致和證券
Concord International Securities Co., Ltd.

致和證券

資安教育訓練

致和證券
Concord International Securities Co., Ltd.

課程大綱

1. 何謂社交工程
2. 社交工程的攻擊手法
3. 如何預防社交工程攻擊
4. 資訊安全政策宣導

致和證券
Concord International Securities Co., Ltd.

什麼是社交工程(一)

- 社交工程(Social Engineering)是指一種操弄人類心理，採取特定行動來蒐集機密資訊的特定技巧。

- 利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取帳號、 通行碼、身分證號碼或其他機敏資料，來突破組織的資通安全防護，遂行其非法的存取、破壞行為。

致和證券
Concord International Securities Co., Ltd.

什麼是社交工程(二)

- 所謂「社交工程」，就是詐騙！

早在資訊還沒發達前，就有所謂的社交工程，最常見的例子就是：詐騙電話。透過電話偽裝身分誘騙您上勾受騙。

—「你兒子現在在我手裡，現在馬上匯20萬過來不然就砍斷他的手。」(背景聲：媽～救我～) 咔，電話掛斷.

以上就是一個典型詐騙手法。社交工程是利用人與人之間的關係，偽裝成受害人信任的對象，如：家人、同事、長官等等。透過人性的弱點進行詐騙，而當受害人認知不足、警覺不夠時，就很容易上當受騙。

致和證券
Concord International Securities Co., Ltd.

社交工程方式

- 在資訊崛起的現今，社交工程的手法也越來越多樣化，常見的攻擊手法包含電子郵件、簡訊、釣魚網站、LINE、FACEBOOK等。

  利用具誘惑性的文字，引導受害者輸入機密資料或點擊有問題的連結，例如：「限時大特價，iphone11只要 9487元。」、「帳號異常登入，請更新會員資料」等字眼，當受害人若未仔細思考判斷，即可能直接點擊惡意網址，並輸入個人資料或下載木馬程式等。

  另外，釣魚網站的部分，攻擊者利用人性的認知不足，透過仿造的網頁，並且以極為相似的網址來混淆受害者。例如：「www.GO0GLE.COM.tw」與「www.GOOGLE.COM.tw」，若不仔細觀察，很難發現網址中英文字母「O」與數字「0」的差異。而通常為了達到攻擊成效，偽冒的網站會與實際的網站十分相似，若沒注意網址的細節，往往都會掉入攻擊者所設下的陷阱。

致和證券
Concord International Securities Co., Ltd.

1 何謂社交工程

2 社交工程的攻擊手法

3 如何預防社交工程攻擊

4 資訊安全政策宣導

致和證券
Concord International Securities Co., Ltd.

社交工程攻擊手法─人

- 偷聽(Eaves dropping)
- 偷看(Shoulder Surfing)
- 偷翻(Dumpster Diving)
- 尾隨(Tailgating)
- 搭順風車(Piggybacking)
- 假冒身份(Impersonation)
  - 裝可憐
  - 裝大牌
  - 裝技術支援裝內部員工

致和證券
Concord International Securities Co., Ltd.

社交工程攻擊手法—電腦

- 廣告郵件/垃圾郵件
- 病毒、木馬（郵件/通訊軟體附檔）
- 偽造郵件
- 釣魚網站
- LINE
- FACEBOOK

致和證券
Concord International Securities Co., Ltd.

