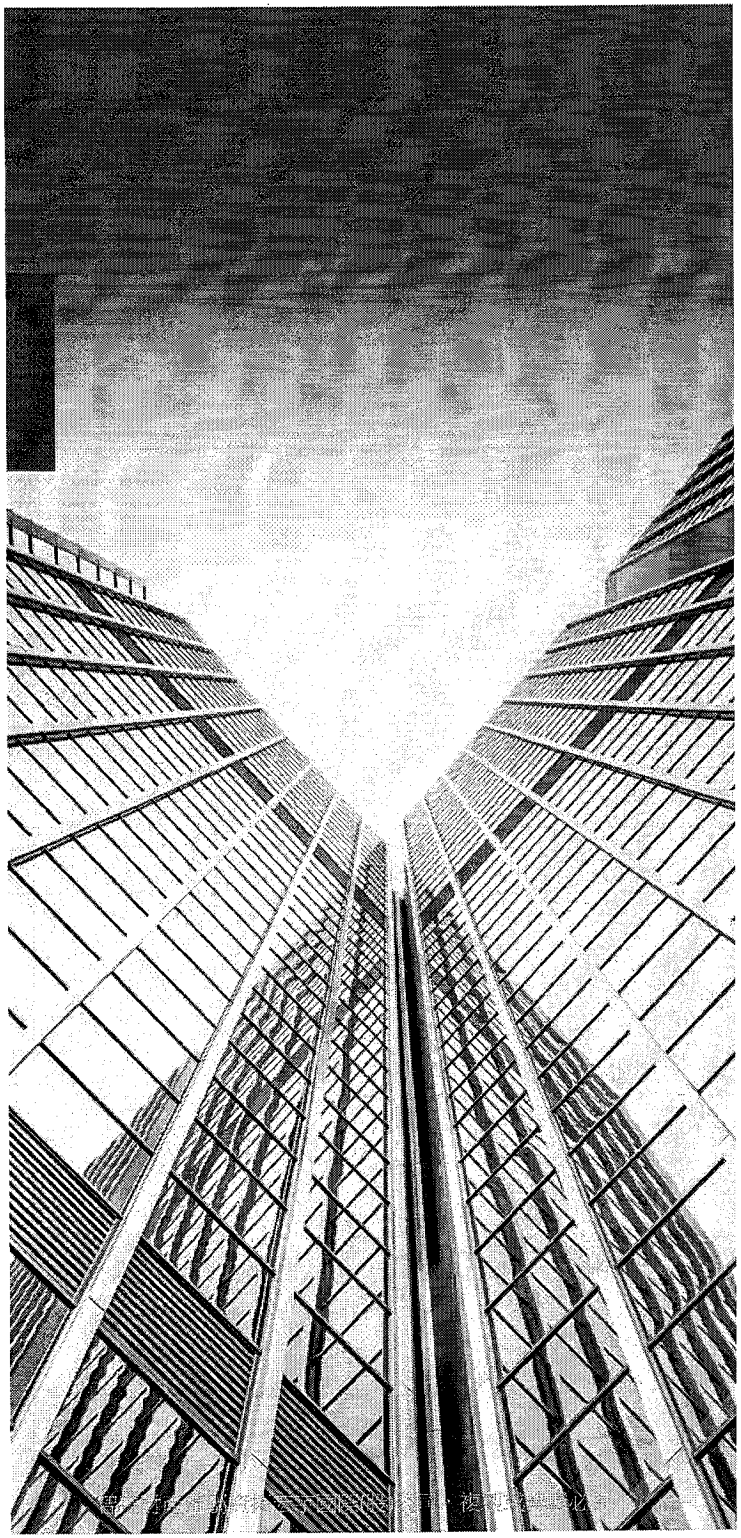


社群網路常見詐騙伎倆

臉書、IG退流行了？

- 《READr讀+》於2020年12月30日至2021年4月26日針對學生族群社交軟體喜好的調查結果
  - 國高中生最愛的前三名：IG、FB與TikTok，小紅書排第6名。
  - 大學生最愛：IG、FB與Dcard，小紅書排名第10。
- 根據2022年Google Play熱門免費項目排行
  - 小紅書囊括「社交」類與「所有類別」的冠軍
  - 其他熱門社交App分別為Twitter排名第5、Instagram排名第6、Facebook排名第9，「TikTok」是「影音播放與編輯」類的第一名，「所有類別」排名第11。
- 有網友擔心會有文化統戰的問題，但也有人認為，小紅書相當實用，資訊的完整度勝過IG。

