防範釣魚郵件五大步驟
眾至設備讓使用者對駭客世界免疫

什麼是釣魚郵件呢? 如果上鉤了會造成什麼後果?

釣魚郵件利用當事人的心理引誘當事人點選信件中的連結以騙取電子郵件帳號密碼。一旦收件者受騙上當並輸入帳號密碼後，駭客極可能會利用這組帳號密碼嘗試入侵其他相關系統，達成進一步入侵。最後結果可能大到讓公司瀕臨絕境，小則很輕易就能被郵件伺服器隔離，結合眾至郵件郵件伺服器的SPF驗證、DKIM驗證、Sandstorm、 與眾至UTM的URL過濾資料庫，多道防線有助於多一份保障及安全。

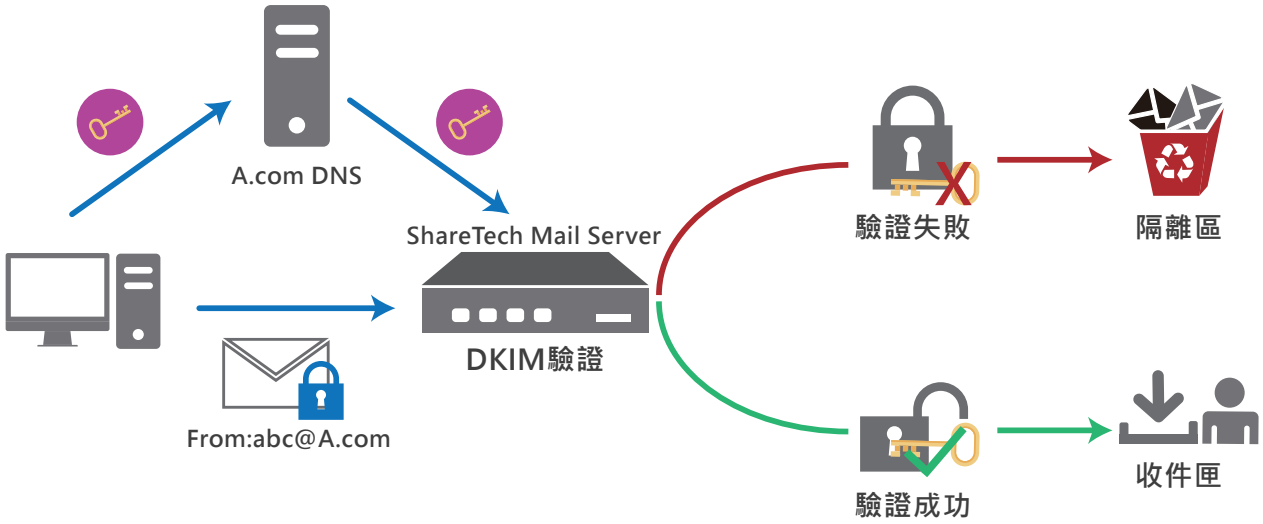
而什麼樣的人最容易被釣魚呢? 通常職業是業務、行銷、會計、進出貨人員、喜愛逛社群網站及購買優惠免費取得的網站最容易中獎。信件裡夾帶著陌生連結誘騙使用者點選。我們就來說說釣魚郵件怎麼送到使用者手上，當使用者收到信件時，郵件伺服器可以從SPF驗證及DKIM驗證過濾，抓出偽造主機所寄出的信件。

一、SPF驗證 (Sender Policy Framework) :
能幫使用者過濾掉非法主機偽造合法網域寄出信件

圖一、SPF驗證過程

台中總公司　04-2705-0888
台中市西屯區西屯路二段256巷6號3F-6
台北分公司　02-2501-1185
台北市中山區松江路129號6F-2
高雄分公司　07-229-8788
高雄市新興區民權一路251號8F-6
免付費專線　0800-666-188
官方網站 | www.sharetech.com.tw
銷售諮詢 | sales@sharetech.com.tw
技術支援 | help@sharetech.com.tw

二、DKIM驗證 (Domain Keys Identified Mail) :
能過濾掉寄件過程中寄件者主旨、內文及附件被冒名竄改信件



圖二、DKIM驗證過程

舉勒索病毒為例，當使用者點擊了不明的網站或者檔案，可能就成為受災戶。 所以若能在電子郵件抵達收件者信箱前，在郵件伺服器做好過濾及把關，就可避免員工一失手成公司的千古恨。

除了以上談到的兩種驗證，常見釣魚郵件還有入侵方式

1.在正常網域情況下連SPF和DKIM驗證正常但它是垃圾郵件

2.釣魚郵件中的網域，有可能是存在的，但連結到外面的網域，內嵌與公司一模一樣的登入頁面，藉由別人主機連到自家公司的Webmail，當使用者輸入帳密準備登入時，這時帳號已經被竊取。