存在生活中的社交工程案例

請開啟連結，填寫個人資料

您的信用卡被盜刷

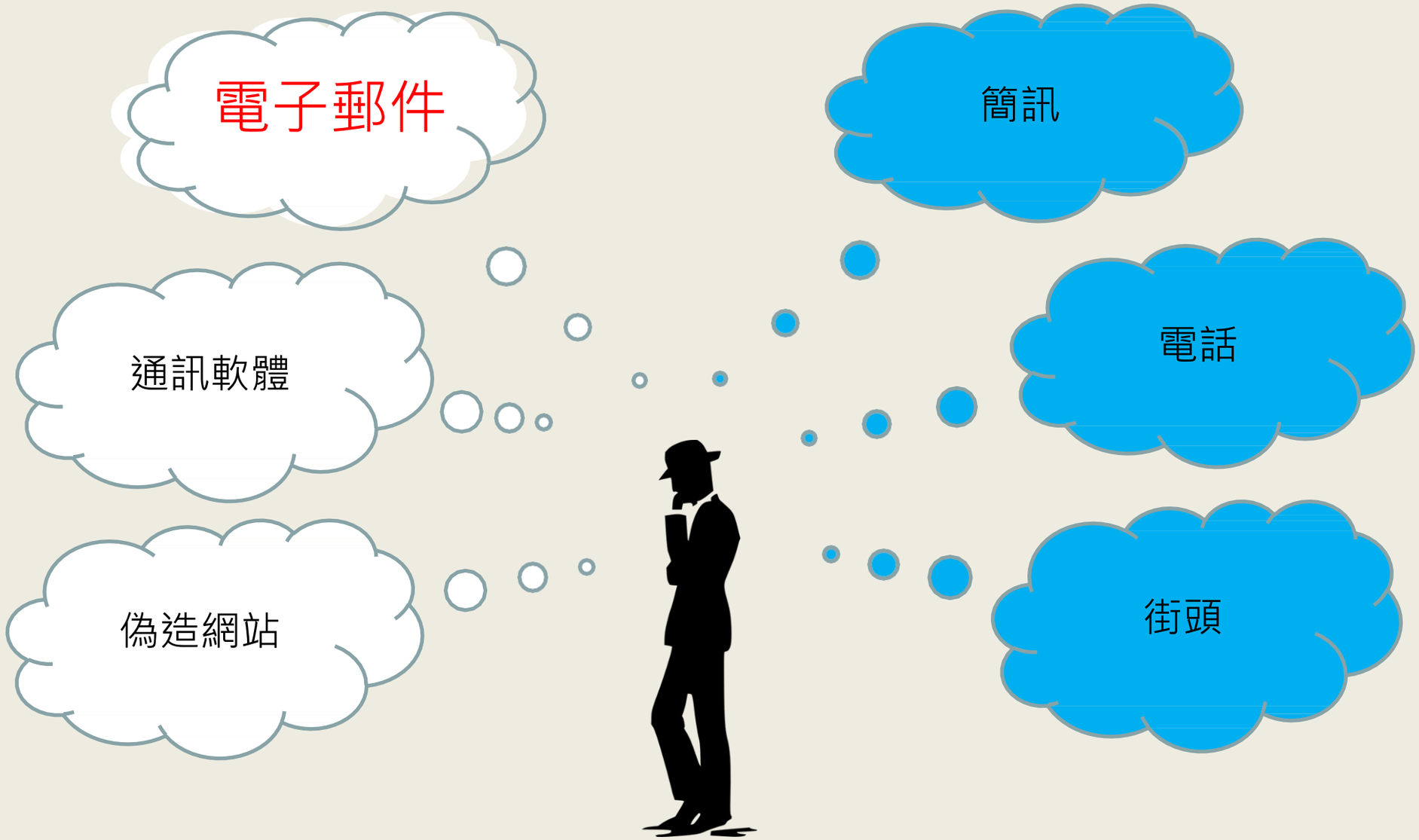
網路購物訂單失敗

你的孩子現在在我手上...，匯贖金

好康到相報

致和證券
Concord International Securities Co., Ltd.

生活中常用的社交工程媒介



致和證券
Concord International Securities Co., Ltd.

1 何謂社交工程

2 社交工程的攻擊手法

3 電子郵件社交工程預防及演練

4 資訊安全政策宣導

致和證券
Concord International Securities Co., Ltd.

電子郵件社交工程手法

取得目標
電子郵件位址

寄發欺騙偽造
電子郵件

誘使目標開啟
信件、圖片、
附件或**URL**

駭客達成目的:
攻擊、詐騙、
廣告、錢

駭客利用各種管道 蒐集目標的電子郵件:

- 網路蒐集
- 系統入侵

- 假冒寄件者
- 使用與業務相關的郵件
- 令人感興趣的郵 件

- 含有惡意程式的附件、連結或圖片
- 利用應用程式之弱點 (包括零時差攻擊)

- 攻擊:主機控制權、 竊取資料
- 詐騙:信用卡資料、 各種帳號密碼
- 廣告:惡意廣告、網頁綁架
- 錢：勒索病毒



致和證券
Concord International Securities Co., Ltd.

疏忽了會有什麼影響?

電子郵件社交工程手法

勒索病毒

機密檔案及文件
遭竊

使用者行為
遭監控

個人相關帳號
密碼遭竊

成為
、殭屍電腦

使用者個人資料遭竊

致和證券
Concord International Securities Co., Ltd.

辨識電子郵件社交工程的方法與技巧

不明信件內附件

- 含有執行檔**(**或是壓縮檔中有執行檔**)**，切勿點擊 執行。
  - 通常是惡意軟體（病毒、木馬或勒索軟體）。
  - exe , com , bat , rar , zip ……
- 駭客利用各種方式讓使用者誤以為不是執行檔
  - **.jar**
  - **.js**
  - **.pif** 等，
- 長檔名
  - **"order_detail.docx.exe"**。

致和證券
Concord International Securities Co., Ltd.

電子郵件社交工程的特徵

- 聳動的電子郵件主旨
- 陌生人或是不熟的朋友突然來信
- 緊急要求或要求提供個人機敏資料
- 好康報給你知道

致和證券
Concord International Securities Co., Ltd.

電子郵件社交工程

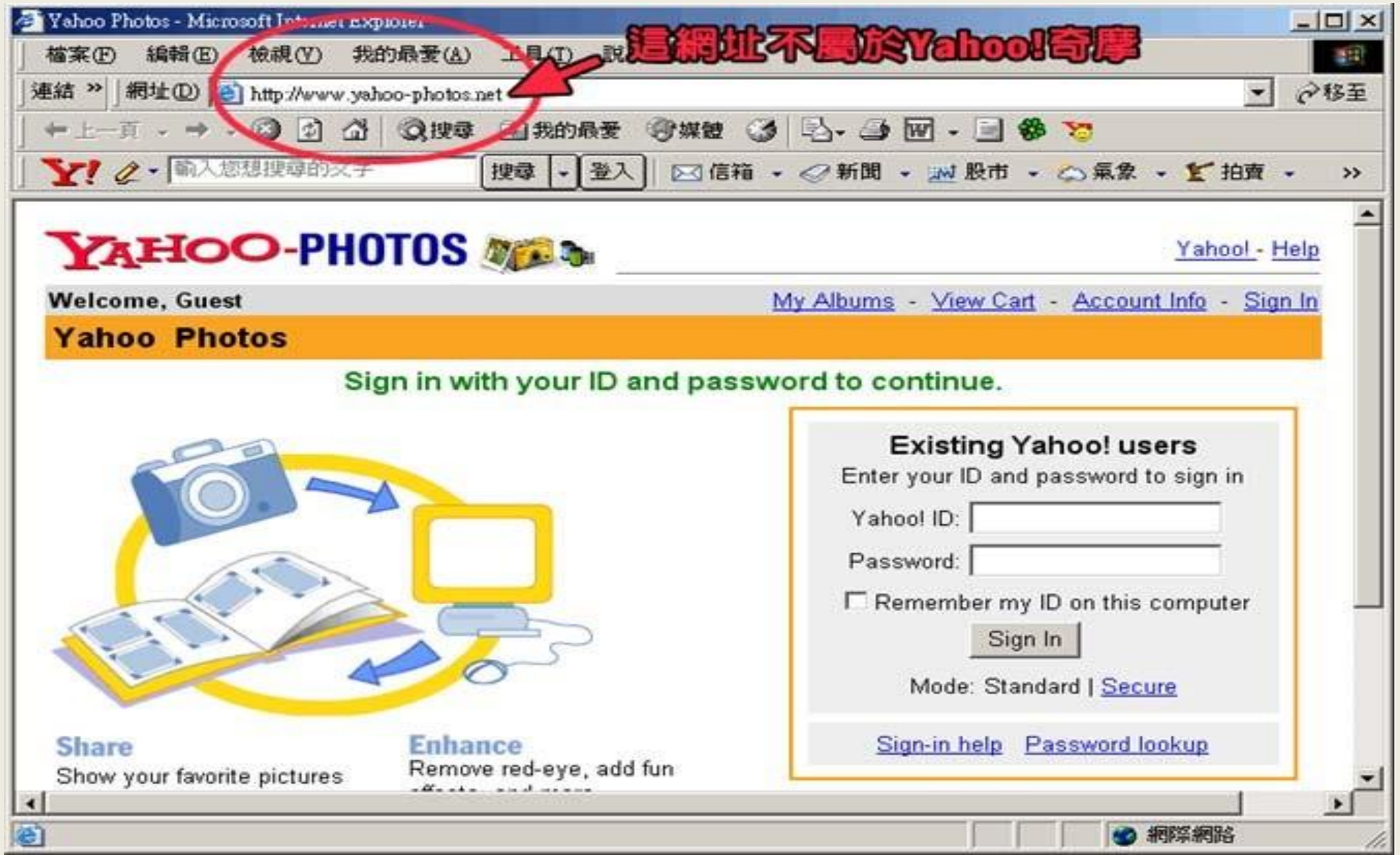
使用的郵件主旨為「政治、公務、健康養生、休閒娛樂、情色」等類型，並在電子郵件內容中夾帶惡意網址連結、圖片或惡意附加檔案，誘使收件者去點擊瀏覽，其目的在於當收件者去開啟或點擊郵件內的相關連結或檔案時，即有可能被植入木馬程式竊取相關電腦資料，或被駭客放置的惡意連結網址，連線至假造的「銀行網站」、「個人信箱網站」等，而造成個人使用的相關帳號密碼遭竊取，除造成個人存放在電腦內的機密資料有外洩的可能外，也有可能造成單位或個人金錢上的損失。

