

和泰保險經紀人有限公司 資訊安全認知教育訓練



資訊安全教育訓練

■ 規劃資訊安全教育訓練計畫

- 應規劃年度資訊安全教育之教育訓練，制訂每年所需接受之資訊安全教育訓練之目標及基本時數。

■ 執行資訊安全教育訓練

- 系統或作業流程如有異動變更，應讓員工瞭解新的工作、設備或流程，避免因操作不當而造成資料錯誤或營運中斷。
- 除了本公司內所舉辦之教育訓練，日常亦應視需要派員參與外界舉辦相關訓練或研討會。
- 本公司人員每年應至少參與教育訓練**2小時**之時數。

■ 資訊安全教育訓練評量與紀錄

- 執行教育訓練應考量設計學習評量機制，如隨堂測驗、抽問、心得分享、案例討論或實作等，以作為評估訓練效果之依據。

課程大綱

1. 資訊安全政策
2. 資訊安全指揮管理規範
3. 人員安全管理規範
4. 資訊設備授權及保護管理規範
5. 安全區域管理規範
6. 辦公室資訊作業管理規範
7. 社交工程新聞回顧
8. 社交工程類型
9. 社交工程攻擊與因應
10. 資訊安全宣導
11. 問題與討論

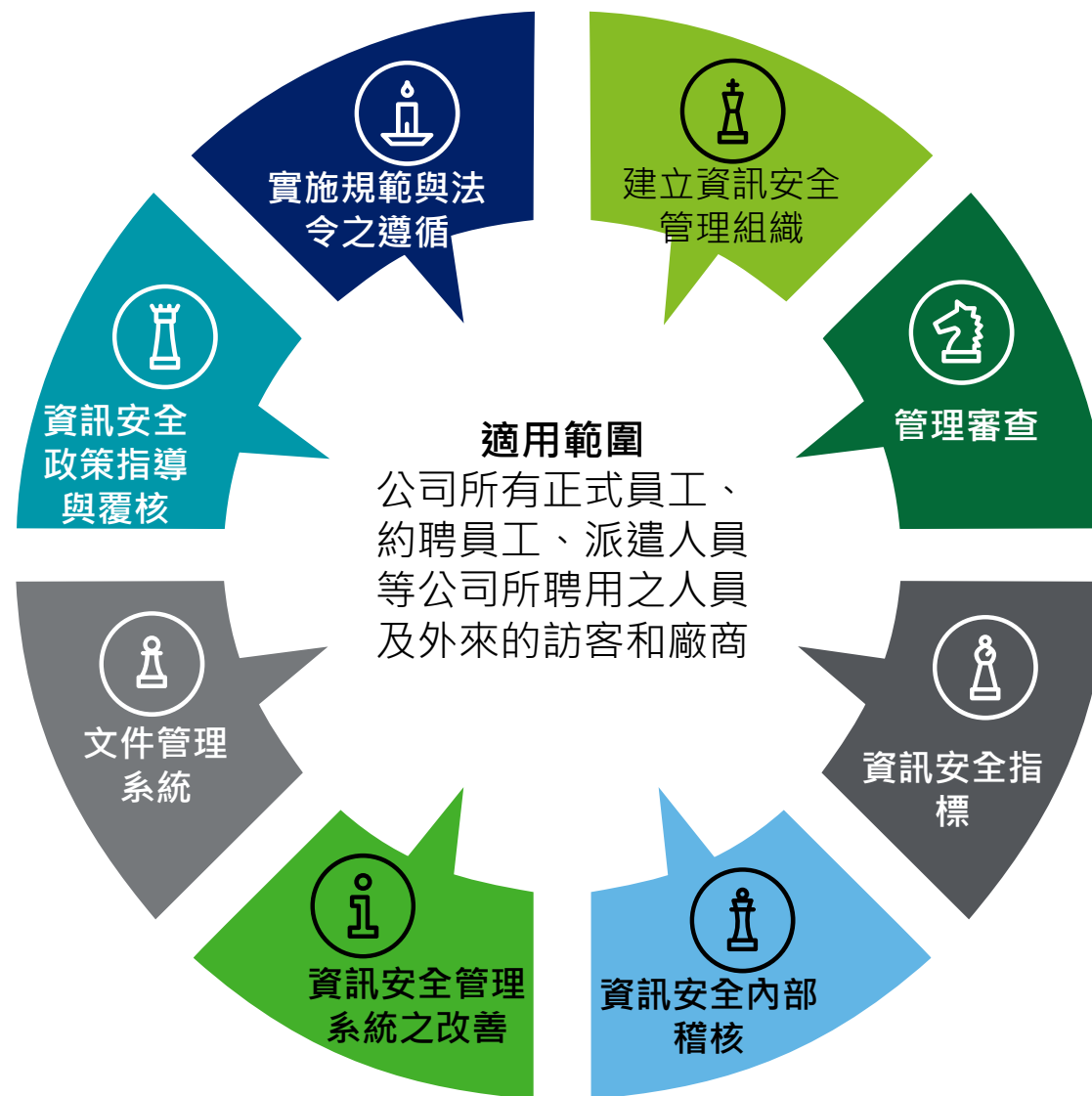
資訊安全政策

SP-001

資訊安全政策

目的

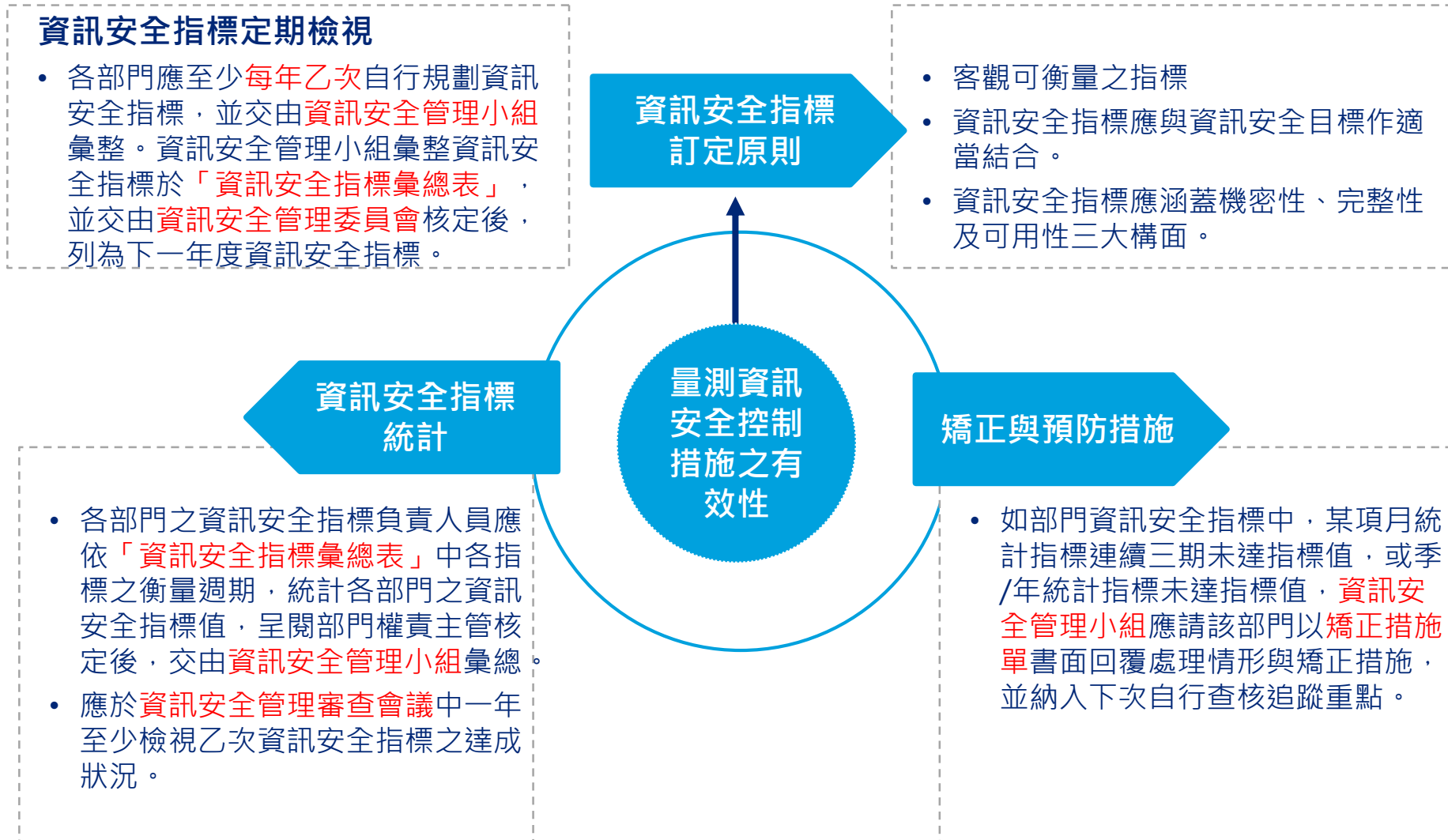
定義和泰保經股份有限公司的資訊安全政策，使全體同仁能遵守並有所依循，輔助使用者之各項業務作業順利運行，並確保各項資訊媒體之安全，以達成公司資訊安全之目標。



資訊安全指標管理規範

SR-003

資訊安全指標管理規範



人員安全管理規範

SR-005

人員安全管理規範

人員之 任用

- 依本公司資源部門相關規定辦理。
- 應對求職者所提供之個人背景、專業資格等進行確認。

聘僱

- 員工保密合約：應要求本公司員工、約聘雇人員簽訂。
- 廠商保密合約：對於協力廠商、委外廠商或顧問於協助執行專案前應要求其簽訂。
- 職能區分：
 - 明確劃分各人之職務和權責。
 - 設置代理人制度：代理人之選擇與指定應事先審查核定，以符合代理人對資訊存取權限之適當性。

離職/ 專案結束

- 人員離職時，應取消該員所有權限，並歸還本公司資產。
- 委外專案結束時，應立即取消廠商相關人員所有權限，並歸還本公司所屬資產。

資訊安全教育訓練

■ 規劃資訊安全教育訓練計畫

- 應規劃年度資訊安全教育之教育訓練，制訂每年所需接受之資訊安全教育訓練之目標及基本時數。

■ 執行資訊安全教育訓練

- 系統或作業流程如有異動變更，應讓員工瞭解新的工作、設備或流程，避免因操作不當而造成資料錯誤或營運中斷。
- 除了本公司內所舉辦之教育訓練，日常亦應視需要派員參與外界舉辦相關訓練或研討會。
- 本公司人員每年應至少參與教育訓練**2小時**之時數。

