Email Threats Sample Report
Q2 2011

Openfind™

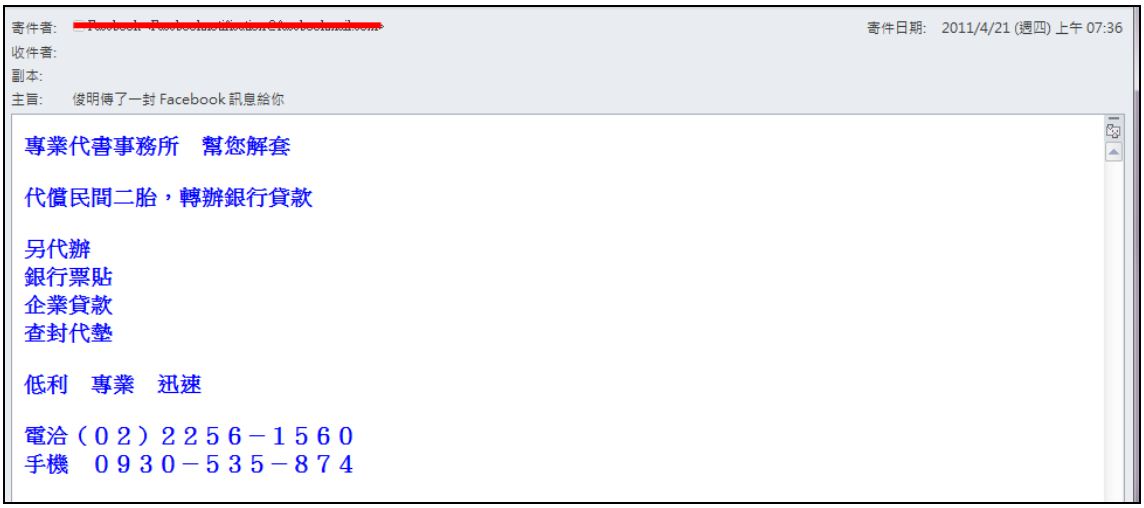
根據 Openfind 電子郵件威脅實驗室於 2011 年 Q2 針對台灣地區電子郵件威脅樣本的觀察，本季中需特別注意的駭客攻擊手法，主要是在信件外部轉址網站連結的威脅與社交工程搭配加密壓縮檔上，使用者面對電子郵件中的超連結或壓縮附檔時，請千萬注意以下細節：

1. **透過轉址服務網站間接轉址（Redirect）：**
   延續上一季的趨勢，利用轉址服務網站，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，仍然持續成為本季攻擊者最愛使用的手法。
2. **社交工程 + 加密壓縮檔的攻擊方式：**
   利用社交工程方式取得使用者信任，開啟信件，同時將木馬或者後門程式藏在加密過的壓縮檔中作為郵件附檔，並將密碼寫在信件中，利用具誘惑力的內容吸引使用者開啟壓縮檔。這樣的手法不但可以規避郵件防護閘道的掃毒引擎，也利用了人性「喜歡窺探機密」的特性，十分經典。
3. **偽裝知名網域的寄件人或直接使用知名郵件服務發送：**
   詳見下述說明。

大部分的垃圾信發送者（Spammer）都發現現今的郵件防護閘道，會使用雲端 IP 信譽防禦機制去阻擋 Botnet、Zombie Network 所發送的信件，同時區域聯防的效果也很快，往往使的廣告信的發送效能不彰；因此，本季漸漸將垃圾郵件的發送方式，轉為直接使用知名郵件服務(Yahoo、Gmail、Hotmail 等)直接發送，原因是這些知名郵件服務通常帶有信譽評價較好的 IP，因此信件到達率高。

以往這一類手法的發送者，通常都使用 Yahoo Group 或 Google Group 等類似服務達到目的（其實本季使用這種手法的攻擊者仍不少），不過值得注意的是本季出現了新的潮流，發送者透過社交工程攻擊盜取來的使用者帳號、密碼，透過 Keyboard Script、SMTP Auth 等方式，持續性且維持一定量的發送，成為本季垃圾信發送方式的新主流。