致和證券
Concord International Securities Co., Ltd.

大家來找碴-找找看哪裡不一樣

致和證券
Concord International Securities Co., Ltd.

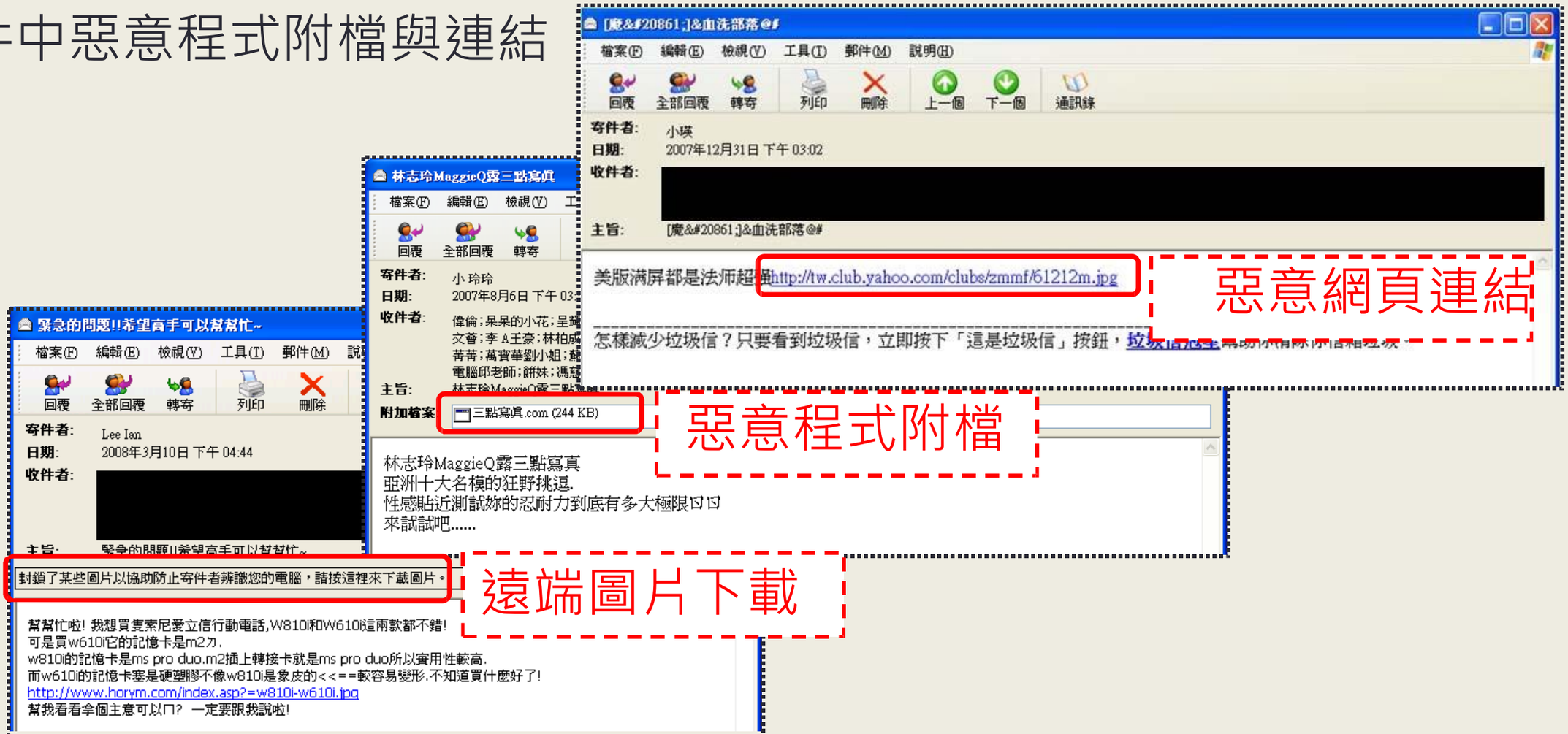
魚目混珠



致和證券
Concord International Securities Co., Ltd.

