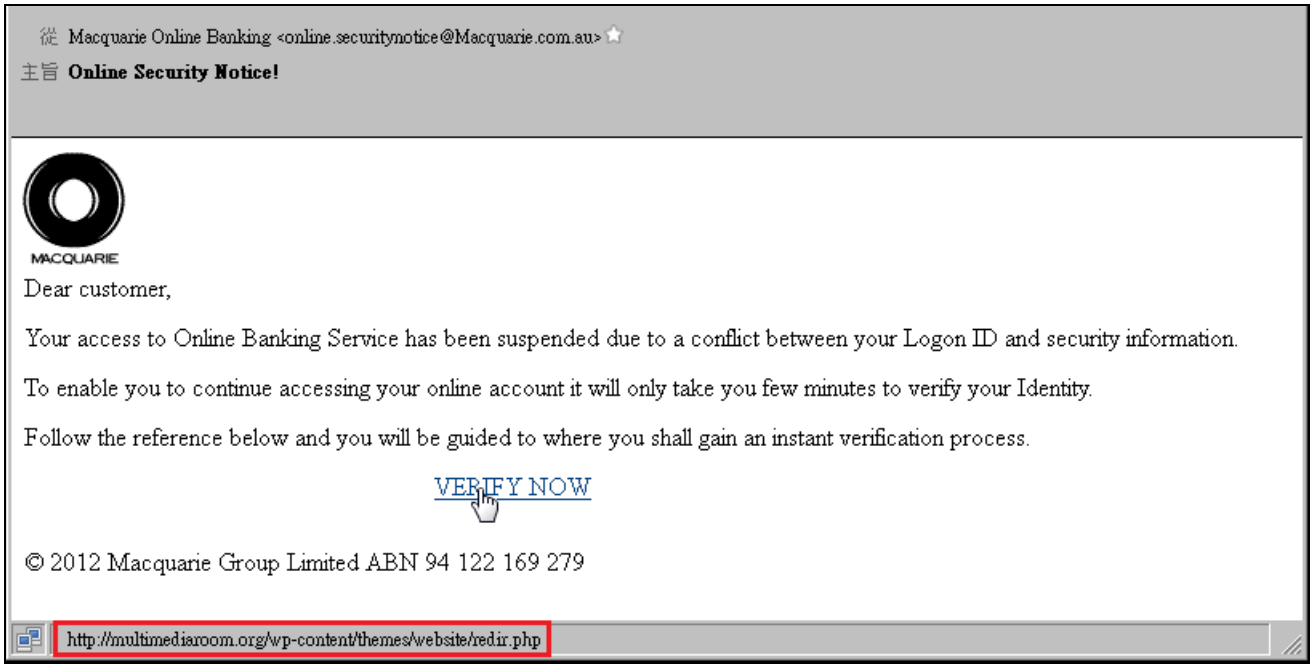

圖 7. 假冒麥格理銀行的帳號警示信的釣魚信件

如上圖，信中表示由於使用者的登入 ID 與安全訊息有衝突，所以線上銀行服務被中止，需要使用者循下方的超連結來進行重新認證的手續，此時使用者應已可注意到，雖然寄件者的網域是在 macquarie.com.au，但信中所附的超連結網域卻是 multimediaroom.org，和麥格理沒有關係；接著實際點選超連結後測試，進入偽造的麥格理銀行帳號登入頁面。