大約在四月中下旬時，因應稅務旺季，有大量「代開發票」性質的廣告信開始氾濫，下列是一封偽造 facebook 來源的此類信件樣本：


寄件者: [redacted]
寄件日期: 2011/4/21 (週四) 上午 07:36
收件者:
副本:
主旨: 俊明傳了一封 Facebook 訊息給你

專業代書事務所　幫您解套

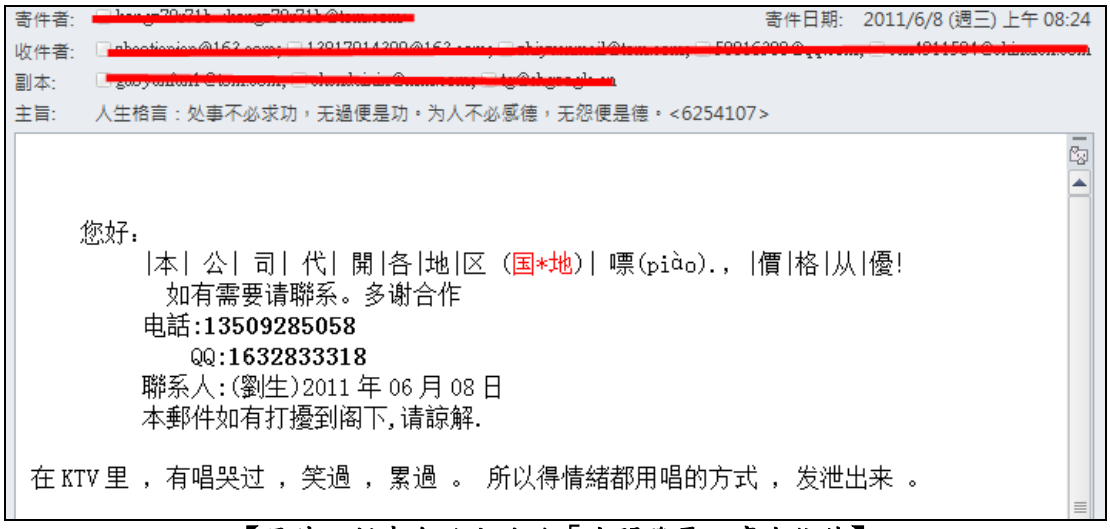
代償民間二胎，轉辦銀行貸款

另代辦
銀行票貼
企業貸款
查封代墊

低利　專業　迅速

電洽（０２）２２５６－１５６０
手機　０９３０－５３５－８７４

【假冒 facebook 寄件人身份的「代開發票」廣告信件】



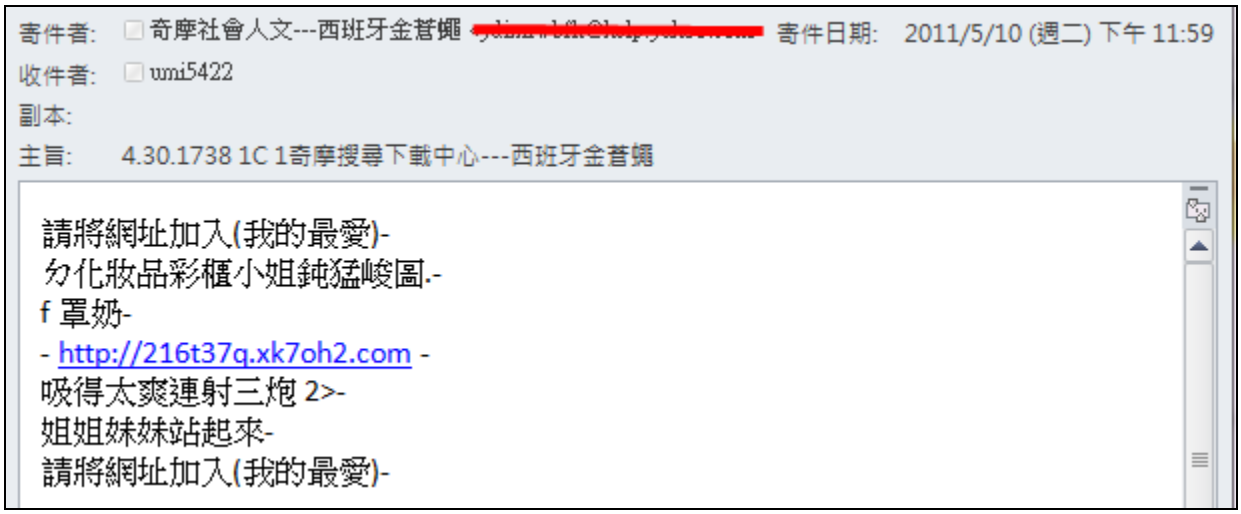
【另外一封來自於大陸的「代開發票」廣告信件】

這一類信件在四月底相當的多，主題明確、特徵明顯，通常還會假冒成讓人較為容易相信的身份，如中國卡巴斯基網站、大陸或台灣知名金控業者等，也會故意在郵件標題加上 Re:等回信的標頭，避免被垃圾信防護閘道攔阻及提高使用者點擊廣告的成功率。

