Email Threats Sample Report
Q3 2011

Openfind™

Q3 2011 Email Threats Sample Report

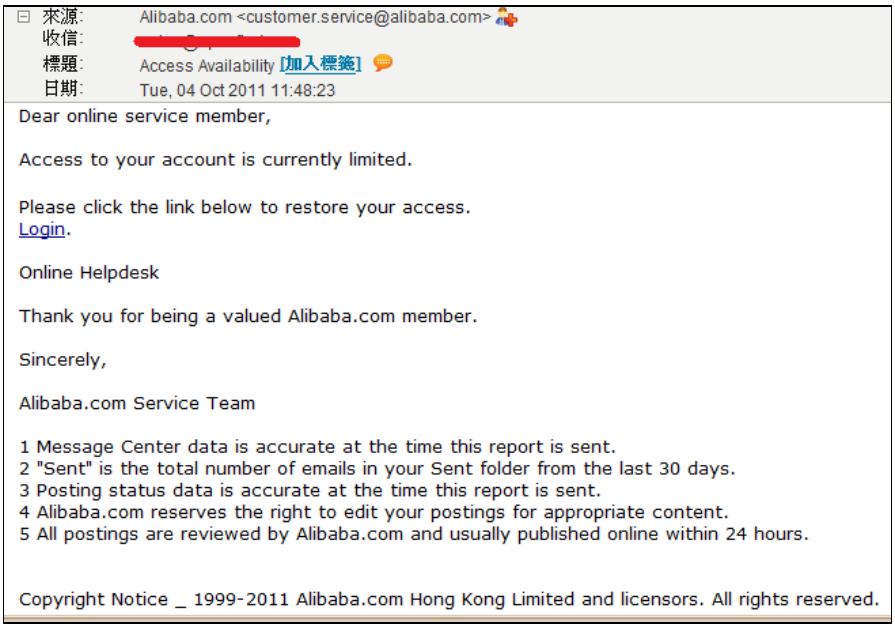
根據 Openfind 電子郵件威脅實驗室於 2011 年 Q3 針對台灣地區電子郵件威脅樣本的觀察，本季中需特別注意的駭客攻擊手法，主要還是在信件外部連結的威脅上，使用者面對電子郵件中的超連結時，請千萬注意以下細節：

1. **假冒知名網站帳號確認信或通知信的釣魚信件：**
   隨著各大社群網站及電子交易平台的興起，許多駭客開始假造各式各樣的網站登入平台，除了意圖騙取使用者的帳號密碼外，還有讓使用者經由惡意連結到廣告網站頁面，此類案例為數眾多多，因此使用者在點選連結時，不可不慎。
2. **透過轉址服務網站間接轉址（Redirect）：**
   由於時下短網址服務的興起，帶給攻擊者相當大的便利性，不但可以隱藏帶有威脅的真實網址位置，同時也可以縮短網址的字數，因此轉址服務儼然成為攻擊者慣用的手法之一。
3. **偽裝知名網域的寄件人或直接使用知名郵件服務發送：**
   延續上一季的趨勢，大部分的垃圾信發送者透過使用知名郵件服務(Yahoo、Gmail、Hotmail 等)直接發送或是假冒發送者。除了這些知名郵件服務信譽評價較好而信件到達率高之外，收信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。

在八月中，本公司發現藉由在電子郵件中嵌入惡意程式碼實施攻擊手法更高明的案例。駭客先在信中夾入一小段的網頁程式碼，待使用者打開信件之後，在信件中的這一小段程式碼會被觸發而下載與執行駭客在網路上儲存他處的網頁程式，接著顯示如下圖中假的重新登入頁面，但其實使用者的瀏覽器以及信箱皆並未發生如示意圖內所顯示的登入問題，若有使用者不假思索的使用其假登入頁面重新登入，則帳號密碼便會被駭客盜走，造成無可預估的風險。