社交工程電子郵件的陷阱

- 郵件中的遠端圖片下載（與ActiveX）
- 郵件中惡意程式附檔與連結



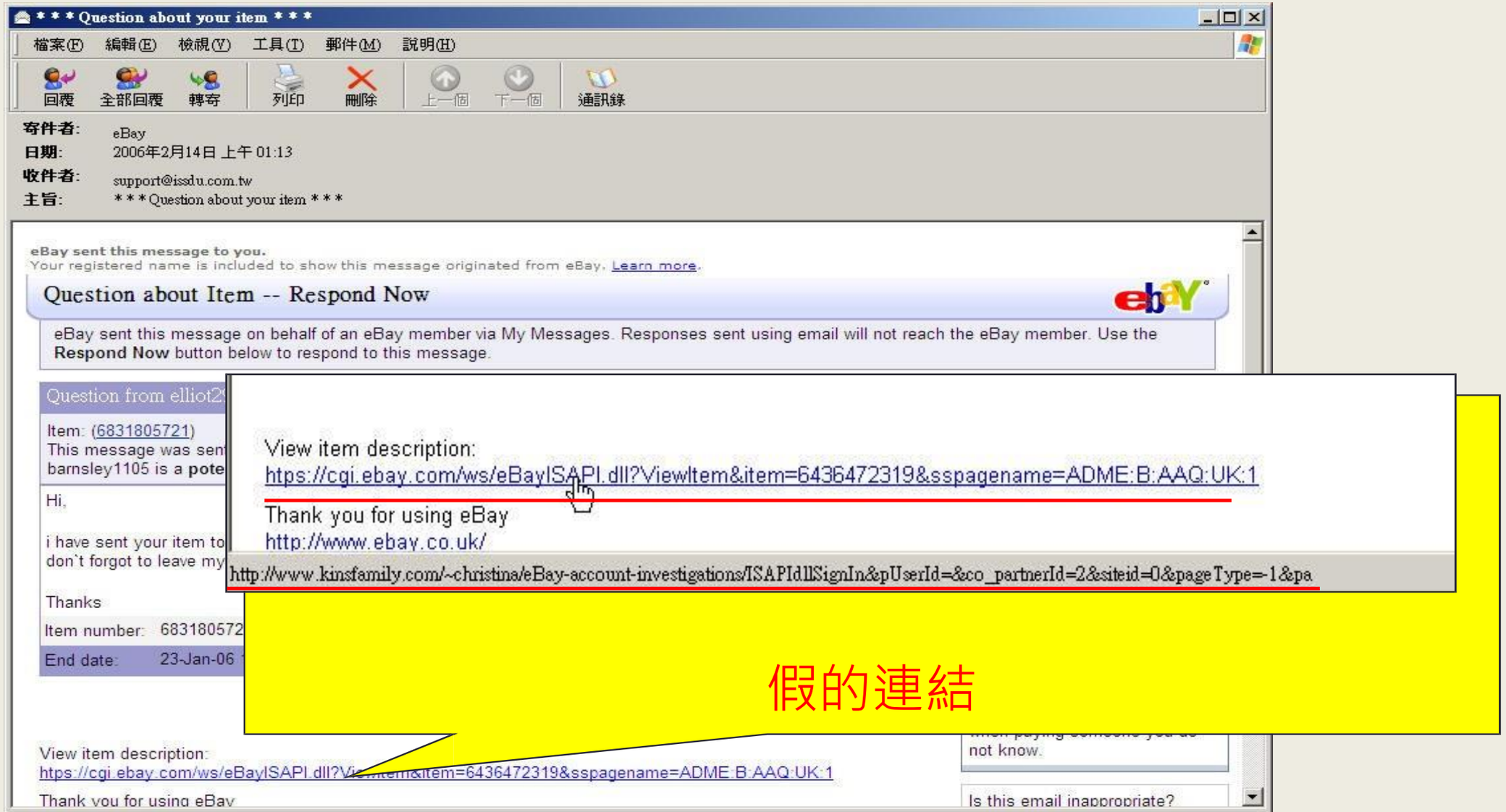
致和證券
Concord International Securities Co., Ltd.

釣魚郵件

- 利用誘人的內容欺騙使用者點擊到偽造網站。使用者輸入機密資料後，即遭竊。
- 技術門檻低。
- 利用使用者的粗心。
- 申請與原本網站類似的網址。
- 大部分使用者不會很注意上方網址。

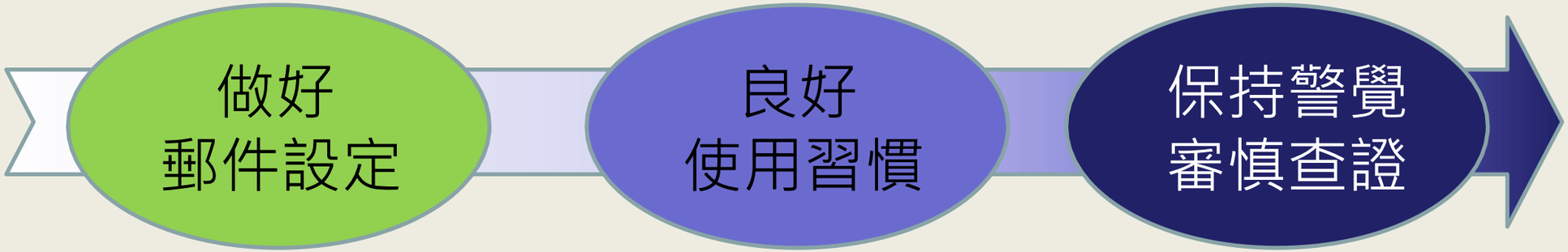
致和證券
Concord International Securities Co., Ltd.

典型的釣魚信



致和證券
Concord International Securities Co., Ltd.

判斷電子郵件安全從自己做起



- 關閉自動下載圖片
- 關閉預覽視窗
- 設定純文字格式讀取郵件
- 不要自動回覆讀信回條

- 不開啟來路不明的電子郵件
- 不轉寄不可信任來源之郵件
(以避免擴大受害者)

- 為何我會收到這封郵件
- 我是否應該收到這封郵件
- 我是否應該開啟這封郵件

致和證券
Concord International Securities Co., Ltd.

自我防護

- 技術面
  - 修補系統漏洞
  - 安裝防毒軟體
  - 安裝間諜程式檢查軟體
  - 關閉信件預覽
- 行為面
  - 開啟信件前請三思
  - 開啟連結時請三思
  - 開啟附件檔案時請三思

致和證券
Concord International Securities Co., Ltd.