另外，在四月份透過轉址網站所發送的廣告信件仍然為數不少，以下是一封網頁設計工作室的廣告信件，其中的連結便是利用知名轉址服務網站 tinyurl，將自己的廣告網址藏匿其後，避免被抓獲：

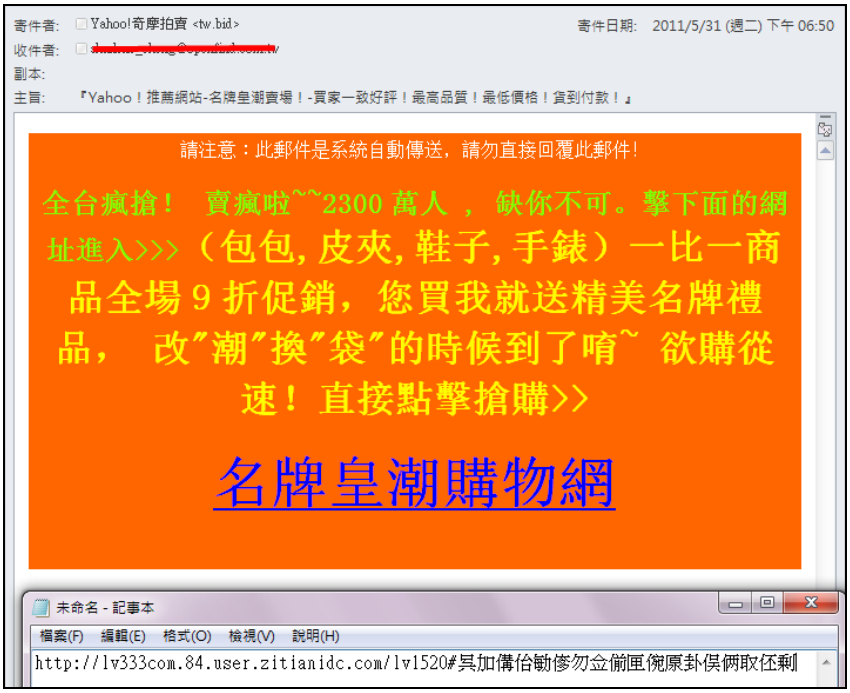
【將廣告網址藏匿在 tinyurl 服務後方的網頁設計廣告信】

通常這樣的廣告信件，都會不斷改變轉址網站網址的內容來規避一般郵件防護閘道的 URL 關鍵字攔截，即使每次藏匿其後的廣告信網址一致，但藉由不斷變換轉址網址，也可以達成信件內容不一樣的規避效果，是 2011 年 Q2 大量垃圾郵件發送者常用的手法。同樣類似的手法，也出現在五月份的色情光碟廣告信上：



【將廣告網址藏匿在轉址服務後方的色情光碟廣告信】

五月份的廣告信則開始走向購物、金融詐騙的趨勢，下方有一封假冒 Yahoo 拍賣的廣告信件，但其實內容為其他購物網站的廣告，這類型信件通常都夾帶誘人的廣告內容，並偽裝冒充合法知名的郵件服務供應商(例如 Yahoo、Gmail、Hotmail 等)：