【假冒 Mail2000 登入頁面的釣魚信件】

比起前述的釣魚案例，下圖的案例較容易防範，這是垃圾信發送者專為騙取 Alibaba 用戶帳號密碼而作的釣魚信件及網頁，可注意到寄件者被偽裝成由 Alibaba 發出的信，但其鏈結的假登入頁面與正版登入頁面比較後即可發現許多不同之處，像是不可變換語系與畫面較陽春，最重要的是網址雖有"alibaba"字樣，但主站點絕對不會是"alibaba.com"，比如在此封信中的假登入網址為 http://bahadaf.ir/cache/mod_footer/alibaba/alibaba.html，而正常登入網址實為 https://login.alibaba.com/，需特別注意。



來源: Alibaba.com <customer.service@alibaba.com>
收信: [redacted]
標題: Access Availability [加入標籤]
日期: Tue, 04 Oct 2011 11:48:23

Dear online service member,

Access to your account is currently limited.

Please click the link below to restore your access.
Login.

Online Helpdesk

Thank you for being a valued Alibaba.com member.

Sincerely,

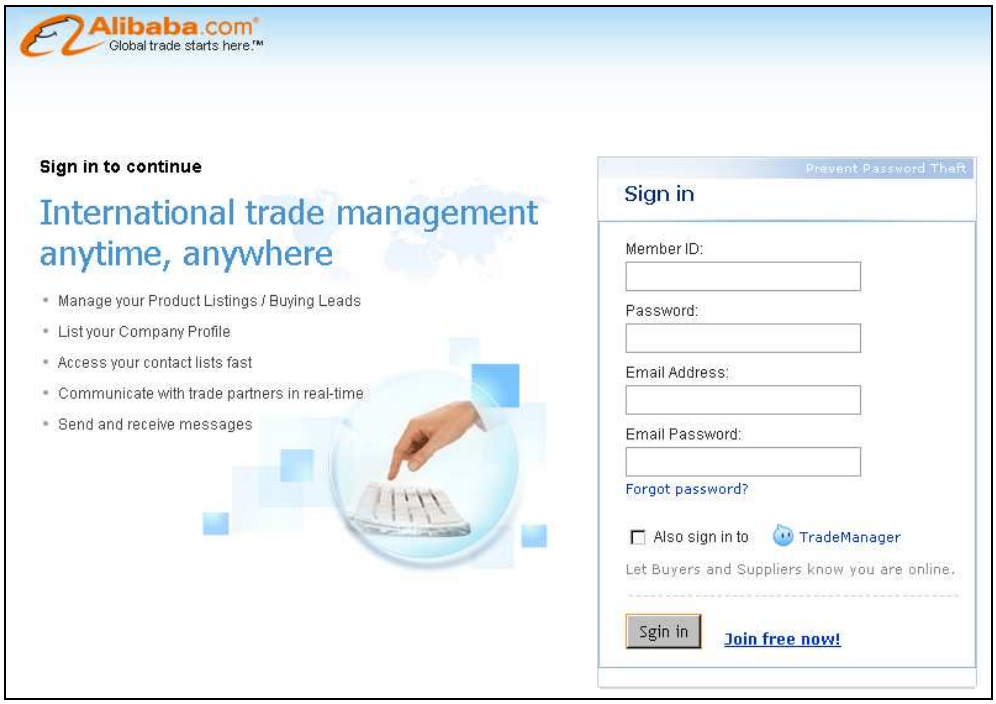
Alibaba.com Service Team

1 Message Center data is accurate at the time this report is sent.
2 "Sent" is the total number of emails in your Sent folder from the last 30 days.
3 Posting status data is accurate at the time this report is sent.
4 Alibaba.com reserves the right to edit your postings for appropriate content.
5 All postings are reviewed by Alibaba.com and usually published online within 24 hours.