使用電子郵件時應有的習慣

- 收信
  - 檢查寄件者、收件者的真偽 (例如：.gov、.org)
  - 確認信件主旨、內容的真實度
  - 不輕易開啟郵件的超連結及附件
  - 開啟超連結或附件前，確認對應軟體 (例如：IE、Office、 防毒軟體) 都保持在最新修補的狀態
- 轉信或寄信
  - 未經查證之訊息不要轉寄
  - 轉寄郵件前先將他人郵件地址刪除，避免別人郵件地址 洩漏
  - 寄送信件給群體收件者時，應將收件者列在密件副件， 以免收件人資訊外洩。

致和證券
Concord International Securities Co., Ltd.

開啟來路不明電子郵件的後果

- 中惡意程式
- 影響資訊安全
- 個資恐外洩
- 檔案被加密
- 大量發送垃圾信件
- 金錢損失

致和證券
Concord International Securities Co., Ltd.

1 何謂社交工程

2 社交工程的攻擊手法

3 如何預防社交工程攻擊

4 資訊安全政策宣導

致和證券
Concord International Securities Co., Ltd.

電腦使用要注意

電腦要設定螢幕保護程式

應用程式不用時請關閉

長時間離開辦公室，請將電腦登出或關機

- 杜絕來自網路破壞
- 防止帳號或密碼被盜用
- 防止重要資料遭竊

辦公室電腦不得任意加裝與工作無關之軟體

致和證券
Concord International Securities Co., Ltd.

應用系統要更新

駭客經常透過漏洞來入侵電腦

作業系統或應用程式設計上的問題

更新軟體的修補程式

- *Windows update*
- *Office update*
- *Acrobat Reader*
- *其他*

致和證券
Concord International Securities Co., Ltd.

防毒軟體要安裝

安裝防毒軟體

更新病毒碼

定時掃毒

隨時注意病毒最新資訊

- 資訊安全通報
- 防毒軟體廠商
- 報章雜誌

不要安裝未經驗證安全的軟體

致和證券
Concord International Securities Co., Ltd.

瀏覽網頁要提防

點選連結網站要確認網址以免受騙

選擇加密網頁登入

社群網站隱私要設定

不要隨意複製或下載不明檔案

網頁瀏覽器建議Chrome或Firefox

致和證券
Concord International Securities Co., Ltd.

安全使用網路

確保您的網頁瀏覽器可以安全使用

- 設定網頁瀏覽器的安全和隱私。
- 設定可信任網站。

遠離網路釣魚犯罪陷阱與詐騙

- 不回應不明公司或技術部門的個人要求隱私或安全資訊。
- 不要點擊來自未知電子郵件的網路連結。
- 不要使用公司網路轉送垃圾郵件。

致和證券
Concord International Securities Co., Ltd.

電子郵件使用要小心

切勿使用非公務信箱收發公務郵件
切勿轉寄公務郵件至非公務信箱
切勿使用公務電子郵件進行外部網站註冊，或以其為帳號

致和證券
Concord International Securities Co., Ltd.

密碼設定要穩固

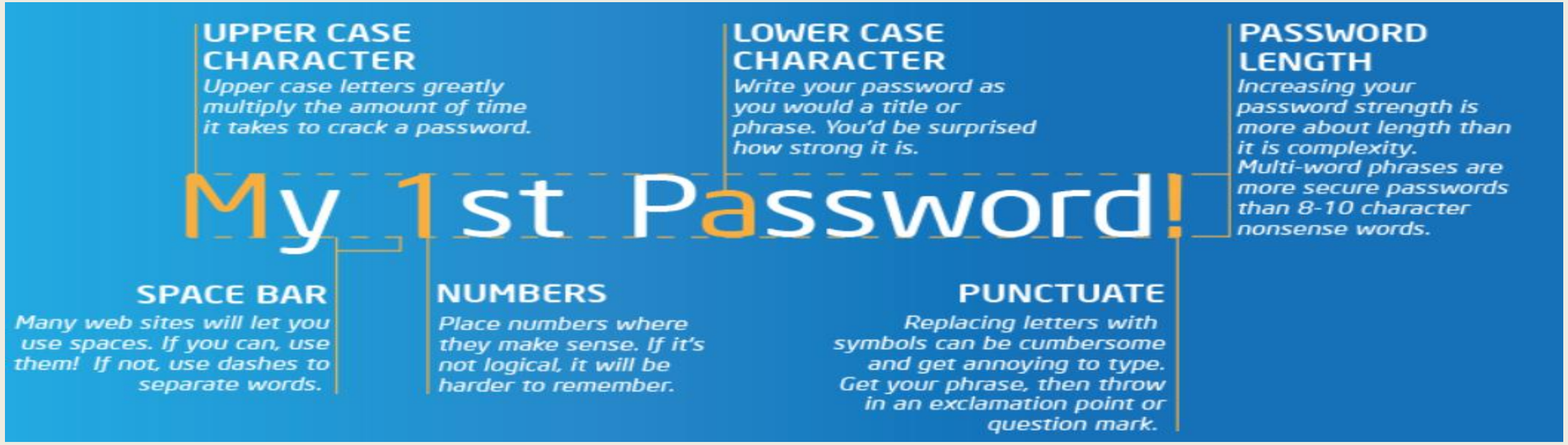
密碼是主要弱點

為節省時間或方便，共用密碼或選擇簡單的密碼

密碼不夠複雜，很容易被別人猜到

定期更改密碼，減少被竊取的危險

不得將密碼張貼於明顯處



致和證券
Concord International Securities Co., Ltd.

密碼設定範例

技巧1

你好嗎(新注音輸入)

Su# cl# a8&

技巧2

abcd + 1234 => a1b2c3d4

技巧3

Birthday往前位移1個字母

Ahqsgczx

技巧4

In God we trust, else we investigate !

IGwt,ewi!

Raindrop keeps following on my head.

Rkfomh

致和證券
Concord International Securities Co., Ltd.

重要資料要備份

備份的重要性

- 預防重要資料或設備損壞遺失
- 確保可用性

三二一原則

- 資料至少要備份3代
- 存放在2種以上的儲存裝置
- 其中1份必須保存在異地

致和證券
Concord International Securities Co., Ltd.

USB使用要謹慎

可移除式媒體優點

- 體積小，攜帶方便
- 儲存容量大
- 便宜

可移除式媒體資安威脅

- 遺失
- 洩密
- 傳播病毒

致和證券
Concord International Securities Co., Ltd.