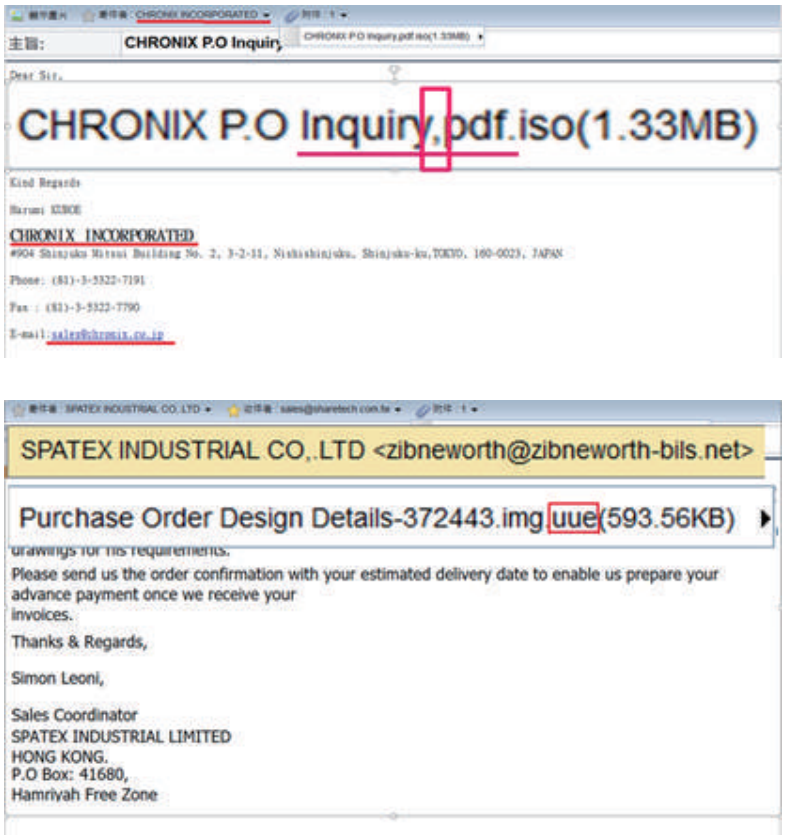
3.釣魚郵件也會通知使用者郵箱容量已經超過，請點URL可以獲得免費加大

4. 亦或告知使用者帳號被盜，需要修改帳密，進而竊取使用者輸入的帳密。

若要做到更完善的釣魚郵件防護，也需仰賴人為的確認。

三、收件者收到熟人的郵件，內文看似正常，但連結夾帶正確檔名

不只檢查寄件人、內文、連結和附加檔案的檔名，以下例子在PDF前從句點變成了逗點，甚至有PDF後面是接一些使用者沒看過的附檔名，都是可疑郵件。



圖三、圖四 釣魚威脅範例

四、可利用郵件原始檔案識破偽造信件

舉例下圖可知返回的路徑(Return-Path)和寄件者(From)一樣代表，這是一封偽造信件。
管理者可開啟郵件原始檔查看確認。

```
Return-Path: <mimeesyc@le.com>
Received: from le.com (unknown [200.11.228.50])
        by scan.sharetech.com.tw (Postfix) with SMTP id 96B212820077
        for <gapps@sharetech.com.tw>; Tue, 14 May 2019 05:12:27 +0800 (CST)
Received: from [172.160.197.63] by mail.naihautsui.co.kr with QMQP; Mon, 13 May 2019 17:10:00 -04
Received: from unknown (HELO mail.gimmicc.net) (Mon, 13 May 2019 17:01:20 -0400)
        by relay-x.misswldrs.com with ASMTP; Mon, 13 May 2019 17:01:20 -0400
Message-ID: <F5C02D5D.88D21A4B@le.com>
Date: Mon, 13 May 2019 17:01:20 -0400
Reply-To: gapps@sharetech.com.tw
From: gapps@sharetech.com.tw
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8.1.24) Gecko/20100317 Thunderbird/2.0.C
MIME-Version: 1.0
To: <gapps@sharetech.com.tw>
Subject: gapps@sharetech.com.tw has been hacked, change your password ASAP
Content-Type: text/html;
        charset="iso-8859-1"
Content-Transfer-Encoding: base64
```

圖五、返回的路徑與寄件者相同的範例

眾至郵件伺服器可以把通聯寄件者與內文寄件者不同的信件，增加垃圾郵件分數，進而減少使用者誤按的機會。

圖六、眾至郵件伺服器

五、請注意網址URL和來信方的關係

點選URL之前請再三確認連結，使用者應先確認超連結的真實網址，也可以把有疑慮的網址丟至Sandstorm分析來判斷此網址是否有無危害。

郵件伺服器也建議企業選購卡巴斯基防毒，協助過濾郵件病毒，若企業想做到更周全的防護，減少使用者未檢查動作或人為誤觸所造成的損失，也建議企業在閘道端建置UTM，並開啟選購URL網址資料庫過濾，可以利用URL黑名單資料庫做阻擋之動作，達到更全面且有效的防禦。