■ 資訊安全教育訓練評量與紀錄

- 執行教育訓練應考量設計學習評量機制，如隨堂測驗、抽問、心得分享、案例討論或實作等，以作為評估訓練效果之依據。

資訊設備授權及保護管理規範

SR-007

系統存取管理

➤ 使用者帳號及權限管理

- 每年應至少清查帳號與權限乙次，以確保權限之適切性。

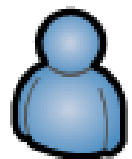
➤ 特殊權限管理

- 特殊權限帳號之使用應僅限於經授權核准之事項，並留存適當之稽核軌跡。帳號管理人員需至少每年檢視一次稽核軌跡是否有異常之處，並視情況限制使用特殊權限之有效時間。

➤ 密碼管理

- 使用者初次登錄時，應要求立即變更密碼。密碼長度不可少於6個字元，內容不得純為數字或英文，且不可具有規則性(如連續或相同之號碼或文字等)，每180天應至少變更一次，更換後之密碼不得與前5次密碼相同。時間同步
- 重要系統最高權限之密碼應彌封於緊急密碼函之中由單位主管妥善保管。

稽核軌跡管理



系統管理者
設定稽核軌
跡開啟內容



針對特殊作
業留存稽核
軌跡

1. 一般使用者帳號登入失敗事件
2. 特殊權限帳號存取紀錄
3. 特殊權限帳號之異動
4. 系統錯誤事件



稽核軌跡應妥善保存防
止未經授權存取及竄改



由系統定期產製
稽核報表



稽核日誌應視其性
質予以備份並設定
保存期限，系統及
網路設備之稽核軌
跡應至少留存一年
以上

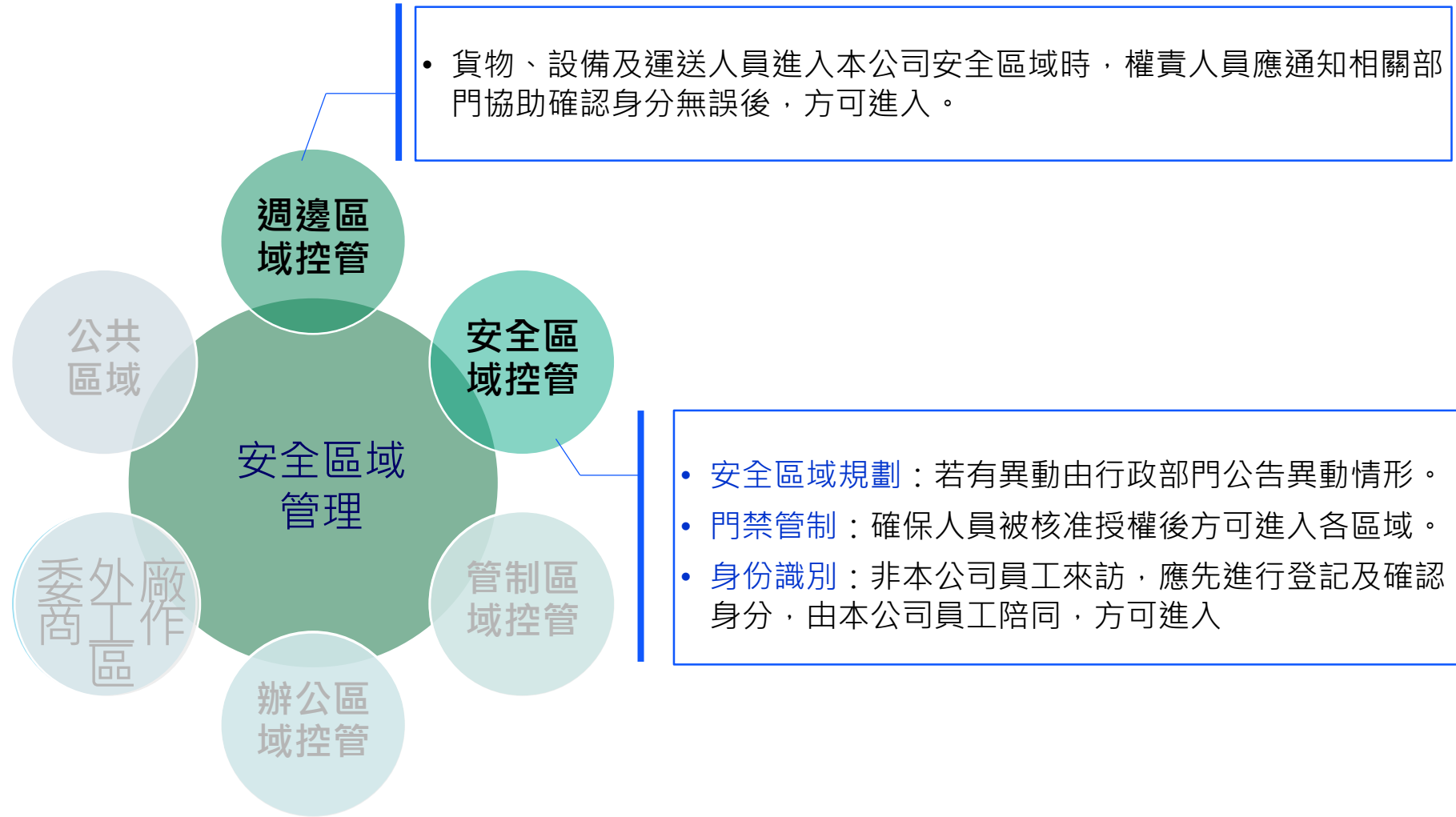


主管定期覆核
報表內容

安全區域管理規範

SR-008

安全區域管理(1/4)



安全區域管理(2/4)



• 進出管理

- 進出大門應有門禁隔離設施以防止未經授權的存取，如門禁刷卡裝置、警報裝備、人工值守的接待區域等，並經過適當記錄。
- 因業務需要，如設備維護，而獲臨時授權進入管制區域之第三方廠商人員，應確實填寫「訪客進出紀錄表」，詳載出入之時間、目的及處理事項。
- 機房之門禁進出許可人員清單應由本公司權責單位至少每半年檢視乙次，以確認進出許可授權之適當性。

• 作業規範

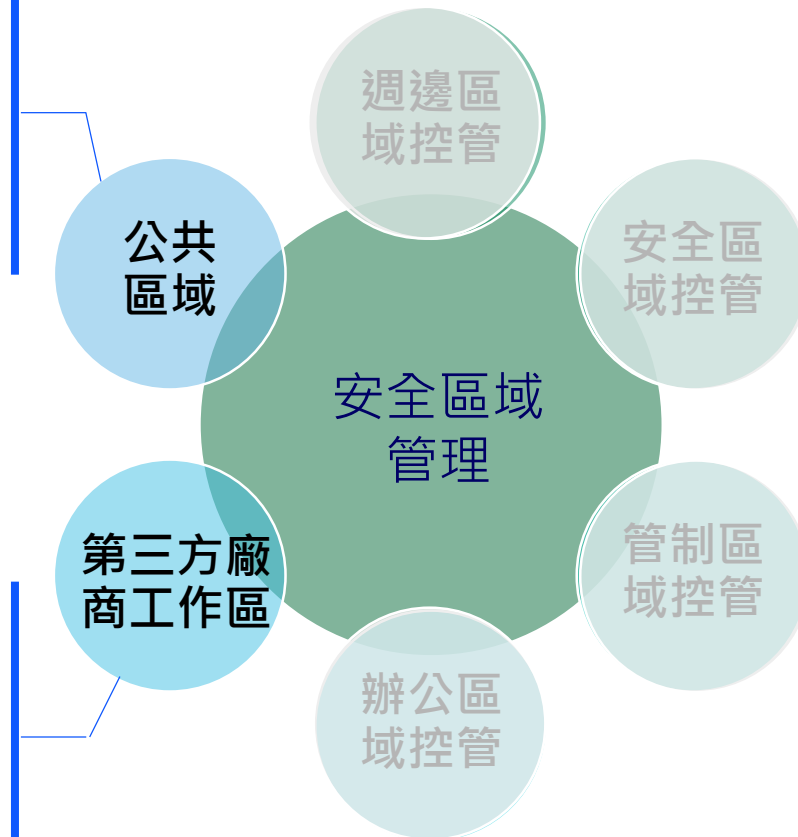
- 危險或易燃物品放置應與管制區域保持安全距離。
- 未經核准不允許堆放或儲存大宗物品。
- 禁止吸煙、飲食或其它與處理管制區域業務無關之行為。
- 離開應確認門窗已確實關閉並鎖上。

- 具有資料複製功能之設備避免放置於公共區域及委外廠商工作區。
- 列印、影印或傳真收發文件時，應立即領取。
- 會議結束應立即清除會議室白板與桌面資料。

安全區域管理(3/4)

- 分機表及通訊錄等具有聯絡資料及身份之文件應避免張貼於公共區域。
- 機密與內部使用等級之文件切勿任意放置於公共區域。

- 委外廠商應於獨立工作區工作。如因工作需求需於管制或辦公區域工作時，應受本公司人員監督。
- 委外廠商工作人員須遵守上述安全區域管理規範。



資訊安全事件管理規範

SR-012

資訊安全事件管理規範

- ❖ 應建立資訊安全事件的正式通報程序及管道，並訂定通報後應採行之行動及措施，以便迅速有效處理資訊安全事件。
- ❖ 資訊安全事件依其影響範圍及影響程度影響等級分為4個級別，如事件之判定可歸屬一個以上等級者，事件分級應以大者為主，相關內容如表：
- ❖ 資安事件影響等級為1(含)以上事件，應分析引發資訊安全事件之原因實施相關之矯正措施，記錄於「**資訊安全事件報告單**」。