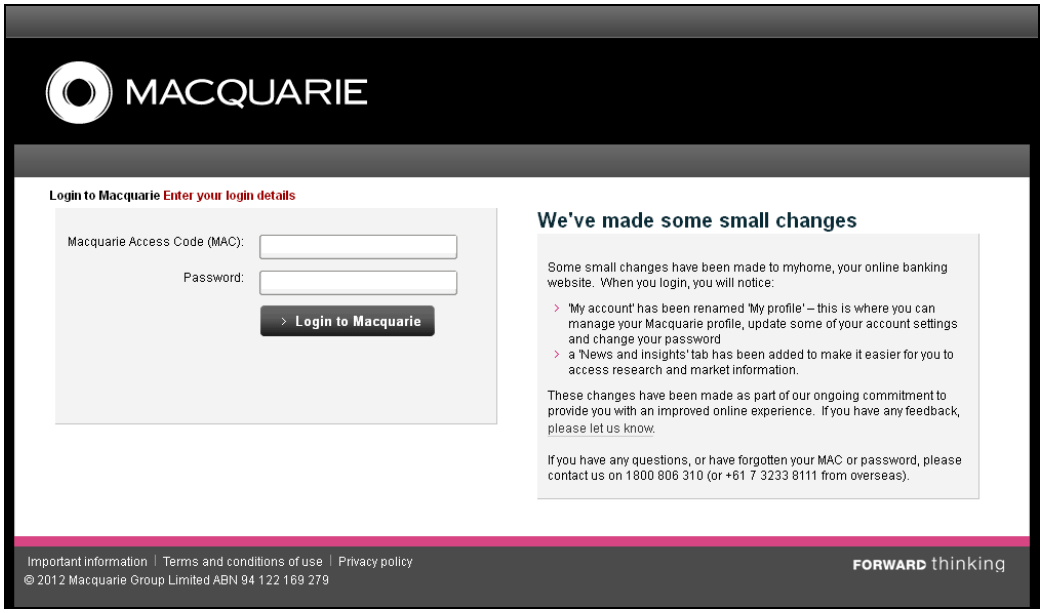

圖 8. 偽造的麥格理銀行帳號登入頁面

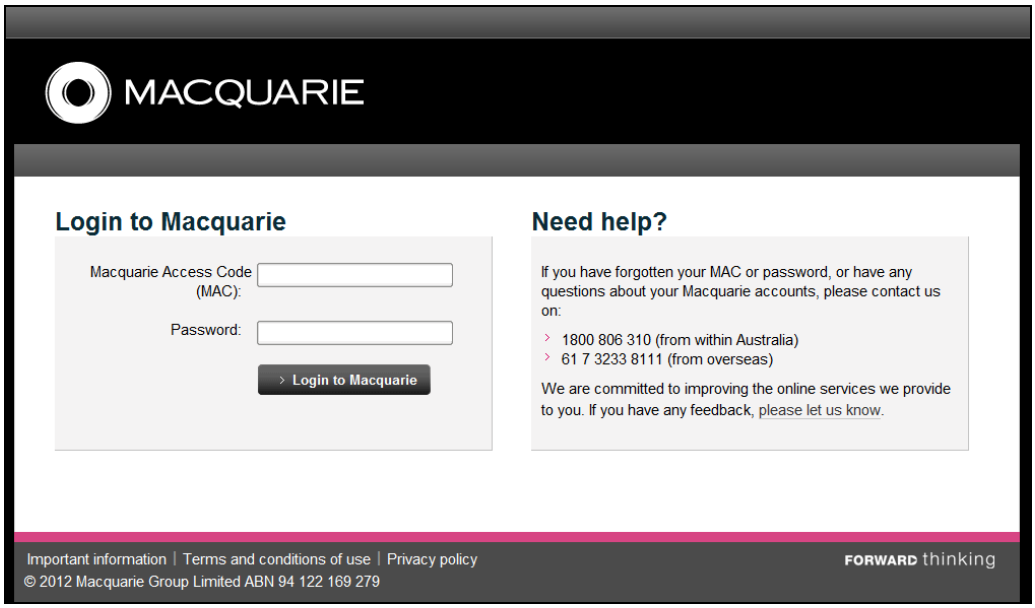

圖 9. 實際的麥格理銀行帳號登入頁面

與真正的麥格理銀行的登入頁面相比較，沒有如前一例有明顯的差別，對一般使用者來說判斷更加不易，若是使用者不察而直接在駭客製作的釣魚頁面登入，帳密則立即被駭客盜取。

除了騙取使用者帳密的釣魚信件外，也有專門用於行銷廣告的釣魚信，請看以下範例：

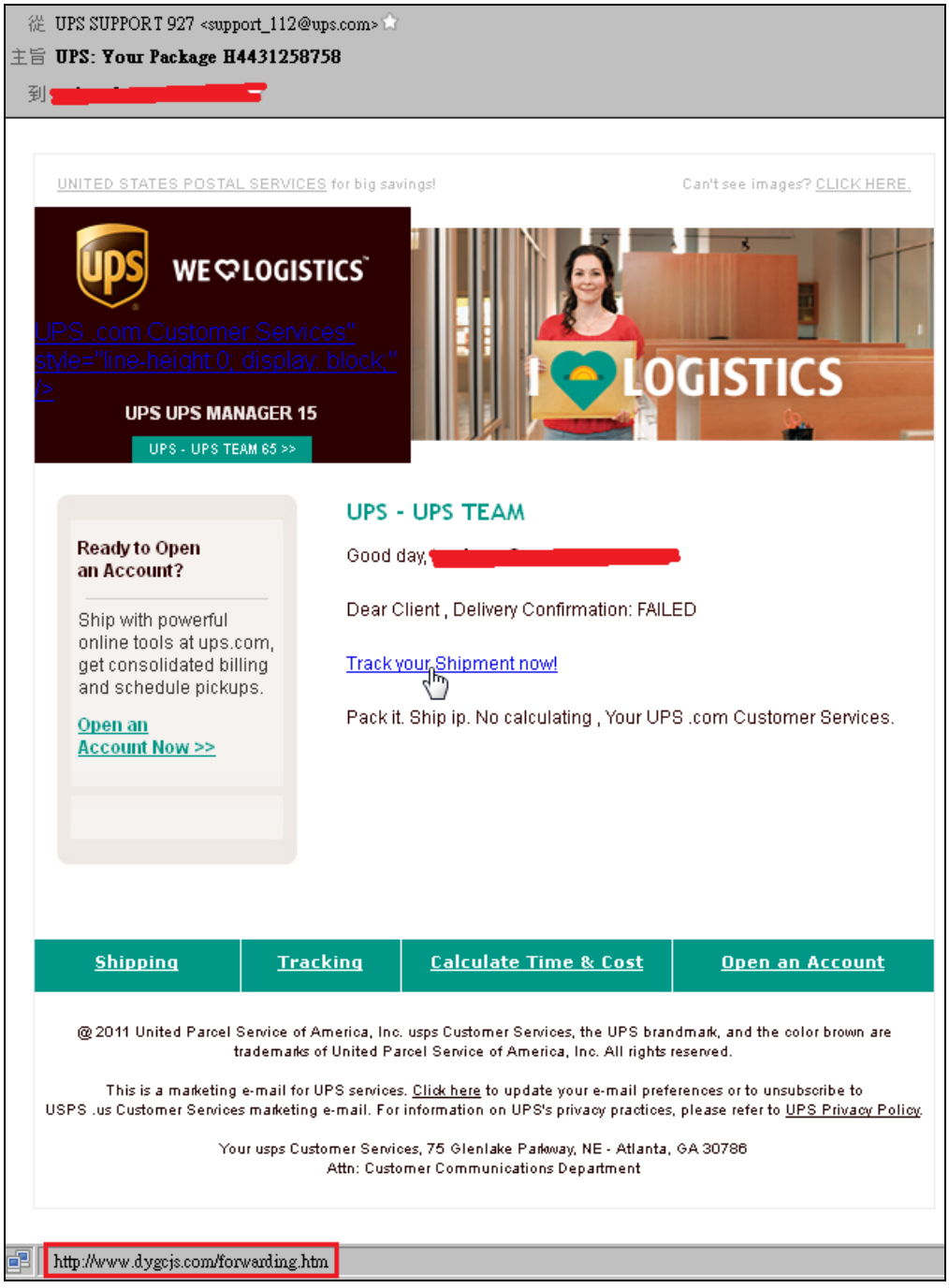

圖 10. 假冒 UPS 通知信的釣魚信

如上圖中假冒 UPS 通知信的釣魚信，照往例先檢查其連結網址是否有疑慮，可發現其網址 (http://www.dygcjs.com/forwarding.htm) 並非 UPS 網域，接著實際點開超連結測試：

圖 11. 假冒 UPS 通知信的釣魚信中連結頁面

點開後發現，其手法和過往的例子相同：網頁秀出「Please wait…」等字樣，之後利用 Javascript 操作瀏覽器轉址或載入木馬的動作，此例中則是將瀏覽器轉址到目前已取消註冊的網域 canadianpanakota.ru，等於使用者一點開連結，便可接觸到該網站的廣告內容。

接著分享一例假冒 YouTube 通知信的釣魚信，也和前一例一樣直接連到目標網站，但較不同的是此例中轉址用的網站是被駭後用來當跳板的第三方網站；點開超連結後，其網頁利用 html 語法將瀏覽器轉址到目前已取消註冊的網域 healthcarelnesshealth.com ，信中超連結也直接連向目標網站。

