# 郵件社交騙術

講師　　呂守箴

# 大綱：

- 郵件社交工程的騙術
  - 防範詐騙停看聽
- 勒索軟體(病毒)的防範措施
  - 無法解毒的惡劣手段
- 行動裝置與電池安全
- 社群網站FB 的隱私設定
  - 如何不讓陌生人偷窺
- 通訊軟體 LINE 的安全設定
  - 如何防範騷擾與封鎖

# 郵件社交工程的騙術

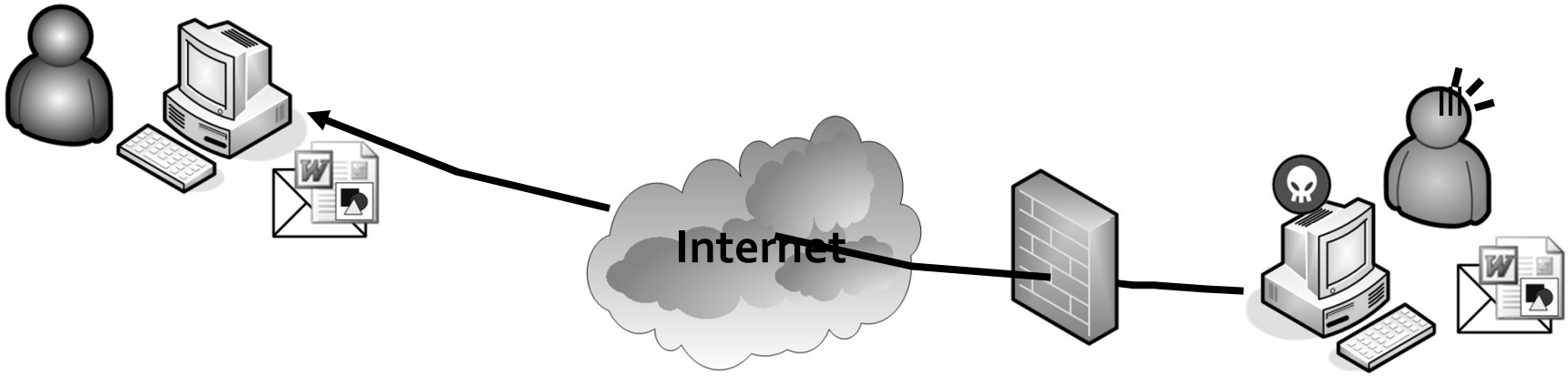
# 郵件社交工程攻擊之定義

- 利用人性弱點、人際交往或互動特性所發展出來的一種攻擊方法

- 早期社交工程是使用電話或其他非網路方式來詢問個人資料，而目前社交工程大都是利用電子郵件或網頁來進行攻擊

- 透過電子郵件進行攻擊之常見手法
  - 假冒寄件者
  - 使用與業務相關或令人感興趣的郵件內容
  - 含有惡意程式的附件或連結
  - 利用應用程式之弱點(包括零時差攻擊)

# 郵件社交工程攻擊模式




1. 駭客設計攻擊陷阱程式(如特殊 *Word* 檔案或外部惡意連結)
2. 將攻擊程式置入電子郵件中
3. 寄發電子郵件給特定的目標
4. 受害者開啟電子郵件
5. 啟動駭客設計的陷阱，將被植入後門程式
6. 後門程式逆向連接，向遠端駭客報到

# 郵件社交工程的手法

- 當收件人
- 開啟惡意電子郵件或
- 預覽惡意電子郵件或
- 點閱惡意電子郵件所附超連結或
- 點閱惡意電子郵件所附件檔案時，
- 即留下紀錄，或者感染病毒

- 並且可以統計
- 該惡意電子郵件的開啟率及
- 該惡意電子郵件的點閱率做為下一次詐騙之依據。

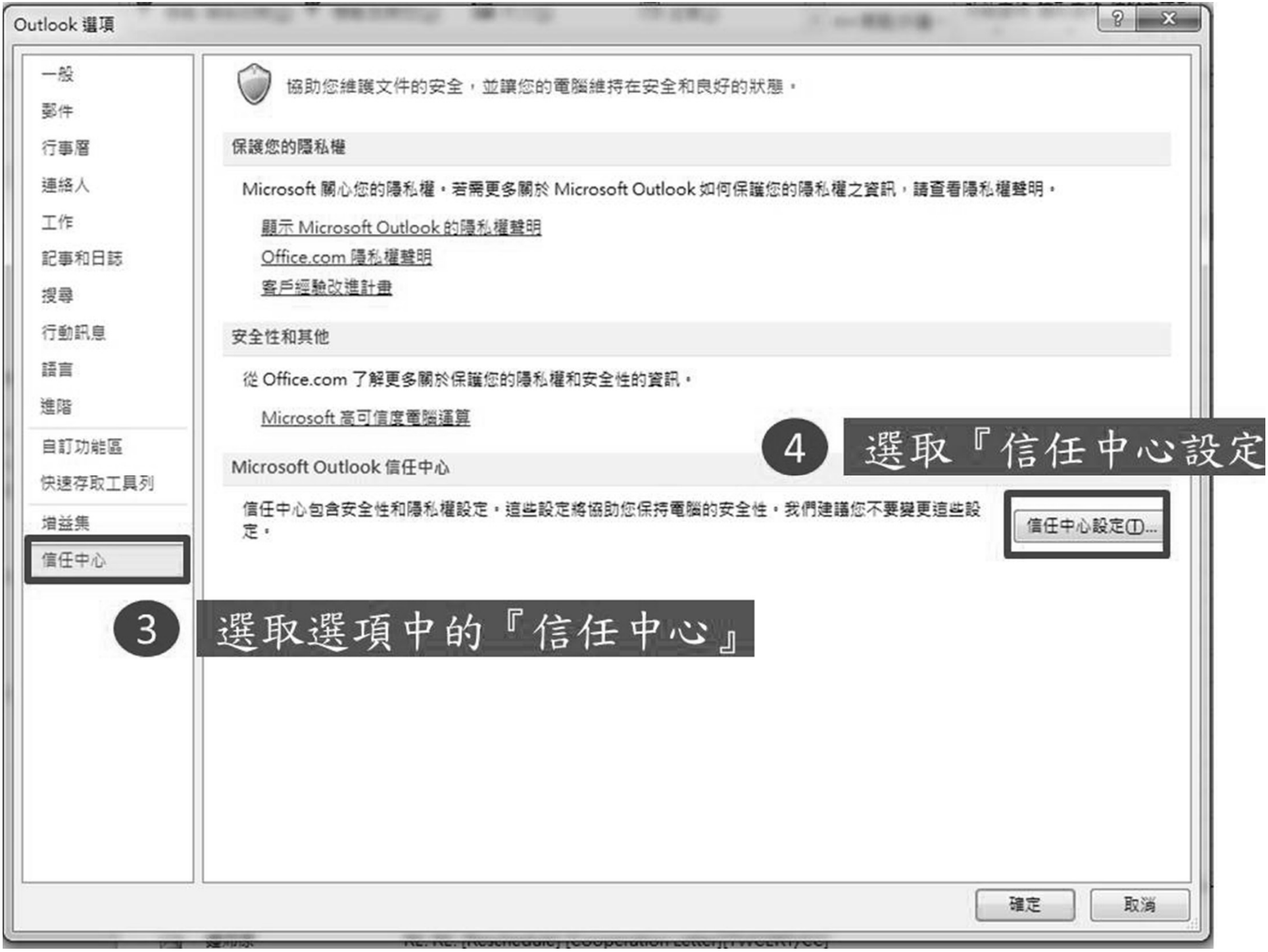
# 使用者防護停看聽(1)