【偽冒知名來源網域的電子商務廣告信】

金融詐騙的信件在五月份也不少，下方是一封看似普通銀行 EDM，卻無銀行相關網站資訊僅有電話，可能實為地下錢莊廣告的詐騙廣告信件，同時，其真實廣告網址理所當然地也藏在轉址網址服務後：


寄件者: 平安银行 [redacted]
寄件日期: 2011/5/16 (週一) 下午 04:31
收件者: hr_cn
副本:
主旨: 借米不再看人脸色

借钱？容易！探亲、结婚 装修、旅游、买车
只要月入2000，完全无需抵押，最快1天到账
急需钱，立即申请！
平安普贷微助您获取无抵押贷款

平安银行

个人贷款

申请人年龄为 22－55 周岁，税后月收入 2000 以上，提供身份证明、收入证明等，即可申请最高 15 万元个人消费贷。

中小企业贷款

注册满一年，额度最高可达 30 万元，满三年可贷 30-100 万，是小型企业首选贷款方案。

1. 放贷更快：无抵押、无担保，资料齐全 3 个工作日放款

2. 利率更低：利率明显优于市场同类产品

【假冒銀行 EDM 的地下錢莊廣告信】


這封郵件以高重要性傳送。
寄件者: 專辦企業銀行借款。 [redacted]
寄件日期: 2011/6/11 (週六) 上午 01:58
收件者: [redacted]
副本:
主旨: 錯過這次不知還要等多少年Sat, 11 Jun 2011 00:06:12 +0600

第一證保金融有限公司

＊本公司營業項目＊

1.機械設定,中小型企業貸款..

2.信保基金,支客票貼現.

3.採月息制,公司票,個人票,月息 3 分

房屋貸款利率﹒,代辦支票、公司票、客票、工廠、企業、公司、

民間房屋貸款﹒,用幾天、算幾天、提前還款還可退息

~請款迅速便利~

~請洽免費服務專線~

第一 [redacted]

【另外一封以誘人標題發送的地下錢莊廣告信】

五月份另一波廣告信件趨勢，當然也不會少了最經典的社交工程。不過一般社交工程都用在「攻擊」手段，有趣的是這一類的信件將社交工程用在「誘導」使用者到達發送者希望露出的內容（如電子報發送系統的廣告），以下是一封在五月中旬發送的郵件樣本：

【社交工程廣告信件】

當然，真實的連結還是藏在轉址網址服務後方，這一封信有趣的地方是最後連結到達的目的地是 Google 搜尋「電子報系統」關鍵字的頁面，而廣告發送者的廣告就在查詢結果中，第一行最醒目的 Google AdSense 廣告，可以說是一封煞費苦心的社交工程廣告郵件。在此提醒，URL 在轉換的過程中，也通常夾帶者 Cross Site Scripting 或漏洞偵測夾帶木馬等行為，是使用者需要注意的地方。

六月份利用社交工程的威脅郵件，當然還是少不了夾帶木馬的魚叉式攻擊手法郵件，通常這類郵件都是以矚目的標題，吸引人的內容，誘使使用者點擊附檔或者開啟連結，以達到植入木馬的可能。尤其這一類攻擊再次進化後，往往會將附檔以加密壓縮的方式，規避郵件防護閘道的防毒引擎（因為無法掃描加密壓縮檔）掃描，並且將密碼寫在電子郵件中，以人類天生喜歡開啟「秘密」的心態，誘使使用者手動開啟含有木馬的加密壓縮檔以達成目的，是最新演化的高明手法，我們稱這類手法為「加密壓縮檔社交工程攻擊」：


