媒體識讀與資訊倫理

網路現象解析X教育現場守則

簡報人：石盛文

新北市立林口國民中學教師　　教育部「中小學資訊素養與倫理推廣計畫」講師

網路與資訊安全

個人資料保護及管理實務分享

花蓮縣教育處教網中心

eliteracy

中小學資訊素養與認知網

::: 相關連結 網站導覽 網路安全政策 隱私權保護

關鍵詞: eteacher.edu.tw 搜尋

最新消息 文章專區 數位教材

宣導教材 互動遊戲 服務資源

網頁小遊戲

HTTPS://ETEACHER.EDU.TW/GAMES.ASPX

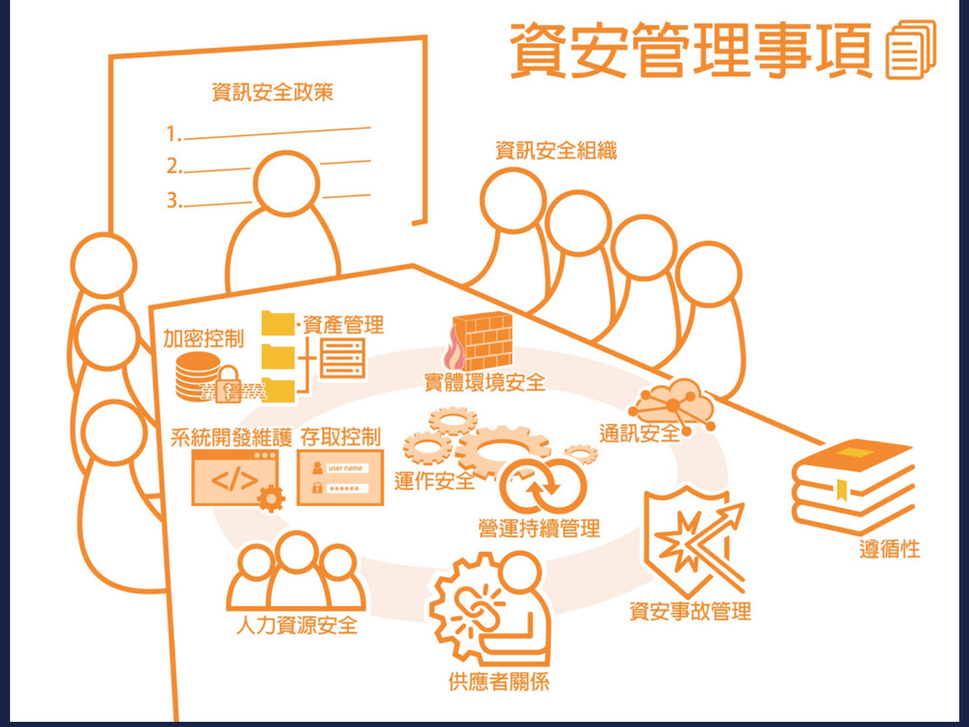
數位公民

大擂台

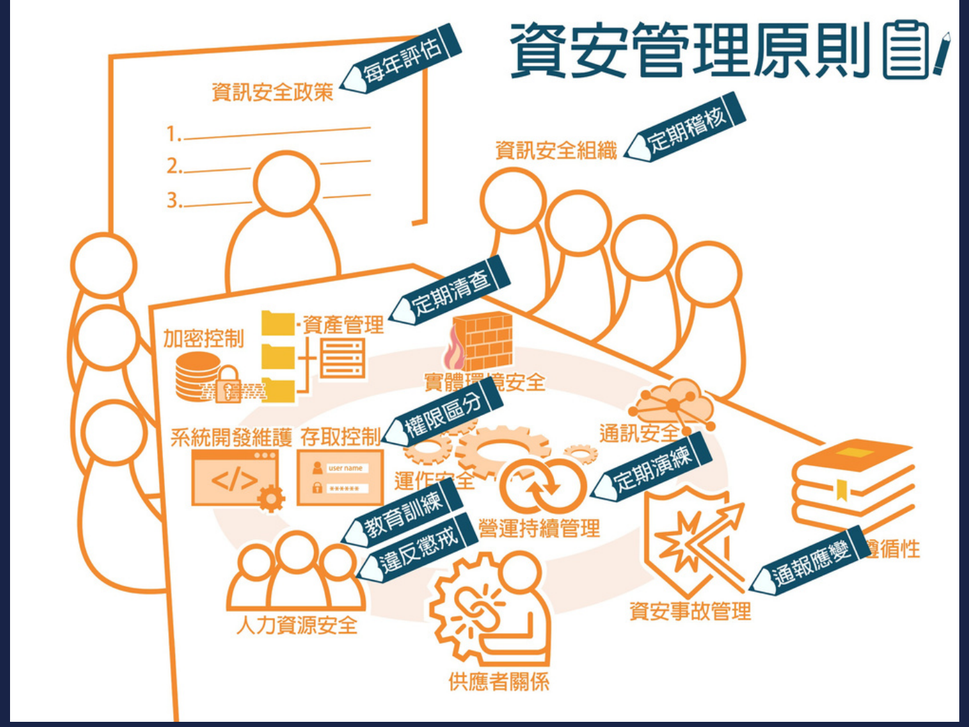
網路成癮檢測

https://eteacher.edu.tw/Games/Addiction/play.htm

資安管理基本守則



- 資訊安全政策
- 資訊安全組織
- 人力資源安全
- 資產管理
- 存取控制
- 密碼學(加密控制)
- 實體與環境安全
- 運作安全
- 通訊安全
- 資訊系統取得、開發及維護
- 供應者關係
- 資訊安全事故管理
- 營運持續管理之資訊安全層面
- 遵循性



1. 重要之資訊資產應**定期清查**、分類分級與進行風險評鑑，並據以實施適當的防護措施。
2. 重要資訊資產存取**權限**應予以**區分**，考量人員職務授予相關權限，必要時得採行加解密(例rar)及身分鑑別機制，以加強資訊資產之安全。
3. 對於資訊安全事件須有完整的**通報**及**應變措**施，以確保資訊系統、業務的持續運作。
4. 應訂定營運持續計畫並**定期演練**，以確保重要系統、業務於資安事故發生時能於預定時間內恢復作業。
5. 相關人員應依規定接受資訊安全**教育訓練**與宣導，以加強資訊安全認知。
6. **定期**執行資訊安全**稽核**作業，檢視存取權限及資訊安全管理制度之落實。
7. **違反**本政策與資訊安全相關規範，依相關法規或本校**懲戒**規定辦理。

資訊資產分類

1. **人員(People)**：包含全體同仁，以及委外廠商。
2. **文件(Document)**：以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。
3. **軟體(Software)**：作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。
4. **通訊(Communication)**：網路設備、網路安全設備、提供資訊傳輸、交換之線路或服務。
5. **硬體(Hardware)**：主機設備等相關硬體設施。
6. **資料(Data)**：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
7. **環境(Environment)**：相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

資訊及系統使用

1. 使用資訊及資通系統前應經其**管理人授權**。
2. 使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。
3. 資訊處理設施的授權過程應制定安全控管使用資訊及資通系統，**新增、異動或使用須經過授權程序**，並制定相關規定以維護其安全。
4. 非本校同仁使用本校之資訊及資通系統，應確實遵守本校之相關資通安全要求，且未經授權不得任意複製資訊。
5. 對於本校計資中心管理之資訊及資通系統，遵循規定確保與資訊處理設施相關的資訊資產加以適切的分類分級，並界定與定期審查資訊資產機密等級與存取限制，以及考量可適用的存取控制政策。

防範惡意軟體

1. Windows作業系統之主機及個人電腦應**安裝防毒軟體**，須安裝至最新之**修補程式及病毒碼**，並即時修補相關安全漏洞。如需使用外來的**可攜式設備或媒體**，應確認設備未遭受病毒感染。**電子郵件**須先經過防毒軟體掃描，並禁止開啟來路不明之檔案或電子郵件及其附加檔案，以避免遭受病毒攻擊。正確配置**瀏覽器之安全設定**，建議設定在中級風險等級(含)以上。
2. 為有效控制「**免費軟體**」或「**共享軟體**」的使用，使用人員須事先瞭解其相關版權規定，並且不得任意自行安裝及散佈未經授權之軟體。
3. 不得私自使用已知或有嫌疑惡意之網站。

電子郵件使用

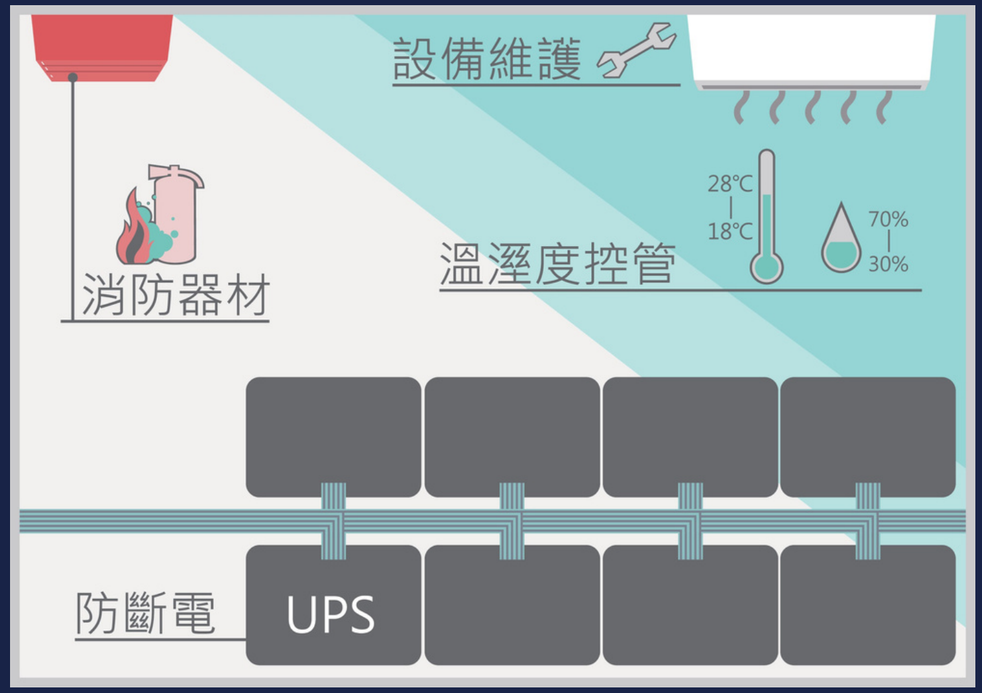
1. **密等**以上的公文不得以電子郵件傳送。
2. 含有**個人資料**之信件必須**加密**傳送。
3. 電子郵件**加簽**以避免發送匿名或偽造。
4. **不得**利用公務電子郵件進行**侵害他人權益、違法**之行為。
5. (包括以電子郵件大量傳送廣告信、連鎖信或無用之信息，或以灌爆信箱、掠奪資源等方式。以電子郵件、線上互動或類似功能之方法散布詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息。)自訂「**校園網路使用規範**」，納入電子郵件使用限制相關條文。

實體環境安全

1. 為確保設備及資料之安全，應採用**有身分識別功能之安全門**，做為必要之安全控管。
2. 除機房管理人員外，其他因業務需要進入電腦機房作業時，應由機房管理人員陪同進入並於「電腦機房進出管制登記簿」上**登記**。
3. 內部人員於進出時應隨時注意是否有**非經授權人員**跟隨進入。
4. 外部人員或委外人員應配帶原公司所製發之**員工證或相關證明**，並應於指定環境內執行作業。
5. **門禁系統之進出記錄**應定期備份、審閱；記錄存放於安全區域並保存一年備查。