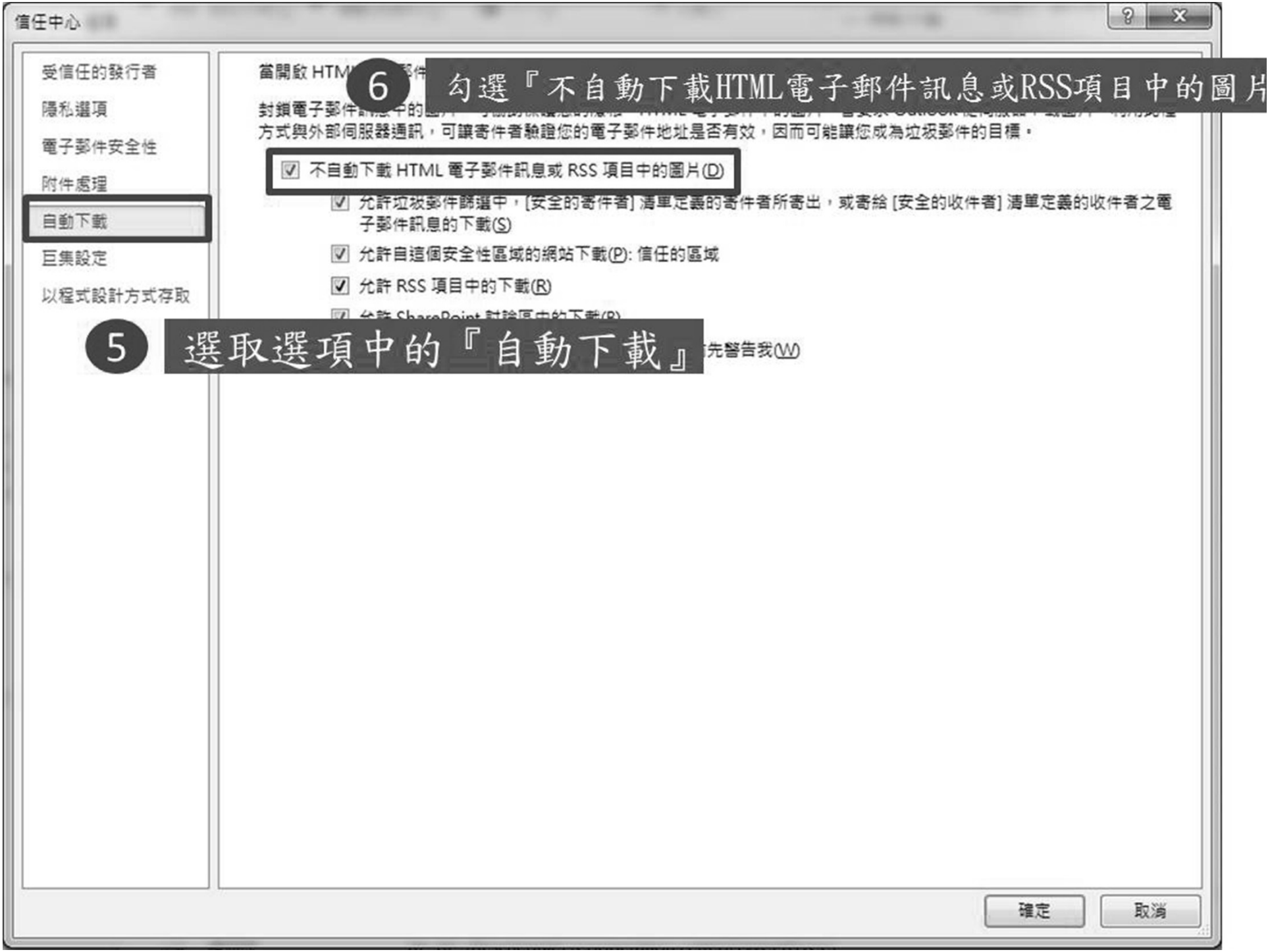
- **停 – 使用任何電子郵件軟體前，必須先確認**
  - 執行各種作業系統、應用軟體設定更新
    - Windows Update
    - Office Update
    - Internet Explorer 安全性設定
  - 必須安裝防毒軟體，並確實更新病毒碼
  - 收信軟體安全性設定
    - 如果可行的話以純文字模式開啟郵件
    - 必須取消郵件預覽功能
  - 防止垃圾郵件
    - 設定過濾垃圾郵件機制
  - 啟用個人防火牆

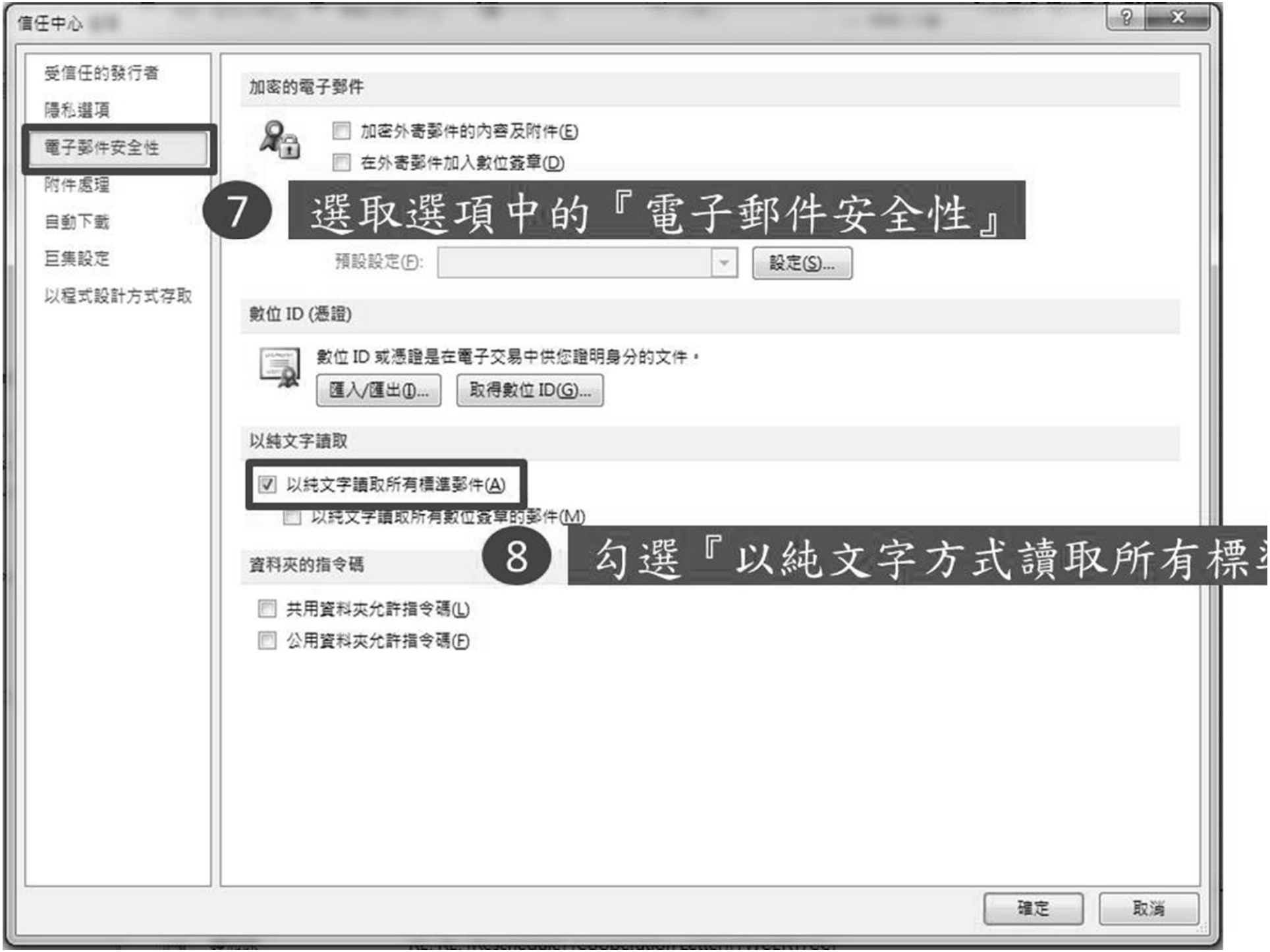
# 純文字模式

針對 Outlook 2003/2010


1
選取上方工具列的『檔案』
檔案
常用
傳送 / 接收
資料夾
檢視
Adobe PDF
另存新檔
儲存為 Adobe PDF
儲存附件
資訊
開啟
列印
說明
選項
結束
2
選取說明中的『選項』
帳戶資訊
boyi@cert.org.tw
POP/SMTP
新增帳戶
帳戶設定
帳戶設定
修改此帳戶的設定並設定其他連線。
清理工具
信箱清除
清空刪除的項目和封存，以管理信箱大小。
管理規則及通知
規則及通知
使用規則及通知可協助組織您的內送電子郵件，並在項目新增、變更或移除時收到更新。


Outlook 選項
一般
郵件
行事曆
連絡人
工作
記事和日誌
搜尋
行動訊息
語言
進階
自訂功能區
快速存取工具列
增益集
信任中心
協助您維護文件的安全，並讓您的電腦維持在安全和良好的狀態。
保護您的隱私權
Microsoft 關心您的隱私權。若需更多關於 Microsoft Outlook 如何保護您的隱私權之資訊，請查看隱私權聲明。
顯示 Microsoft Outlook 的隱私權聲明
Office.com 隱私權聲明
客戶經驗改進計畫
安全性和其他
從 Office.com 了解更多關於保護您的隱私權和安全性的資訊。
Microsoft 高可信度電腦運算
Microsoft Outlook 信任中心
信任中心包含安全性和隱私權設定，這些設定將協助您保持電腦的安全性。我們建議您不要變更這些設定。
信任中心設定(T)...
確定
取消
3
選取選項中的『信任中心』
4
選取『信任中心設定


信任中心
受信任的發行者
隱私選項
電子郵件安全性
附件處理
自動下載
巨集設定
以程式設計方式存取
6
勾選『不自動下載HTML電子郵件訊息或RSS項目中的圖片
方式與外部伺服器通訊，可讓寄件者驗證您的電子郵件地址是否有效，因而可能讓您成為垃圾郵件的目標。
不自動下載 HTML 電子郵件訊息或 RSS 項目中的圖片(D)
允許垃圾郵件篩選中，[安全的寄件者] 清單定義的寄件者所寄出，或寄給 [安全的收件者] 清單定義的收件者之電子郵件訊息的下載(S)
允許自這個安全性區域的網站下載(P): 信任的區域
允許 RSS 項目中的下載(R)
5
選取選項中的『自動下載』
確定
取消