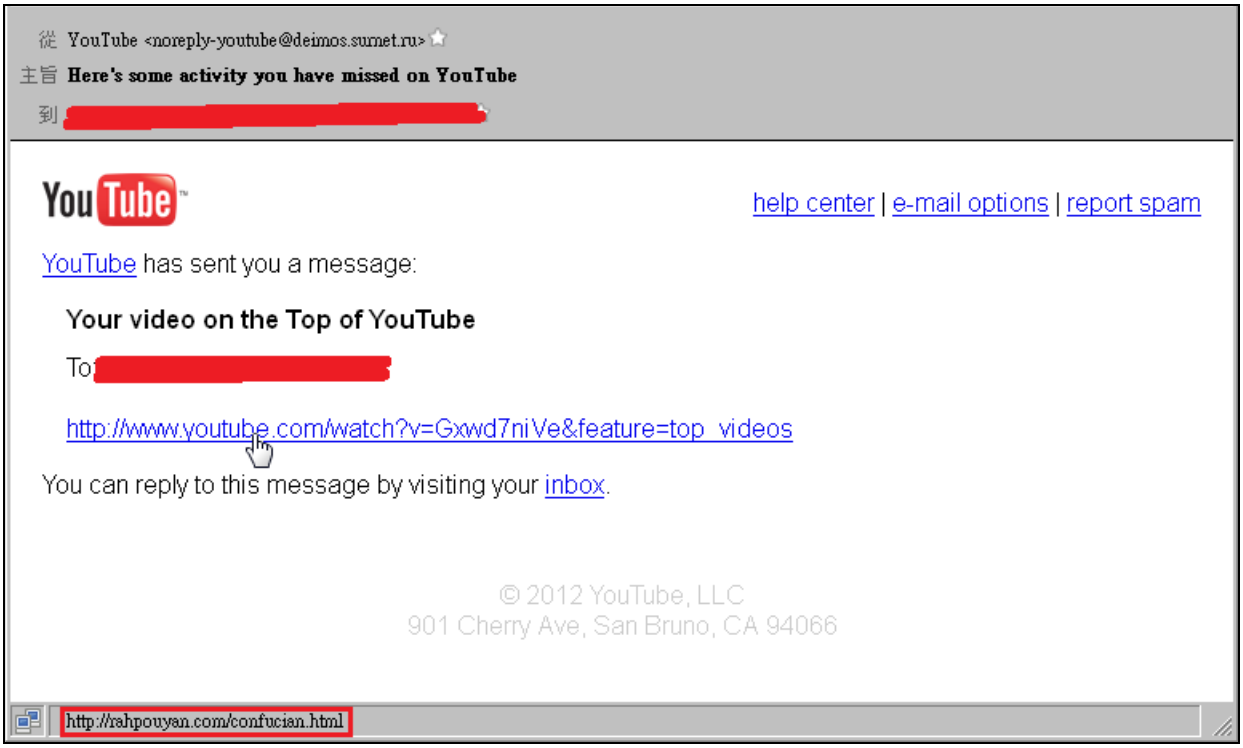

圖 12. 假冒 YouTube 通知信的釣魚信

以上的釣魚信件案例，玄機都藏於信件中之超連結目標，建議收件者平時需多加注意郵件內含超連結是否有可疑之處， 只要多一點細心，便可防範此類釣魚信件攻擊。

在本季出現的廣告垃圾信中主要有利用政府單位名義、搭乘時事話題發布等特色，誘使收件人點選，接著我們來看看兩則廣告垃圾信範例：

圖 13. 旅遊廣告信

如上圖為某旅遊活動的廣告信，雖然信中內文看似為同事、好友間轉寄，且又是政府單位主辦，但此信實際上仍是廣告信，且信中的超連結使用第三方網站的短網址服務來隱藏其真實網址，點開其超連結後，發現連至 http://yimg7.com/click.html?soroq1&_qrand=41219.5228301968，應是垃圾信發送者為垃圾信而設的站點。

第二則範例為搭乘時事話題發布的廣告信，標題雖然一看就知道是垃圾廣告信件，但仍會有收件人在好奇心的驅使下，不小心失去警覺而點選。以下範例即是一例，2012 年下半年李宗瑞事件鬧得風風雨雨，而在本季中就觀察到出現大量以李宗瑞為主題的廣告信，廣告目標正是色情光碟銷售網站。