資料來源：風傳媒

台灣年輕人間爆紅的「小紅書」是什麼？

- 「小紅書」是中國知名的「網路購物」和「社交APP」，人稱「中國版的IG」。電商可PO文，一般人也能分享「好物」。
- 操作與IG差不多，可發文(小紅書稱為筆記)、限時動態(小紅書稱發佈瞬間)、介面也是圖片影音為主，亦有按讚、分享、留言等基本社群功能。
- 可分享美妝、穿搭；也能紀錄生活大小事。可透過「標籤」將自己包裝成網紅。
- 小紅書是中國時下少女追蹤流行資訊必備的搜尋平台。
- 不少人把小紅書當成Google、百度等搜尋引擎。
- 購物或潮流相關問題都先使用小紅書搜尋，或直接使用APP內的「商城」購買商品。
- 台灣00後妹子笑「IG是老阿姨玩的」！
- 很多年輕人都改用小紅書。

資料來源：風傳媒

小紅書、TikTok 排行

For you | Top charts | Kids | Cate

熱門免費項目 | 類別

1 小紅書-找到妳想要的生活
社交
4.4★

2 手機優化大師
工具
4.4★

3 智能清理大師
工具
4.5★

4 强力清理大師
工具
4.2★

5 文件管理器：資源管理器...
工具
4.5★

Games | Apps | Movies | Books

For you | Top charts | Kids | Cate

熱門免費項目 | 社交

1 小紅書-找到妳想要的生活
社交
4.4★

2 Zenly：你的專屬地圖，你...
社交
4.4★

3 Omi - 實現超輕鬆配對
社交
3.6★

4 Dcard
社交
4.5★

5 Twitter
社交
更新

Games | Apps | Movies | Books

For you | Top charts | Kids | Cate

熱門免費項目 | 影音播放與編輯

1 TikTok-有趣的人都在這裡
影音播放與編輯
4.4★

2 bilibili-高畫質無廣告追星...
影音播放與編輯
3.2★

3 CapCut
影音播放與編輯
4.3★

4 LINE TV - 精彩隨看
影音播放與編輯
4.2★ 編輯精選

5 friDay影音-院線電影、跟...
影音播放與編輯
4.3★

Games | Apps | Movies | Books

資料來源：風傳媒 https://www.storm.mg/lifestyle/4195441

「小紅書」爆紅原因？與IG的差異？

- 小紅書的功能與Instagram相似，例如：
  - 以圖和影音為主的介面呈現
  - 發佈瞬間豐富濾鏡(類似IG story)
  - 發文私訊按讚分享等社群功能
- 與Instagram的差異是：
  - 新註冊用戶可依興趣選擇喜好內容
  - 推薦貼文不侷限單一主題，能自動延伸相似內容
  - 演算法自動推送貼文至手機通知
  - 內建熱門音樂庫、精美影集模板，讓用戶直接套用
  - 以「教程」為主的影片內容，網紅專家一分鐘內「包教包會」

資料來源：風傳媒

「小紅書」畫面範例

資料來源：風傳媒 https://www.storm.mg/lifestyle/3443657

網路上的假訊息

定義	以不實資訊誤導大眾，以帶來政治、經濟、市場、或心理得到成就感和利益的新聞或宣傳，包括通過傳統新聞媒體（印刷和廣播）或線上社群媒體傳播的故意錯誤資訊或惡作劇。
目的	➢ 造成恐慌 ➢ 扭曲事實或掩蓋真相 ➢ 牟取利益(經濟、政治) ➢ 帶風向

是她還是他？

- 利用繪圖軟體的合成功能與網路的匿名性及無限想像空間，網紅圈粉、有心人士進行詐騙與犯罪行為。

資料、圖片來源：奇摩新聞

你以為的 vs 實際上的

圖片來源： 木棉花 、天下雜誌

假消息的特徵

- 太過於誇張、聳動、讓人不禁想點擊的標題，都有可能是惡意的「點擊誘餌」。
- 網址很可疑，魚目混珠。
- 新聞內容出現許多錯字或網站版面編排不正常。
- 很多明顯經過刻意修圖的照片或圖片。
- 沒有附註發布日期。
- 未註明作者、消息來源或相關資料。