信任中心
受信任的發行者
隱私選項
電子郵件安全性
附件處理
自動下載
巨集設定
以程式設計方式存取
加密的電子郵件
加密外寄郵件的內容及附件(E)
在外寄郵件加入數位簽章(D)
7
選取選項中的『電子郵件安全性』
預設設定(F):
設定(S)...
數位 ID (憑證)
數位 ID 或憑證是在電子交易中供您證明身分的文件。
匯入/匯出(I)...
取得數位 ID(G)...
以純文字讀取
以純文字讀取所有標準郵件(A)
以純文字讀取所有數位簽章的郵件(M)
資料夾的指令碼
8
勾選『以純文字方式讀取所有標
共用資料夾允許指令碼(L)
公用資料夾允許指令碼(F)
確定
取消

# 關閉預覽窗格

針對 Outlook 2010


2 選取上方工具列的『檢視』
3 選取『讀取窗格』
1 選取要調整的資料夾
4 選取『關閉』
檢視
Adobe PDF
讀取窗格
右(R)
下(B)
關閉(O)
01_FIRST (12317)
02_APCERT (692)
03_IR (1151)
04_IR處理回覆 (172)
05_SM MoU (6)
06_公文 (175)
07_TWCERT@cert.org.tw (1447)
08_文件翻譯 (10)
09_Member-Service (335)
10_Security Reports (2222)
11_IR@cert.org.tw (452)
12_Spam (2983)
13_應徵者資料 (62)
14_TANet CERT (48705)
15_A-SOC
16_TWNIC相關 (69)
17_KISA
18_測試-新通報平台 (13311)
草稿
寄件備份
刪除的郵件 (970)
RSS 摘要
垃圾郵件 [1028]
搜尋資料夾
日期: 今天
Ian Cook [1st NEWS] [DNB] Anatomy of a virus call centre scam
Ian Cook [1st NEWS] [DNB] Microsoft Safety Scanner
Ian Cook [1st NEWS] [DNB] BlackBerry is going the way of the Filofax
Ian Cook [1st NEWS] [DNB] Cell Phone Guide for Occupy Wall Street Protesters (and Everyone Else)
Ian Cook [1st NEWS] [DNB] MIKKO HYPPONEN - safe internet will lead the future
Ian Cook [1st NEWS] [DNB] SEC Asks Companies to Disclose Cyberattacks, Data Breaches
日期: 昨天
Ian Cook [1st NEWS] [DNB] Measuring the black web
Ian Cook [1st NEWS] [DNB] Big data centers spending big bucks on big hardware
Ian Cook [1st NEWS] [DNB] PIN Entry Devices Modified to Copy Card Information
Ian Cook [1st NEWS] [DNB] A Detail Analysis of an Advanced Persistent Threat Malware
Ian Cook [1st NEWS] [DNB] Web inventor Tim Berners-Lee on vision for the future of IT security
Ian Cook [1st NEWS] [DNB] Gov't cameras in your car? E-toll patent hints at Big Brotherish future
Ian Cook [1st NEWS] [DNB] US SEC lays out cyber attack reporting guidelines
Ian Cook [1st NEWS] [DNB] Security researcher threatened with vulnerability repair bill
Duhig, Nora [1st-t] Details of applications October 2011
Ian Cook [1st NEWS] [DNB] Welcome to the World of Cyber-Terror Vulnerability
Ian Cook [1st NEWS] [DNB] DC4420 - London DEFCON - October meet - Tuesday October 18th 2011
Ian Cook [1st NEWS] [DNB] Mr. Evans goes to Washington?!
Ian Cook [1st NEWS] [DNB] Classic: on Twitpic
Ian Cook [1st NEWS] [DNB] Cyber spies are hiding behind Anonymous
First Secretariat [1st-t] Maintenance and Update for FIRST Website
日期: 上禮
Ian Cook [1st NEWS] [DNB] SEC tells companies to disclose cyber attacks
Ian Cook [1st NEWS] [DNB] Occupy Wall Street protests: Rally to go global via London on Saturday
Ian Cook [1st NEWS] [DNB] U.S. Commerce Dept mum on Huawei block, citing security
Ian Cook [1st NEWS] [DNB] Gaddafi 'being tracked by satellite'
Ian Cook [1st NEWS] [DNB] VeriSign Withdraws Request To Suspend Malicious Domains

# 使用者防護停看聽(2)

- **看－**開啟電子郵件前應先依序檢視：

  (1)、【寄件者】的信箱來源

  (2)、【郵件主旨】是否與公務相關

  (3)、【附加檔案】不要直接點選打開，應另存新檔掃毒。

☺【寄件者】或【郵件主旨】與公務無關者，建議應立即刪除，連預覽都不要開啟郵件。

# 郵件社交工程：主旨

- 誘使你開啟的主題
- 特徵：
  - 情色
  - 健康、飲食
  - 折價、消費
  - 新聞、時事
  - 公務、意見表達、陳情
- 出現 RE: 與 FW: 之不同點。
- 單純從主旨是無法判斷真假的，除非事先有設定約定俗成的記號。

# 郵件社交工程：郵件內容：文字

- 文字：
- 眼睛所看到的文字，並非『純』的文字。而是由 HTML 網頁語法所產生的效果。
- 因此可撰寫惡意的HTML來產生病毒傳輸的效果。
- 變更成『純文字』的設定，才能避免在眼睛看不見下被動手腳！

# 郵件社交工程：郵件內容：超連結

- 超連結：
- 利用網路釣魚的手法將含有惡意程式的網址，採用偽裝的技巧詐騙使用者點選。
- 進階偽裝：
  - 網址編碼
  - 短網址
  - QR Code

# 郵件社交工程：附加檔案

- 誘使你開啟/點選的名稱
- 誘使你開啟/點選的副檔名(請問那些副檔名可能會暗藏病毒？)
  - Exe,com,bat,vbs
  - Doc,xls,ppt,pdf
  - Zip,rar
  - Jpg,bmp
  - Mp3,mpg,avi
- 防毒軟體掃毒機制
  - 收到信在主機端就掃描？
  - 收到信在使用者端掃描？
    - 打開收信軟體時掃描？
    - 點選信件時掃描？
    - 打開附件檔才掃描？
    - 偵測到有毒時才掃描？

# 使用者防護停看聽(3)

- **聽 – 若懷疑郵件來源，必須進行確認**
  - 透過電話或電子郵件向寄件人確認郵件真偽

# 防騙停看聽

| | |
|---|---|
| 停 | 安裝防毒軟體，確實更新病毒碼<br>關閉信件自動下載圖片及其他內容<br>以純文字模式開啟信件<br>取消信件預覽功能<br>設定過濾垃圾郵件機制 |
| 看 | 信件是否來自政府單位(gov.tw)或教育單位(edu.tw)<br>標題或內容是否與本身業務相關<br>其餘信件應視為垃圾郵件 |
| 聽 | 透過電話向對方確認信件真偽<br>透過電子郵件再次確認 |

# 勒索軟體(病毒)的防範措施

# 勒索程式 第一課

## 定義、原理和後果

### 什麼是勒索程式？

勒索程式是一種會挾持資料的嚴重資安威脅，它會讓檔案和系統功能無法使用，甚至讓整台電腦都無法使用。受害者必須支付一筆贖金來贖回自己的檔案和系統。

# 何謂勒索軟體(Ransomware)?

- 勒索軟體 Ransomware是一種特殊的惡意軟體，讓你失去對自己系統或資料的控制，而且如果不付錢給這攻擊的背後黑手也就無法拿回來。**基本上，你的系統或資料成為了人質，讓你被迫去支付贖金**。這也就是它被稱為「勒索軟體」的原因。

- 勒索軟體散播也有十年了。第一個版本早在2005年就在俄羅斯出現。

- 勒索軟體是如此地成功，甚至還從一般電腦發展到Android系統上。

# 它為何是一項資安威脅？

勒索程式早已從最初發現的那種沒有實質傷害性的恐嚇程式，演化成具備精密檔案加密能力的加密勒贖程式。


**2006**

俄羅斯出現一種可將受害者的**檔案壓縮**並加上密碼的勒索程式變種。

**2011**

出現一種要求受害者必須**發送高費率簡訊**到某個號碼的簡訊勒索程式。

**2012**

歐洲、美國和加拿大出現大量**假冒當地警察**而非留下勒索訊息的勒索程式。

**2013**

一種名為CryptoLocker的新型勒索程式出現，除了會鎖定系統之外，還會將檔案加密。

**2014**

所有 **48,000** 個偵測到的勒索程式當中有 **15,000** 個屬於**加密勒贖程式**，較首次發現以來成長了**27%**。

# 勒索軟體

- 通常是透過**釣魚郵件**傳播，使用者若是誤擊勒索軟體，電腦或是網路硬碟中若是存有被破壞的目標檔案類型，這些檔案就會全數被加密。

- 該軟體完成加密之後，使用者的電腦畫面，就會**跳出支付贖金來換取檔案解密的倒數通知**，要求被害者在指定之內，支付贖金。否則，只要時間一到，就會銷毀能夠解密的金鑰。

- 勒索軟體：
  - CryptoLocker
  - CryptXXX V1,V2,V3
  - TeslaCrypt V1,V2,V3,V4
  - SNSLocker
  - Roveton
  - CryptoWall
  - TorrentLocker
  - Curve-Tor-Bitcoin (CTB) Locker