行動裝置注意事項

不要瀏覽可疑的網站及下載來路不明的檔案

不要從未認證過之App Store下載應用程式

仔細查看任何要安裝的應用程式，確認是否合法以及要求哪些權限

採用最新韌體版本

使用手機防毒軟體

致和證券
Concord International Securities Co., Ltd.

五招判斷行動裝置存在資安威脅徵兆

電池壽命變短

通話經常不尋常中斷

電信費用異常

自動下載軟體

手機效能變差

致和證券
Concord International Securities Co., Ltd.

機敏資料要保護

紙本

機密及敏感文件不可遺留於桌面上，必須存放於抽屜或檔案櫃並加以上鎖

作廢敏感文件不得回收再利用

電子資料

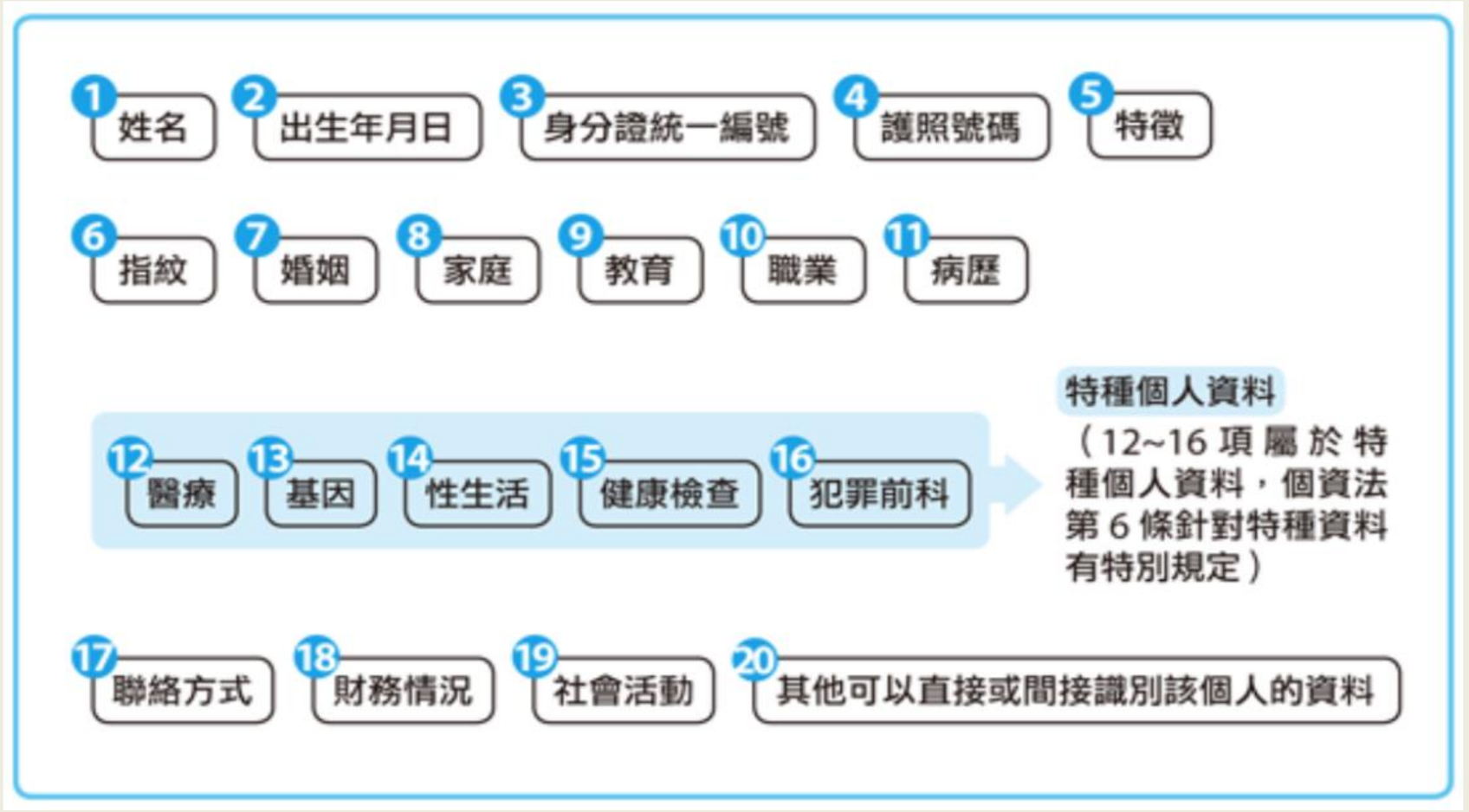
重要或敏感檔案要分開存放

設定密碼或以加密軟體保護

建議避免共用資料夾

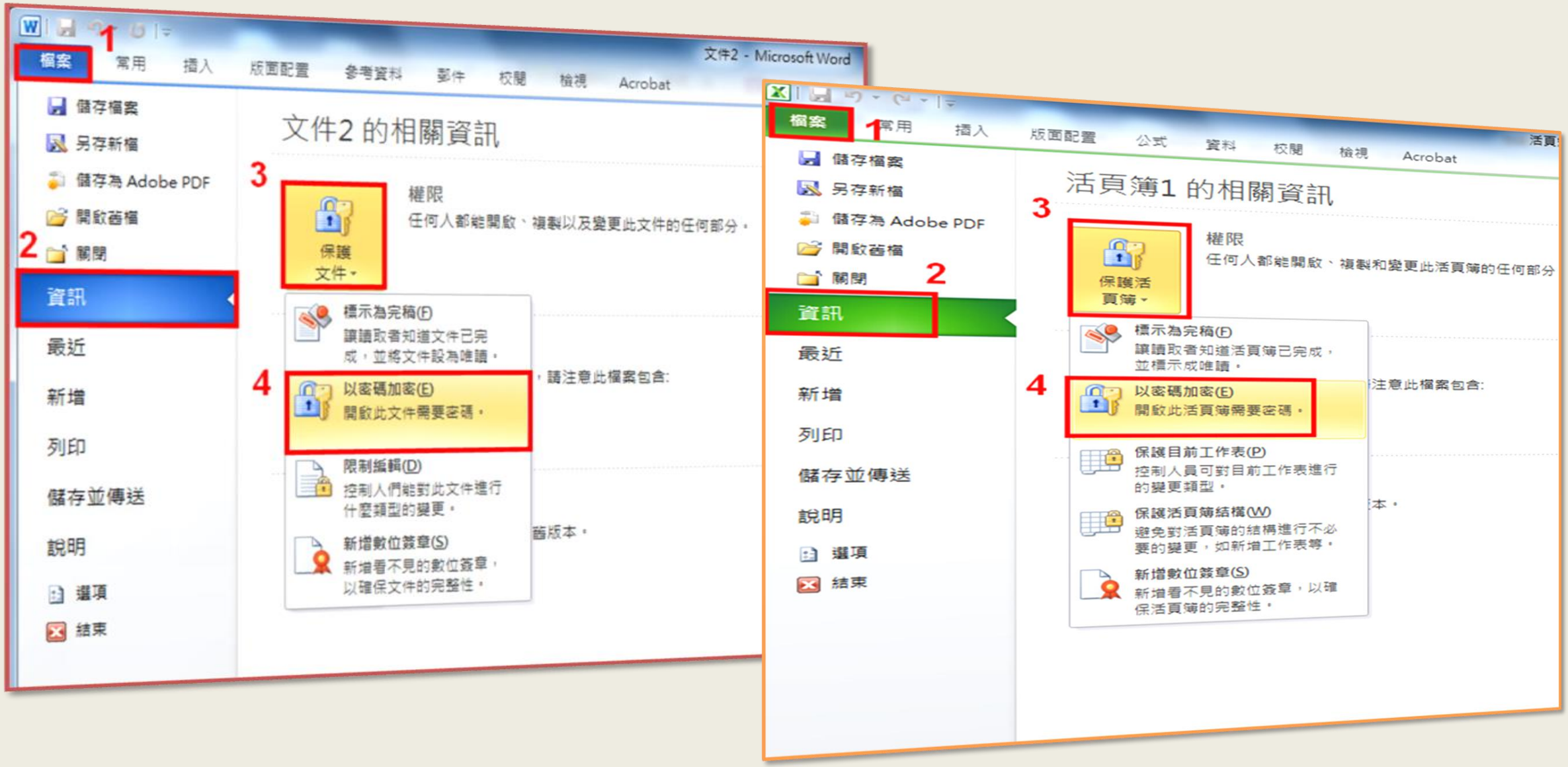
致和證券
Concord International Securities Co., Ltd.

個人資料



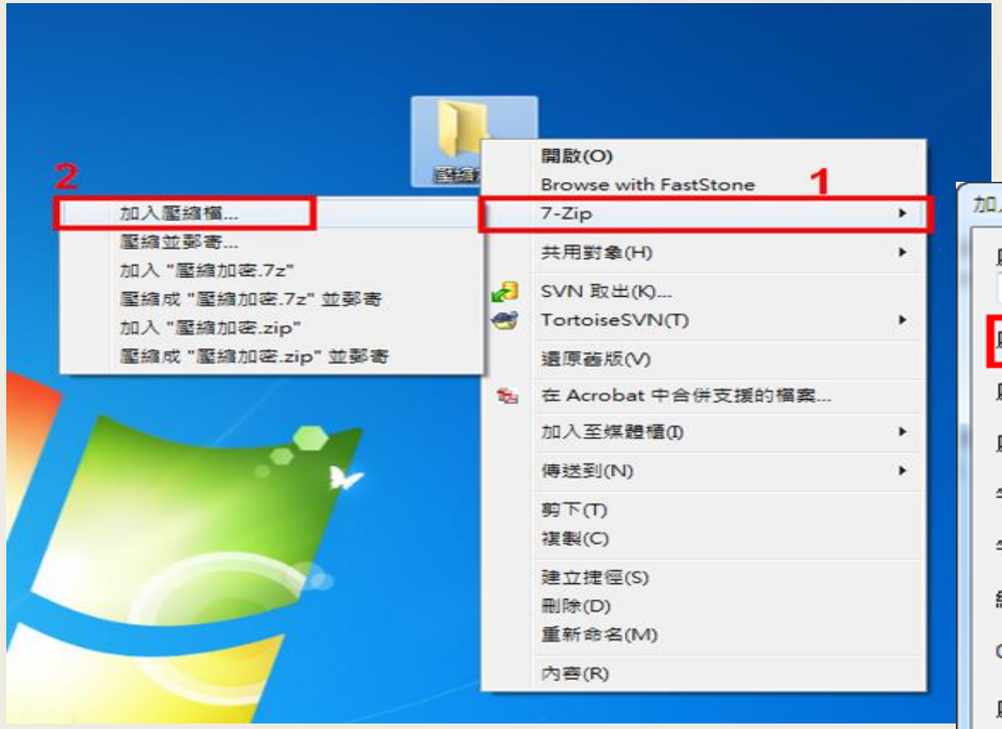
致和證券
Concord International Securities Co., Ltd.