性質等級	機密性	完整性	可用性
3	機密級或敏感資料遭洩漏。	核心業務系統或資料遭嚴重竄改;抑或關鍵資訊基礎設施系統或資料遭竄改。	核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作;抑或關鍵資訊基礎設施運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作或無法於可容忍中斷時間內回復正常運作。
2	核心業務(含關鍵資訊基礎設施)一般資料遭洩漏。	非核心業務系統或資料遭嚴重竄改;抑或核心業務系統或資料遭輕微竄改。	非核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。
1	非核心業務一般資料遭洩漏。	非核心業務系統或資料遭輕微竄改。	非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。
0	資料未遭洩漏。	資料未遭竄改。	業務運作未受影響或系統未停頓。

資訊安全事件報告單

資訊安全事件報告單

文件編碼：SR-012-F01
頁數：1/2
版次：1.0
公佈日期：

表單編號：

通報	通報人員		部門 主管	簽名	通報時間
	所屬部門				
	發生時間				
	事件描述				
執行風險 評估與分 類	事件等級 判定	<input type="checkbox"/> 第 1 級事件 <input type="checkbox"/> 第 2 級事件 <input type="checkbox"/> 第 3 級事件			
事件調查(由資訊安全管理小組人員填寫)					
影響範圍	<input type="checkbox"/> 網路 <input type="checkbox"/> 伺服器 <input type="checkbox"/> 系統 <input type="checkbox"/> 其他：_____				
持續時間	小時 分鐘				
問題原因					
處理說明					
因應方案					
結束日期		發生部門 主管核准			
緊急應變小組		資訊安全 管理委員會			

本表單於呈請核准後，自公布日起實施，修正及廢止時亦同。

事件說明與處理

- 進行最初判定：
- 傳達意外事件：(依資訊安全事件通報程序進行通報)
- 抑制損毀和降低風險：(針對該資安事件依其嚴重程度和安全性原則進行緊急處理措施)
- 指出受害的類型和嚴重性：(判斷資安事件發生的類型、所牽涉之系統)
- 保護證據：(針對收集的證據，維護有跡可循的監管鏈。為保護證據，應記錄由誰收集、如何收集、何時收集以及誰有存取權)
- 通知外部機構：(依資訊安全事件通報程序進行通報)
- 系統復原：
- 矯正因應措施：(進行矯正因應措施)
- 通報層級： 部門主管 總經理

承辦人	部門主管
緊急應變小組	資訊安全管理委員會

辦公室資訊作業管理規範

SR-017

辦公室資訊作業管理規範



- 個人辦公桌面應維持清潔，**下班前**應將業務上使用之文書歸檔整理。
- **不再使用之機密文書資料**，應使用碎紙設備或其他無法還原原始資料之銷毀方式進行銷毀。
- 個人電腦與終端機應設定**一定時限**內自行啟動密碼螢幕保護程式或自行登出。

- 所有人員未經權責主管核可，不得將機密等級資料儲存於可攜式電腦設備或可攜式儲存媒體內。
- 所有人員未經權責主管核可，不得將自攜裝置連接內部網路與伺服器主機，或是進行傳輸、處理、儲存任何本公司業務資料。

- 依據「資訊資產暨風險評鑑管理規範」之分類原則，將**內部使用等級以上文件**放置於**上鎖的文件櫃中**。

辦公室資訊作業管理規範

- 應針對惡意軟體及惡意網站採取適當預防措施。
- 應加強員工認知。
- 惡意軟體防範應考量之原則如下：
 - 禁止使用未取得授權之軟體。
 - 禁止使用來路不明或內容不確定的儲存媒體。
 - 安裝防毒軟體並定期更新病毒碼。
 - 應避免存取來路不明或內容不確定的外部網站或網址連結(hyperlink)。



- 所有員工應至少**每月**主動更新其所使用電腦作業系統與軟體之重大修正檔。
- 第三方服務承包廠商人員之可攜式電腦設備於連接本公司內部網路**前**應確認其已更新所有重大修正檔。
- 行動裝置上的軟體或作業系統，應定期安裝更新修補程式，以確保資訊安全。

- 未經授權核准嚴禁自行架設無線分享器。
- 未經授權核准嚴禁使用雲端儲存平台等可能造成公司資料外洩之管道，例如Drop Box、Google Drive...等。
- 禁止使用P2P(Peer-to-Peer)檔案分享程式、抓檔軟體、續傳軟體等任何可能對網路的正常傳輸造成不利影響之軟體。

課程大綱

- 社交工程新聞回顧
- 社交工程類型
- 社交工程攻擊與因應
- 資訊安全宣導
- 問題與討論



社交工程新聞回顧

駭客假稱IG藍勾勾認證騙帳密 這些網紅、藝人都中招

新聞日期

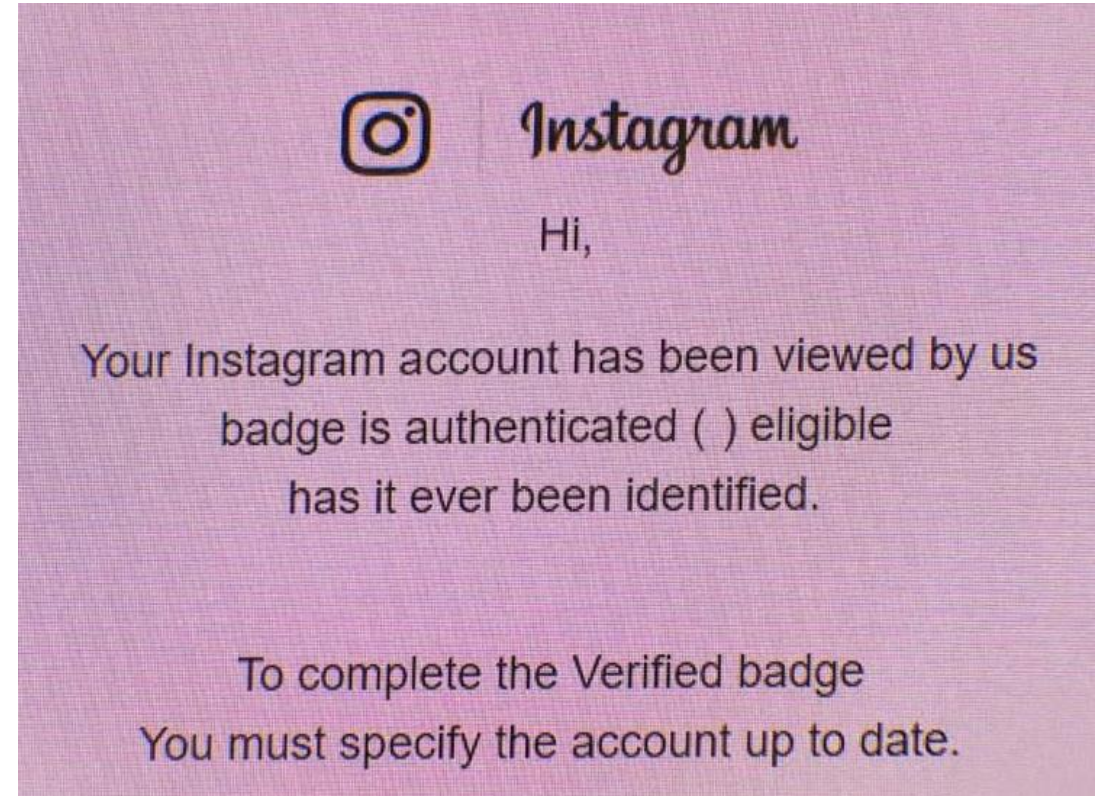
2018-7-3

資料來源

民視新聞

社群網站像是Facebook或是IG，都會特別標記公眾人物「藍色勾勾」，認證是本人帳號，但最近傳出有不肖駭客，假冒官方寄信，說要提供藍勾勾認證要求一些網紅或藝人提供帳號密碼，被害人不察因而上當，不但沒得到認證，整個帳號都被盜用，包括Youtuber蔡哥還有藝人四葉草都受害。

知名Youtuber蔡哥，開心向同事炫耀，自己收到社群軟體Instagram官方通知。聲稱可以獲得官方認證「藍勾勾」，開心的手舞足蹈，沒想到一切，原來是騙局一場。



印度 ATM 還在用 Windows XP，恐成駭客眼中的肥羊

新聞日期

2018-7-2

資料來源

科技新報

ATM 使用**不再有安全更新的 Windows XP 系統**，將成為駭客眼中的肥羊。2016 年轟動一時的第一銀行 ATM 盜領案，國際網路犯罪集團盜領金額高達約 8,300 萬元，這些歹徒能得手的其中一項原因就是 ATM 還在使用沒有安全更新的作業系統。微軟 (Microsoft) 在 2001 年發表 Windows XP，直到 2014 年停止支援，不再開發新的安全更新，但如今許多印度銀行 ATM 還在使用 Windows XP。

RBI 官員表示銀行處理系統老舊問題的進展相當緩慢，RBI 應該要嚴肅看待這件事。銀行直到 7 月底才會向 RBI 提出執行計畫，至少要在 8 月完成基本安全措施並在 9 月開始更新 ATM 系統，預計 2019 年 6 月完成。



勒索軟體再度來襲，手法與WannaCry相似！

新聞日期

2018-6-27

資料來源

KNOWING新聞

Action Fraud上週五稱，兩天前收到了300份詐騙郵件。這些郵件試圖欺騙讀者，使他們相信自己的電腦已被病毒感染，除非用比特幣支付罰金，否則檔將被刪除。實際上，這些郵件只是一個網路釣魚活動，主要使為了向不知情的受害者勒索錢財。Action Fraud在警告中稱：

