Email Threats Sample Report
Q1 2011

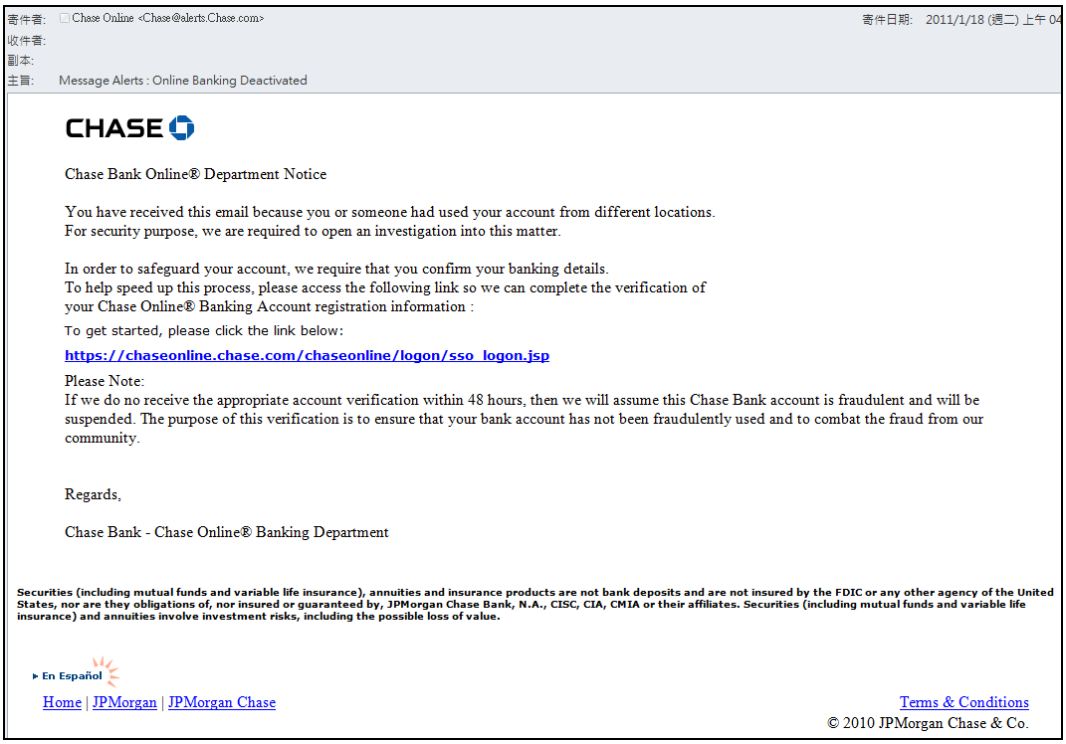
Openfind™

Q1 2011 Email Threats Sample Report

根據 Openfind 電子郵件威脅實驗室於 2011 年 Q1 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. **偽裝知名網域的連結：**
   利用似乎可信任的來源：Google Groups、Yahoo Groups、eBay 等，讓超連結的名稱出現這些字樣，提供使用者信任度並進而增加點擊率。
2. **透過轉址服務網站間接轉址（Redirect）：**
   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，是本季攻擊者最愛使用的手法。
3. **透過知名網站的 Cross Site Script 漏洞夾帶網址：**
   有不少知名網站在 Cross Site Script 的防範並未完整，因此帶給攻擊者機會；攻擊者可以將自身的網址附加於知名網站的連結尾部，藉由 Cross Site Script 的方式，將使用者帶往夾帶木馬的目的地。

大約在一月底的時候，有駭客假冒美國三大銀行之一的 CHASE，大量散布了偽冒身份的釣魚信件，信件內容將會告訴使用者，有人從別的地方使用您的銀行帳戶登入，因此請使用者遵循郵件中的連結，進行登入確認動作；而該連結其實是一個隱含惡意木馬，同時趁機騙取使用者真實帳號、密碼的釣魚網站：



寄件者: Chase Online <Chase@alerts.Chase.com>　　寄件日期: 2011/1/18 (週二) 上午 04
收件者:
副本:
主旨: Message Alerts : Online Banking Deactivated

CHASE

Chase Bank Online® Department Notice

You have received this email because you or someone had used your account from different locations.
For security purpose, we are required to open an investigation into this matter.