寄件者: Jack Chang
寄件日期: 2011/6/11 (週六) 上午 09:41
收件者:
副本:
主旨: 女生一夜情以後如果發現懷孕了會怎麼辦

投票結果在副檔密碼是 123 哦^^

1. 想盡方法要找到對方~叫他負責 結婚生子

---

2. 想盡方法要找到對方~叫他給錢 拿掉孩子

---

3. 推給現在的男朋友或老公 騙他是彼此愛的結晶~生下來

---

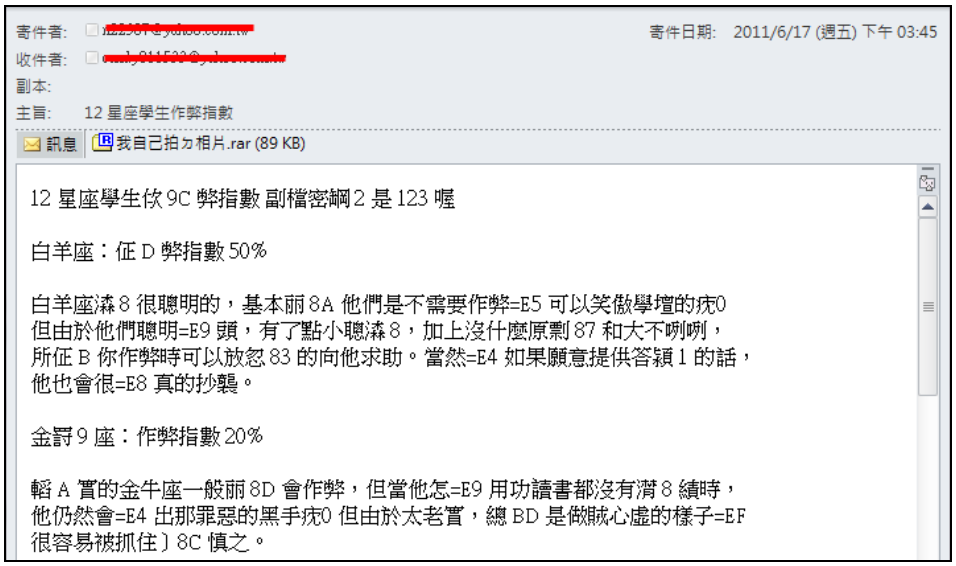
4. 給現在的男朋友或老公 騙他是彼此愛的結晶~拿掉

---

5. 跟好姐妹討論

【夾帶含有木馬的加密壓縮檔社交工程攻擊信件】

這一類手法的信件在六月達到了質量上的巔峰，利用情色、星座、線上遊戲等大眾較為注目的話題，並且同樣利用較為知名的郵件服務網域（此次此類手法的大宗郵件寄送網域來源是 Yahoo 的電子郵件服務）不斷發送含有木馬或後門程式的加密壓縮檔，成了規避郵件閘道防護最流行的方式：


寄件者:
寄件日期: 2011/6/17 (週五) 下午 03:45
收件者:
副本:
主旨: 12 星座學生作弊指數
訊息 我自己拍ㄉ相片.rar (89 KB)