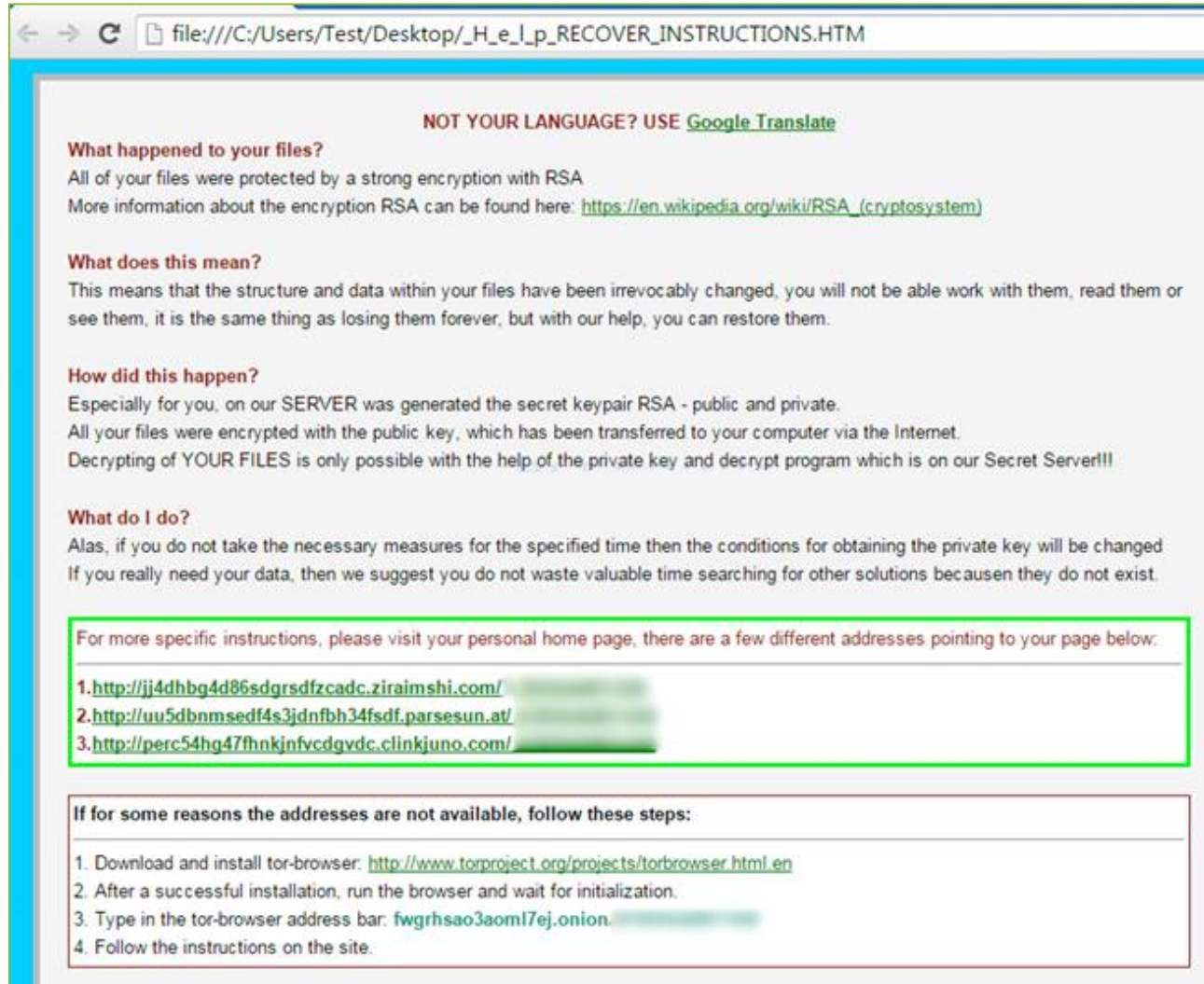
「Wanna Cry郵件的設計是為了引起恐慌，讓用戶相信自己的電腦已經感染了Anna Cry病毒。實際上，這些電子郵件只不過是一種網路釣魚活動，目的是勒索錢財。」

Action Fraud提供了幾個技巧，教用戶如何防止被Wanna Cry勒索病毒及其他病毒的攻擊：

「如果你收到這種類型的郵件，刪除它們，不要給騙子發電子郵件，也不要用比特幣付款。此外，你也應該經常更新電腦的防病毒軟體和定期操作系統，並遵循我們關於如何處理勒索病毒的建議。」



勒索軟體信件 (Tesla Crypt)



file:///C:/Users/Test/Desktop/_H_e_l_p_RECOVER_INSTRUCTIONS.HTM

NOT YOUR LANGUAGE? USE [Google Translate](#)

What happened to your files?
All of your files were protected by a strong encryption with RSA.
More information about the encryption RSA can be found here: [https://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our SERVER was generated the secret keypair RSA - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program which is on our Secret Server!!!

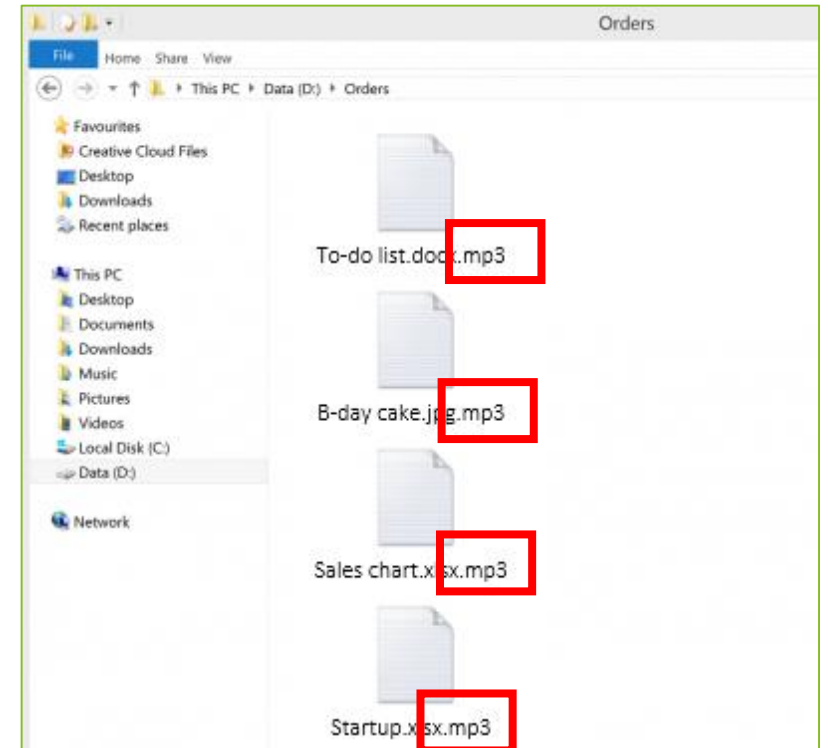
What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed. If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. <http://jj4dhbg4d86sdgrsdfzcadc.ziraimshi.com/>
2. <http://uu5dbnmsedf4s3jdnfbh34fsdf.parseun.at/>
3. <http://perc54hg47fhkjinfcgdgdc.clinkjuno.com/>

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the tor-browser address bar: fwgrhsao3aoml7ej.onion
4. Follow the instructions on the site.



檔案全部被加密成MP3格式!!

勒索軟體特徵

受害者的桌面出現「**你的個人檔案已被加密**」的勒索訊息，並寫道：這台PC上的相片、文件、影片等檔案是以專為本電腦產生的**RSA-2048bits**獨特公共金鑰加密

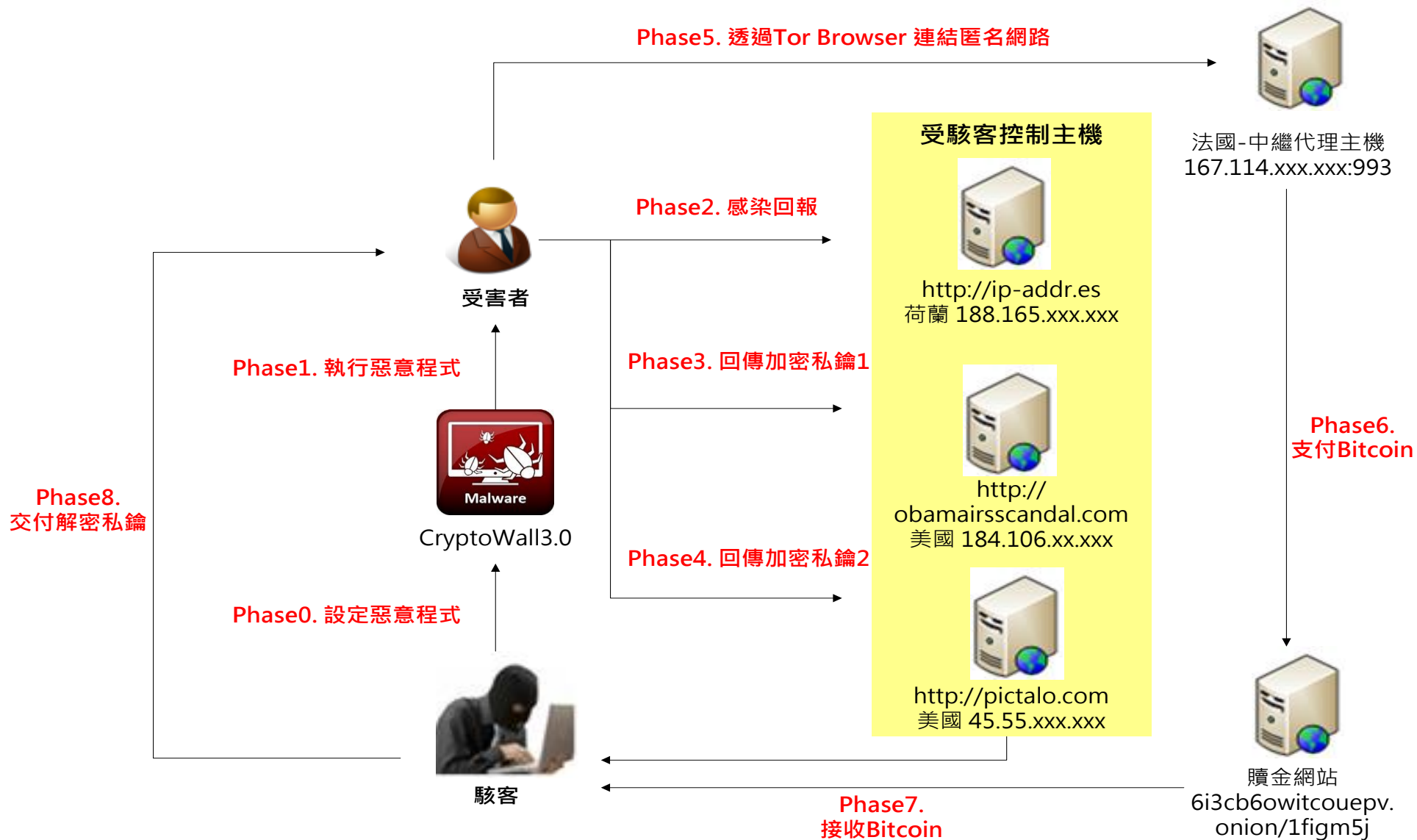
研究人員發現大多惡意軟體接受比特幣支付，支付過程則是透過位於**TOR**網域的網站來處理，因此**很難進行追查**。



常見勒索軟體
Coin Vault
Bitcryptor
Tesla Crypt
Linux.Encoder.1
Crypto Locker

- Tor用於防範網際網路上廣泛存在的流量過濾、嗅探分析。Tor在由「洋蔥路由」組成的表層網（overlay network）上進行通訊，可以實作匿名對外連線、匿名隱藏服務。

勒索軟體實際案例流程



緊急處理加密勒索軟體威脅

- 中斷網路連線
- 即刻發現，應立刻關機
- 緊急宣導、清查
- 評估災情
- 系統重灌
- 保持現場狀況，請求支援
- 付錢...