# 您如何感染？

您可能在不知情的狀況下經由下列其中一種管道感染到勒索程式：

**遭到入侵的網站**

**垃圾郵件**

**其他惡意程式**

**它如何挾持資料？**

1 進入使用者電腦

2 **勒索程式** 鎖定螢幕

2 **加密勒贖程式** 搜尋某些檔案並將其加密

3 顯示勒索訊息

**檔案加密如何運作？**

**如何支付贖金？**

# Locky 勒索病毒利用 Flash 和 Windows 系統核心漏洞散布

不過，使用者所面臨的威脅還不只這樣。最近，趨勢科技發現這項攻擊又增加了一個新的技巧。除了利用 Flash 漏洞之外，駭客更利用一個 舊的 Windows 權限升級漏洞 (CVE-2015-1701) 來躲避資安軟體的沙盒模擬分析技術。

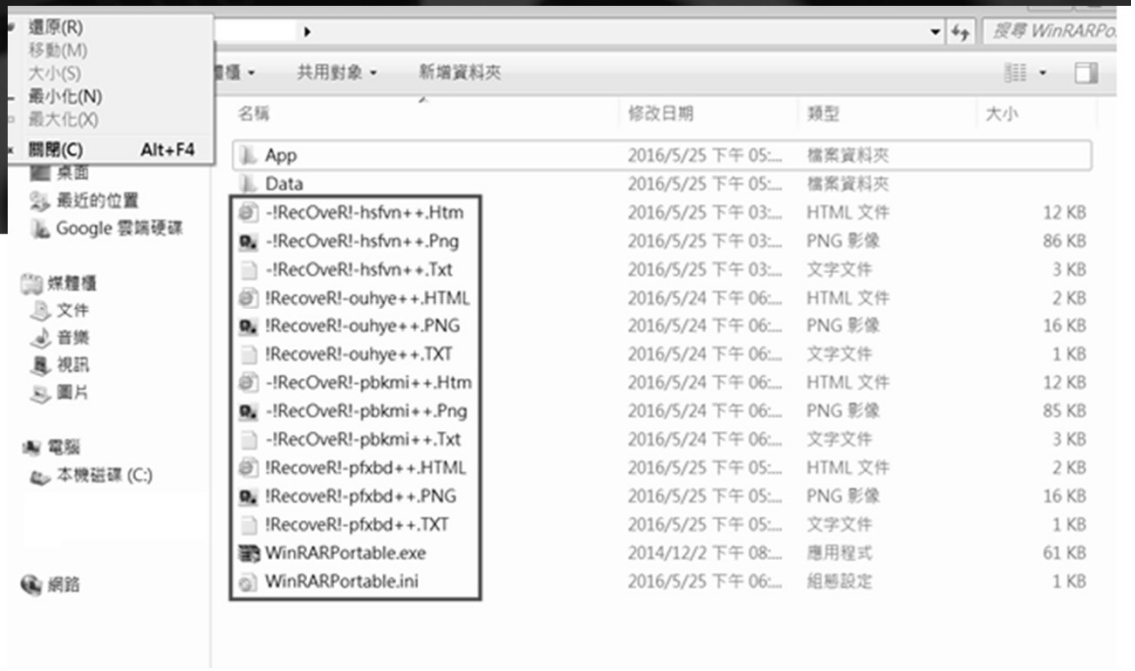
*隱匿的惡意行為*

趨勢科技不僅分析了擷取到的網路流量，也分析了一個相關的檔案下載程式 (也就是 TROJ_LOCKY.DLDRA)。從網路流量可發現此威脅利用的是 CVE-2016-1019 漏洞。至於檔案下載程式，則是利用了一個罕見的 Windows 核心漏洞。檔案下載程式可藉此連上其幕後操縱 (C&C) 伺服器 (IP：202.102.110.204:80)，並且下載Locky勒索軟體到系統上。這項技巧利用了多項核心層級的系統機制，包括：工作項目、系統執行緒以及非同步程序呼叫 (APC)。由於這些機制在使用時都不需要透過任何檔案，因此惡意程式可以在不被偵測的狀況下植入系統中。

# 勒索病毒 RANSOM_Waltrix ( CryptXXX) 爆災情!

透過惡意廣告發動攻擊;電腦若沒更新修補程式,
光瀏覽網頁就可能會中招!

據受害者反映, 瀏覽新聞網站、入口網站以及常在 Facebook 上分享的一些內容農場網站文章之後,
開始出現感染徵狀…



**近期感染勒索病毒（RANSOM_Waltrix or CryptXXX）災情嚴重主因:惡意廣告**

近期RANSOM_Waltrix(CryptXXX)勒索病毒災情頻傳，感染案件遽增的原因是駭客透過惡意廣告發動攻擊，所謂惡意廣告是駭客偽裝成廣告主，將他們製作的惡意廣告透過廣告商推播至各大網站或部落格。因此瀏覽一般正常網站也可能遭遇惡意廣告因而感染勒索病毒，尤有甚者駭客會利用漏洞攻擊套件(Exploit Kit)攻擊作業系統及應用程式的漏洞，若使用者電腦沒有更新修補程式，只是瀏覽一般網頁就可能會中勒索病毒。

此波肆虐台灣的勒索病毒利用Flash/SilverLight/IE的漏洞進行攻擊，據受害者反映，瀏覽新聞網站、入口網站以及文章常在 Facebook 臉書上被分享的一些內容農場網站之後，開始出現感染勒索病毒的情況，建議盡快更新Flash/SilverLight/IE的修補程式以降低遭遇勒索病毒攻擊的風險。

此類攻擊模式未來只會更多不會更少，遭受攻擊的軟體種類必會愈來愈多防不勝防，因此趨勢科技提醒您，請保持作業系統及各種應用程式更新到最新以防堵各種資安漏洞。

這篇報導:網頁廣告成勒索軟體散播溫床，紐約時報、BBC、MSN 皆中招,文中指出"攻擊者透過廣告聯盟及軟體漏洞，透過大型網站如《紐約時報》、BBC 、MSN 等的廣告，藉此安裝勒索軟體 Ransomware。

惡意廣告並非新的產物；它是已經存在了十多年的犯罪手法。早在 2004年，就出現當訪客連到科技網站「The Register」被流氓廣告攻擊的事情，它利用一個 Internet Explorer中的零時差漏洞來植入BOFRA惡意軟體。在過去十年間，許多高知名度的網站因為他們的廣告網路在不知情下成為網路犯罪市場的幫兇。受害者包括紐約時報、Google和赫芬頓郵報等數不清的例子。

# 您如何保護自己？

感染勒索程式目前還沒有解藥，不過使用者可以藉由下列方法來防止自己感染：

**定期備份資料**

遵守 3-2-1 原則：3 份備份、2 種儲存媒體、1 個不同的安全存放地點。

**將網站加入書籤**

將您經常瀏覽及信任的網站加入書籤當中，可防止您意外打錯網址的風險。

**檢查電子郵件來源**

在開啟任何電子郵件中的連結或下載其中的檔案之前，務必先仔細核對寄件人的地址是否在您的通訊錄當中。

**更新您的防護軟體**

保持最新狀態的防護軟體可讓您多一層保障，因此請務必定期更新，讓您有防範最新勒索程式變種的能力。

# ESET 的解密工具：

- 發布公告：
  http://support.eset.com/kb6051/?viewlocale=en_US

- TeslaCrypt 解密工具下載處：
  http://download.eset.com/special/ESETTeslaCryptDecryptor.exe

# 趨勢科技勒索病毒檔案解密工具

- 此工具支援解密的勒索病毒家族，下表所列的勒索病毒種類及檔案類型是此工具最新版本可以解開的。

| 勒索病毒種類 | 被加密後的檔案名稱及副檔名格式 |
|---|---|
| CryptXXX V1, V2, V3* | {原始檔案名稱}.crypt |
| TeslaCrypt V1** | {原始檔案名稱}.ECC |
| TeslaCrypt V2** | {原始檔案名稱}.VVV 或 CCC 或 ZZZ 或 AAA 或 ABC 或 XYZ |
| TeslaCrypt V3 | {原始檔案名稱}.XXX 或 TTT 或 MP3 或 MICRO |
| TeslaCrypt V4 | 檔名及副檔名均未被變更 |
| SNSLocker | {原始檔案名稱}.RSNSLocked |
| AutoLocky | {原始檔案名稱}.locky |

- 被 CryptXXX V3 加密的檔案，可能無法完整還原成原始檔案(部分解密)。
- RansomwareFileDecryptor 1.0.xxxx MUI 僅能解密 TeslaCrypt V3、TeslaCrypt V4。
- 若屬於 TeslaCrypt V1、TeslaCrypt V2，請下載 TeslacryptDecryptor 1.0.xxxx MUI 解密工具。
- 下載網址：
- http://esupport.trendmicro.com/solution/zh-TW/1114221.aspx