實體環境安全

1. 應保護設備免於**電源**失效，及因其他支援之公用服務事業失效，所導致之中斷。
2. 電腦機房**溫濕度**採固定區間控制，溫度應維持在18℃至28℃，相對溼度維持在30%至70%。
3. 電腦機房應設置專用之**消防**器材或系統，如熱感應、煙霧偵測、火災警報、滅火設備、火災逃生設備等，同時應符合相關法規並定期檢測、記錄。
4. 電腦機房維運設備(如消防、電力、空調設備等)或重要資訊設備(如主機、網路設備等)應與合格專業廠商簽訂**維護合約**，定期實施保養與妥善維護，以確保設備的完整與安全。



實體環境安全

1. 依據桌面淨空與螢幕淨空安全控管規定，應實施**桌面淨空**，重要文件應妥善保管。
2. 依據可移除式媒體的管理規定，將機密資料存放於**可攜式設備與媒體**時，應採取適當**加密處理或保護措施**，避免遺失時洩漏資訊。為降低媒體劣化之風險，無法讀取前加以**備份**。
3. 依據資訊資產處置規定，**密級、限制使用、內部使用**等級的資訊類資訊資產以任何型式儲存均須**置於上鎖區域保管**，並設有存取控制。
4. 依據應用系統測試/正式環境、資料庫之安全維護規定，應將**敏感性系統隔離**。
5. 針對**存有個人資料之紙本文件**及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖。

電腦使用安全

1. 同仁應遵循「實體環境安全管理辦法」桌面淨空與螢幕淨空安全控管規定，個人電腦、伺服器或主機應設定**螢幕密碼保護程式**，下班時應**關閉**不需使用之個人電腦。
2. 同仁應遵循「資訊作業管理辦法」軟體安裝之限制，為有效控制「**免費軟體**」或「**共享軟體**」的使用，須瞭解其相關版權規定，並且**不得任意安裝及散佈未經授權軟體**。
3. 同仁應遵循「資訊作業管理辦法」防範惡意軟體規定，Windows主機與個人電腦皆須安裝**防毒軟體**。
4. 同仁應遵循「資訊作業管理辦法」運作中系統之軟體安裝規定，主機系統、網路設備、軟硬體常更新**修正程式**。
5. 同仁應遵循「實體環境安全管理辦法」保全之辦公室、房間及設施規定，**列印後應立即將資料取走**。

行動設備安全

1. 同仁應遵循「資訊資產管理辦法」可移除式媒體的管理規定，使用**可攜式設備與媒體**時，應謹慎防範資訊洩漏或妨害組織利益等情節發生，資料攜入或攜出，主管應盡控管之責，提醒使用人員自我要求。私人可攜式設備與媒體，應**評估風險**後方可存取公務資料。
2. 處理**內部使用等級以上資料工作區域**，未經許可禁止使用相關設備進行拍攝或是螢幕畫面捕捉之行為，使用時需有**工作區域管理人員在場陪同**。

即時通訊軟體

1. 同仁應遵循「網路安全管理辦法」網路通訊服務傳遞規定，利用網路通訊服務，如電子郵件、**即時通訊軟體**或外部應用系統或資訊交換平台時，應依據「資訊資產管理辦法」資訊資產處置規定，針對**不同等級的資訊類資訊資產，建立適當的資訊控管程序**，以確保資訊資產受到適當等級之保護。
2. 避免非授權人員取得機密性資料，應依據「資訊資產管理辦法」與「資訊安全存取管理辦法」，**建立存取權限管理原則**，並據以執行。

限制大陸製品

1. 除因業務需求且無其他替代方案外，**不得採購及使用**主管機關核定之廠商生產、研發、製造或提供之**危害國家資通安全產品**。
2. 必須採購或使用危害國家資通安全產品時，應具體敘明理由，**經主管機關核可後**，以專案方式購置。
3. 對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品，應**列冊管理**，且應**指定特定區域及特定人員使用**，**不得與公務網路環境介接**，**不得處理或儲存機關公務資訊**，**測試或檢驗結果應產出報告**，購置理由消失或使用**年限屆滿應立即銷毀**。
4. 本校每個單位在執行購案時，資通訊產品必須要求廠商在簽約時提供**無大陸製品(品牌)之切結書**。

資安懲處辦法

1. **未依法規**或機關內部規範**辦理**下列事項，**情節重大**：

（一）**資通安全情資分享**作業。

（二）訂定、修正及實施**資通安全維護計畫**。

（三）提出資通安全維護計畫**實施情形**。

（四）辦理資通安全維護計畫實施情形之**稽核**。

（五）配合上級或監督機關資通安全維護計畫實施情形稽核結果，提出**改善報告**。部規範之行為，情節重大。

（六）訂定**資通安全事件通報及應變機制**。

（七）資通安全事件之通報或應變**作業**。

（八）提出資通安全事件**調查、處理及改善報告**。

1. 辦理資通安全業務經主管機關、上級或監督機關評定績效不良，經疏導無效，情節重大。
2. 其他違反本法、本法授權訂定之法規或機關內部規範之行為，情節重大。
3. **對業務督導不力**，致其屬員、所屬或所監督機關之人員有前三款情形。

何時要做資安通報?

1. 公務電子郵件遭遇到侵害權益、假冒來源、內容有惡意連結時。
2. 公務上使用通訊軟體未重視資安問題，像是群組傳遞敏感資料時。
3. 公務電腦遭遇無法解決的病毒、木馬，或有人使用可疑的免費共享軟體時。
4. 各單位機房的門禁出問題或發生重大異常事件，辦公室的敏感資料外流時。

資訊科技對我們的影響

資訊科技帶來的影響

數位金融與系統安全
社會秩序與隱私安全
人工智慧與道德規範

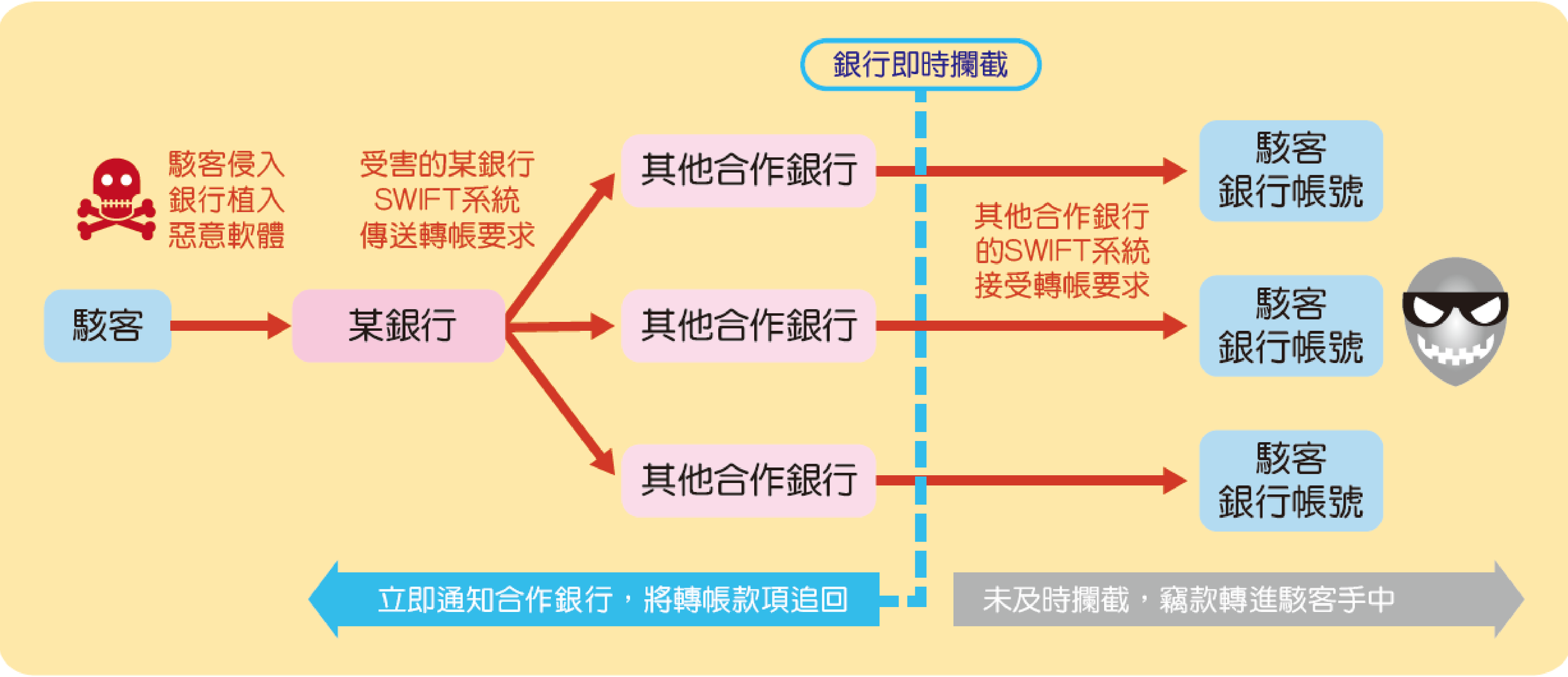
資訊科技對社會的影響

資訊科技的發展為生活帶來便利也伴隨著資訊安全隱憂，除了對個人層面的影響，也會對整體社會帶來新的生活形態與影響。

數位金融與系統安全

數位金融是指透過網路所進行各種金融服務，在數位時代裡全球眾多國家難以計數的金融機構之間要能順利的進行交易資訊的溝通，則仰賴銀行業者之間訂定的共同標準。

2017年10月，某銀行使用的環球銀行金融電信協會（SWIFT）系統遭到入侵。駭客破解SWIFT系統進行網路攻擊，取得SWIFT系統的操作權限，並植入惡意軟體，將某銀行高達六千多萬美元的金額轉到偽造的帳戶，雖然後來經由國際刑警組織及SWIFT的調查與協助，將損失降到最低，但仍然顯示出數位金融帶來的效率與便利背後，其實潛藏著相當大的風險。



銀行SWIFT遭駭手法說明

駭客

在資訊安全中，駭客指的是試圖破解系統程式，進而非法登入系統後，盜用或毀損系統內的資料。

當資訊科技帶來的便利服務越深入影響人們的生活，往往也伴隨著更巨大的隱憂。數位金融服務除了自身流程漏洞或安全防護不足而受到攻擊之外，仍有一大部分的安全威脅來自使用者的安全觀念薄弱或者使用習慣不佳。

例如：使用者進行網路購物或是使用網路銀行所衍生的金融交易損害時有所聞，包含密碼設定過於簡單，可能被猜中密碼冒用身分登入或是網路銀行在使用後未登出等，更可能因此留下讓不法之徒可趁之機，成為侵入系統的途徑，造成金融秩序的危害。


網路安全【誰用了我的帳號】
Share
我沒有發訊息給你們啊！
Watch on YouTube

✕ 密碼設定過於簡單

✕ 網路銀行未登出

因此，便利的服務更需要搭配充分的防護機制與正確的使用態度。

全球性的數位金融交易系統，隨著人們仰賴其快速便利而蓬勃發展，並且日趨複雜龐大。當資訊科技發展深入人們各種生活的系統後，一旦發生安全隱憂，影響層面更是廣泛且深遠。這些都是值得我們關注的系統流程或架構上的安全議題，平時更應加強提升使用者養成良好習慣。

資訊處理作業時應注意事項

- 不可將密碼使用便利貼貼在螢幕或主機上
- 離開電腦要鎖定螢幕或登出
- 公務電腦離開桌面，敏感性紙本要先收好，不可隨便置於桌面
- 不要在公務電腦安裝非法軟體，以造成系統漏洞
- 紙本敏感性資料，繕打錯誤或不用時一定要碎掉，不可變成資源回收品