社交工程類型

A man in a dark blue suit, white shirt, and brown tie is holding a white rectangular sign. He is pointing with both index fingers towards the text on the sign. The background is plain white.

何謂社交工程?

社交工程

社交工程 (Social Engineering) 係利用**人性弱點**來進行詐騙，是一種非全面技術性的資訊安全攻擊方式，通常是利用大眾的疏於防範的小詭計，讓受害者掉入陷阱，藉由**人際關係的互動**，來突破資通安全防護，遂行其非法的存取、破壞行為。**該技巧通常以交談、欺騙、假連結、假冒或口語用字等方式**，以獲取帳號、通行碼、身分證號碼或其他機敏資料。



社交工程目的- 顯著的商業利益

一旦你的資料被竊取，
就等於是開放給所有的網路詐騙集團...

指定入侵帳號價格:

- Facebook: 100 美金
- Gmail : 100 美金

信用卡重製: 25 美金

垃圾簡訊發送: 3到150美元

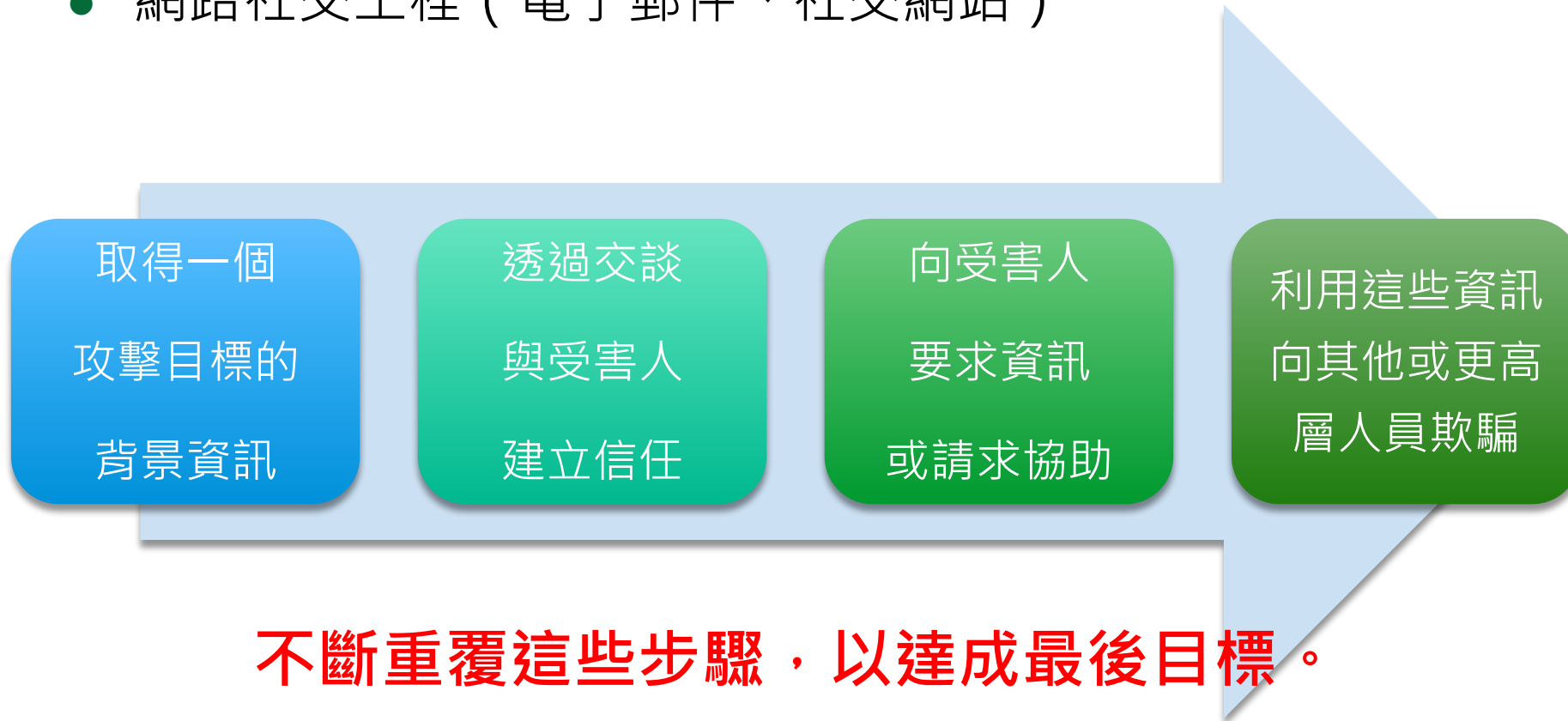
偽造釣魚網站: 5-20美元

網路釣魚用網域: 50 美金



社交工程手法

- 傳統社交工程（電話詐騙）
- 網路社交工程（電子郵件、社交網站）

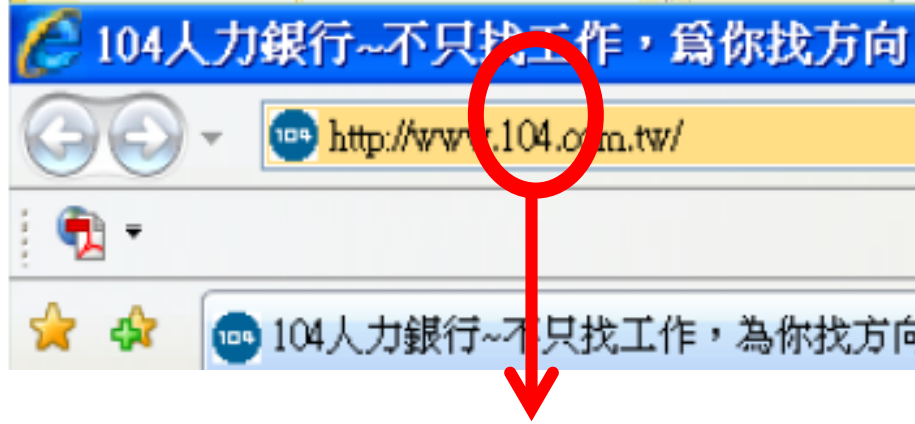
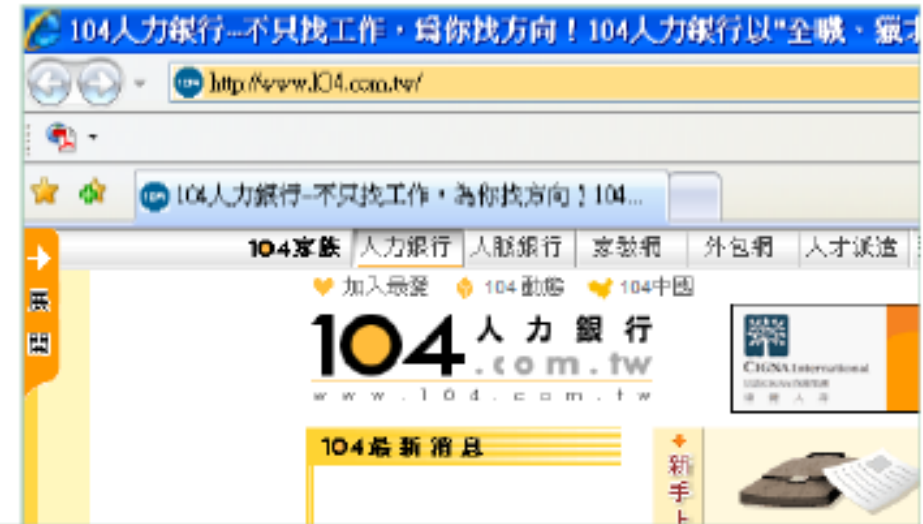
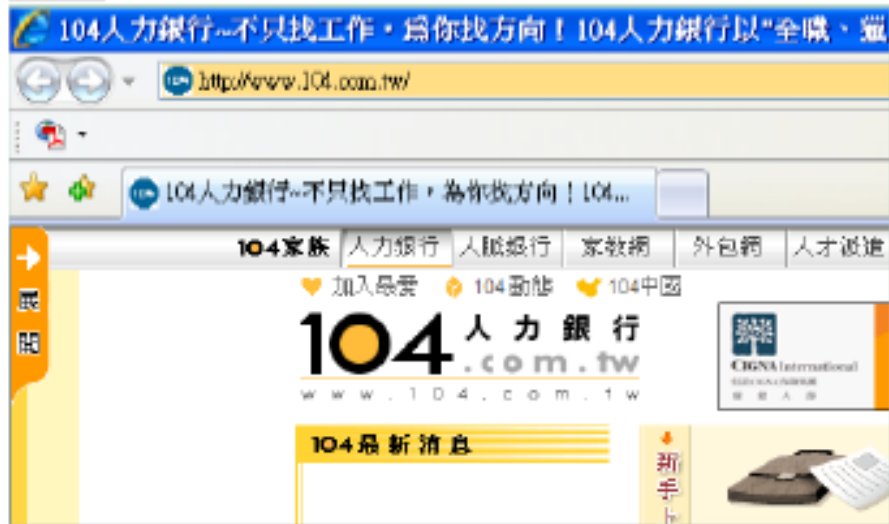