# 工具限制：

- 將 TeslaCrypt V1、TeslaCrypt V2 解密功能從原本的解密工具中分離出來額外提供。

- 目前並**不支援**解密 CryptXXX V2、CryptXXX V3 所加密的純文字檔案。

- 目前並**不支援**解密 CryptXXX V3 加密過的壓縮檔。

- 被 CryptXXX V3 加密的檔案，可能**無法完整還原**成原始檔案(部分解密)。

# 關於 CryptXXX V3 重要說明：

- CryptXXX V3 的勒索病毒加密方式較特別，屬進階加密方式，目前被加密的檔案只有部分有機會可以被解密，但即便被解密也可能需要用到第三方檔案修復工具進行修復。 (例如：公開原始碼的 JPEGSnoop)

- 舉例來說，當照片或圖檔僅有部分內容被解密，可能會發生只看得到部分照片或圖檔的內容，如果該檔案是您的重要檔案，或許可以使用第三方工具或更專業的檔案復原服務來協助。

- 加密之前的原始圖檔

- 部分資料經過解密後的圖檔

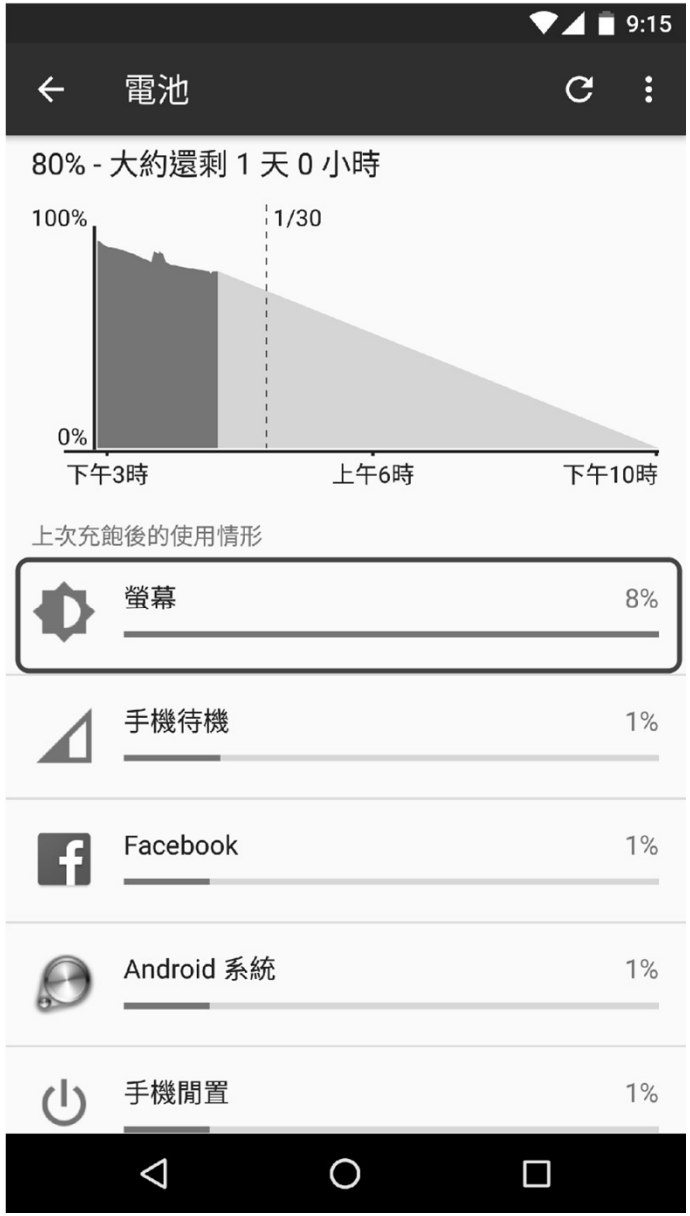
- 趨勢科技技術支援中心對於第三方檔案復原工具與服務所能提供的支援相當有限，因此無法提供相關工具或諮詢給使用者。

# 行動裝置與電池安全

# 智慧型手機『耗電』前三名：

1. 螢幕**亮度**。
2. 網路連線。(耗電量 **4G>3G** > WiFi > 藍芽)
3. 背景執行的系統或APP程式。(例：LINE、FB)

- 註：
- 4G/3G訊號越差越耗電，電磁波也越強。
- GPS不斷**移動定位**會耗電。
- **震動**比鈴聲耗電，電量低時切成靜音或無聲比較省電。



# 電池的使用：

- 優良的鋰電池深度放電的次數可以達到 500 ~1000 次以上，換句話說，雖然**深度充放電(充滿、耗盡)的動作對鋰電池來說並不好**，耗盡的次數越多，你的電池歸西的時間就會提早到來！

- 把鋰電池電量用光關機之後再去充電。
- **←錯誤！過度放電會導致電壓過低，反而會充不了電。**

- 重點：
- 鋰電池一直插著充電不會延長壽命，反而會過熱燒掉。
- 新電池第一次使用時，不用充電 8~12 小時。
- 鋰電池不怕充，但是怕熱、怕過充、怕摔。
- 鋰電池本身就有壽命限制，但通常還未到達壽命之前，先換掉的是『手機本身』。

# 社群網站FB 的
# 隱私設定

# 帳號安全


8:35
設定
一般
帳號安全
隱私設定
動態時報與標籤
定位服務
封鎖
語言
通知
手機簡訊
追蹤者
應用程式
廣告
交易付款

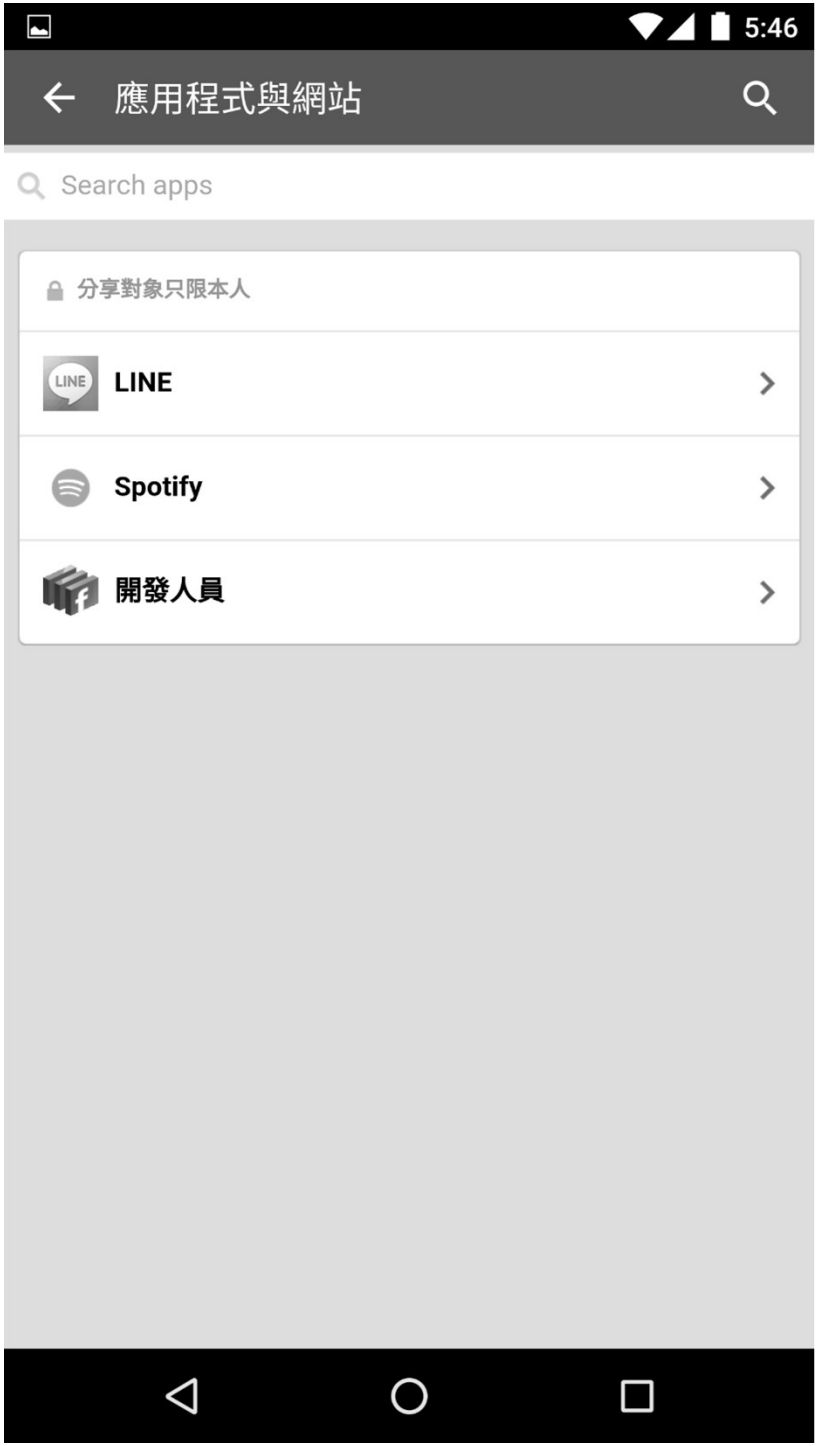

8:35
安全性設定
登入警告
任何人從新的裝置或瀏覽器登入你的帳號時接收通知。
登入許可開啟
第三方驗證器
信賴的聯絡人
信賴的聯絡人是每當你無法存取帳號時，可以安全地幫你恢復存取權的朋友。
應用程式密碼
認可的裝置 4
有效的連網。 7