12 星座學生佽 9C 弊指數 副檔密鋼 2 是 123 喔

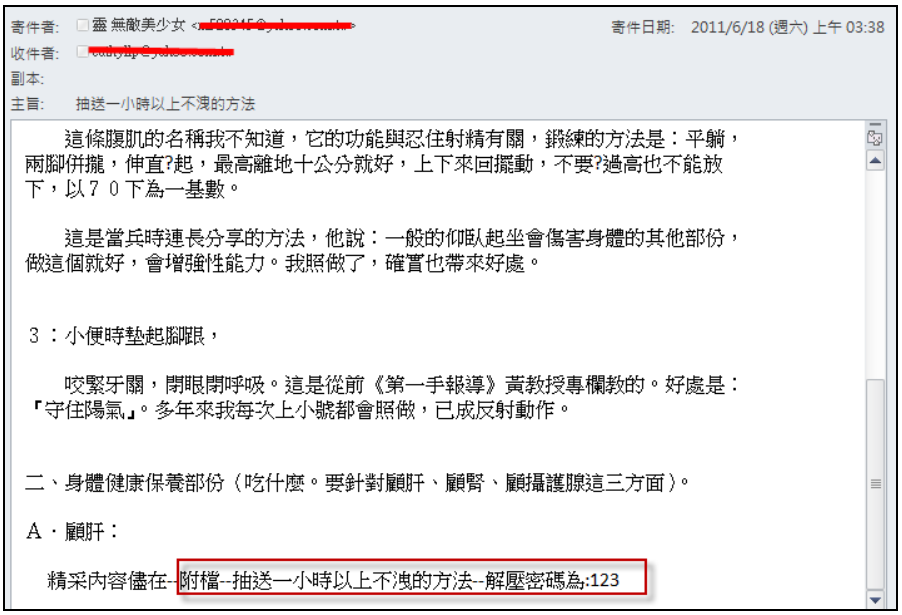
白羊座：征 D 弊指數 50%

白羊座滊 8 很聰明的，基本丽 8A 他們是不需要作弊=E5 可以笑傲學壇的疣0
但由於他們聰明=E9 頭，有了點小聰滊 8，加上沒什麼原剽 87 和大不咧咧，
所征 B 你作弊時可以放忽 83 的向他求助。當然=E4 如果願意提供答穎 1 的話，
他也會很=E8 真的抄襲。

金罸 9 座：作弊指數 20%

輜 A 實的金牛座一般丽 8D 會作弊，但當他怎=E9 用功讀書都沒有潸 8 績時，
他仍然會=E4 出那罪惡的黑手疣0 但由於太老實，總 BD 是傲賊心虛的樣子=EF
很容易被抓住〕8C 慎之。

【使用星座話題的加密壓縮檔社交工程攻擊信件】


寄件者: 靈 無敵美少女 <[redacted]>
寄件日期: 2011/6/18 (週六) 上午 03:38
收件者: [redacted]
副本:
主旨: 抽送一小時以上不洩的方法

這條腹肌的名稱我不知道，它的功能與忍住射精有關，鍛練的方法是：平躺，兩腳併攏，伸直?起，最高離地十公分就好，上下來回擺動，不要?過高也不能放下，以７０下為一基數。

這是當兵時連長分享的方法，他說：一般的仰臥起坐會傷害身體的其他部份，做這個就好，會增強性能力。我照做了，確實也帶來好處。

３：小便時墊起腳跟，

咬緊牙關，閉眼閉呼吸。這是從前《第一手報導》黃教授專欄教的。好處是：「守住陽氣」。多年來我每次上小號都會照做，已成反射動作。

二、身體健康保養部份（吃什麼。要針對顧肝、顧腎、顧攝護腺這三方面）。

Ａ．顧肝：

精采內容儘在-附檔--抽送一小時以上不洩的方法--解壓密碼為:123

【使用情色話題的加密壓縮檔社交工程攻擊信件】


寄件者: [redacted]
寄件日期: 2011/6/24 (週五) 上午 04:30
收件者: [redacted]
副本:
主旨: 免費楓之谷洗錢機

副檔密碼是 123 喔

還在當乞丐和人要錢嗎?不用要了 快來下載吧!楓之谷洗錢機用過的人都說讚喔

別當小偷小白

記得回 3Q

載點:下載請按我 載點在副檔

安裝說明都有寫

【使用線上遊戲話題的加密壓縮檔社交工程攻擊信件】

另外，還記得 Openfind 2011 年第一季電子郵件威脅樣本報告提到的 XYZ 大補帖廠商系列嗎？在六月垃圾郵件盛行的季節裡，XYZ 當然不會缺席；而且不只沒有缺席，手法更再度進化，利用了 Google Group 或 Yahoo Group 服務，XYZ 再度活躍地發送了大量的垃圾廣告郵件，以下是其中一封這類型郵件的樣本：

【再度進化，使用 Google Group 服務發送廣告信件的 XYZ 系列】

最後，與大家分享一封反應世事民情的廣告信件。這一封信件本身沒有什麼特別之處，僅是介紹居住於大陸的婦女赴港生產的廣告，由此可見大陸社會一胎化及醫療方面問題的嚴重性。廣告信的趨勢其實也一定程度的反應了國家與社會的需求、問題，觀察後可以發現，其中也是有值得令人省思之處。

【對居住於大陸的婦女宣傳赴港生產的廣告信件】

Openfind 電子郵件威脅實驗室，特別從 2011 年第 2 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/。