社交工程手法：人

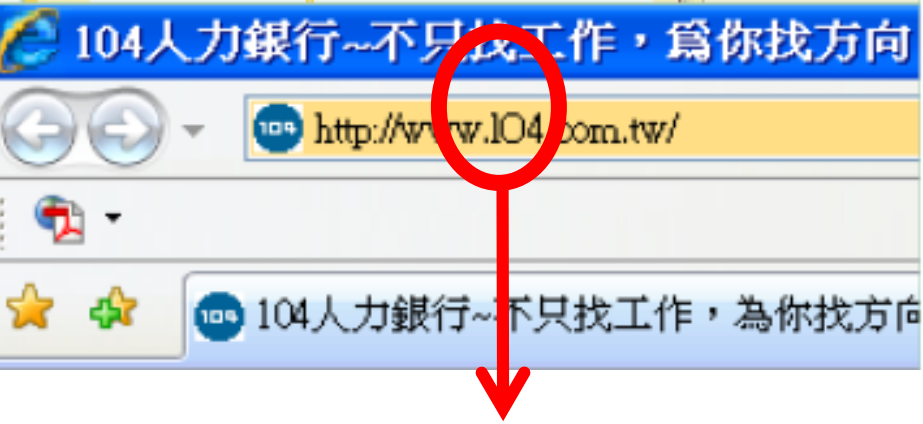
- 偽裝內部員工
- 偽裝重要人士
- 偽裝第三方組織
- 偽裝技術支援
- 直接攻擊
 - 偷窺強記(Shoulder Surfing)
 - 垃圾翻找(Dumpster Diving)
 - 尾隨(Piggybacking)



社交工程手法1：假官網網址(1/3)



阿拉伯數字 0



大寫英文字母 O

社交工程手法1：假官網網址(2/3)

兩岸駭客設假網站釣密碼 數十萬筆個

入口網站 - Windows Internet Explorer
http://www.landbank.com.tw/

入口網站 - Windows Internet Explorer
http://www.landbank.com.tw/

入口網站 - Windows Internet Explorer
http://www.landbank.com.tw/

入口網站 - Windows Internet Explorer
http://www.landbank.com.tw/

以及電腦科技公司等，至少有50個知名網站遭到仿冒。

小寫英文字母 **l** ;

阿拉伯數字 **1**

社交工程手法1：假官網網址(3/3)

The image shows two browser windows side-by-side. The left window displays the legitimate Yahoo! Auctions website (http://tw.bid.yahoo.com/), with the URL highlighted in a red box. The right window displays a phishing website (http://tw.bids-yahoo.com/login.htm?e=ed&f=s&v=kjv/h/and&v=jv), with the URL also highlighted in a red box. The phishing site mimics the legitimate one but has a misspelled URL. A login form on the phishing site is highlighted with a red box, showing fields for '帳號' (username) and '密碼' (password), and a '登入' (login) button. A '啟用安全' (enable security) button is also visible.

正確網址： <http://tw.bid.yahoo.com/>
詐騙網址： <http://tw.bids-yahoo.com/>

社交工程手法2：關鍵字廣告

- 關鍵字廣告-中國南方航空公司網頁
- 關鍵字廣告- LINE的網頁鬧雙胞

南方航空
找到约 10,700,000 条结果 (用时 0 15 秒)

中国南方航空公司官方网站 | csair-1w.tk
www.csair-1w.tk
南方特价机票预订, 票改签/改期, 退票办理, 南航客服热线: 400-814-5432.

中国南方航空-官方网站 | czyu6.xxuz.com
www.czyu6.xxuz.com
南方航空航班预订, 2-7折特价, 轻松预定, 国内/国际7*24小时服务: 400-602-9336

中国国航-官方网站 | airchina.com.cn
www.airchina.com.cn
航空, 提前订票2.5折, 手机平台购票, 送500公里, 更赠充值话费

600029 - 南方航空 (上海证券交易所) - 添加到 iGoogle
谷歌财经 新浪财经 搜狐证券 网易财经 和讯 东方财富 证券之星 金融界

7.80 -0.03 (-0.38%) 9月1日 上午11:30 北京时间

开盘: 7.80 成交量: 5,533,979
最高: 7.89 平均成交量: 无
最低: 7.78 资本总市值: 765.77亿

LINE

相關詞: [line 電腦版下載](#), [line 官方網](#), [line 主題](#), [line 點閱區](#) 免費2013, 更多...

LINE 相關廣告

免費傳訊的應用程式「LINE」 | line.me
LINE 是一款全新型態的通訊應用程式, 讓您隨時隨地傳訊、免費通話等!
假

line.me/zh-hant

顯示網址同

免費通話、免費傳訊的應用程式「LINE」
LINE 是一款全新型態的通訊應用程式, 讓您隨時隨地傳訊、免費通話等!
... 動態消息 供您利用文字、照片、影片、貼圖與好友分享您的近況, 或是轉發新消息。 標記
真

line.me/zh-hant 庫存頁面 · 更多此站結果

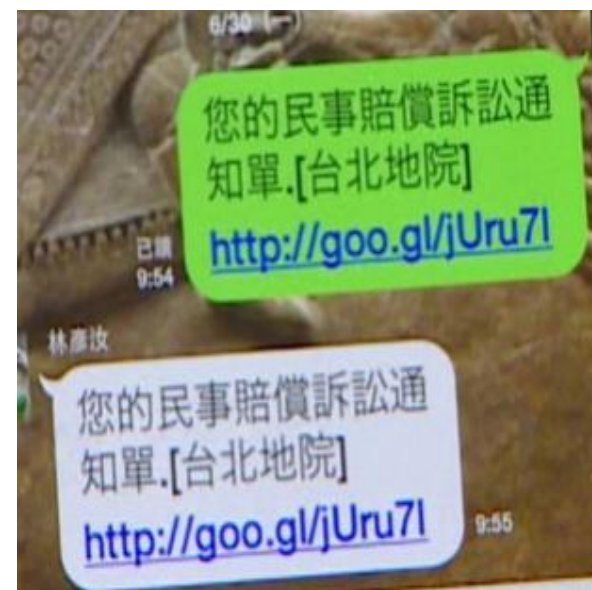
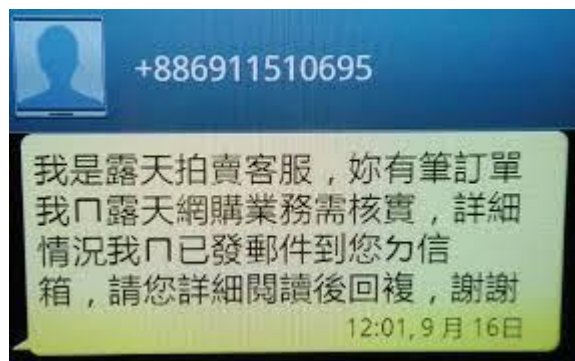
LINE | Facebook
LINE. 104,144 likes · 915 talking about this. 各種App情報介紹, 分享, 討論! 行生! (LINE App的官方粉絲團在<https://www.facebook.com/taiwan.line>, 不是這邊囉 www.facebook.com/pages/LINE/312206095465041 庫存頁面 · 更多此站結

社交工程手法3：網路活動廣告

- 駭客藉由世界盃足球賽，建立以假亂真的精美網站詐騙。
 - » 例如使用Cielo (巴西信用卡服務龍頭) 來偽裝巴西VISA信用卡服務的代表頁面、萬事達卡、巴西電視節目主持人的照片等。



社交工程手法4：詐騙簡訊(1/3)



社交工程手法4：詐騙簡訊(2/3)

* 常見詐騙簡訊一覽表：

1. 「fb 免費送貼圖,把此消息轉發十五個 LIE 好友,可免費領取價值一百的貼圖” 」
2. 「○○○被偷拍的是你嗎?」
3. 「○○○女士您有交通罰單逾期未繳...」
4. 「尊敬的客戶您好，您的手機正在申請6800元的網絡支付，如非本人操作請加載電子憑證確認取消...」
5. 「0809.....，用手機打給我一下，新辦的,幫忙測試一下」
6. 「○○○女士,您的電信本月應繳費賬單,查詢電子帳單...」
7. 「您的快遞簽收通知單，收件電子憑證」
8. 「○○○這是上次聚會的照片，你好好笑」
9. 「○○○先生,你的露天商品已經送達門市...」
10. 「○○○這是你那晚沒來的照片，我被整慘了...」
11. 「○○○我在墾丁拍的照片，你覺得哪張最好看。」
12. 「○○○這是上次同學聚會的照片，大家都有來」
13. 「○○○朋友家狗狗參加人氣比拼，幫忙讚一下」



社交工程手法4：詐騙簡訊(3/3)

- 詐騙簡訊利用對象整理：
 - » 假冒親友
 - » 假冒警察局
 - » 假冒法院
 - » 假冒電信商
 - » 假冒Facebook
 - » 假冒宅配業者
 - » 假冒台電
 - » 假冒各類帳單付費
 - » ...etc.



簡訊詐騙近日已達高峰，
2018年五月份台灣就出現60筆詐騙簡訊
內含的惡意網址，
共騙取了889,514萬次的點擊數，
平均每天就有2萬8千多次詐騙成功。

社交工程攻擊與因應

社交工程手法-電子郵件

電子郵件社交工程(一)