In order to safeguard your account, we require that you confirm your banking details.
To help speed up this process, please access the following link so we can complete the verification of
your Chase Online® Banking Account registration information :

To get started, please click the link below:

https://chaseonline.chase.com/chaseonline/logon/sso_logon.jsp

Please Note:
If we do no receive the appropriate account verification within 48 hours, then we will assume this Chase Bank account is fraudulent and will be suspended. The purpose of this verification is to ensure that your bank account has not been fraudulently used and to combat the fraud from our community.

Regards,

Chase Bank - Chase Online® Banking Department

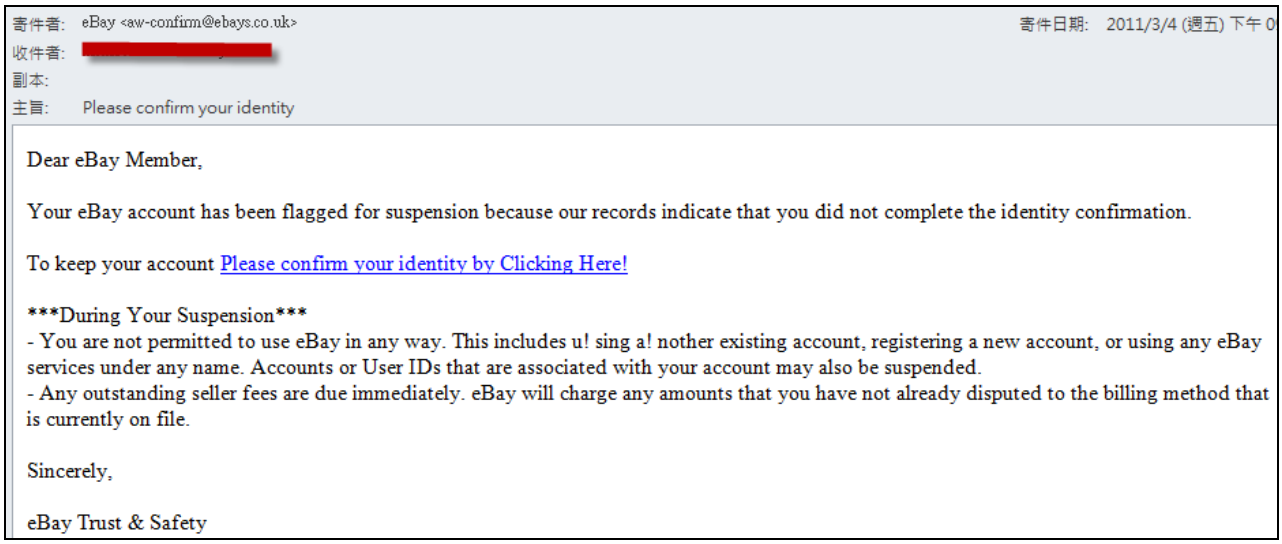
Securities (including mutual funds and variable life insurance), annuities and insurance products are not bank deposits and are not insured by the FDIC or any other agency of the United States, nor are they obligations of, nor insured or guaranteed by, JPMorgan Chase Bank, N.A., CISC, CIA, CMIA or their affiliates. Securities (including mutual funds and variable life insurance) and annuities involve investment risks, including the possible loss of value.

▸ En Español

Home | JPMorgan | JPMorgan Chase　　Terms & Conditions
© 2010 JPMorgan Chase & Co.

【假冒 CHASE Bank 身份的釣魚信件】

這樣幾可亂真的手法，其實大量充斥在第一季的郵件威脅中，不要任意點選電子郵件中的外部超連結，以及透過其他現實世界中的方式確認各種通知訊息的真偽，將成為未來免除這類型信件的第一步，類似的手法也出現在部份假冒 eBay 拍賣網站的垃圾釣魚信件中：



寄件者: eBay <aw-confirm@ebays.co.uk>　　寄件日期: 2011/3/4 (週五) 下午 0

收件者: [redacted]

副本:

主旨: Please confirm your identity

Dear eBay Member,

Your eBay account has been flagged for suspension because our records indicate that you did not complete the identity confirmation.