密碼安全設定原則

- 不使用懶人密碼
- 使用長度與複雜度較強密碼
- 密碼無明顯含義
- 定期更新

不使用懶人密碼

- 懶人密碼就是使用者貪圖一時方便，使用極為簡單的密碼設定如
- **1. 123456**
- **2.** 使用空白密碼
- **3.**密碼與帳號設定相同

這種毫無強度的密碼設定十分危險！

長度與複雜度

密碼強度不足，使你危機四伏
密碼長度應至少8碼以上，並且混合大小寫英文字母、數字及特殊符號，一個複雜度符合安全要求的密碼應至少包含：
大寫英文字母
小寫英文字母
數字特殊字元，如：! @ # $ % &等

密碼被暴力破解的實驗統計結果

密碼長度	英文字母 (26 字元)	英文字母+數字 (26+10 字元)	英文字母大小寫 (52 字元)	含特殊符號字元 (96 字元)
4	0	0	1 分鐘	13 分鐘
5	0	10 分鐘	1 小時	22 小時
6	50 分鐘	6 小時	2.2 天	3 個月
7	22 小時	9 天	4 個月	23 年
8	24 天	10.5 個月	17 年	2287 年
9	21 個月	32.6 年	881 年	21 萬 9000 年
10	45 年	1159 年	45838 年	2100 萬年

測試密碼強度軟體

- 密碼強度檢測器（**PASSWORD STRENGTH CHECKER**）是一個檢測密碼強度工具，只要輸入密碼，就會自動幫你偵測密碼強度，不過若密碼太弱的話，你就要自己修正其密碼安全度，這網站只提供檢測服務，並沒有密碼產生的功能喔！
- HTTP://WWW.REFLY.NET/PASSWORDCHECKER/

不要使用無明顯含義的密碼

- 密碼與帳號相同
- 使用生日、身分證字號、英文名字等個人資料
- 使用公司、部門、單位名稱
- 使用與系統管理名詞（如**ADMIN**、**PASSWORD**等）
- 不設定密碼（空白密碼）
- 使用簡單字元組合（如**1234**、**ABCD**、**111111**等）

手機上網安全

1. 手機實體安全防範
2. APP 使用風險與安全建議
3. 享受社群網路服務同時保護個人資料

手機實體安全防範(避免手機遺失風險)

- **1.**個人資料:手機裡儲存的個人資料, 親朋好友的手機號碼。
- **2.**網路登錄帳號密碼:手機登入自己或公司的電子郵件、在**FACEBOOK** 上與朋友互動、上傳**YOUTUBE** 影片的帳號密碼
- **3.**網路交易資料:手機上進行線上購物、買票、銀行轉帳交易，甚至現在手機還可以當作是進出高鐵閘門的票券！
- 一旦手機遺失，也代表這些個人帳號、密碼、交易資料，都有洩漏的可能。

幾個基本的手機實體安全小撇步

- 設定手機密碼保護手機
- 記下你的手機唯一識別碼 **(IMEI)**
- 安裝搜尋手機軟體

設定手機密碼保護手機

- 手機密碼是指當開機時須輸入的密碼。
- 一般手機的預設密碼值是 **1234** 或 **0000**，建議使用者必須更改為自己的密碼。

安裝搜尋手機軟體

- 當遺失手機時可以找尋手機位置，還可以遠端清除資料
  - **FIND MY IPHONE(IOS)**
  - **FIND MY PHONE (ANDROID)**

絕對不把密碼儲存在手機中

- 許多人為了方便或擔心忘記，會把密碼（尤其是不常使用的密碼）儲存在手機中，在你的電話遭竊或遺失時，這樣的做法是很危險的！

APP 使用風險

- 智慧型手機、平板電腦等行動設備其實也是一種電腦
- 有處理器、記憶體與儲存空間，可以安裝各種軟體，能夠上網、玩遊戲和瀏覽影音等
- 像一般電腦一樣可能存在惡意程式竊取你的資料，或偷偷執行其他動作。

APP STORE與GOOGLE PLAY比較

	APP STORE	GOOGLE PLAY
支援作業系統	IOS	**ANDROID**
APP審核機制	由APPLE審核	採使用者審核
惡意APP	較少	較多

手機病毒的危害

- 導致使用者資訊遭竊
- 傳播非法訊息
- 使手機無法運作

如何判別手機惡意程式?

- 注意該**APP** 的星級評價
- 觀察使用者對該**APP** 之評論
- 查看該**APP** 的存取權限設定

手機的社群網路應用個資保護

- 只接受你認識的朋友邀請
- 謹慎思考要張貼哪些資訊
- 幫朋友打卡與**TAG** 前，先取得同意
- 定期檢視你的隱私權設定

正確而且安全的使用觀念

- 確保個人電腦維持在安全的狀態，除自身需具備充足的資訊安全觀念，亦建議安裝防護軟體並隨時更新，更加提昇安全性。

使用現金交易或是數位支付各有優缺點。如果未來都只能使用數位交易時，可能產生什麼隱憂呢？

社會秩序與隱私安全

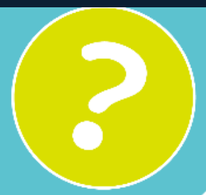
不論是居家安全、公共環境監測或是產業的需求，都和資訊科技發展有密切關係。自從有了監視系統，人們不再需要親自到達現場，透過監視系統即可同時觀看不同地點的即時影像。透過無遠弗屆的網路，能突破空間限制建構遠端即時監控系統。例如：智慧校園或公寓大樓安全防護網的影像監視系統、高速公路即時路況資訊等。

校園或公寓社區中常見的監視器

監視系統能幫助我們將環境中的變化記錄下來。

高速公路即時路況資訊

隨著科技發展與網路普及，加上社會秩序維護的需求，我們生活的周遭裡出現了越來越多的影像監視設備。當發生治安事件時，警察機關可以透過影像監視設備，快速掌握各種犯罪行為。而如果影像監視設備遭到不當使用，就可能會發生個人隱私被監看的疑慮。

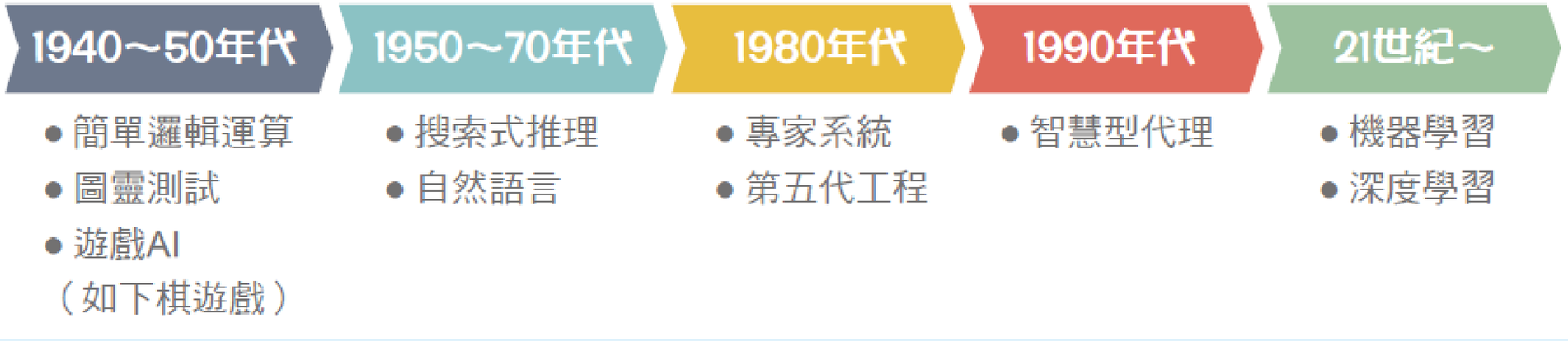


在維護社會秩序與保障個人隱私之間，影像監視設備應該怎樣規範才合理？

人工智慧與道德規範

資訊科技的進步使得電腦運算能力大幅提升，輔以大量數據探勘技術、網路普及與分散運算技術的發展，各種資訊系統處理資訊的能力也突飛猛進。以此為基礎，電腦系統能根據大量的數據分析而做出反應，模擬人類的思考表現，甚至具有學習、推理的能力，也就是近來資訊科技領域熱門探討的「人工智慧」（Artificial Intelligence，簡稱AI）。

人工智慧的發展源自古典哲學家使用機械符號解釋人類思考的過程，意即人工智慧具有「人類思考過程可以被機械化、程式化」的基本假設，20世紀40、50年代的科學家們開始探討製造人工大腦的可能性，直到1956年在美國東部達特茅斯學院舉行的會議才正式確立了人工智慧研究領域並成為學科。



- **圖靈測試**：如果一臺機器能夠通過電傳設備與人類展開對話，而且不被人類辨識出其機器的身份，可以稱這臺機器具有智能。
- **專家系統**（Expert System）：能夠在特定領域中解決專業問題的程式系統。程式系統透過運用龐大的知識庫並模擬專家的思維，有效地解決需要專家才能夠解決的複雜問題。
- **第五代工程**：在 1981 年由日本投注經費發展的計畫，目標是打造出能夠與人類對話，翻譯語言，解釋圖像，並且可以像人類一樣進行邏輯推理的機器。
- **智慧型代理**（Intelligent Agent）：可以觀察周遭環境並作出決定以達到目標的自主實體，此自主實體通常是指軟體或是由軟體控制的裝置。
- **機器學習**（Machine Learning）：機器學習為透過樣本（可在資料中找到）訓練機器辨識出運作模式，並非用特定的規則來編程。簡單來說，機器學習是一種弱人工智慧（narrow AI），可從資料中得到複雜的函數（或樣本）來學習並創造演算法（或一組規則），也可利用它來做預測。
- **深度學習**（Deep Learning）：此為實現機器學習的技術，這技術也被稱為深度神經網絡（deep neural networks - DNNs）。

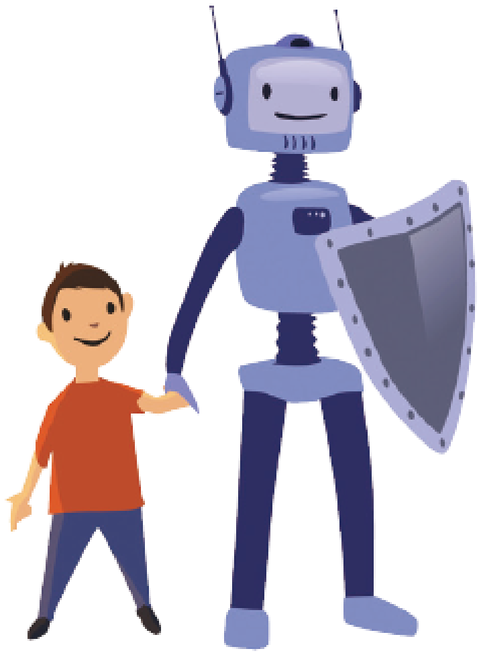
人工智慧的發展歷程

若說人工智慧科技發展出一個會思考又可以協助人們處理工作，甚至還可以幫我們帶小孩、洗衣服、做飯的智慧型機器人，確實是一個引人矚目的議題之一。但是，同時也讓我們擔心害怕的問題更多，例如：如果有一天機器人不聽從人的指令工作時，怎麼辦？如果有一天機器人完全取代了我的工作，怎麼辦？

最新研究報告指出，未來人工智慧仍然是科技主戰場，包含臺灣在內全球許多國家也都把人工智慧當作未來科技產業發展的重要戰略之一。因此，隨著人工智慧的發展，人們對於機器人的恐慌可說是有增無減，不論是擔心機器人會搶走工作機會，亦或是機器人總有一天會統治地球，種種的擔憂促使著人們訂定屬於機器人的法規。未來AI世界的人類和機器應該如何一起攜手，共創未來呢？