8:37
你的人際關係鏈
誰可以看到我的個人檔案資料？
直接從個人檔案管理個人檔案資料的隱私設定。
貼文
誰可以查看你往後的貼文？
公開
限制你設定和「朋友的朋友」以及「公開」分享貼文的分享對象？

# 應用程式
# 設定


8:35
設定
一般
帳號安全
隱私設定
動態時報與標籤
定位服務
封鎖
語言
通知
手機簡訊
追蹤者
應用程式
廣告
交易付款


5:46
應用程式與網站
在 Facebook 上，你的姓名、大頭貼照、封面相片、性別、人脈網絡、用戶名稱和用戶 ID 一律是公開顯示給用戶和應用程式。瞭解原因。應用程式也可以存取你的朋友名單，以及你選擇公開的任何資訊。
使用 Facebook 帳號登入
LINE 、 Spotify 和開發人員
平台
開啟
你已經授權 3 個應用程式和你的 Facebook 帳號互動。
別人使用的應用程式
已關閉
看得到你的資訊的人，都可以將你的資訊帶往他們使用的應用程式。使用這個設定可控制哪些類別的資訊可以讓他們帶往他處。
舊版的手機專用 Facebook
只限本人
對於你使用沒有內聯分享對象選擇器的舊版 Facebook 手機應用程式（像是舊版的 Blackberry 專用 Facebook 應用程式）所張貼的內容，這個設定可以幫你控制隱私設定。


5:46
應用程式與網站
Search apps
分享對象只限本人
LINE
Spotify
開發人員


5:47
LINE
LINE
應用程式的能見度
只限本人
這個不能控制誰可以看見你在應用程式的活動，或你被其他人標註在應用程式的動態。
你提供的資料：
公開的個人檔案 （必填）
呂守箴、大頭貼照、 21 歲以上、男性和其他公開資訊
電子郵件
shooujen@gmail.com
你從 Facebook 移除所安裝的應用程式後，應用程式可能還保有你的資料。聯絡應用程式開發人員以移除此資料。
深入瞭解如何控制權限。
應用程式條款
隱私政策
移除應用程式
舉發應用程式


5:46
應用程式與網站
在 Facebook 上，你的姓名、大頭貼照、封面相片、性別、人脈網絡、用戶名稱和用戶 ID 一律是公開顯示給用戶和應用程式。瞭解原因。應用程式也可以存取你的朋友名單，以及你選擇公開的任何資訊。
使用 Facebook 帳號登入
LINE 、 Spotify 和開發人員
平台
開啟
你已經授權 3 個應用程式和你的 Facebook 帳號互動。
別人使用的應用程式
已關閉
看得到你的資訊的人，都可以將你的資訊帶往他們使用的應用程式。使用這個設定可控制哪些類別的資訊可以讓他們帶往他處。
舊版的手機專用 Facebook
只限本人
對於你使用沒有內聯分享對象選擇器的舊版 Facebook 手機應用程式（像是舊版的 Blackberry 專用 Facebook 應用程式）所張貼的內容，這個設定可以幫你控制隱私設定。


5:47
開放平台
遊戲邀請和應用程式通知
是否要收到遊戲邀請和應用程式的通知？
是
否
應用程式和網站
允許你使用 Facebook 帳號玩遊戲，以及登入其他應用程式與網站。
編輯

# 隱私設定


9:03
隱私捷徑
誰可以看到我的個人檔案資料？
誰可以看到我的東西？
誰可以與我聯絡？
我該如何防止別人騷擾我？
隱私設定基本資訊
更多設定
資料政策


9:04
隱私捷徑
誰可以看到我的個人檔案資料？
誰可以看到我的東西？
誰可以查看你往後的貼文？
公開
我可以在哪裡檢查我發佈的內容或是被標註內容的分享對象？
查閱動態紀錄
誰可以與我聯絡？
我該如何防止別人騷擾我？
隱私設定基本資訊
更多設定
資料政策


9:04
隱私捷徑
誰可以看到我的個人檔案資料？
誰可以看到我的東西？
誰可以與我聯絡？
誰可以傳送交友邀請給我？
朋友的朋友
我該如何防止別人騷擾我？
隱私設定基本資訊
更多設定
資料政策


9:04
隱私捷徑
誰可以看到我的個人檔案資料？
誰可以看到我的東西？
誰可以與我聯絡？
我該如何防止別人騷擾我？
你可以封鎖某些人，和他們解除朋友關係，以防止他們和你對話，或是看到你張貼在動態時報上的內容。你封鎖的對象仍可查看及評論你分享於社團、應用及其他地方的貼文。
新增姓名或電子郵件
封鎖
已被封鎖的人
12
隱私設定基本資訊
更多設定
資料政策

# 活動紀錄


晚上09:16
活動紀錄選項
活動紀錄
只限本人可以看到你的活動紀錄
篩選條件
你的貼文
2015年4月
2015年3月
2015年2月
2015年1月
2014年
2013年
2012年
2011年
2010年
2009年


晚上09:16
活動紀錄選項
活動紀錄
只限本人可以看到你的活動紀錄
篩選條件
你的貼文
2015年4月
2015年3月
2015年2月
2月26日
呂守箴更新了他的近況。
編輯隱私設定
在動態時報中隱藏
刪除
公開
2月18日

# 通訊軟體 LINE 的安全設定

# LINE 的資安疑慮： (詐騙、中毒)

- Line為新興詐騙手法之工具：可能傳遞惡意連結造成手機中毒、小額付費連結等。

- LINE 的詐騙與中毒手法： (簡訊社交工程)
  - 破解帳號密碼偽裝朋友身分，詐騙購買點數卡。
  - **傳遞連結至惡意網站/偽冒網站的網址。**
  - **傳遞具有下載觸發惡意程式的貼圖/圖片。**
  - 傳遞觸發小額付款的付費連結。
  - **透過免費貼圖的下載與後台統計資料，廣告商可取得使用者行為的大數據分析。**

- 資安案例：

# 帳號不被盜!
# 好友不受騙!

LINE

1.設定「換機密碼」



2.不需要使用電腦登入LINE，
請關閉「允許自其他裝置登入」

3.使用電腦登入LINE，
建議「使用行動條碼登入」


4.不要使用太
簡單的密碼

NPA署長室提供幾項
建議使用的安全機制，
降低LINE帳號被盜用的風險

NPA署長室


LINE 安全
設定
(降低詐騙)


晚上11:11
其他
P 0
LINE Points
加入好友
貼圖小舖
主題小舖
官方帳號
LINE Pay
LINE TV
禮品小舖
LINE Q
LINE Points
最新資訊 NEW
LINE採用新的移動帳號流程
推薦項目


我的資訊

- 個人資料
- 我的帳號
- 隱私設定
- 移動帳號設定
- Keep

商店

- 貼圖
- 主題
- 我的錢包

基本設定


- 我的錢包

基本設定

- 提醒
- 圖片・影片
- 聊天・語音通話
- 好友
- 群組
- 動態消息

詳細資訊

- 關於LINE
- 常見問題


晚上11:12
我的帳號
電話號碼
設定電話號碼
ID
尚未設定
設定電子郵件帳號
設定已完成
Facebook
解除
連動中的應用程式
允許自其他裝置登入
開啟此項即可使用電腦和 iPad 版的 LINE，
並且登入其他 LINE 網頁服務。
刪除帳號
刪除帳號


晚上11:13
隱私設定
密碼鎖定
若您忘記密碼，必須先刪除LINE，再重新安裝。
請留意：您過去的聊天記錄將會被全數刪除。
允許利用 ID 加入好友
其他用戶可透過 ID 搜尋將您加入好友。
阻擋訊息
開啟本功能後即可阻擋不是來自好友的訊息。
更新行動條碼
廣告最佳化


移動帳號

**非必要時，請勿變更設定。**
將此設定變更為「ON」，即可將帳號移動至其他智慧手機。
變更為「ON」經過一定時間後，或確實移動帳號後，設定將會再次改回「OFF」。


LINE採用新的移動帳號流程
2016-4-27

LINE由4/27 10:00起，採用新的移動帳號流程！新流程取代原來的「換機密碼」方式，提升便利性與安全性。

**換手機的事前準備(請在「原本的手機」上進行)**
平時即確認綁定電子郵件帳號
電子郵件帳號密碼的設定路徑：其他 > 設定 > 我的帳號 > 點選「設定電子郵件帳號」設定帳密 * 請勿與原郵件密碼相同 > 進行認證 > 認證手續完成後，點選「確定」

**進行移動帳號**
「舊手機上」
需先於舊手機上開啟並使用全新的「移動帳號」模式：其他 > 設定 > 兩階段認證 > 開啓「移動帳號」ON（「移動帳號」平常自動設定為OFF，開啓ON後，24小時後會恢復為OFF）。

「新手機上」
在新手機安裝LINE之後，開啟，選擇「用戶登入」，輸入設定的電子郵件帳號與密碼後，按確定
輸入新手機電話號碼，並輸入收到簡訊之4位數認證碼
完成移轉