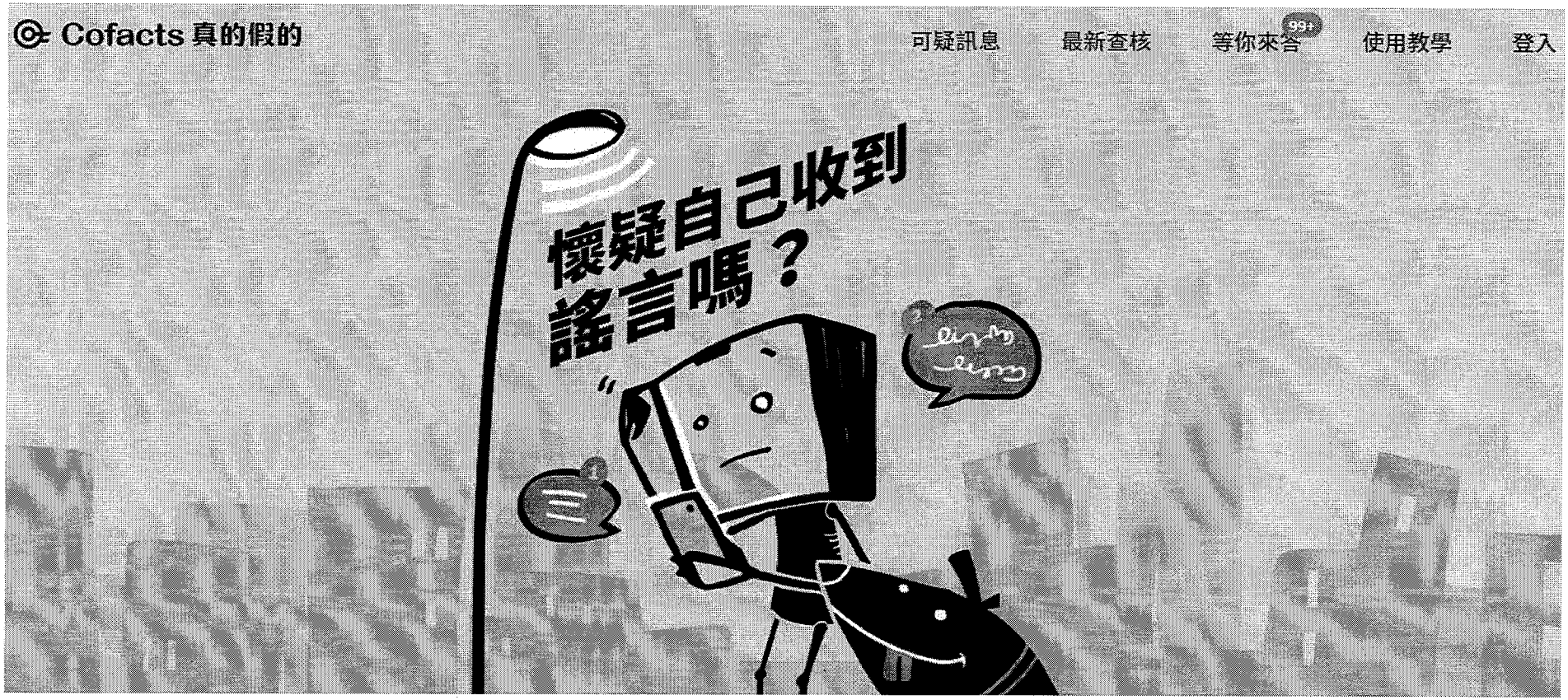
如何避免成為假消息的受害者與傳播者

- 提高警覺：不輕信令人嘩然的圖片或文章。
- 查證訊息來源：判斷新聞的可信度。
- 不要只看標題：可能文不對題，要看完內文。
- 留意評論：參考讀者留言以釐清謬誤。
- 注意日期：檢查報導日期，是否舊聞新推。
- 搜尋相片：利用Google圖片搜尋，看看是否舊圖亂用，或文圖不符。
- 有片未必有真相：要判斷片段前後發生甚麼事。
- 調查及統計數據要細心讀：避免統計誤植。
- 小心斷章取義：要審視邏輯，有無扭曲。