電子郵件社交工程是目前駭客最常使用的攻擊手法，動輒對企業造成嚴重損失，包括：

企業內資訊設備遭入侵 / 挾持 / 控制

營運機密外洩

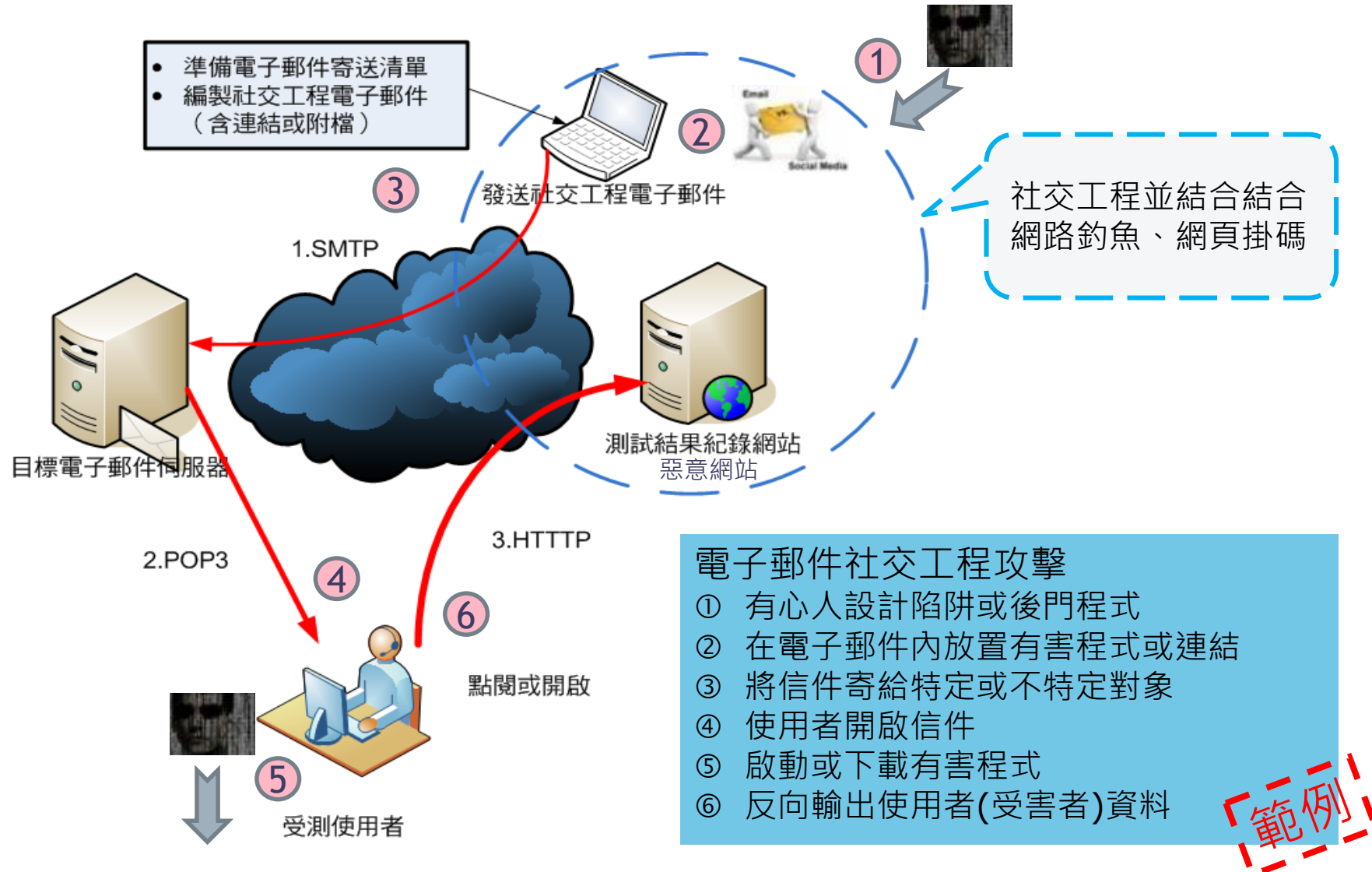
客戶個人資料遭竊取

商譽損失

電子郵件社交工程攻擊手法可繞過一些既有的防禦縱深機制，
必須靠**使用者加強電子郵件使用之警覺及良好習慣**方能預防



電子郵件社交工程(二)



電子郵件社交工程型攻擊的風險



電子郵件社交工程型攻擊的目的在於誘騙收信者提供個人資料(如：帳號、密碼)，或引誘收信者透過下載方式來執行以圖片、連結、夾檔所偽裝的惡意軟體(malware)，成為入侵者所控制的殭屍網路電腦(botnet)。

由於這類的攻擊，如：下載圖片、點選連結，實際惡意軟體的資料是由使用者電腦直接向提供者下載取得，並不會經過郵件伺服器的防毒機制，即使過濾夾檔也有零日病毒(zero-day virus)的問題，在郵件伺服器端僅能過濾已知的病毒，加上現今的電子郵件瀏覽器為了方便，都開啟「自動下載圖片功能」，如果沒有做好管控，駭客即可輕易攻進企業內部，因此是駭客最常使用的攻擊方式。若未做好適當的預防、控管，對企業會產生極大的風險。

收到郵件後，必須注意

- 郵件主旨是否與本身業務相關
- 審慎開啟郵件內含連結
- 審慎開啟郵件內含附件

可疑的電子郵件特徵

- 過於聳動的主旨與緊急要求，以引誘收信人開啟信件及回覆
- 不正常的發信時間
- 來路不明之電子郵件或少往來對象之來信
- 認識的人（同事或朋友）來信但主旨或內容與其習性不符
- 要求輸入私密資料送出
- 連結金融機構網址更改基本資料
- 假冒寄件者
- 垃圾郵件
- 含有惡意程式的附件
- 利用零時差攻擊

過於聳動的主旨

使用收信者有興趣的生活、政治、工作、情色等相關議題的主旨

電子郵件社交工程攻擊常見信件主旨

郵件	郵件種類	郵件標題	寄件者
1	網路新知	太神奇！日本發明可觸摸3D影像	影像世界<viewer@capital.com.tw>
2	金融財經	美內政陷角力 影響基金投資	理財快訊<Timer@capital.com.tw>
3	新奇新聞	什麼？ iPhone 7 外型及功能曝光	新奇新聞<apple@yah00.com.tw>
4	公務宣導	助妳好孕 - 打造友善生養城市	Sandy<sandy68418@hotmail.com>
5	廣告	部落格放廣告 做公益也貼補家用	部落客<Blogger@bloggerads.net>
6	新奇新聞	iPhone6S 0元手機帶回家	TAIWAN PHONE<iphone@gmail.com>
7	新奇新聞	子彈穿腦 男「哈啾」噴出	水果快訊<appnewa@apple.com >
8	旅遊休閒	今年來去東京過聖誕節 !!!	YOKOSO<japan@yokosojp.com>
9	旅遊休閒	旅展優惠爆乎你知	長榮假期<fun@evaair.com>
10	公務宣導	Fw: 試算你家的二代健保費	Tina<Tina10608@hotmail.com>

緊急要求 - 過於急迫而顯得真實

威脅若不立刻進行更新，則可能危及你的帳戶

- 日前刑事局網站發布消息指出收到高雄從事保全業的鍾姓男子，看到有一則 Facebook Notification傳來的訊息通知，內容如下：

「警告BLOCKING FACEBOOK，即時確認！Facebook要求用戶確認各自的帳戶作為證據的真實性。這是因為很多人用假身分和假的個人資料圖片，在他們的帳戶。違反使用條款的，可能在一個臨時帳戶永久關閉。請確認您的帳戶，在下面的地址：http://face-book-bookmark-protection.hol.es/checkpoints_next.html為保障您的帳戶**立即在24小時內**確認您的facebook帳戶。如果您不確認，**系統將自動永久關閉您的帳戶**。感謝您的幫助，以改善我們的服務。」

- 鍾先生一開始不以為意，但對方一直不斷傳訊息過來，而且鍾先生也有用臉書玩遊戲，一旦帳號被封鎖，所有的點數都會消失，於是就點選訊息內提供的連結，再依照指示輸入自己的帳號密碼。

假冒寄件人

你分的出來以下兩個寄件人信箱的差別嗎？

test1@mail.com → 數字“1”

testl@mail.com → 小寫“L”

偽造連結 / 惡意附件

將木馬程式或病毒通常藏在一般檔案內，並使用各種生動有趣的字眼，誘使您點選連結或執行該檔案。惡意程式常被種植在以下檔案中：

- 含有執行檔(exe)
- 含有惡意程式的影音檔(wmv)
- 含有惡意程式的Office文件(doc)
- 含有惡意程式的圖檔(jpg)
- 含有惡意程式的壓縮檔(zip, rar)



社交工程攻擊與因應

如何防範社交工程攻擊？

餌再怎麼做，它還是一個餌...

社交工程雖然利用人性弱點來騙取機敏資料，讓人覺得防不勝防，但如果能隨時提高警覺，未經確認不隨意提供資料、不開啟來路不明的電子郵件及附加檔案、不連結及登入未經確認的網站、不下載非法軟體及檔案，就能避免社交工程的攻擊傷害。



如何識別釣魚信件？(1/4)



寄件者: **旅遊局 <eDM@travel.gov.tw>** 寄件人看似(存在之)知名公司或機構 寄件日期: 2015/4/1 (週三) 下午 12:02
收件者: Chen, Tony W. (TW - Taipei)
副本:
主旨: **國家旅遊局E-DM** 信件主題具誘惑、吸引人想開啟(符合時事)
📎 訊息 **必看Agoda快速搶便宜教學!.docx (171 KB)** 信件附檔具有與主題、內容相關之引誘標題

<2015 春假國內旅遊 你計劃好了嗎?春假國內旅遊訂房搶先預訂 保證最低價!>

春假想要好好放鬆一下，帶著家人度過一個美好的假期，每到春假 各旅遊景點飯店旅館一房難求 國內旅遊，這個月起很多飯店旅館都已開始預約訂房了，如果您有計劃國內旅遊!一定要提早訂房喔!國內旅遊，春假期間熱門旅遊景點的房價不僅比平時高，甚至是你有錢都訂不到啊!

現在我要推薦你一個很棒的訂房系統→ [Agoda](#) (附件內有 Agoda 網站訂房操作教學)

信件本文內容含連結，促使人想點選

如何識別釣魚信件？(2/4)



寄件者: 美食達人 <fattyfood1@mail.esas.tw> 寄件日期: 2015/9/2 (週三) 下午 05:08

收件者: Chang, Marcus M. (TW - Taipei) 寄件人看似(存在之)知名公司或機構

副本:

主旨: [休閒]秘!!「奶油刀牛肉」鮮嫩多汁到讓人驚艷 信件主題具誘惑、吸引人想開啟

訊息 [W]不可不知的牛排經典部位剖析!.docx (99 KB) 信件附檔具有與主題、內容相關之引誘標題

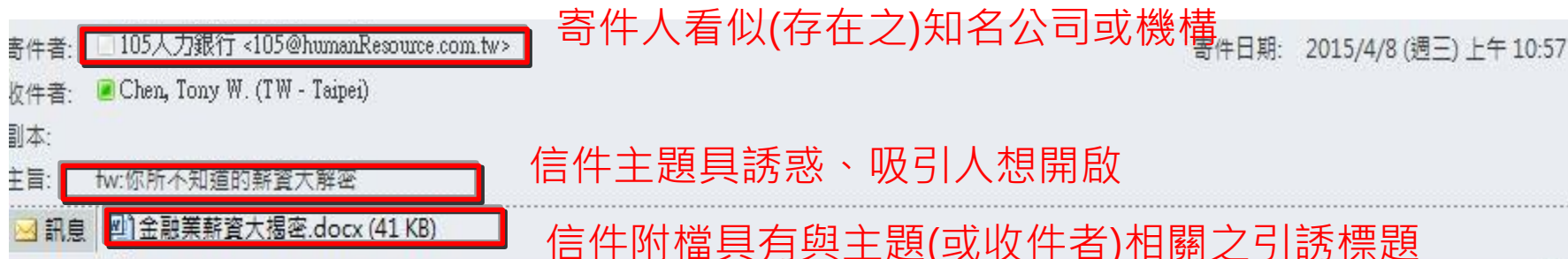
秘傳!!「奶油刀牛肉」鮮嫩多汁到讓人驚艷!!