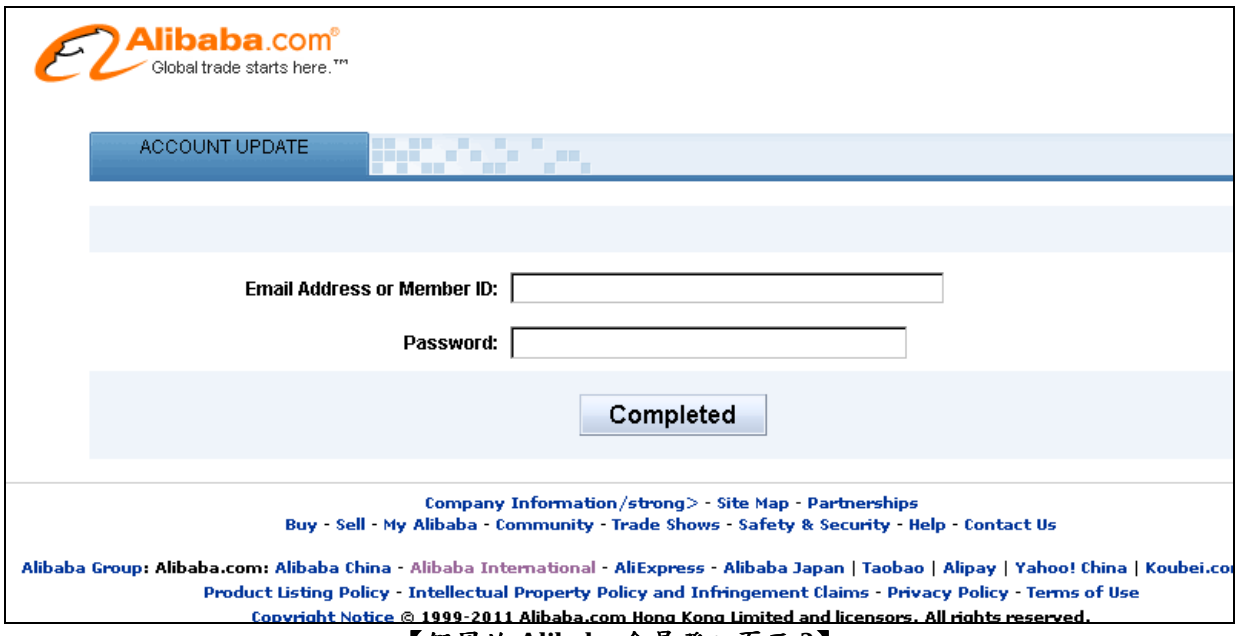
Copyright Notice _ 1999-2011 Alibaba.com Hong Kong Limited and licensors. All rights reserved.