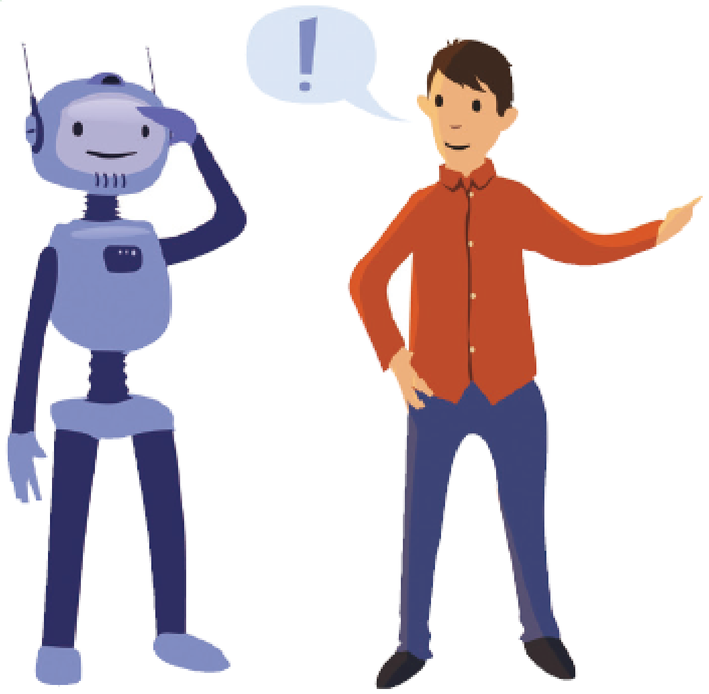
Isaac Asimov 在 1942 年對機器人技術的發展提出 3 大法則

1



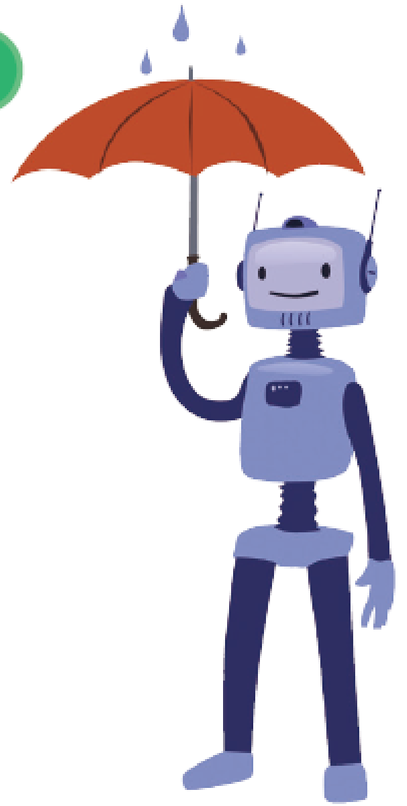
第 1 原則是機器人不得傷害人類，或看到人類受到傷害而袖手旁觀。

2



第 2 原則是機器人必須服從人類的命令，除非這條命令與第一條相矛盾。

3

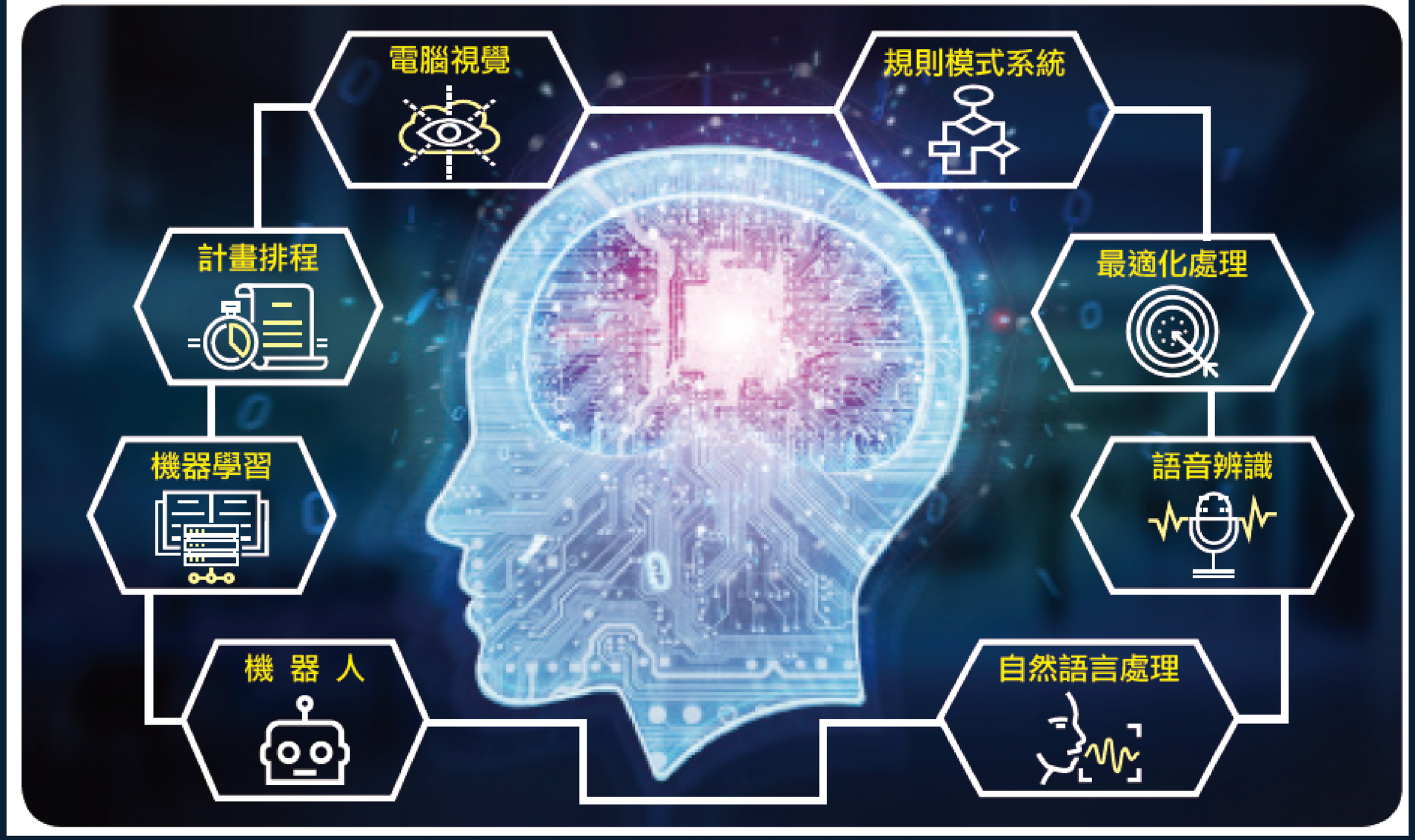


第 3 原則是機器人必須保護自己，除非這種保護與以上兩條相矛盾。

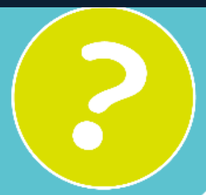
人工智慧系統具有提升生產的能力。當人工智慧系統不再只是控制機器進行簡單重複的工作，進一步發展到足以取代需要思考創造方面的人力時，除了會造成人力工作權的相對剝奪及貧富差距擴大問題外，對於人工智慧的決策或預測能力，是否也會發生誤判的可能性，進而引發道德層面的問題。

這也顯示人們開始思索，人工智慧技術發展除了為社會帶來應用，也將對道德規範產生衝擊影響。而人工智慧並不專指人形機器人的應用，許多能偵測環境、分析偵測結果進而採取預測或是決策的系統發展，都可以視為人工智慧應用。

近年來興起的自動識別技術（Automatic Identification and Data Capture，AIDC）應用風潮，例如：人臉辨識系統建立的保護機制，確實為生活增加了便利性與安全性。但若各種監看、辨識、感應系統大量串連後，例如：有辨識能力的系統與金融、戶政、警政等服務系統整合，發展為具有學習、預測、決策與控制秩序能力的人工智慧系統，是否也會造成人工智慧系統過度掌握隱私或是侵犯隱私的道德議題。



各種系統整合串聯的AI人工智慧應用



人工智慧應用發展出具有思考決策能力的機器人，或應用在生活中的自動識別技術，各有什麼優缺點呢？

回顧

資訊科技對社會的影響

- 數位金融與系統安全

  安全威脅來自使用者的安全觀念薄弱或者使用習慣不佳。例如：使用者進行網路購物時，常因為密碼設定過於簡單，可能被冒用身分登入或是網路銀行在使用後未登出等，成為侵入系統的途徑，造成金融秩序的危害。

回顧

社會秩序與隱私安全

自從有了監視系統，人們不再需要親自到達現場，透過監視系統即可同時觀看不同地點的即時影像。例如：智慧校園或公寓大樓安全防護網的影像監視系統、高速公路即時路況資訊等。相對也會衍生影像監視設備，可能會影響個人隱私的負面疑慮。

回顧

人工智慧與道德規範
未來人工智慧仍然是科技產業發展的重要戰略之一。而人工智慧並不專指人形機器人的應用，許多能偵測環境、分析偵測結果進而採取預測或是決策的系統發展，人工智慧技術發展也將對道德規範產生衝擊影響。

資訊科技對我們的影響

資訊科技帶來的便利與資安防護

認識資訊安全
使用電腦與網路的資安防護
個人數位金融安全防護
智慧型裝置的資安防護

資訊科技帶來的便利與資安防護

隨著資訊科技發展，人們的許多生活方式也跟著改變。然而資訊科技對個人的影響除了帶來便利外，也產生許多個資安全防護議題。

認識資訊安全

當我們享受著資訊科技發展所帶來的便利時，不知不覺中也讓許多的個人資訊在各種媒介與服務之中流傳。例如：社群平台中存有個人的隱私資料、通訊軟體中存有與他人的對話記錄、網路硬碟中存有生活記錄的媒體檔案等。更因為網路的存取便利，如果沒有養成良好的安全防護習慣，可能會導致個人資訊受到披露、盜用或是毀損，產生資訊安全風險的可能性。

廣泛的資訊安全定義是指資訊的機密性（Confidentiality）、完整性（Integrity）與可用性（Availability），簡稱CIA。這三項資訊安全的原則需要同時運作，當缺少任何一項時，所產生的資訊安全風險就會大大提升。

機密性　資訊安全三原則（CIA）

機密性

只有擁有權限的人員或程式，才能存取受到安全機制保護的資料及資源，避免被隨意破壞、存取、使用或竄改。

完整性

只允許有權限的人員或程式可以修改資料內容，使得資料或者資源能夠維持原來的狀態，資料能保存完整。

可用性

當擁有權限的人員或程式提出服務需求時，資訊系統皆會給予服務，並且是可持續使用、享受同樣的服務。

個人生活中經常會使用的電腦與網路、數位金融服務與智慧型手機等，讓大家除了享受便利以外，還需要注意便利的背後可能產生哪些資訊安全隱憂與如何養成良好的使用習慣。

資訊安全

通常是指保護檔案或資訊系統不被未經授權的進入、使用、披露、破壞、修改、檢視、記錄及銷毀。

使用電腦與網路的資安防護

生活中有許多層面都很仰賴電腦與網路的使用，例如：進行輔助學習、休閒娛樂等，但使用時除了帶來便利外也可能遇到資訊安全上的問題。在輔助學習方面的便利有：可利用線上課程平台進行學習、透過網路蒐集資料、使用電腦軟體製作專題作業、進度規劃、學習評量、依賴網路進行檔案存取與交換等。