若無舊手機，或舊手機不能使用，或其他情況，請填寫客服反應表，尋求協助：http://contact.line.me/zh-hant
詳細移動帳號流程介紹請參考部落格文：http://lin.ee/fsJTNKK 。

# LINE正確換機SOP

## 情況1

### 舊手機仍可使用


## 其他情況

- 舊手機遺失
- 舊手機無法使用
- 其他情況

填寫LINE客服反應表

https://contact.line.me/zh-hant/


## 再也不用擔心訊息被擷取

LINE的最新版(5.3.0版本)中，新增兩大資安功能：

- 「訊息保護(Letter Sealing)」：

採用點對點加密技術(End-to-End Encryption, E2EE)
來保護訊息(Letter Sealing)，
所有LINE的**文字訊息與位置訊息**
都將直接在用戶的手機上加密，
金鑰不需要在網路上傳遞，

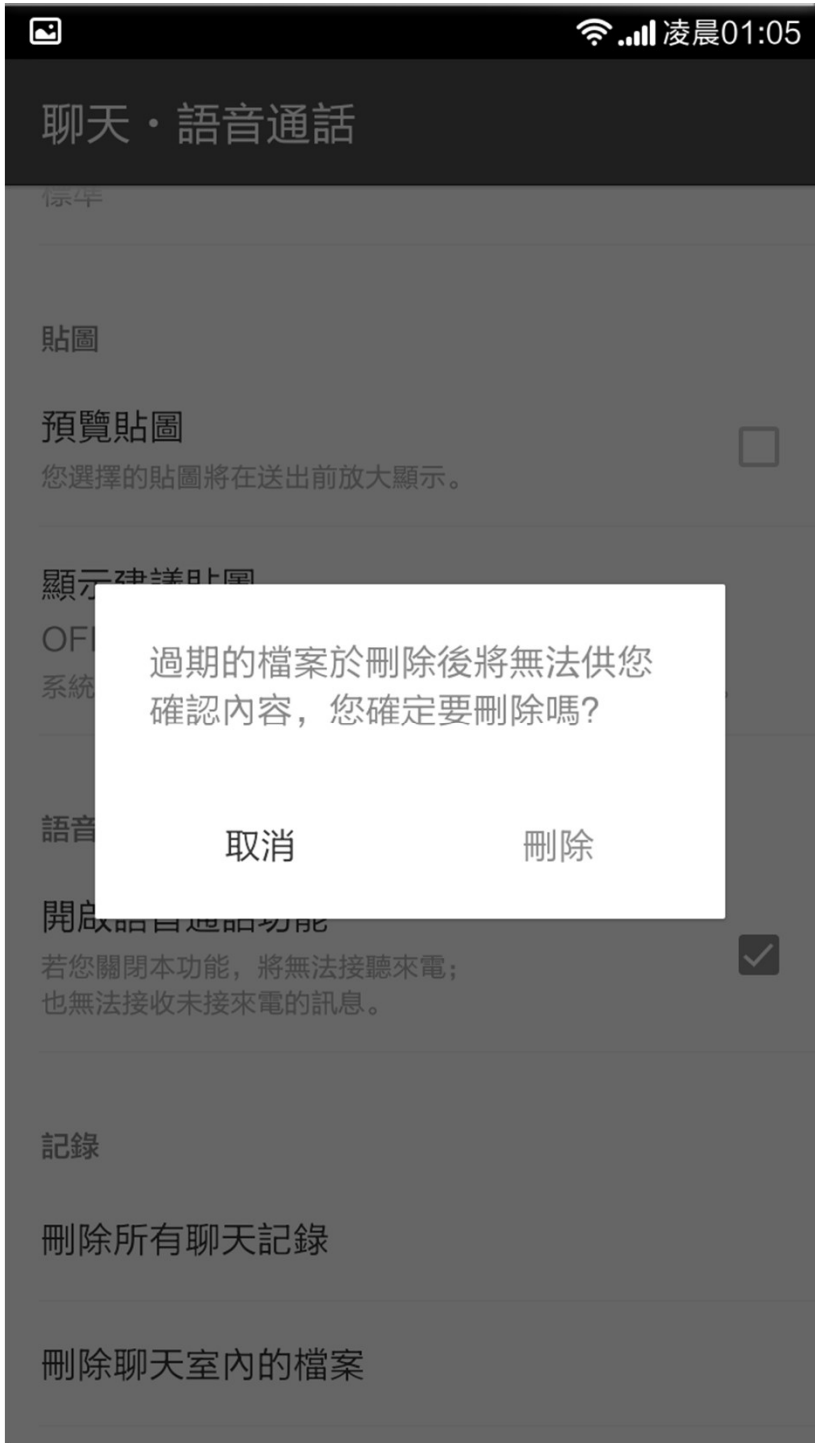
只有對話的雙方可以為彼此的訊息加密與解密，
任何第三方都將無法解密也無法窺知任何文字訊息與位置訊息。

LINE的這項功能是目前即時通訊產業中第一個
可同時橫跨Android、iOS及Windows、Mac等作業系統的訊息保護功能。

- 「完整刪除(True Delete)」：

更新至5.3.0版本以上的用戶所刪除的訊息，
將無法再透過本人、任何手機使用者或第三方還原，
這項功能將徹底避免手機上已被刪除的對話紀錄被他人還原、使用，
此功能也可以跨平台使用。


晚上11:14
聊天・語音通話
使用進階加密功能可保護訊息。 但僅限於和同時開啟
Letter Sealing功能的好友聊天時有效。
貼圖
預覽貼圖
您選擇的貼圖將在送出前放大顯示。
顯示建議貼圖
OFF
系統將會依您輸入的文字，顯示適合該文字的貼圖或表情。
語音通話功能
開啟語音通話功能
若您關閉本功能，將無法接聽來電；
也無法接收未接來電的訊息。
記錄
刪除所有聊天記錄
刪除聊天室內的檔案


凌晨01:05
聊天・語音通話
貼圖
預覽貼圖
您選擇的貼圖將在送出前放大顯示。
過期的檔案於刪除後將無法供您
確認內容，您確定要刪除嗎?
取消
刪除
若您關閉本功能，將無法接聽來電；
也無法接收未接來電的訊息。
記錄
刪除所有聊天記錄
刪除聊天室內的檔案


加入好友

自動加入好友

通訊錄的好友將自動加入好友名單。
如需手動更新，請點選更新圖示。

允許被加入好友

允許其他用戶使用我的電話號碼搜尋並自動加我好友。

管理好友

隱藏名單

封鎖名單

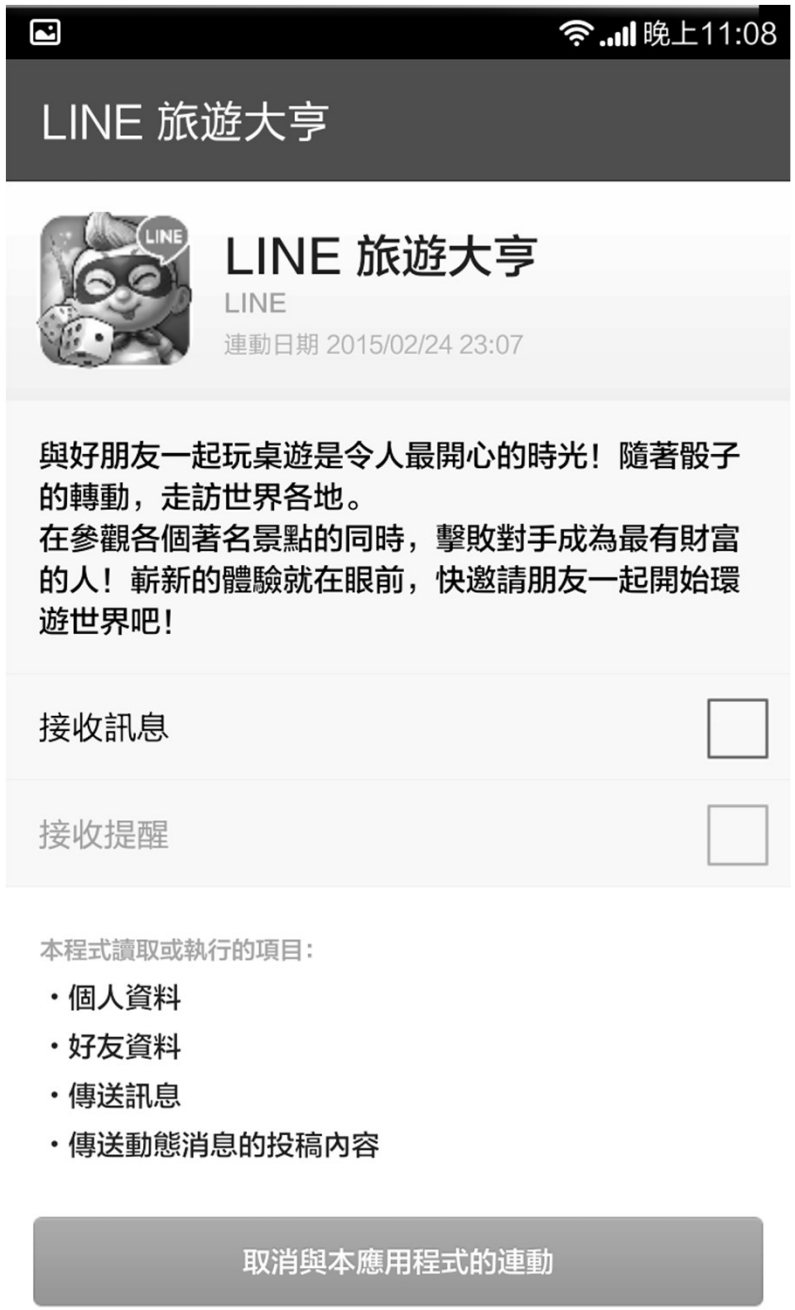
# LINE 安全設定(防止騷擾)