景氣差的情況下，平日已經夠省吃儉用了！工作之餘，還是要慰勞自己一下。像很多餐廳紛紛推出優質卻平價的「牛排」，其實都可以去嚐嚐！特別的是，用塗麵包的「奶油刀」就可以切下的優質和牛，其肉質的細嫩多汁，又怎能錯過？

自從飯店業者推出「極黑牛-奶油刀饗宴」晚間套餐之後，這一款以奢華頂級的 16oz 美國冷藏和牛肋眼，充分滿足了「老饕們」的心。於是餐廳就把這一款頂級和牛留在單點菜單裡，讓沒吃到的人還可品嚐到「鮮嫩多汁」的肉香。

↓圖：用塗麵包的「奶油刀」就可以切下的優質和牛肋眼。

如何識別釣魚信件？(3/4)



<推動全民加薪潮 基本工資明年看漲>

信件本文內容含連結，促使人想點選

快報：逾七成企業 今年會加薪，快來看看有沒有我們！

勞動部長陳雄文指出，今年基本工資有調漲空間，調幅由第三季舉行的基本工資審議委員會決定；去年政府決定從今年7月起調漲基本工資至20008元，若今年基本工資審議委員會又調高基本工資，明年基本工資可望再往上墊高。

如何識別釣魚信件？(4/4)



FW: [SPAM] Webmail Update Dept — Inbox

Delete Junk Reply Reply All Forward Print To Do

From: Webmail Update <fixwebm@stargatesg1.com> **From a strange address**
Subject: FW: [SPAM] Webmail Update Dept **自可疑的email地址發送**
Date: May 25, 2010 3:27:38 PM EDT
To: Liberty Student <imachampion@liberty.edu>

Attention, **Not addressed to you specifically** 一般的問候語 (未有特定之收件人)

This message is from the Webmail Fix Web messaging center to all webmail account owners. We are currently carrying out an upgrade on our system, hence it has come to our notice that one of our subscribers infected our Network with a worm like virus and it is affecting Our database. **Poor grammar/spelling** 文法、拼字錯誤或語意不清

We are also having congestions due to the anonymous registration of accounts, so we are shutting down some accounts, and your account was among those to be that needs to be updated due to this condition. **Dire warning for not complying** 試圖創造一種緊迫感

To resolve this problem all subscribers must reply to this email immediately, and enter your User Name here (*****) And Password Here (*****) to have them Cleared against this virus. **Asking for personal information in reply** 要求回覆重要個人資料

Failure to comply will lead to the termination of your Email Account.

Hoping to serve you better.
Webmail Support Update Dept.

<http://www.suntrustcards.com/portal/index.php> **Strange URL** 連結到未知或拼字錯誤的網站

SCAM

如何預防電子郵件社交工程攻擊？(1/2)

- 注意郵件主旨與寄件者是否與本身業務相關，**不開啟來路不明的電子郵件**
- 注意內含其他網站連結之郵件，**不連結及登入未經確認的網站**
- 注意內含附件之郵件，**不開啟或下載非法軟體或與業務無關之檔案**
- 對不明或未經確認來源之八卦、休閒...等**與業務無關之分享郵件**，應特別留意其連結與附檔安全性
- 注意內含確認或提供資料要求(如：確認訂單、重設密碼...等)之郵件，**不隨意提供資料(如：帳密、個資...等)予未經確認之來源**
- 若懷疑郵件或訊息來源，應先**通報及確認**

如何預防社交工程攻擊？(2/2)

開啟以下檔案時，必須特別注意：

*.jpg, *.wmv (圖檔、影音檔)

*.exe (執行檔)

*.scr (螢幕保護程式)

*.doc, *.xls, *.ppt (Office檔案)

*.bat (批次檔)

*.vba (巨集)

*.zip, *.rar (壓縮檔)



收到訊息/郵件應有的警覺性觀念：

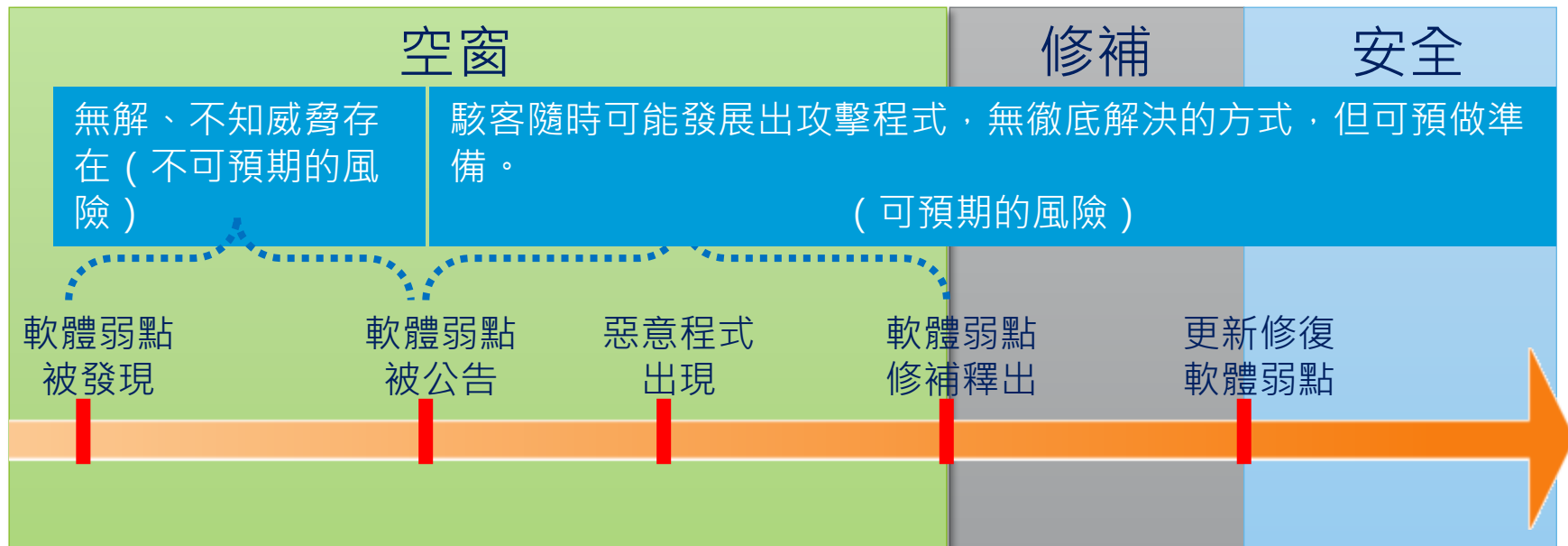
- 我為何會收到這封郵件？
- 我是不是應該收到這封郵件？
- 我是不是有必要開啟附件或點選連結？

資訊安全宣導

防毒軟體不是100%的保障！

只要是軟體即有**可能存在弱點**，若未能及時修補弱點，即可能讓駭客入侵成功。

軟體弱點在沒有任何修補方式前，出現相對應的攻擊行為，此類攻擊稱為「零時差攻擊」(Zero-day Attack)。



注意可疑人士

- 若遇不明人士在辦公區域內走動，應主動詢問其來意。
- 發現可疑狀況應加以制止或通知相關人員處理。
- 即使是認識之同仁，進出其沒有權限出入之區域，也要加以勸阻或通知相關人員處理。



桌面與螢幕淨空

- 因處理業務保有敏感性、機密性電腦資料或檔案者，應加強安全保護措施，如下班時應該**上鎖**或以其他方法妥為收存。
- 不再使用之機密文書資料，應使用碎紙設備或其他**無法還原原始資料之銷毀**方式進行銷毀。
- 個人電腦與終端機應設定一定時限內自行啟動密碼**螢幕保護程式**或自行登出。
- 人員離開座位前，應**登出個人電腦或鎖定螢幕**。



傳輸注意事項

- 電子郵件僅供業務作業使用，禁止發送私人廣告郵件、垃圾郵件、騷擾郵件或使用郵件炸彈等，並嚴禁任何利用電子郵件進行違法行為。

以電子郵件傳送機密資料時，應進行**加密**並以**不同封信件**或其他方式告知密碼。

勿開啟或轉寄來歷不明的電子郵件附加檔案。

- 非必要且經授權，不得將機密文件攜出。
- 機密文件以人工傳遞需妥善保護（如：專人親送、密封）
- 使用傳真前需確認電話號碼正確性。
- 傳真後應確認對方是否收到。
- 傳真、影印、列印之文件應立即取走。



可攜式電腦設備管理

- 設備使用應採用一定的保護措施，如身分識別與鑑別機制，以避免這些設備所儲存和處理的資訊遭到非法存取或外洩，並留意設備遺失及遭竊之風險。
- 內含機密等級資訊的可攜式電腦設備應避免無人看管，並考量使用專用電腦鎖來保障設備的安全。
- 未經權責主管核可，不得將機密等級資料儲存於可攜式電腦設備。



惡意軟體防範

- 防毒軟體的偵測與防範功能只有在該軟體有**在運作**、且有**時常更新病毒碼**情形下，才會產生效用。
- 防範訣竅：
- **安裝防毒軟體或反間諜軟體。**
- **不關閉、不刪除防毒軟體。**
- **隨時注意防毒軟體的病毒碼是在最新的狀態。**
- **定期執行掃毒。**
- **不要隨意複製或下載不明檔案。**
- **不要隨意開啟檔案。**