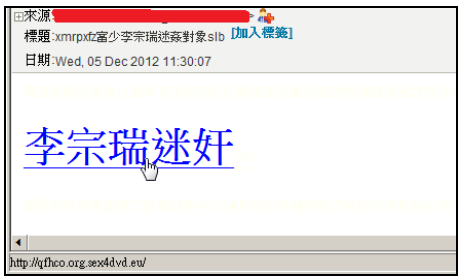

圖 14. 以李宗瑞當主題的廣告信

近來大陸方面的廣告信仍明顯可見，其中以如下二圖的商務課程及代開發票廣告信等案例為最大宗，

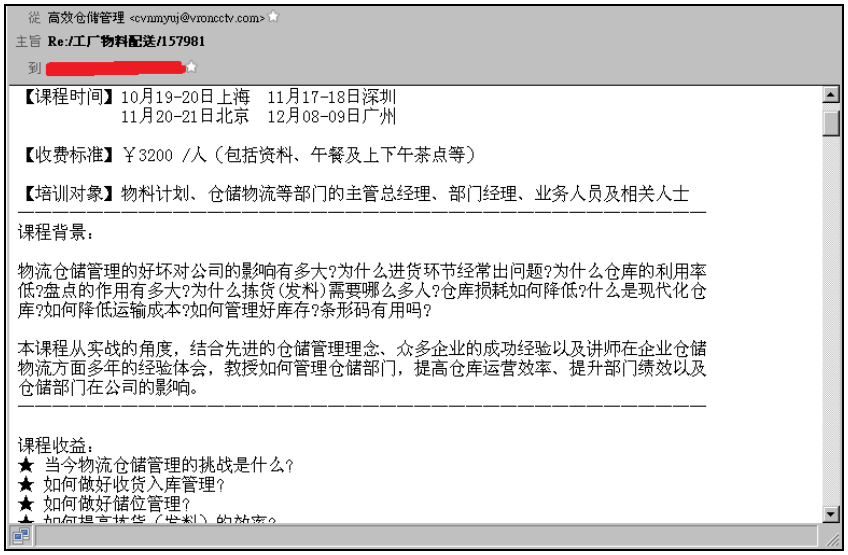

圖 15. 簡體商務課程廣告信

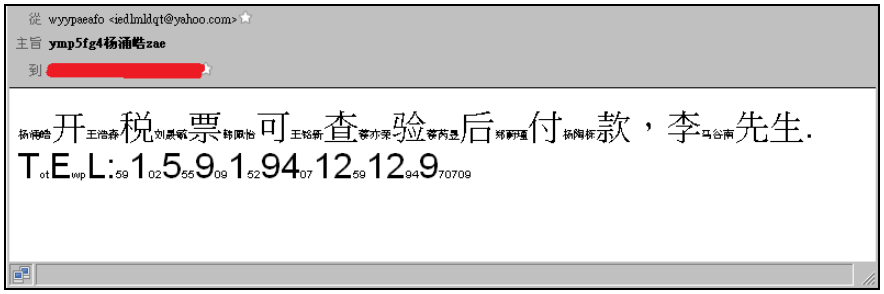

圖 16. 簡體代開發票廣告信

此外也有仿 EDM 的廣告信，如下圖的婚博會廣告：

圖 17. 仿 EDM 廣告信

此例看似正常 EDM，卻無退訂用超連結，且其超連結雖會將瀏覽器轉址到目標網域 591wed.com 下的廣告頁面，但若是直接連到轉址用網域 yindasan.com，其頁面則是一片空白，不似正常網站，推斷其網域應是垃圾信發送者為垃圾信而設。

本季報告的最後一則範例，以日本地區為主，目前觀察到的垃圾信主題則以成人約會最多，如下圖例；此類垃圾信大多利用註冊甚無價值的亂數域名作為轉址用網站，如此例中的網域 d8zvrfpt24.info，及其它一系列的 xxxxxx.info、xxxxxx.biz、xxxxxx.mobi、xxxxxx.asia 等，絕大多數都是垃圾信發送者用來發送垃圾信時方便夾帶其中的廣告網址，若使用者碰到此類垃圾信，切勿嘗試點開超連結，因為除了廣告垃圾信的麻煩以外，更可能在其網頁中夾帶有惡意程式，使自身陷於資安危機中。