To keep your account Please confirm your identity by Clicking Here!

During Your Suspension
- You are not permitted to use eBay in any way. This includes u! sing a! nother existing account, registering a new account, or using any eBay services under any name. Accounts or User IDs that are associated with your account may also be suspended.
- Any outstanding seller fees are due immediately. eBay will charge any amounts that you have not already disputed to the billing method that is currently on file.

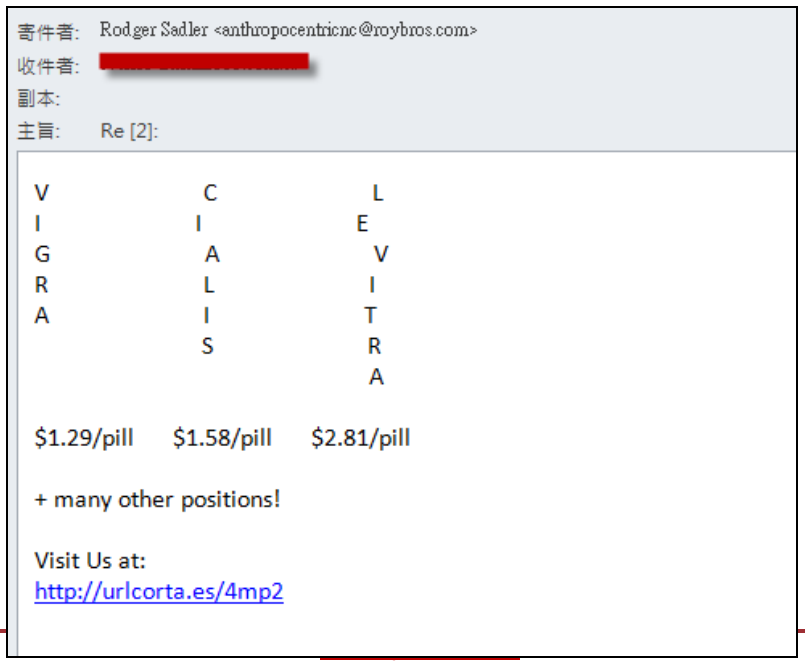
Sincerely,

eBay Trust & Safety

【假冒 eBay 身份的釣魚信件】

當然，內附的連結也是不折不扣，帶有木馬和病毒的釣魚網址。

同樣在一月底的時候，也出現了一些有趣的廣告信件，為了躲避傳統垃圾郵件防護閘道的偵測技術，這類型郵件往往將文字以直行的方式重新排列，以躲避傳統使用詞庫或者語意分析技術的垃圾郵件攔截技術，範例如下：



寄件者: Rodger Sadler <anthropocentricnc@roybros.com>

收件者: [redacted]

副本:

主旨: Re [2]:

V C L
I I E
G A V
R L I
A I T
S R
A

$1.29/pill $1.58/pill $2.81/pill

+ many other positions!

Visit Us at:
http://urlcorta.es/4mp2

【直行排列以躲避詞庫、語意分析攔截技術的信件】

類似的手法在二、三月的時候大量出現在簡體中文內容的廣告信件上，通常信件尾部也會附上帶有木馬的惡意連結或釣魚網址，以吸引使用者點擊。這類我們通稱為魚叉式網路釣魚的攻擊方式，手法都很類似，均以先躲過垃圾郵件防護閘道的偵測為目的，達成傳送到使用者信箱的目的後，再進而誘使使用者點擊，進入到下一個入侵階段，使用者接收到此類信件時，應提高警覺。

二月初期，也出現了一系列利用社交工程手法，想要欺騙使用者並奪取個資的垃圾郵件，例如底下便是一封透過偽冒英國 MasterCard 身份，假借微軟行銷活動中獎的名義，誘騙使用者回傳個人資料：

寄件者: MASTERCARD® / MICROSOFT® PROMOTIONS <info@mastercard.co.uk> 寄件日期: 2011/1/30 (週日) 下午 07
收件者: undisclosed-recipients:
副本:
主旨: INTERNATIONAL MEGA JACKPOT.