訊息辯真偽

收到可疑訊息(新聞、郵件、簡訊...等)，可至『Cofacts 真的假的』網站查詢訊息的真偽。

- **網址**：https://cofacts.tw/
- **Facebook**：https://zh-tw.facebook.com/cofacts.tw/



社交工程與網路釣魚

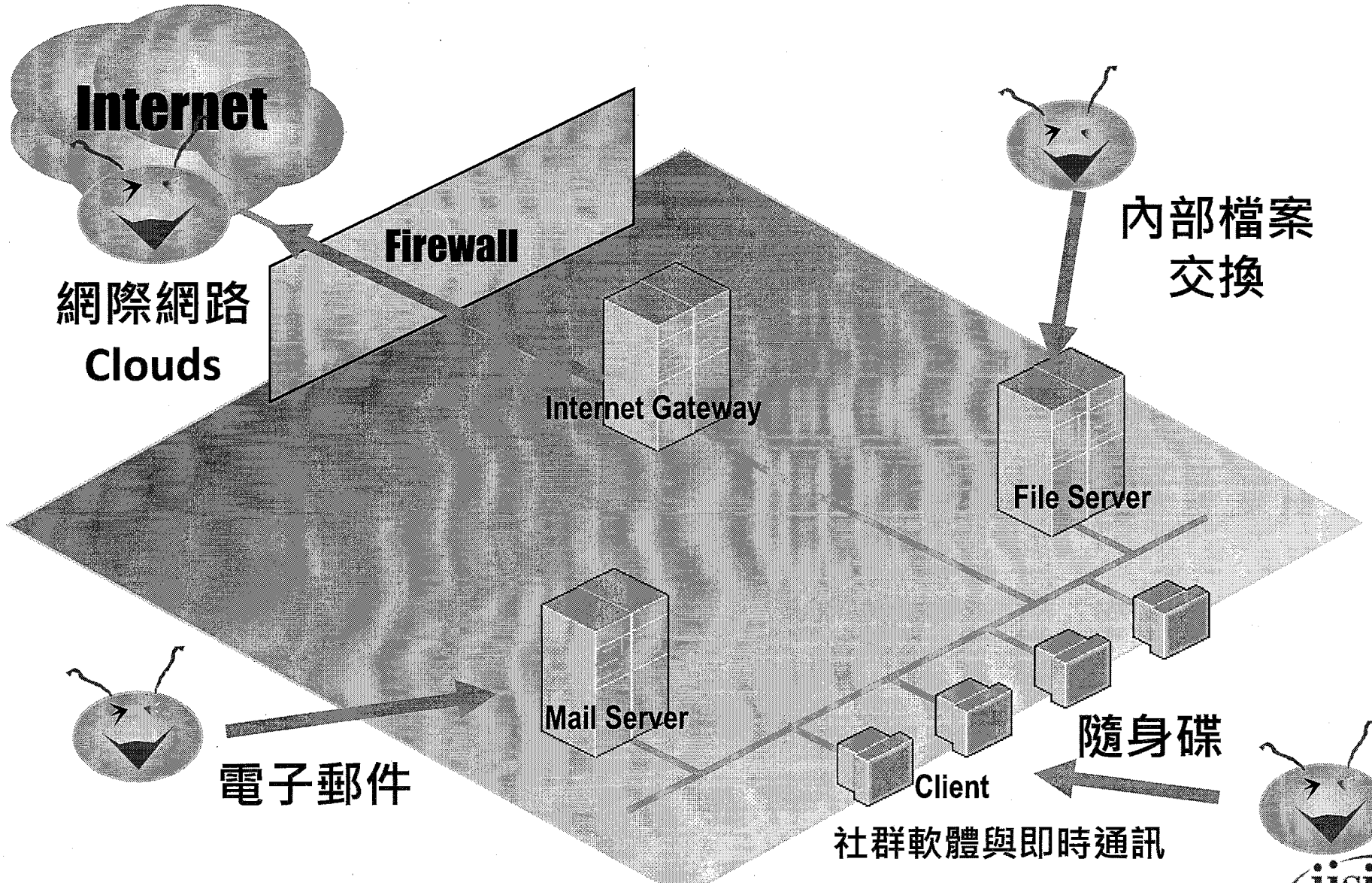
- **網路釣魚(Phishing)是網路上常見的社交工程**
  - 請求某種動作：執行檔案、點選連結、觀看影片，甚至是程式自動執行的功能，如郵件預覽、Script。
  - 在執行某種動作後，受害者的電腦可能就此被操縱，然後再繼續攻擊其它的電腦。
  - 智慧型手機、平板電腦等行動裝置案例愈來愈多
- **詐騙管道**
  - 電子郵件
  - 社群軟體
  - 即時通訊