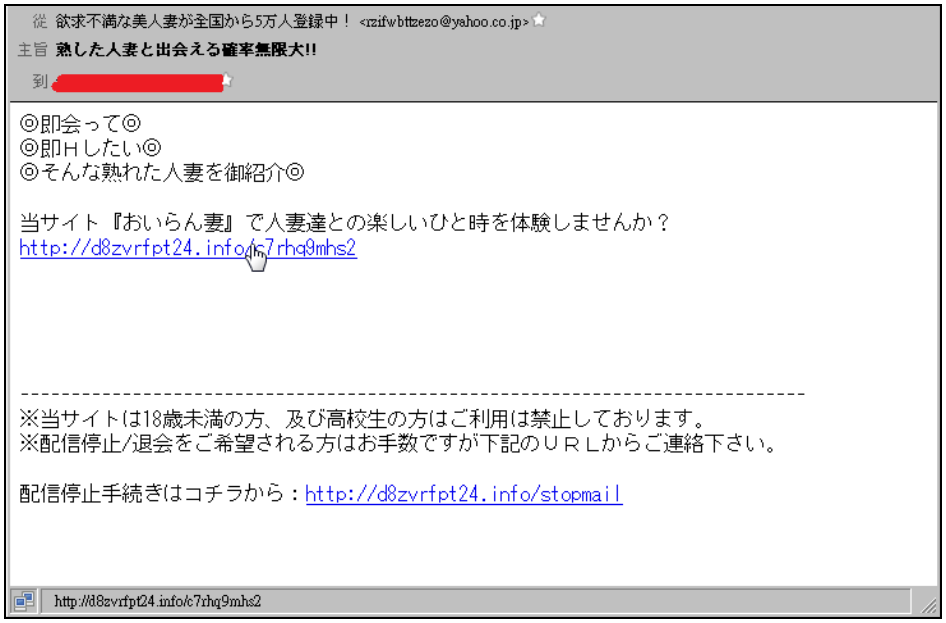

圖 18. 日本成人約會廣告信範例

Openfind 電子郵件威脅實驗室，特別從 2012 年第四季的電子郵件威脅監控行動中，挑選出這些值得您一覽的電子郵件威脅樣本供您參考，同時這些類型郵件都已經透過 Openfind 的雲端防護攔截技術，在發現威脅的下一秒，即已全面部署至 MailGates 郵件防護系統，以零時差、立即生效的特性，協助全球客戶立即免除以上郵件威脅。

關於 MailGates 郵件防護系統

MailGates 是一款結合郵件系統保全、內容過濾、郵件稽核與加密、統計報表與系統負載平衡設計的全方位郵件防護系統，其具備的雙雲端郵件過濾引擎，結合在地化樣本與全球即時探測的零時差防禦技術，能精準地攔截惡意、垃圾與病毒信件的威脅。同時，MailGates 提供的郵件稽核與紀錄追蹤功能，能讓管理者完整管控郵件伺服器的郵件傳遞政策與使用狀況，預防機密郵件外洩及追查郵件不當使用，捍衛企業訊息安全，並提升組織營運競爭力。更多產品訊息，請瀏覽產品網頁 http://www.openfind.com/taiwan/products/mailgates/info.html

Openfind 全產品率先支援 IPv6

隨著全球 43 億個 IPv4 位址即將耗盡，啟用 IPv6 也正式進入倒數計時。為達成網際網路 IPv6 全面化的理想目標，以加速因應雲端科技所帶動的網路成長需求，Openfind 網擎資訊各產品 - Mail2000 / MailBase / MailGates / OES，已於 2011 年 12 月全面完成測試，正式率先支援 IPv6，大幅提升網路環境相容性。更多訊息，請瀏覽 Openfind 最新消息 http://www.openfind.com/taiwan/newsevents/news_detail.php?news_id=2429

關於 Openfind

Openfind 成立於 1998 年 1 月，長期致力於網際網路相關技術研發，為企業用戶與廣大網友提供高品質、高穩定與高擴充性的軟體與服務。從企業市場搜尋引擎系列產品、電子郵件伺服器或郵件防護、稽核、歸檔系統，到一般使用者的電子郵件信箱與企業郵件代管服務，Openfind 堅守「創新技術與優質服務」的企業文化，以提供使用者最符合成本效益的解決方案。更多訊息，請瀏覽公司網站 http://www.openfind.com/。

關於鴻璟科技

鴻璟科技成立於 2003 年，為一家創新網路安全方案的全球供應商。鴻璟科技開發資安晶片、資安軟體以及特徵碼資料庫服務，協助客戶如網路服務供應商、網路設備製造商、晶片設計商於新世代防火牆、統一防禦系統(UTM)、電信服務商之家用閘道器、以及行動裝置產品中提供完善並且垂直整合的資安服務。鴻璟科技的技術包含第七層深度網路封包偵測晶片與授權、資安軟體與內容偵測軟體、及包含防病毒、入侵偵測、應用程式與裝置控管、可疑網址與網頁網址分類的特徵碼資料庫系統，所創新研發的技術，可協助客戶抵禦日益嚴重以及巨量暴增的資安威脅和攻擊。更多訊息，請瀏覽公司網站：http://www.lionic.com