晚上9:18
設定
我的錢包
基本設定
提醒
圖片・影片
聊天・語音通話
好友
群組
動態消息
詳細資訊
關於LINE
常見問題


晚上9:18
提醒
提醒
若強制結束應用程式，提醒訊息將有可能延遲送達或無法接收。
暫停
鈴聲
震動
LED
暫停1小時
暫停至早上8點
提醒
顯示訊息內容
您可以透過提醒查看訊息。
螢幕開啟時
OFF
休眠狀態時
OFF


晚上9:18
提醒
顯示訊息內容
您可以透過提醒查看訊息。
螢幕開啟時
OFF
休眠狀態時
OFF
自訂設定
LINE Pay
群組邀請
動態消息提醒
OFF
連動中的應用程式
您可對連動應用程式設定提醒功能
未連動的應用程式
關閉此設定後，即可拒收未允許連動的應用程式訊息。


晚上11:07
連動中的應用程式
連動中的應用程式
LINE 旅遊大亨
連動日期 2015/02/24 23:07


晚上11:08
LINE 旅遊大亨
LINE 旅遊大亨
LINE
連動日期 2015/02/24 23:07
與好朋友一起玩桌遊是令人最開心的時光！隨著骰子的轉動，走訪世界各地。
在參觀各個著名景點的同時，擊敗對手成為最有財富的人！嶄新的體驗就在眼前，快邀請朋友一起開始環遊世界吧！
接收訊息
接收提醒
本程式讀取或執行的項目：
・個人資料
・好友資料
・傳送訊息
・傳送動態消息的投稿內容
取消與本應用程式的連動


晚上10:44
設定
主題
我的錢包
基本設定
提醒
聊天・語音通話
好友
群組
動態消息
詳細資訊
關於LINE
常見問題


半夜12:52
動態消息
8
設定開放範圍
自動向新好友公開
您的動態消息及主頁的內容，將自動向新加入的好友公開。
隱藏動態消息的用戶名單
凌晨02:00
設定開放範圍
您動態消息及主頁上的更新內容將會向好友公開。（官方帳號除外）您還可以選擇要向哪些好友公開喔！
@LINE就是LIE
未公開
未公開
未公開


LINE 設定
(刪除、隱
藏、封鎖)


下午2:59
呂守箴(OpenBlue)
邀請
提醒OFF
封鎖
編輯訊息
贈送禮物
相簿
照片
聊天設定
免費通話
視訊通話
已讀
下午2:40
可以
測試刪除
下午2:40
將我刪除後，你那邊可以收到訊息嗎？
下午2:41
已讀
下午2:41
可以，會重新出現新的聊天訊息。
測試封鎖
下午2:42
將我設定封鎖，你那邊可以收到訊息嗎？
下午2:43


下午2:59
聊天
呂守箴(OpenBlue)
下午2:43
將我設定封鎖，你那邊可以收到訊息嗎？
呂守箴(OpenBlue)
呂守箴(OpenBlue)
聊天
隱藏
刪除
LINE
LINE系統提醒您，您目前已登入LINE CHROME。 "登入中的裝置: Chrome"


下午3:00
好友
加入好友
自動加入好友
通訊錄的好友將自動加入好友名單。
如需手動更新，請點選更新圖示。
允許被加入好友
允許其他用戶使用我的電話號碼搜尋並自動加我好友。
管理好友
隱藏名單
封鎖名單 (1)


當您在封鎖名單上刪除該用戶之後，將不會收到來自該用戶的訊息。
刪除後，若您需要向該用戶傳送訊息，請利用ID搜尋、行動條碼、搖一搖等方式重新將該用戶加入好友名單內。
呂守箴(OpenBlue)
編輯
下午3:00
封鎖名單
當您在封鎖名單上刪除該用戶之後，將不會收到來自該用戶的訊息。
刪除後，若您需要向該用戶傳送訊息，請利用ID搜尋、行動條碼、搖一搖等方式重新將該用戶加入好友名單內。
呂守箴(OpenBlue)
編輯
呂守箴(OpenBlue)
解除封鎖
刪除

# 您確定要知道這個殘酷的真相嗎？

1. 送訊息後，對方長時間都顯示未讀(判斷率50%)。
2. 看不見對方的首頁、投稿內容(判斷率65%)。
3. 送貼圖，對方顯示已有此貼圖(判斷率90%)。
4. 拉對方進群組測試(判斷率95%)。

# 帳號被盜

# 7種最常被盜的登入密碼

簡單密碼方便記，駭客盜用也容易！快去換一組安全的LINE登入密碼吧！

1
一組密碼
走天下

2
生日


3
純數字


4
密碼太短

5
跟帳號一樣


6
常見單字


7
連續字母

# 帳號無法登入，或疑似被盜時的正確因應。

- 不能登入的狀態，不等於帳號已經被盜。因此，如果遇到這樣的情況，正確的步驟應為：

  1. 試著登入：如果登入發現無法更改登入密碼，請立即填寫問題反應表。

  2. 填寫「**問題反應表**」：如果已經無法登入，切勿急於註冊一個新的帳號。在特定狀況下，即便客服很想協助您，但仍可能救不回帳號，包括所有您購買的項目像是貼圖跟主題，以及好友名單等，都無法恢復。

- 為了避免這樣的狀況發生，請注意：
  1. 千萬**不要自行刪除**帳號。
  2. 千萬**不要把原帳號綁定**的項目，像是電話號碼、Email，或Facebook，也同時綁在「新帳號」上。

- 資料來源：
- LINE 台灣官方 BLOG ~ 帳號無法登入，或疑似被盜時的正確因應。
- http://official-blog.line.me/tw/archives/37500029.html

# 其實最好不要用(可惜大多數人辦不到)，那麼要用就要先學保護自己的方法。

- Line 台灣官方「問題反應表」：
- https://line.naver.jp/cs/zh-hant/

- 說明：
- Line帳號被盜的情況頻傳，甚至衍生出詐騙案件，經過刑事局和Line公司協調之後，基於打擊犯罪的共同目標，即日起民眾可以透過Line問題反應表的連結，就可以立刻請求 LINE 公司處理，同時讓被害人拿回原帳號。

# 評估風險再決定使不使用！


- 應該這麼說，這是一個跨國的企業、
- 韓國的公司、日本發行、台灣代理。

- 並非完全不能使用Line，而應該是說想用這種通訊軟體，就必須知道它的風險。

- 了解它所造成的影響再根據自己能接受的風險(被側錄、過濾、詐騙簡訊、違法貼圖)，再決定使不使用。

- 如同前一陣子討論公務機關到底開不開放使用MSN、雅虎奇摩即時通等通訊軟體一樣，需要事先評估資安風險。

- 註：Line 有提供『電腦版(桌面版)』可以安裝，也須評估資安風險。

# LINE 台灣官方部落格 ~ 安心使用教學

- (一) 新手註冊時的設定：
- http://official-blog.line.me/tw/archives/30500821.html

- (二) 隱私安全與廣告訊息阻擋設定：
- http://official-blog.line.me/tw/archives/34654629.html

- (三) 更改與設定密碼的技巧：
- http://official-blog.line.me/tw/archives/37682230.html

- 設定您的換機密碼：
- http://official-blog.line.me/tw/archives/39661081.html

- 帳號無法登入或疑似被盜時的正確因應：
- http://official-blog.line.me/tw/archives/37500029.html

- 關於「群踢」的那些事... 該如何預防？
- http://official-blog.line.me/tw/archives/36307488.html

- LINE 常見問題 Q & A ：
- https://help.line.me/line/android/pc?lang=zh-Hant

# 結論：

- 郵件社交工程的騙術
  - 防範詐騙停看聽
- 勒索軟體(病毒)的防範措施
  - 無法解毒的惡劣手段
- 行動裝置與電池安全
- 社群網站FB 的隱私設定
  - 如何不讓陌生人偷窺
- 通訊軟體 LINE 的安全設定
  - 如何防範騷擾與封鎖

- 講師：　呂守箴
- E-Mail：shoujen@gmail.com

- FB粉絲團：
  - 個人FB：facebook.com/openblue
  - 網路攻防戰：facebook.com/netwargame
  - 簡報力：facebook.com/PPTPower
  - Hacker x Maker：facebook.com/hackerxmaker

- Google+：
  - 個人：google.com/+openblue
  - 網路攻防戰：goo.gl/AzbbnS (區分大小寫)
  - Hacker x Maker：goo.gl/ZFdAx7 (區分大小寫)

- 網路教學直播網址：youtube.com/c/openblue/live
- YouTube 頻道：youtube.com/c/openblue