惡意程式與假消息散播管道

- 社群軟體
  - 如：Line、FB、IG 等軟體使用, 由於使用者眾多, 特別適合利用此平台來散佈病毒與假消息。
- E-mail
  - 開啟了含有病毒的 E-mail 附加檔, 就會中毒。為了避免中毒, 建議您不要隨意開啟 E-mail 裡的附件檔, 甚至是連結的網址。
  - 病毒利用自動散佈病毒信給通訊錄名單中的人, 每一次有人中毒再轉寄此信時, 就會變更新的信件主題和內文。
- 網頁瀏覽與下載檔案
  - 病毒隨著網頁、下載的檔案傳播。特別容易被植入像是木馬程式, 以致個人電腦中的資料被竊取或遺失。
- 儲存媒體
  - 如光碟片、隨身碟等, 只要執行或開啟儲存媒體中的檔案, 病毒便會感染其他的程式, 或常駐在電腦中。
- 內部網路的資料交換
  - 利用一般企業、公司、政府機構、學校、研究單位、軍事單位所架設的區域網路來傳播病毒。

智慧財產權屬資拓宏宇國際(股)公司 · 複製或轉載必究

我們的資料保護有哪些破口？



智慧財產權屬資拓宏宇國際(股)公司，複製或轉載必究

社交工程的類型

- 面對面
  - 蒐集資訊或進行各種詐術
  - 金光黨
- 電話詐騙
  - 電信詐騙集團
- 電子傳訊管道
  - 網路詐騙或網路釣魚(Phishing)
  - Email/Line/Skype/QR code/Facebook