取得學程

檔案交換

網路蒐集資料

進度規劃

評量

專題製作

資訊科技用於輔助學習

在休閒娛樂方面，許多人透過線上遊戲調劑身心、用於追劇或聽音樂的影音娛樂服務、使用各種線上購物平臺購買各式商品或是美食分享等。

資訊科技用於休閒娛樂


霸凌 按讚，小心個人資料洩漏了！
Copy link
免費
你難道不知道
Watch on YouTube

當我們透過電腦網路享受這些輔助學習與休閒娛樂便利時，許多個人資訊也以數位化形式，存放在方便攜帶的隨身儲存媒體（例如：隨身碟、外接硬碟）、電腦與網路平臺之中。

因這些數位化裝置而產生的資訊安全威脅案例也時有所聞。例如：隨身儲存媒體保管不當遺失、各種網站平臺帳號遭到盜用或是電腦受到病毒感染等，都可能使個人隱私資料受到披露、盜用或毀損而造成損失。

我們仰賴電腦與網路帶來的便利生活時，就更應該時刻提醒自己養成良好的資訊安全態度，以避免個人隱私資料的資訊安全風險。檢視自己是不是每次都有做到以下事項：

運用公共電腦登入系統時，應避免「記憶密碼」，並在使用完畢後登出系統。

不隨意下載不明來源之檔案。

應定期檢查電腦更新，並安裝更新檔。

應安裝防毒軟體，並定時更新防毒版本。


霸凌
電腦病毒□□走
Copy link
有時候他們會讓網路掛掉，
Watch on YouTube

不簡單的密碼設定

由於網路平台的興起，現代人往往有多個系統需要登入，有人因為常常忘記密碼造成無法登入或是帳號被鎖，便傾向將密碼設定得簡單好記就好，或是直接讓電腦「記住密碼」。但忽略了越簡單的密碼也越容易被破解，使用「記住密碼」也容易讓帳號被他人冒用登入！


唉!我帳號被盜了啦...
我也是...
角色東西都不見了...
你們最近登入的情況
還有密碼是什麼？
我在圖書館用電腦
好像忘記登出了...
我常忘記密碼，所
以密碼就改成123
4567了...
這樣不行啦！
使用公共電腦帳號要記得登出
，或是使用無痕模式。
密碼也不要因為好記就設定很
簡單的，這樣才安全哦！

延伸討論

1. 當帳號被盜用且無法再登入時，應該採取什麼行動呢？
2. 除了提升密碼的強度之外，還有什麼方法能降低帳號被盜用的風險呢？

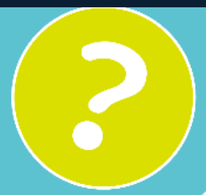
設定密碼時，除了增加字元長度以外，也應避免設定容易被破解的密碼類型，來提升密碼安全性，達到保護個人帳戶內的隱私資料目的。建議絕對不要採用的密碼類型有？

提醒大家除了密碼的安全等級能符合建議之外，最重要的還是個人的使用習慣與態度，否則再安全的密碼遇上個人粗心的使用習慣，也是沒辦法保護我們的資料安全的！

此外，也要留意在無線網路服務隨手可得的環境裡，使用免費Wi-Fi服務時，盡量能夠選用具有Wi-Fi 存取保護（Wi-Fi Protected Access，簡稱WPA）加密傳送的無線網路來使用，對個人的資訊安全可以再多增加一層防護！

Wi-Fi Protected Access

是一種保護無線網路（Wi-Fi）存取安全的技術標準，其中一項是在登入Wi-Fi前，需輸入正確的密碼才能使用網路。



生活中有哪些行為，可能導致自己的資訊安全存在隱憂？應該具備哪些良好的使用習慣呢？

個人數位金融安全防護

資訊科技時代不斷發展出各種服務，同時也改變了人們的交易買賣方式。以往的交易行為主要透過實體貨幣的方式進行買賣，例如：從遠古時代透過貝殼交易發展到今日的紙鈔。現在則發展出了多元的數位支付的方式，例如：行動支付、悠遊卡、一卡通、電子錢包等各種電子交易載具。

數位金融改善人們的金融交易方式並帶來許多便利性，例如：從以往帶著個人身分證件到郵局或銀行臨櫃辦理金融業務。數位化後則可以透過金融服務系統識別個人資訊來進行各項金融業務，或是藉由各家銀行自行設置的網路銀行辦理。

金融業務除了到櫃檯辦理外，
亦可透過網路銀行辦理

轉換

網路郵局
ipost.post.gov.tw

身分證(ID)登入　帳號登入

存簿帳號　劃撥帳號　公債帳號

帳　　號　請輸入14位數字

使用者代號　User Code

網路密碼　Web Password

輸入驗證碼　共四碼　登入

4660　更換

壽險請選擇存簿或劃撥帳號登入　常見問題

LINE Pay Money綁定三倍券
首次連結郵局送100元
早鳥加碼回饋享200點

和數位金融一樣方便的還有使用載具進行交易，例如：智慧型手機的電子錢包、金融卡、悠遊卡等。透過載具交易，讓我們不再被口袋裡大大小小的硬幣困擾。生活中也變得更加快速與便利。

除了硬幣外，亦可透過載具付款

行動支付

行動支付是指使用行動裝置進行付款的服務。在不需使用現金、支票或信用卡的情況下，消費者可使用行動裝置支付各項服務或數位及實體商品的費用。

電子交易載具

泛指可以進行交易扣款、記錄相關交易資訊的裝置或設備，例如：卡片裝置或智慧型裝置等。

數位金融交易帶來便利的同時也產生相對的風險與隱憂。例如：釣魚網站透過模仿網路銀行系統的畫面，騙取使用者的網路銀行帳號密碼來竊取存款；信用卡遭到側錄複製後，產生巨額的盜刷費用；各種卡片載具保管不慎遺失後，讓有心人士拿去盜用，因而蒙受損失；電腦或智慧型手機被入侵或植入木馬後門程式引發異常交易等。

因此當我們享受數位金融時代所帶來的便利時，也應該建立正確的使用態度。除了妥善保管各種金融載具以外，更應該養成使用數位金融時的良好習慣。

安裝行動安全防護軟體的好處，例如：封鎖詐騙惡意網站、阻擋勒索病毒、Wi-Fi 安全性檢查、封鎖惡意程式、手機失竊防護、防假網銀／購物應用程式等安全防護。

- 不要安裝或下載來路不明的金融軟體或 App。
- 網路銀行使用完畢確實登出並且不依賴瀏覽器記憶帳號密碼。
- 智慧型手機的 NFC 感應功能必要時才開啟。
- 電腦使用金融卡片完畢後務必從讀卡機取出。
- 安裝電腦防毒軟體或是智慧型手機專用的行動安全防護軟體。

資料參考來源：趨勢科技行動安全防護

NFC

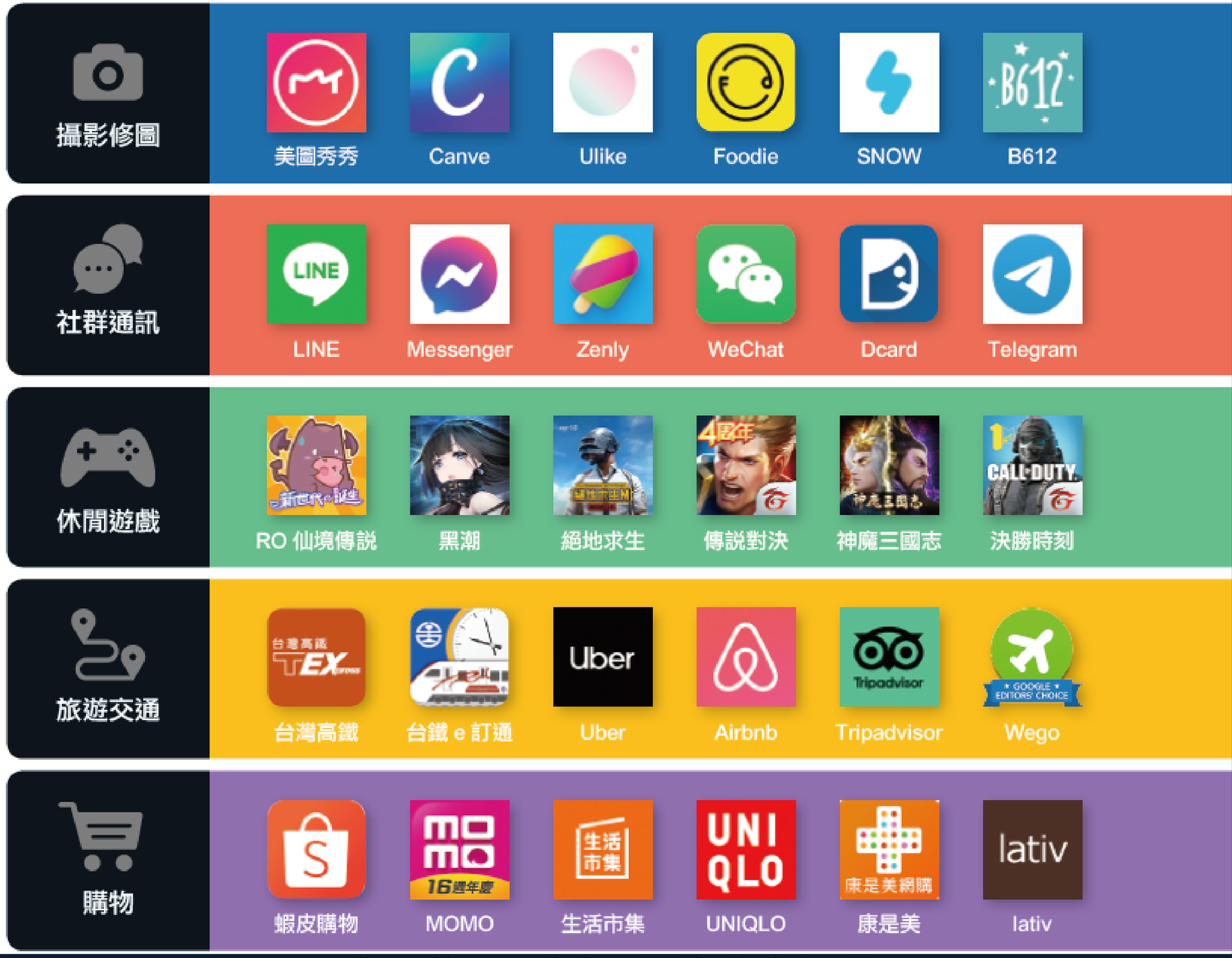
近距離無線通訊（Near-Field Communication，簡稱NFC）是一套通訊協定，可以讓兩個電子裝置進行通訊，進而分享兩個裝置間的內容。

為了避免電子交易載具遭到盜用盜刷，平時應該養成哪些良好習慣，降低可能造成的損害？

智慧型裝置的資安防護

由於行動網路與智慧型裝置的普及，透過安裝各種行動應用程式（Mobile Application，簡稱App）在日常生活中帶來許多便利，例如：攝影修圖App幫助我們留下美好的生活記憶；社群通訊App使我們掌握時勢脈動並維持好友聯繫；休閒遊戲App提供我們暫時放鬆心情調劑忙碌的生活；旅遊與地方資訊App幫助我們了解交通工具的動態、購票或是飯店預訂等服務；購物App可以讓我們不用出門就買到需要的東西等。

除此之外，還有許多不同類型App的推出，都是為了讓我們的生活更便利。



不同類別的App為生活帶來許多便利

不單純的權限開放

在安裝軟體的過程中，你是否注意過服務條款及使用者授權合約？或是為了趕快下載並安裝此軟體，就直接同意開放所有權限？請多留意使用者授權合約並思考授權項目的必要性，否則你的個人資料跟隱私可能正一點一滴地受到侵害喔。