【假冒 Alibaba 帳號確認信的釣魚信件】

【正常的 Alibaba 會員登入頁面】

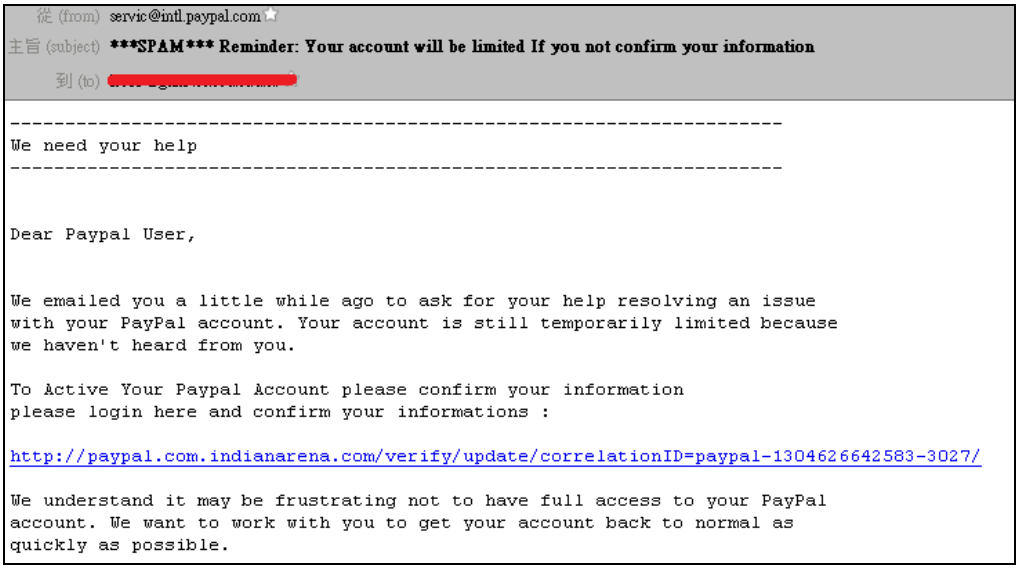


【假冒的 Alibaba 會員登入頁面 1】



【假冒的 Alibaba 會員登入頁面 2】

另外下圖範例同樣使用冒充寄信者的手法，意圖提升自身的可信度，但其信中提供的網址卻漏了餡，信件內網址：http://paypal.com.indianarena.com/verify/update/correlationID=paypal-1304626642583-3027/ 中有 PayPal 字樣，看似可放心使用，但其實此網址主站點為"indianarena.com"，與 PayPal 八竿子打不著關係。



從 (from) servic@intl.paypal.com
主旨 (subject) ***SPAM*** Reminder: Your account will be limited If you not confirm your information
到 (to) [redacted]

We need your help

Dear Paypal User,

We emailed you a little while ago to ask for your help resolving an issue
with your PayPal account. Your account is still temporarily limited because
we haven't heard from you.

To Active Your Paypal Account please confirm your information
please login here and confirm your informations :

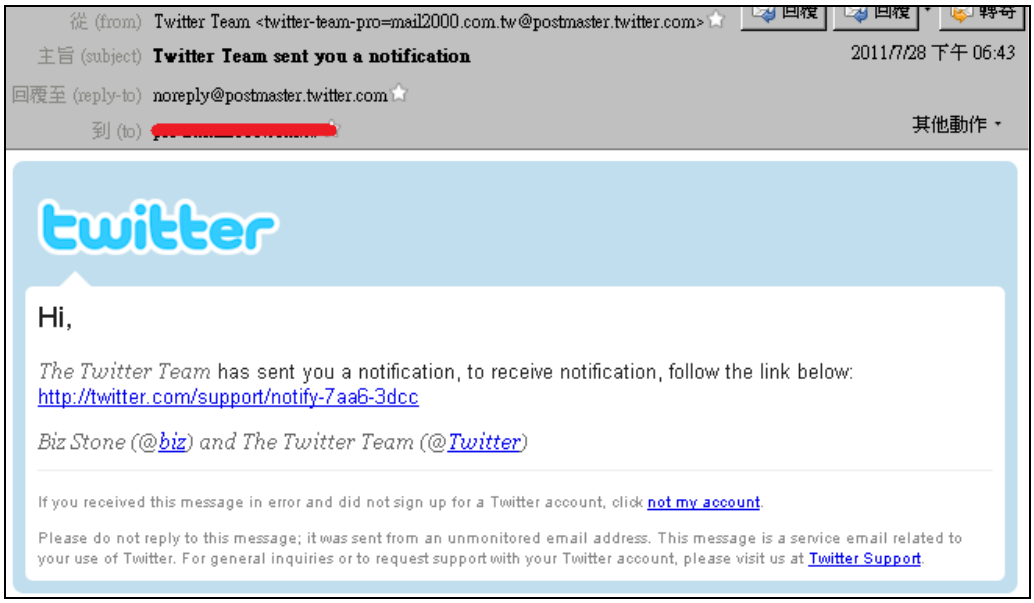
http://paypal.com.indianarena.com/verify/update/correlationID=paypal-1304626642583-3027/

We understand it may be frustrating not to have full access to your PayPal
account. We want to work with you to get your account back to normal as
quickly as possible.