常見的網路社交工程手法

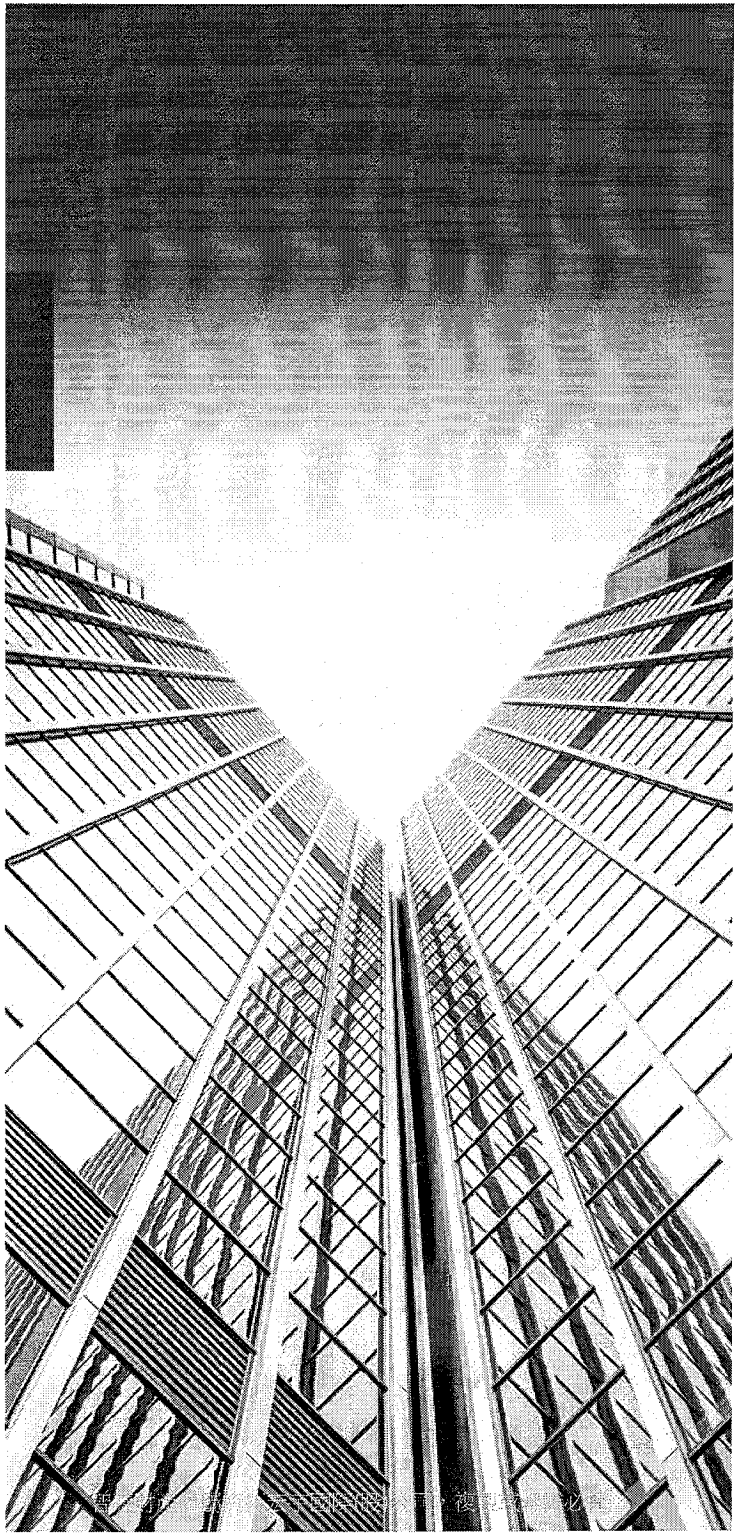
- 常見的詐騙與攻擊手法：
  - 假冒為同事或新進員工
  - 假冒廠商、客戶或政府單位
  - 假冒具有權威的人
  - 假冒系統廠商，表示欲提供系統修補程式或更新程式
  - 假冒好心人士，告訴對方如果電腦發生問題可以找他，然後製造問題，讓受害人打電話來求援...等。
  - 使用流行或特定關心的議題

都有一個假網址

- 社交工程攻擊常鎖定的目標：
  - 一般人員
  - 新進員工或特定業務人員

社交工程郵件與訊息的特徵

1. 非正常的發信時間或是認識的人來信但主旨或內容與其習性不符，這時候都應該要提高警覺。
2. 陌生寄件者郵件: 因為此類信件就有可能是偽冒寄件者之偽造的電子郵件(有時會冒充公務機關、微軟、Google等具知名度名稱寄信者，要特別注意)。
3. 來信郵件多包含惡意圖片、連結及附件檔案，檔案格式為ZIP、PDF、EXE、BAT、XLS、DOC等要特別小心。



社群網路安全使用守則

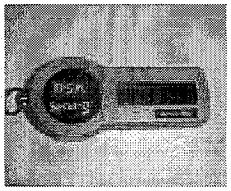
社群軟體安全最佳守則

- 啟用多重因子身分驗證(MFA)。
- 不要在不同平台使用相同密碼。
- 定期更新各平台的安全設定。
- 縮小您的朋友圈範圍以減少未知威脅。
- 關注社群媒體的安全風險。
- 瞭解網路釣魚攻擊的模式。
- 留意您帳戶內的假冒行為。

資料來源：Fortinet https://www.fortinet.com/blog/industry-trends/7-best-practices-for-social-media-security-and-privacy

多重身份驗證

- 多重身份驗證(Multi-Factor Authentication，MFA）需要成功驗證下列3種中的2種身分證明。
- **1.你知道的事物Something you know：知識型驗證**
  它可以是一個密碼、預設的安全問題、或圖形的形式出現，基本上它通常是個「知識因素(knowledge factor)」。
- **2.你持有的事物Something you have：權杖型驗證**
  這可以是一個小型的硬體設備，例如智慧晶片卡或是智慧型手機token。它們能產生獨特的一次性密碼，通常是由使用者手機上的應用程式所產生或被傳送過來的；這種驗證方法被認為是「持有因素 (possession factor)」。



- **3.你本身的特徵Something you are：生物特徵辨識為基礎的驗證**
  這通常需要一個生物特徵辨識器，用來偵測某一個人擁有的身體特徵，例如指紋、虹膜、臉孔、掌紋、筆跡或是聲音。這類的驗證因素定義為「與生擁有因素 (inherence factor)」。

為何要多重驗證?