你這張照片好好看喔！
我用這個相機App拍的，超好用!你趕快去載!
需開放以下功能，軟體才可正常運作。
相機
麥克風
位置
訊息和連絡人資訊
不過為什麼要開放這些權限？每個都要允許嗎？
當然要全部允許呀！你看我裝這麼多App ，全都允許手機也沒壞呀！
等一下啦！
不是手機壞不壞的問題哦！是要考慮這些權限合不合理！否則你的個人資料和隱私可能會受到侵害的！

延伸討論

1. 你認為該授權哪些項目給相機App呢？
2. 個人資料及隱私比較可能經由哪些項目開放授權而洩漏出去呢？

智慧型裝置上的App可以為我們帶來許多便利，但背後也隱藏了許多資訊安全上的隱憂，當我們發現不合理的權限要求時，應該提高警覺多方查證，也可以尋找其他功能相似而要求權限在合理範圍內的App來替代。

除相機 App 之外，當我們在生活中越來越依賴智慧型裝置時，同時也可能帶來許多風險隱憂，例如：

- 語音通話在不知不覺中被監聽或錄音。
- 訊息、郵件或瀏覽記錄被監控或披露。
- 聯絡資料、影音檔案等被他人取得或複製。
- 手機儲存的各種帳號密碼、虛擬金融資訊等遭受竊取。
- 行動裝置定位資訊受到監控。

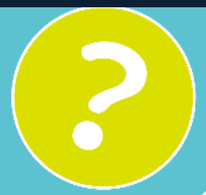
所以，當我們在使用智慧型裝置時，除了確認App權限要求合理才進行下載安裝的良好態度，或是安裝行動裝置安全防護軟體以外，透過Android與iOS系統本身的安全機制也可以為我們的資訊安全增加一道保護。

Android Google Play 安全防護

- 設定啟動密碼保護或圖形驗證。
- 啟用 Google 帳戶雙重驗證。
- 開啟〔掃描裝置中的安全性威脅〕。

iOS AppStore 安全防護

- 設定啟動密碼保護或圖形驗證。
- 啟用 Apple ID 雙重驗證。
- 非必要時不開啟 [App 內購買]。



為使用智慧型裝置的時候，還有哪些行為可能造成資訊安全的威脅？

回顧

資訊科技帶來的便利與資安防護

認識資訊安全

網路的存取便利，如果沒有養成良好的安全防護習慣，可能會導致個人資訊被盜用或是毀損，產生資訊安全風險的可能性。

藉由資訊安全三原則，提醒大家這三項資訊安全的原則必需同時運作，當缺少其中任何一項時，所產生的資訊安全風險就會大大提升。

回顧

使用電腦與網路的資安防護
當我們透過電腦網路享受這些輔助學習與休閒娛樂的便利時，應時刻提醒自己養成良好的資訊安全態度，以避免個人隱私資料、密碼遭到披露、盜用的資訊安全風險。

回顧

☞個人數位金融安全防護

數位金融交易帶來便利的同時也產生風險與隱憂。建立正確的使用態度及妥善保管各種金融載具外，不要安裝或下載來路不明的金融軟體或App。

回顧

☞智慧型裝置的資安防護

智慧型裝置上的App可以為我們帶來許多便利，但背後也隱藏了許多資訊安全上的隱憂。確認App權限要求合理才進行下載安裝，或是安裝行動裝置安全防護軟體，可以為我們的資訊安全增加一道保護。

網路資料使用維護

個人資料保護與著作合理使用

個人資料保護

認識個人資料保護法
保護個人資料的做法

個人資料保護

資訊快速流通且存取更加便利，相對地個人資料外洩或者被不當利用的風險也提高許多，因此個人資料保護的意識與良好習慣更顯得重要。

想一想

哪一些資料屬於個人資料呢？

認識個人資料保護法

個人資料保護法制定的目的就是為了規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料合理利用。

我國有關個人資料保護的法律實施演變過程

民國 84 年時

公布施行《電腦處理個人資料保護法》

民國 99 年時

修法更名為《個人資料保護法》，民國 101、104 年陸續調整修法

權利知多少

人格權

維護每個人的身體、健康、名譽、自由、信用、隱私、貞操等基本權利。

資料財產權

科技記者沃澤爾認為，隱私的核心意義是「控制權」，白話文來說，網路隱私就是個人資料的控制權。

數位公民權

聯合國將網路隱私視為一種基本人權，包含：上網自由、網路言論自由、免於網路霸凌的自由等。

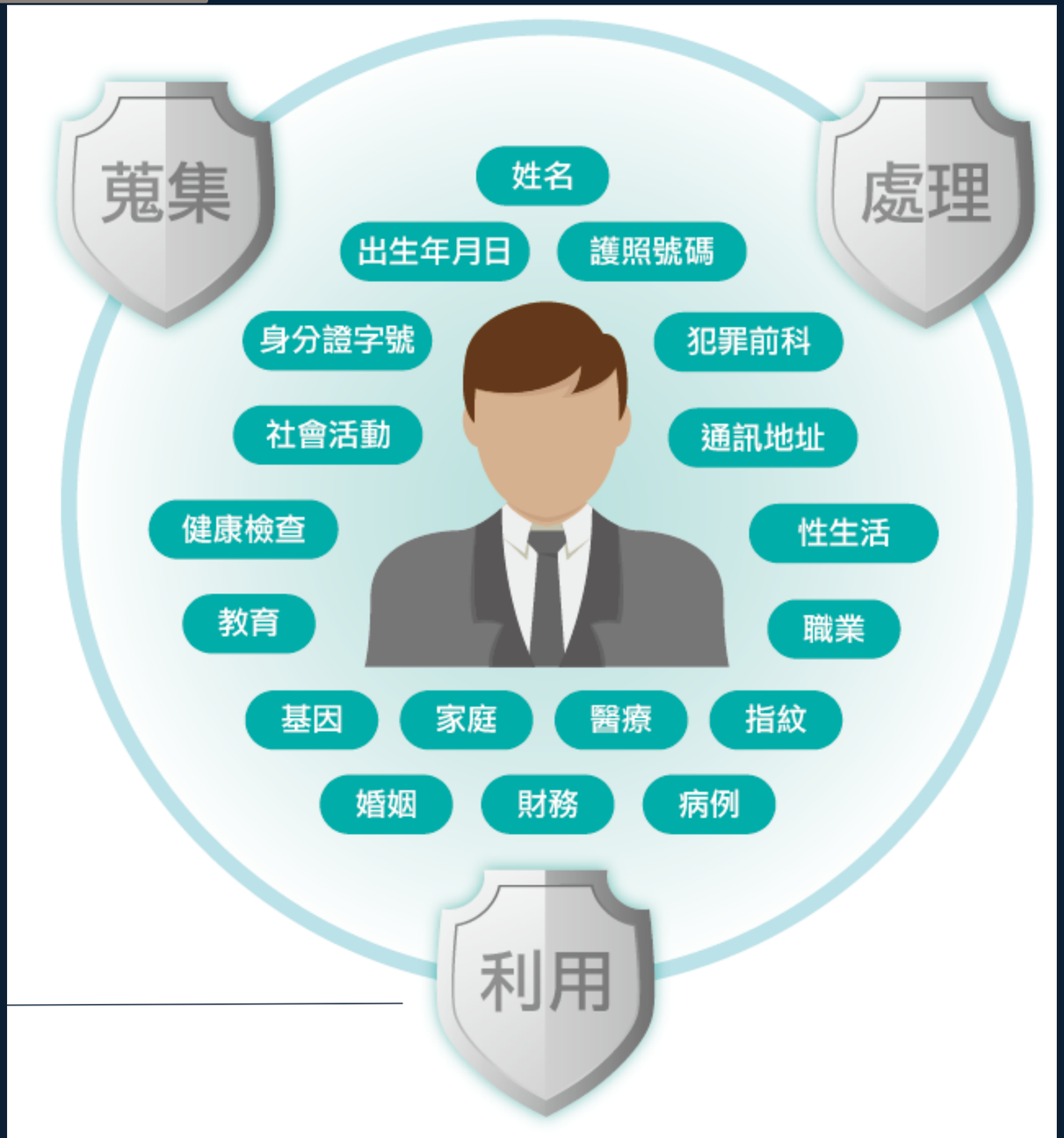
個人資料保護法的內涵

蒐集

指以任何方式取得個人資料

利用

指將蒐集之個人資料為處理以外之使用。



處理

指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。

深偽影片事件

Deepfake
深偽影片事件

2020年至2021年間台灣網紅濫用Deepfake技術的事件

網紅利用人工智慧深偽技術(Deepfake)置換藝人、明星人臉於影片中販售牟取暴利，是否觸犯《個人資料保護法》？

新聞時事通

個人資料保護法作為保護個人資料的重要法律，規範了蒐集者應盡到告知的義務，如果蒐集的資料超越了所告知的範圍或是擅自進行其他應用，都是違反了個人資料保護法，也侵害了個人的權利哦！

保護個人資料的作法

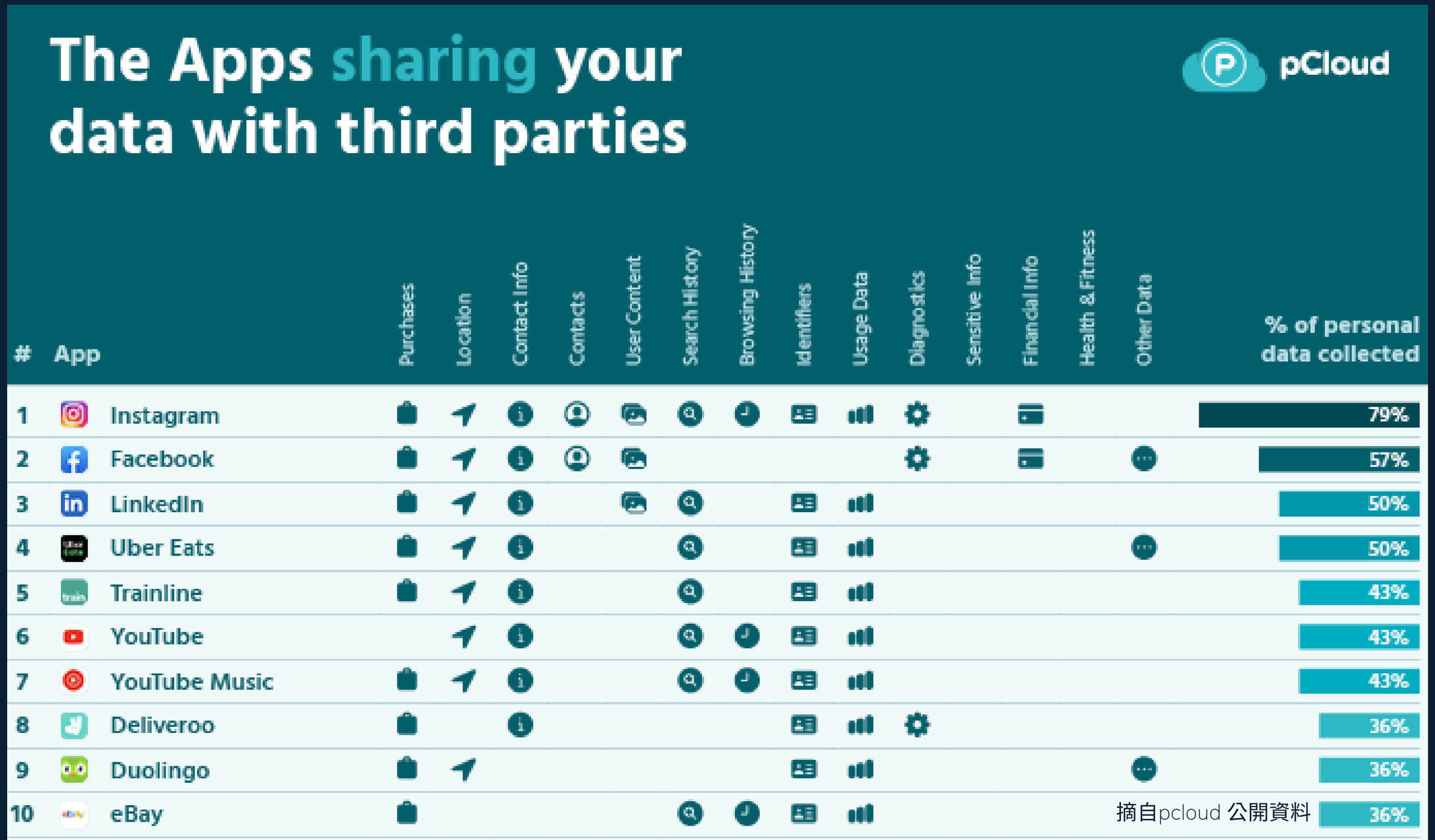
法律對於個人資料蒐集、處理與利用進行規範以外，也賦予我們對於個人資料保護的權利，而且這些權利是不能被事先要求放棄或以合約限制的。