【假冒 PayPal 帳號確認信的釣魚信件】

而接著標榜 twitter 的這封信中的網址看似正常：http://twitter.com/support/notify-7aa6-3dcc，主站點是 twitter 沒錯，但若是查看其原始信件內容中關於其網址的程式碼：

http://twitter.com/support/no=tify-7aa6-3dcc



從 (from) Twitter Team <twitter-team-pro=mail2000.com.tw@postmaster.twitter.com>
主旨 (subject) **Twitter Team sent you a notification**
2011/7/28 下午 06:43
回覆至 (reply-to) noreply@postmaster.twitter.com
到 (to) [redacted]
其他動作

twitter

Hi,

The Twitter Team has sent you a notification, to receive notification, follow the link below:
http://twitter.com/support/notify-7aa6-3dcc

Biz Stone (@biz) and The Twitter Team (@Twitter)

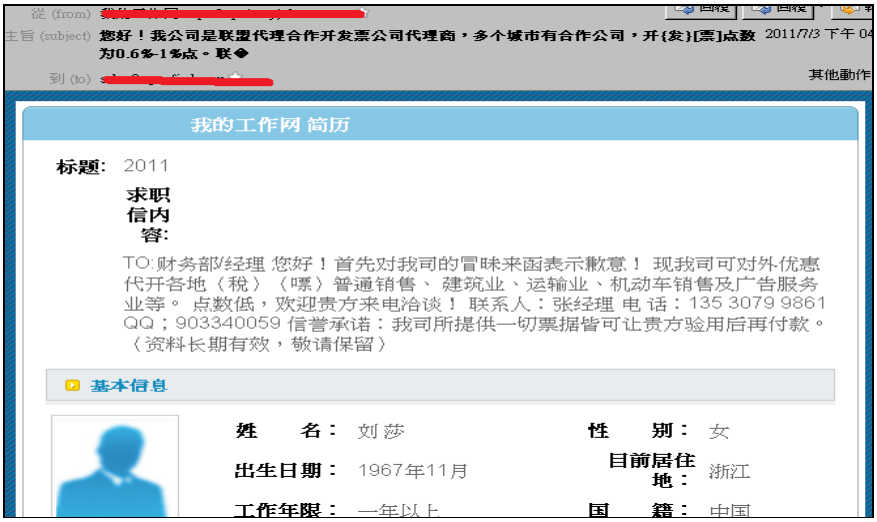
If you received this message in error and did not sign up for a Twitter account, click not my account.

Please do not reply to this message; it was sent from an unmonitored email address. This message is a service email related to your use of Twitter. For general inquiries or to request support with your Twitter account, please visit us at Twitter Support.

【假冒 twitter 通知信的釣魚信件】

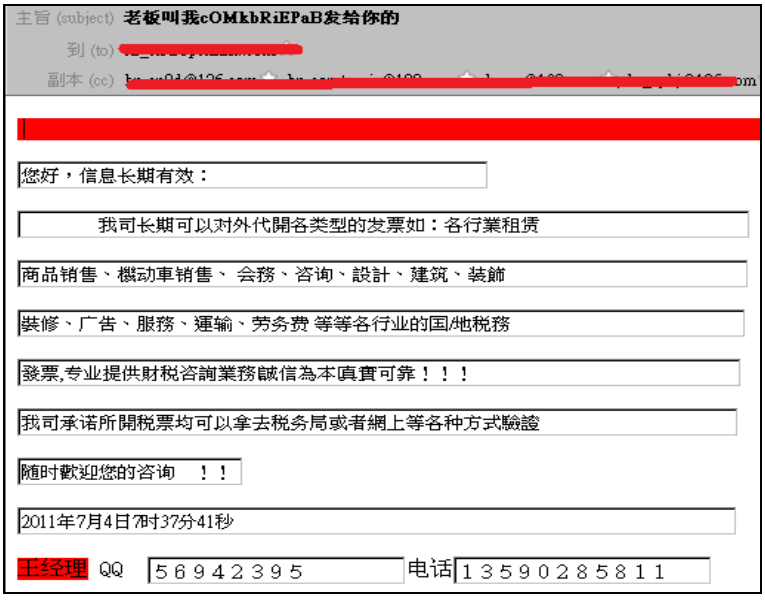
可發現到其實際的超連結位址和表面上的不一樣，若是使用者使用滑鼠點選直接複製選項，則複製到的其實是垃圾信發送者提供的廣告網址而非 twitter 的網址，此點也是使用者需要相當小心的地方。