--
MASTERCARD® / MICROSOFT® PROMOTIONS.
INTERNATIONAL MEGA JACKPOT.

Dear email user,

Your email address was selected by MasterCard® Int'l in conjunction with Microsoft® Corporation UK. in the 2011 International Mega Jackpot, the selection was carried out through the Computerized Email Balloting System in a database of over one million emails, you were selected among the three lucky winners, you have been approved the sum of £452,000.00GBP(Four Hundred And Fifty Two Thousand Great British Pounds).

You are to contact your assigned claims agent with the following details requirement:

{1} Full names:
{2} Home address/Country:
{3} Phone number:
{4} sex/Age:
{5} Occupation:

Claims Agent: Mr. Lopez Anderson
Email: lopezanderson_claimsunit@live.co.uk

Yours sincerely,
Mrs. Rebecca Williams
Head of customer service.

Copyright© 2011 MasterCard® Inc. UK.

【意圖騙取個人資料的釣魚信件】

偽冒身份發送郵件以騙取使用者信任的郵件，還不此上述類型，有的攻擊者會透過發送正流行的電影、書籍、話題清單，誘使使用者點擊超連結而進行後續木馬攻擊的釣魚信件：

寄件者: HBO <webmaster@hboasiamails.com.sg>
收件者: [redacted]
副本:
主旨: Cinemax Asia Schedules - Week of 31 January 2011

您好，下面是 HBO 这征 8 周呈献的影片!

Cinemax Asia Schedules - Week of 31 January=2011 (GMT +8)

Monday, 31st January 2011

01:30am - 異形絽 82 結 2
03:00am - 暴力徽 A9 仇記
04:30am - 13 號星溙 C 五
06:00am - 大地霽 87
08:15am - 房客=/a>
10:00am - 血灑髽 98 棉
12:00pm - 黯夜麦 8B 子
02:00pm - 雷霆穿 BF 梭人
04:00pm - 魔星 2
06:00pm - 醝唅拽 89 戰役
08:00pm - 特務衽 8C 不行
10:00pm - Pacific Heights
11:45pm - Epad On Max 95

【假冒 HBO 名義，發送電影上映資訊的釣魚信件】

這類型郵件的特色是超連結的部份，通常都不是發信者假冒身份的網域，而是使用一系列轉址服務網站的方式隱藏其背後的真實連結，像是：

http://tracker.thevelo=itee.com/tracking/clickthrus/redirect.html?job_id=115706&email=tk27052=27@mail2000.com.tw&replacement_id=&url=http%3A%2F%2Fwww.cinemaxasia.co=%2Findex.php%2Fhomepage%2FmovieDetail%2F27%2F18%2F5491

確認信件的寄件者來源，並在點選超連結前，請先睜大眼睛確認細節，已經成為預防這類型郵件最重要的步驟。

提到台灣的垃圾郵件，就絕對不能不提大名鼎鼎的 XYZ 大補帖廠商系列，身為國內知名的地下盜版軟體供應商，XYZ 儼然成為台灣垃圾郵件圈中最為知名的發送者，由此可知，XYZ 也不會在這份報告中缺席。在整個二月中，可能為了趕上農曆新年的紅包檔期，XYZ 非常活躍地發送了大量、且具有特別針對性的垃圾廣告郵件，以下是其中兩封樣本：

【XYZ 系列垃圾郵件】

這類信件的特徵是訊息簡短、廣告文字直接呈現，並且透過附加知名網域（如此封樣本顯示的 google）的方式提高使用者對超連結的信任度，進而達到使用者點擊前往觀賞、消費、甚而埋下木馬的目的；這類以 http://www.coolsite.to/ 為首的 XYZ 集團，發送的類似廣告信件，在整個二月到三月的時候達到高峰。

Openfind 電子郵件威脅實驗室，特別從 2011 年第 1 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

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/。