- 單因素驗證已經過時
  - 密碼容易破解：精巧的密碼破解工具與無比強大的處理器
  - 雲端密碼破解服務（分散式電腦運算的Cloud Cracker）：嘗試300萬次的密碼破解只需不到20分鐘
  - 只要有時間和運算資源，沒有任何一種加密方法是絕對安全的
- 持有因素(智慧晶片卡，手機或硬體token)：
  - 優點：比密碼安全，不易破解
  - 缺點：登入時必須持有，可能遺失
- 與生擁有的因素(生物特徵)
  - 優點：不用記密碼，不用持有物件
  - 缺點：樣本檔損毀或辨識設備精準度不夠

行動載具優缺點

- 透過手機驗證的缺點：
  - 必須手機不離身，否則會有登入麻煩
  - 手機遺失、遭竊或毀損，將導致無法登入
- 透過手機驗證的優點：
  - 提供密碼之外的第二道防線
  - 結合手機生物辨識技術，達多重(3重)驗證之安全性

Google Authenticator

- 進入gmail登入畫面，輸入密碼。(如圖1)
- 打開手機的Google Authenticator 驗證器App，查看驗證碼。(如圖2)
- 將手機顯示的驗證碼輸入gmail兩步驟驗證畫面後，按〔驗證〕登入信箱

圖1

圖2

注意社群軟體的安全設定

Advice from social media platforms

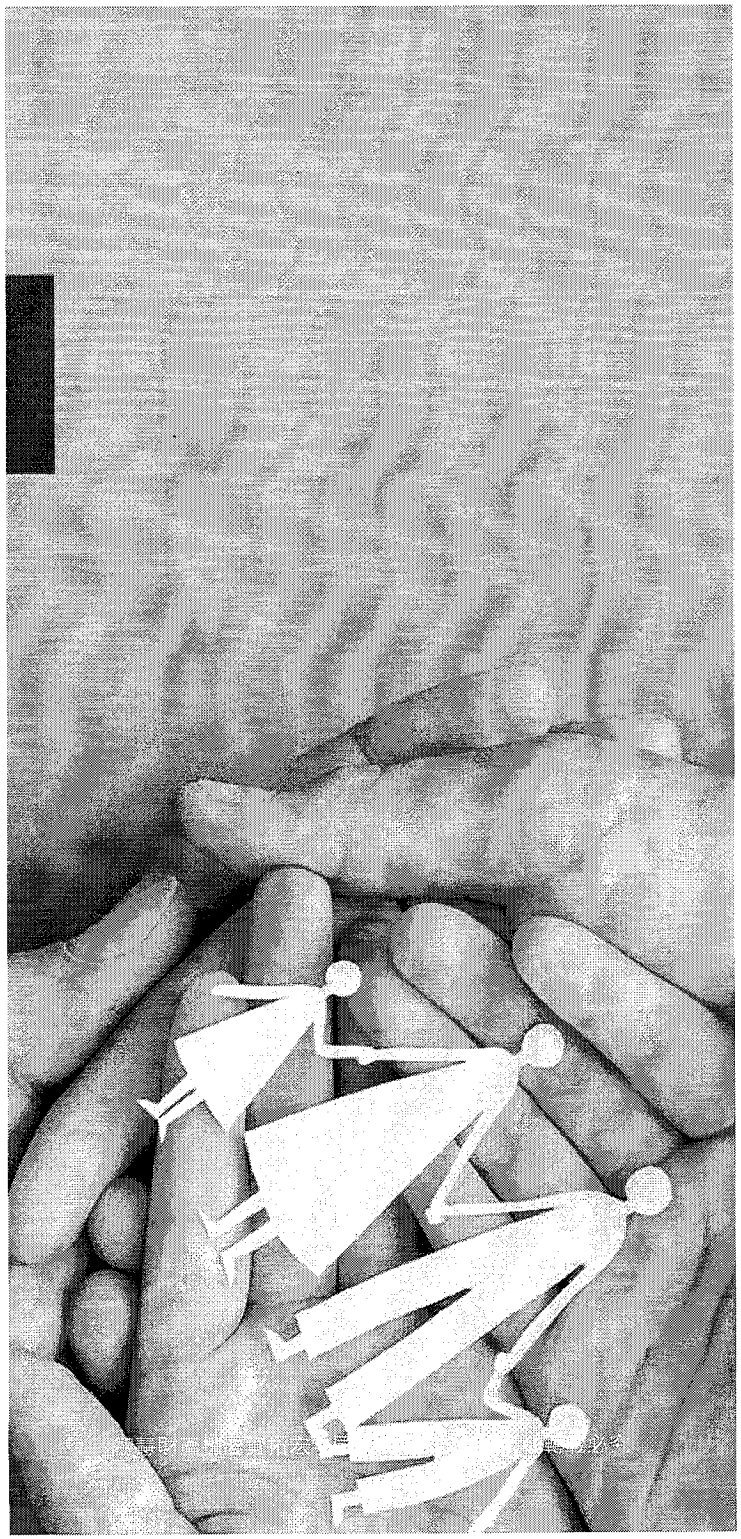
The following guidance is provided by each of the major social media platforms.
Click to read detailed information.