此外許多發送大陸發票廣告信的垃圾信發送者為規避垃圾信防護閘道的攔阻，在廣告信中嘗試許多不同的變形方法，如下圖，此信雖主旨明顯是發票廣告，但內文卻夾雜個人履歷的資料來魚目混珠，以混淆垃圾信判斷工具攔阻的效果。



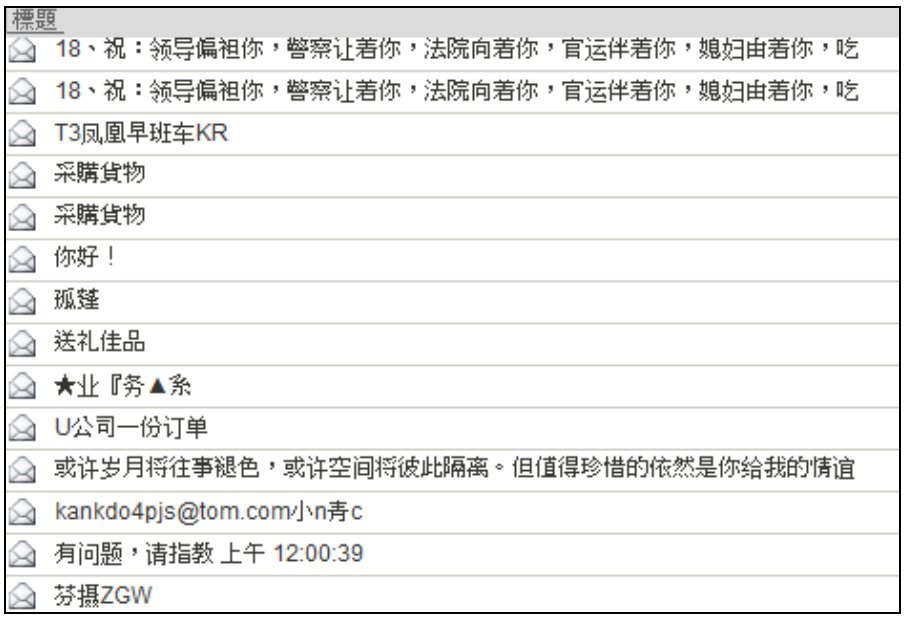
【變形的大陸「代開發票」廣告信件 1－內文混淆】

然而有的大陸發票廣告信會讓收信者一眼就可看出為垃圾信件，但因發送者將其廣告詞放入 html 表格中，意圖降低詞庫、語意分析攔截技術工具判斷的效果。



【變形的大陸「代開發票」廣告信件 2－內文放入 html 表格】

此類的變形信件數量較多，垃圾信發送者以廣告主題無關或者根本無意義的詞句當作廣告信的主旨，讓收信者在無法得知其信件實為廣告信的情形下誤開信件，迫使收信者閱覽廣告，且此類信件內文幾乎只有一張放入廣告內容的圖片，藉以降低垃圾信防護閘道的攔阻效果。



【變形的大陸「代開發票」廣告信件 3－多種變型主旨】

【變形的大陸「代開發票」廣告信件 3－內文為圖片】

另外垃圾信發送者延續上半年的垃圾廣告信的風格，加入了一些新手法，如圖例中的信件，除了一貫的偽裝寄件者手法外，其內文中還加入為數不少的亂碼字，意圖降低詞庫、語意分析攔截技術工具判斷的效果，

【偽冒知名來源網域的電子商務廣告信】

此外也去掉原本有的超連結，並在看似應為 URL 的藍色英文字中加入與背景同色的亂碼字樣，以規避 URL 黑名單的攔截。

【URL 的藍色英文字中加入與背景同色的亂碼字樣】

Openfind 電子郵件威脅實驗室，特別從 2011 年第 3 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/。