每次安裝APP時，你有詳細閱讀隱私權政策，了解APP會取用哪些個人資料嗎？

個資又不是氣體，要怎麼外洩？


霸凌 你今天打卡了嗎？
Copy link
說不定會發生什麼危險耶！
Watch on YouTube

隱私資料蒐集排行


The Apps sharing your data with third parties
pCloud
App
Purchases
Location
Contact Info
Contacts
User Content
Search History
Browsing History
Identifiers
Usage Data
Diagnostics
Sensitive Info
Financial Info
Health & Fitness
Other Data
% of personal data collected
1 Instagram 79%
2 Facebook 57%
3 LinkedIn 50%
4 Uber Eats 50%
5 Trainline 43%
6 YouTube 43%
7 YouTube Music 43%
8 Deliveroo 36%
9 Duolingo 36%
10 eBay 36%
摘自pcloud 公開資料

保護個人資料的做法

在網路上申請會員時，應詳細閱讀會員條款。

不使用即時通訊軟體傳送個人帳號、密碼等資料。

不要在不可信任或的網站留下個人資料及謹慎點選網路上的超連結。

建立正確觀念與習慣

安裝防毒軟體或防火牆等保護軟體，定期掃毒並時常更新病毒碼。

不要將密碼、其他能識別個人身分等機密資料儲存在電腦硬碟中。

避免使用電子郵件傳遞金融帳號密碼和信用卡資訊。

進行網路線上交易時，使用可信任的電腦，避免使用公用電腦。

不要開啟來路不明的郵件或可疑的附件、檔案等。

回顧

個人資料保護

☞認識個人資料保護法

「個人資料保護法」前身是民國84年公佈施行的「電腦處理個人資料保護法」。個人資料保護法目的就是為了規範個人資料之蒐集、處理及利用，避免人格權受侵害，並促進個人資料合理利用。

個人資料保護法主要從蒐集、處理和利用這三個層面來規範個人資料的合理利用。

回顧

個人資料保護法規範蒐集者應盡到告知的義務，明確告知當事人進行蒐集的機關名稱、蒐集目的、資料類別、資料使用期間、地區、對象及方式、當事人得行使之權利及方式。

回顧

保護個人資料的作法

除了法律所賦予我們的權利，具有正確的觀念與習慣也是保護個人資料不可或缺的一環，尤其我們生活在科技發達與網路普及的時代，防範個人資料不慎在網路上洩漏或遭到詐取更是重要。


霸凌
名偵探阿龍
Copy link
Watch on YouTube

網路使用與社會議題

網路交友與
網路成癮

網路交友
網路成癮

網路交友與網路成癮

由於現代各式社群通訊、影音娛樂等網路服務的興起，人們對於網路的依賴性越來越高，近年來青少年網路交友及網路成癮的相關議題也逐漸受社會大眾注意。

網路交友

隨著資訊科技的普及化，越來越多的中學生有電腦或智慧型裝置可以使用，且每日平均使用時間逐漸拉長，寒假、暑假期間更是學生族群上網的巔峰期，學生們常透過網路進行資料搜尋、休閒娛樂、網路交友等活動。


霸凌 我們的網友
Copy link
你該不會是嫉妒我吧！？
Watch on YouTube

網路成癮

一般而言，網路成癮是指使用者長時間且週期性地使用網路而產生過度依賴的結果，若離開網路一段時間則會產生心理不安、焦慮、憂鬱等症狀，並進一步影響現實生活的作息，嚴重者甚至可能出現暴力或自傷等行為。

如同菸草、酒精、毒品、賭博等已知的上癮物一樣，沉迷於網路的人可能也對網路產生戒斷症狀，容易出現焦慮、憂鬱、憤怒等情緒，且即使知道繼續接觸上癮物可能會危害身心健康或日常生活，卻無法停止此行為，最後達到失控的地步。

現今常見上網行為包括玩線上遊戲、使用社群軟體與他人互動、觀看網路電視影集、瀏覽各式網站等等，若長時間進行上述行為而造成日常生活失序，則較會被認定是網路成癮，現在我們來看看網路成癮的症狀吧。

Q&A

別把自己困在虛擬的世界中...

請大家仔細想想並分享文章中的網路成癮，你是否有相關的經驗，或是周遭的親友們是否有相似的情況發生。

網路成癮會對生活造成許多負面影響，無論是青少年或成年人都須謹慎面對網路成癮的問題，我們可以透過參與多元的休閒活動來釋放生活上的壓力，不一定要靠玩線上遊戲或觀看線上影音來達到放鬆的目的；擬定生涯發展目標並按計畫逐步實行，也可以避免漫無目的地把時間都花在網路上；保持各種交友管道暢通，別僅侷限於網路交友；若真的發現有網路成癮現象，也可盡早向專業醫療人員諮詢。


網路沉迷【你也是藍光人嗎？】
Share
凱凱~~凱凱~~~
Watch on YouTube

回顧

網路交友與網路成癮

網路交友

相較於以往面對面交友，透過網路這個交友管道不必受時空的限制，我們在網路上接觸到他人的機會大幅增加，但網路的隱密性讓人們更不容易看清楚對方的真面目，在與網友做進一步接觸時更需注意自我保護。

回顧

我們在網路交談聯繫階段、見面自我保護階段、事後處理階段都要做好相對應的防護措施，才能減少憾事發生。

回顧

☞網路成癮

長時間使用電腦網路並不一定是網路成癮，須注意有沒有強迫性、戒斷性、及耐受性，若有這些徵兆請誠實面對問題，否則會對生活產生許多負面影響。

回顧

我們可以透過參與多元的休閒活動來釋放生活上的壓力、擬定生涯發展目標並按計畫逐步實行、保持多元的交友管道、或是請求專業醫療人員協助，來降低網路成癮對我們造成的傷害。

網路使用規範倫理

網路使用與社會議題

網路言論與網路霸凌

網路言論自由與責任

網路霸凌

網路言論與網路霸凌

在網路上可以自由、快速且隱密地發表文字及影音資訊，但如果濫用這些網路特性而隨意發表不當訊息，可能會造成嚴重後果並須負起相對應的責任。

網路言論自由與責任

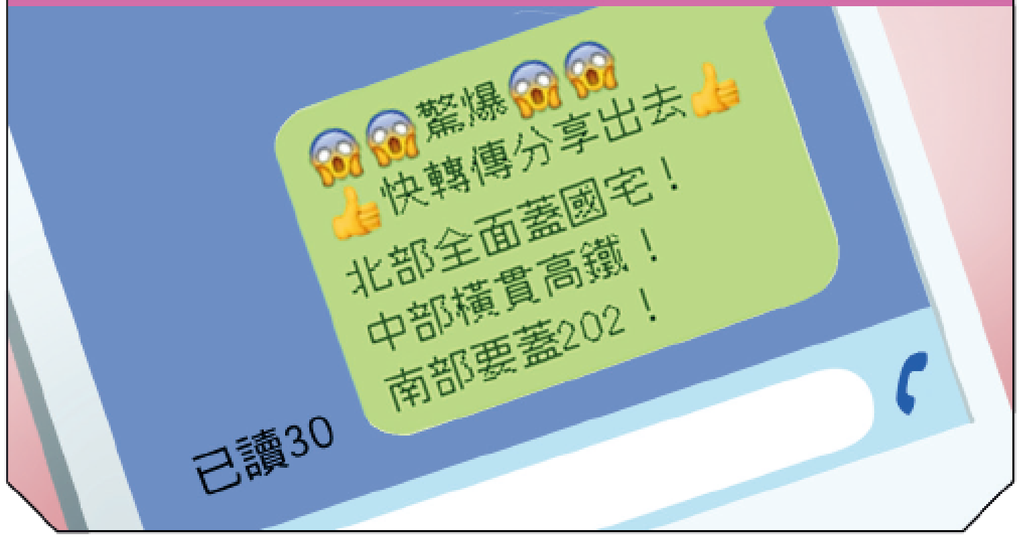
在現今社會中，人與人之間的溝通方式不再侷限於面談、電話、書信聯絡等方式，因透過網路溝通有「不受時空限制」及「訊息內容的多樣化」等特性，皆為一般溝通方式無法取代，以致越來越多人選擇使用網路進行溝通。

從早期的電子郵件，到現在的社群網站、通訊軟體、線上論壇、線上遊戲，人們已逐漸習慣在網路上傳遞文字、圖片、影音等訊息，然而，隨著網路流通的訊息越來越多，這些訊息的真實性，以及訊息是否恰當的問題也隨之而來。

Q: 請大家分享一下，自己曾經看過的假訊息，你怎麼處裡，又該怎麼防範呢?

留言人身攻擊

轉貼假新聞



誹謗店家產品、服務

張貼他人隱私訊息

失控的網路言論

公然侮辱與網路誹謗

凡在網路上透過社群網站、通訊軟體、線上論壇等管道公開發表、轉傳不當訊息或惡意中傷之言論，導致當事人身心受創、名譽受損，或商家營業範疇受損害者，依據其訊息內容可能犯下公然侮辱或誹謗罪。當受害者訴諸法律行動時，若無法掌握對方真實身分，則需要仰賴網路警察以追查電腦位置的方式找到犯人。

►開啟命令提示字元->鍵入 ipconfig->即可查詢到自己的IP位址

如何查看自己IP位址

公然侮辱罪

刑法第309條：「公然侮辱人者，處拘役或九千元以下罰金。以強暴犯前項之罪者，處一年以下有期徒刑、拘役或一萬五千元以下罰金。」

Google

公然侮辱罪

(請大家上網搜尋相關新聞並分享你所看到的)

誹謗(毀謗)罪

刑法第310條：「意圖散布於眾，而指摘或傳述足以毀損他人名譽之事者，為誹謗罪，處一年以下有期徒刑、拘役或一萬五千元以下罰金。散布文字、圖畫犯前項之罪者，處二年以下有期徒刑、拘役或三萬元以下罰金。對於所誹謗之事，能證明其為真實者，不罰。但涉於私德而與公共利益無關者，不在此限。」

誹謗(毀謗)罪

(請大家上網搜尋相關新聞並分享你所看到的)

小強平時在網路上撰寫美食相關文章，並擁有一群死忠粉絲固定收看小強發文的內容。有一天，小強來到了知名牛肉麵店...

Q: 請大家想想，現在的網紅與美食部落客對店家的評價或是業配，造成那些效應?