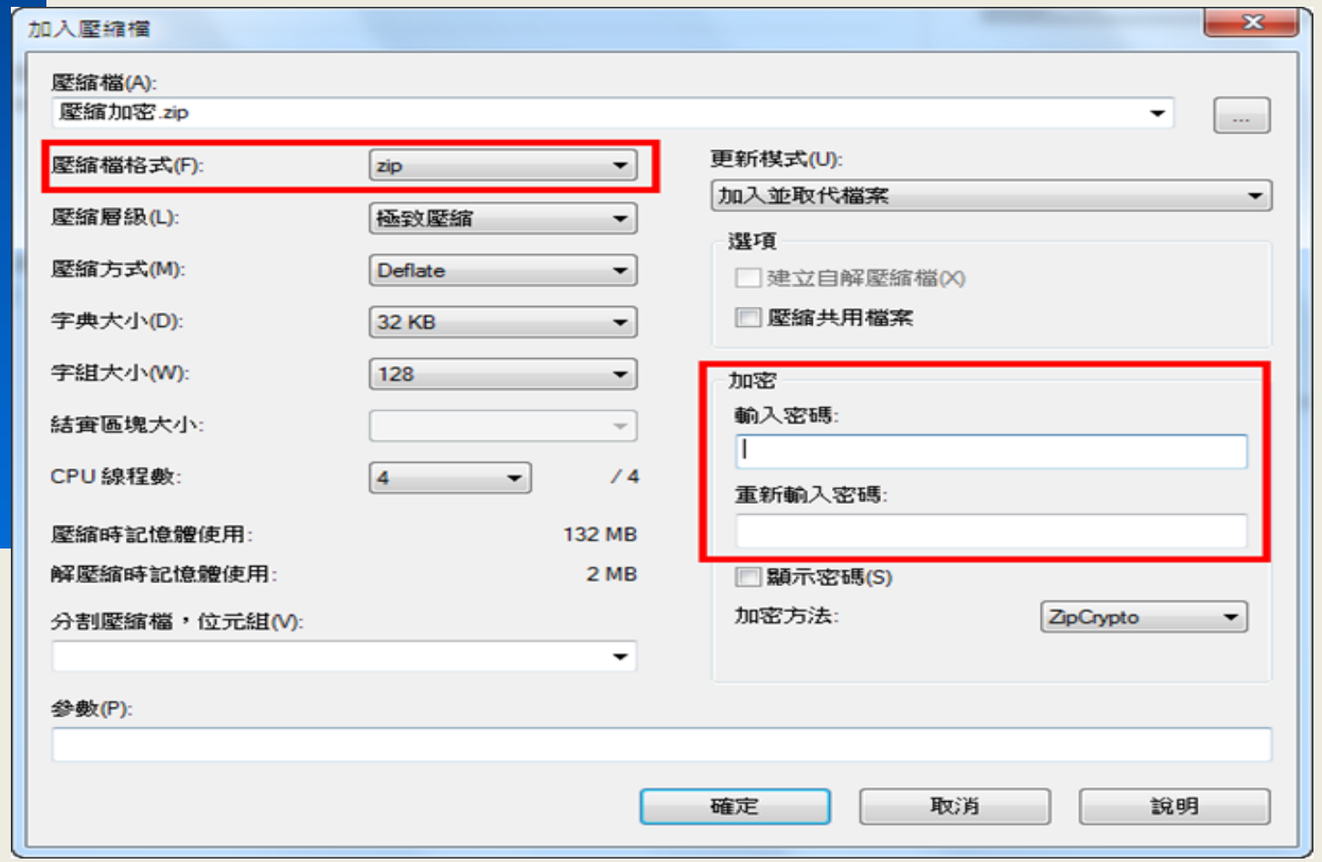
Office加密



致和證券
Concord International Securities Co., Ltd.

壓縮加密





致和證券
Concord International Securities Co., Ltd.

物聯網 & 網際網路

物聯網 – 非建立起人與人的網路，而是物與物的網路

致和證券
Concord International Securities Co., Ltd.

何物連上物聯網

只要「物」夠大，可裝網路傳輸器，且又有自己專用的可識別位址

- 家用電子設備
- 家電
- 汽車
- 醫療設備
- 各種飛行器
- 從家到國家任何可以監控的東西

致和證券
Concord International Securities Co., Ltd.

智慧化設備

- 透過連上物聯網的設備，通稱智慧化設備 (如智慧電視、智慧電冰箱等)
- 其實設備本身不需要智慧化，但籍由與其 他連線設備的互相合作，產生智慧化的應 用。

致和證券
Concord International Securities Co., Ltd.

隱私問題

- 物聯網最大的問題，可能是隱私。
- 這麼多感應器與智慧設備，會收集關於你 的大量訊息。
- 大量的監視攝影機及智慧手機裡頭的全球 定位系統(GPS)晶片 ，追蹤你的行動。

致和證券
Concord International Securities Co., Ltd.

隱私及資安問題

物聯網連接的設備經常監視和跟蹤消費者 的行為，以此來調整和改善消費者體驗； 然而用戶可能根本沒有被告知哪些數據將 會被收集，又如何被使用。

裝置上所蒐集的資料誰可以擁有，不同組 織或商業團體間互相交換這些資料是否合 法等議題，目前皆未有明確法令的規範。

致和證券
Concord International Securities Co., Ltd.

物聯網安全攻擊威脅

- 竊聽任何透過網路傳送的未加密資訊 監聽攻擊
- 攻擊來封鎖或阻慢對某些網路或設備的使用 阻斷服務攻擊
- 加密通訊的金鑰被竊或入侵網路或連到特定網路的設備 金鑰淪陷攻擊與基於密碼的攻擊
- 第三者會竊走雙方或設備間傳輸的資料

致和證券
Concord International Securities Co., Ltd.

結語

防護技術是反應攻擊的保護機制

新型態攻擊發生時，「人」是安全防範關鍵

使用者的資安認知教育為防範的基礎

時時刻刻保有警覺心

致和證券
Concord International Securities Co., Ltd.

深度偽造

指使用電腦合成或其他科技方法製作或散布涉及真實人物實際未發生的行為舉止影像紀錄、動態圖像、錄音、電子圖像、照片及任何言語或行為等技術表現形式。

致和證券
Concord International Securities Co., Ltd.

深度偽造最常見方式

深度偽造最常見方式是AI換臉技術，此外還包括語音模擬、人臉合成、視頻生成等。它的出現使得篡改或生成高度逼真且難以甄別的音視頻內容成為可能，觀察者最終無法通過肉眼明辨真偽

致和證券
Concord International Securities Co., Ltd.

深度偽造防範建議一

■使用影像視訊方式進行身分驗證時應使用一次性密碼(OTP)、專人電訪或查驗本人並核對證件照片等方式強化驗證。

■使用影像視訊時應確認真實視訊環境（如隨機問答），以防止透過科技預先錄製影片。

致和證券
Concord International Securities Co., Ltd.

深度偽造防範建議二

■多重驗證，確認身份，比如在涉及錢款時，儘量通過電話詢問具體信息，確認對方是否為本人

■保護信息，避免誘惑。對於不明平台發來的廣告、中獎、交友等鏈接提高警惕，不隨意填寫個人信息，以免被騙子“精準圍獵”

■相互提示，共同預防做好宣傳防範工作。尤其是提醒老年人在接到電話、短信時，要放下電話，再次撥打家人電話確認，不要貿然轉賬