- **Facebook**
  Basic privacy settings and tools
- **Twitter**
  How to protect and unprotect your Tweets
- **YouTube**
  Privacy and safety
- **Instagram**
  Privacy settings and information
- **LinkedIn**
  Account and privacy settings overview
- **Snapchat**
  Privacy settings
- **Tiktok**
  Privacy and security settings

資料來源:https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

社交工程訊息之防範方式—提高警覺

- Q:為何我會收到這封郵件或訊息?
  - 寄件人不認識就不要開啟
- Q:我是否應該收到這封郵件或訊息?
  - 與業務或本身職務無關主旨不要開啟
  - 信件主旨雖與業務有關，但寄件者郵件非公務信箱
- Q:我是否應該開啟這封郵件或訊息?
  - 與業務或本身職務無關
  - 不隨意點選郵件超連結



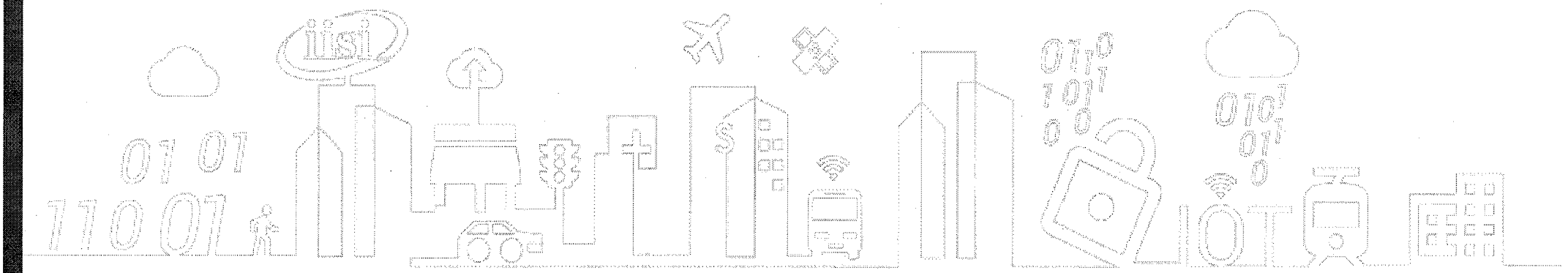
總結

時時警覺可保安全無虞

- 使用資通設備須注意安全，避免個資外洩。
- 發現問題應依循組織紀律與程序處理，切勿隱瞞。
- 作業系統與應用軟體應注意更新與防毒。
- 妥善保護自己與他人的個資以增加防禦力。
- 資通安全，人人有責。

智慧財產權屬資拓宏宇國際(股)公司，複製或轉載必究

- 敬請指教 -



資拓宏宇國際股份有限公司
International Integrated Systems, Inc.
公司總部：22041 新北市板橋區縣民大道二段7號6樓
電話：(02)8969-1969　　傳真：(02)8969-3359