老闆牛肉麵
我是美食部落客，幫你們寫業配文，讓我先進去吧！
不行，請排隊。
好吃是好吃，可是排了一小時，幹嘛不讓我先插隊，越想越不爽。
1 2
3 4
老闆牛肉麵 90則評論
小強吃透透
根本不好吃，老闆態度惡劣還有蟑螂！噁心！
看我在網路上罵死你，哈哈！
店家看到訊息後，怒告小強誹謗
我們法院見！
申告鈴
對不起！原諒我！

網路霸凌

霸凌是指長時間、重複地對另一方施以負面行為，加害方跟受害方皆有可能是單一個人或一個群體。網路霸凌的加害方可以透過網路很快地將負面訊息傳遞出去，並且可以一整天不間斷地對受害方造成傷害，在社群網站上也更容易發生聚眾情況，使更多人加入一起霸凌受害方。又因在網路上傳遞負面訊息時，大多數是匿名且不用實際接觸受害方，導致現今網路霸凌所造成的傷害比以往更加嚴重。

常見的網路霸凌行為

(請大家分享還有哪些呢)

網路文字

歧視意味

殘酷嚴厲

令人難堪

負面言語

嘲笑

性暗示

私密照被公開

圖像騷擾

照片移花接木

惡意洩漏個資

影片騷擾

恐嚇訊息

不雅文字

不雅圖像

天啊！這不是我！

Copy link

網路霸凌行為可能涉及法律責任

網路霸凌行為	可能涉及法律責任
發表或散播批評、誹謗、不實的言論，包含舉辦或參與惡意票選活動	可能涉及違反《刑法》公然侮辱罪、誹謗罪、民法侵權行為
發表警告、恐嚇的言論	《刑法》恐嚇危害安全罪
上傳或散播不雅、破壞他人名譽的照片／影片，包含移花接木的不實照片	《刑法》公然侮辱罪、誹謗罪、妨害風化罪、妨害秘密罪、散布或販賣猥褻物品及製造持有罪

表格內容取自：親子天下(2021-11-19)。https://www.parenting.com.tw/article/5091342

網路霸凌行為可能涉及法律責任

網路霸凌行為	可能涉及法律責任
上傳攻擊行為的影片	《刑法》傷害罪
公布他人個資，包含人肉搜索後 po 他人個資	《個人資料保護法》、《刑法》妨害秘密罪
盜用他人帳號（以便冒名進行以上行為）	《刑法》無故入侵電腦罪

表格內容取自：親子天下(2021-11-19)。https://www.parenting.com.tw/article/5091342

網路霸凌申訴管道

國家發展委員會於2019年的調查結果顯示，各年齡層都有人表示自己曾遭遇過網路霸凌，其中又以青少年族群自認遭遇過網路霸凌的比例最高，所以在國中階段建立對網路霸凌受害者的支持與幫助管道是相當重要的。

當你或周遭的親朋好友遇到網路霸凌時，除了可以向你信任的師長求援以外，政府或民間單位也有許多求援或申訴管道。

如教育部的「防制校園霸凌專區」，你可以在這個網頁裡寫下事件經過，或直接撥打教育部反霸凌投訴專線（1953），便會有專人協助處理；白絲帶關懷協會的「iWIN網路內容防護機構網頁」上也有網路霸凌的宣導資料、申訴信箱及申訴專線。

教育部 1953 反霸凌專線

iWIN 網路內容防護機構 Institute of Watch Internet Network

教育部防制校園霸凌專區

教育部防制校園霸凌專區參考網址： https://bully.moe.edu.tw/index

回顧

網路言論與網路霸凌

☞網路言論自由與責任

因網路的高度自由與隱密性，有些人在網路上常肆無忌憚地發言，導致公然侮辱與誹謗的事件層出不窮，發表不當言論除了自己可能因此須負法律刑責以外，也對網路世界及整體社會造成相當大的負面影響。

回顧

☞網路霸凌

霸凌是指長時間、重複地對另一方施以負面行為，加害方跟受害方皆有可能是單一個人或一個群體。因網路傳遞訊息速度快、隱匿性高、且訊息難以抹滅等特性， 現今社會中網路霸凌甚至比以往事件來得更加嚴重，切忌不要因一時好玩或衝動，做出助長霸凌事件的行為。

網路使用與社會議題

網路倫理與法律

- 網路倫理規範
- 網路犯罪與法律

網路倫理與法律

在透過網路進行互動時，由於其相對隱密的特性，人們較容易忽略這些禮節，甚至做出觸犯法律的行為。若是每個人能加強網路倫理觀念，並在互動時尊重彼此，相信能共同營造良好的網路環境。

Q: 請大家想想，自己在與人對話的時候，有常常把請、謝謝、對不起掛在嘴邊嗎?

網路倫理規範

相對於面對面溝通的情境，人們在網路世界裡擁有高度的自由及隱密性，也因此較容易忽略彼此應互相尊重的禮節，甚至網路上的負面言語、訊息造成之傷害越來越嚴重，且無法輕易抹滅。制定相應的法律規範固然重要，但唯有每個人加強網路倫理觀念、做好自我規範，方能迎來良好的網路環境。

網路倫理涵蓋的範圍很廣，包含七年級時學到的個人資料保護與智慧財產權相關議題在內，同學們只要記得人與人互動時最基本的「尊重」，便能避免越過倫理規範之界線。以下是在網路上常見的不適當行為，希望同學們能重新檢視自己的上網習慣，避免犯下相同錯誤喔。

轉發不當訊息

在社群軟體蓬勃發展的現代，人們在網路上的社群常常比一般生活的社群還豐富多元，在網路社群裡隨時可以發送訊息相互聊天或是轉發覺得有意思的文章、圖片。但也由於轉發訊息過於便利，部分網路社群版面常被未經證實或刻意捏造的假訊息所佔滿，導致真相難以識別、或其他有意義的訊息不容易被看見，降低社群互動的品質。

轉發 不當訊息


哇！太令人震驚了！
趕快轉傳給大家看！
震撼！
發現外星人！
據可靠消息來源
指出，美國太空
總署收到來自外
太空外星人的訊
息，目前正……
立馬PO臉書
原來真的有
外星人！
趕快發IG
轉發推特

發表

不當言論

即使在網路上發言時可選擇匿名，發言時仍需要謹慎思考，避免造成他人困擾，如果他人要追究你的言論責任或是報警處理，到時就算馬上道歉並刪除訊息，改稱只是開玩笑的請不必當真，仍無法完全免除責任。

發表

不當言論


是小華耶！
可以跟你拍照嗎？
可不可以加好友？
可惡，大家都只注意小華。
1 2 3 4
有沒有校園校草的掛？
整天被一堆人包圍，自以為了不起，看了很不舒服。
小光：看他不爽很久了！
阿南：一起鬧他，報他料啊。
小明：好啊，想鬧他很久了。
大天：他常遲到、挑食 ...
警察局
他愛遲到！不吃青菜！
愛哭鬼！怕了吧！
受不了了！我要去報警
我開玩笑的啦，沒有欺負他，也沒有誹謗他。而且我說的也是事實啊 ...

在網路上發表言論的時候，只要講的都是事實就不會有問題嗎？

網路犯罪與法律

如果每個人都能尊重彼此、以禮相待，或許在網路世界中便不需要制定那麼多法律規範，但總有人會利用網路快速傳播、隱匿性、高度自由等特性，為了金錢或某種特定目的做出違反法律之行為。常見的網路犯罪議題除了網路誹謗及網路霸凌之外，還有網路詐欺與網路駭客，以下將分別說明其定義、法律條文、及案例分析。

網路詐欺

網路詐欺是指在網路上，利用人性弱點進行詐欺的行為。與以往面對面詐欺或是電話簡訊詐欺的手法相似，詐欺犯常設計情境讓被害人陷入恐懼或貪婪的狀態，而人們在那種情況下常無法正常思考並做出錯誤判斷，下場通常是被騙取金錢或其他資源，且不容易追回。

Q: 請大家想想，詐騙電話最常說的口頭禪?
如果是你遇到了，你會怎麼應對呢?

那我也要加入購買這支手機！

由於網路的隱匿性及快速傳播訊息的特點，加上網路購物平台蓬勃發展，線上金流也比實體銀行或ATM匯款方式更為快速，導致越來越多詐欺案是在網路上發生。我們平時可多留意內政部警政署「165全民防騙網」，網站上會有最新的詐欺案例與作案方式，有助於你分辨事情的真偽，或可撥打「165」反詐騙專線進行求證喔。

內政部警政署165全民防騙網

內政部警政署165全民防騙網參考網址： https://165.npa.gov.tw/#/

假網拍交易

詐騙犯常在網路上以低於行情的價格兜售當紅商品，吸引買家上門觀看並詢問問題，此時賣家會在網路上保證是真品，並公告數量有限要搶要快。當買家匯款後，有些賣家會直接消失，或是有時候會寄出假貨，這種情況往往買家難以舉證賣家詐騙的事實，或是要花上很大的心力去跟賣家求償，一不小心還可能被賣家反告網路誹謗

假網拍交易


如果你是買家，
你會怎麼做？
最新款手機
促銷優惠價
只要 999 元
馬上訂購
7:44
這麼便宜，
趕快訂購！
怎麼會是
一臺模型!?

盜用或假冒他人帳號進行詐騙

是指詐騙犯盜用或假冒他人在社群網站上的帳號，再向該帳號之聯絡人進行詐騙。當該帳號傳來訊息時，人們通常會先相信是該帳號主人發言，此時詐騙犯便趁機對被害人提出金錢或其他要求，有些人會認為只是在幫助朋友，便將金錢等資源交給了盜用帳號的詐騙犯。

手法及話術解析

請大家想想下面的情境

（資料來源：內政部警政署刑事警察局）

詐騙集團盜取民眾LINE、IG、FACEBOOK...等帳號，再以盜用帳號傳訊息給其親友。

- 朋友參加攝影比賽，麻煩幫忙投票WWW.XXXX.COM?
- 手機送修，麻煩提供手機號碼，以便接收簡訊認證碼...
- 剛才出車禍急需用錢，可以匯款給我嗎？
- 現在不方便繳錢或匯款，可以幫忙嗎？
- 現在不方買點數卡，可以幫忙買張點數卡嗎？

預防策略

- 當朋友傳送訊息要求協助匯款或代購遊戲點數時，務必提高警覺，撥通電話再行確認。
- 多組帳號勿使用同組密碼，避免因帳號遭破解被盜用，並應定期更改密碼。
- 避免在公用電腦登入私人帳號密碼使用。
- 如果訊息中帶有不明連結，請先向發送訊息的朋友確認。
- 勿下載來源不明或非官方認證應用程式，以免個資外洩。

（資料來源：內政部警政署刑事警察局）

盜用或假冒他人帳號

進行詐騙

常見的

網路攻擊

網路釣魚
勒索軟體
惡意軟體
物聯網風險

資料參考：https://www.cisco.com/c/zh_tw/products/security/common-cyberattacks.html

法律知識站

入侵、破壞電腦之相關法律條文

- 第358條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

別因為好玩，毀了一輩子

法律知識站

入侵、破壞電腦之相關法律條文

- 第359條：「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

開玩笑會需要

付出代價的!!

法律知識站

•第360條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

「戒除貪念」
天下沒有白吃的午餐

法律知識站

•第362條：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

小心謹慎
個人資料不外洩


霸凌
網路如虎口，行人當心走
Copy link
卻很難消掉了。
Watch on YouTube

回顧

網路倫理與法律

☞網路倫理規範

在網路上進行互動時，有些人會忽略基本的禮節，在網路上發表不當的訊息可能會對他人造成相當大的傷害。除了倚賴法律條文約束之外，我們更要加強自身網路倫理觀念，才能迎來更好的網路世界。

回顧

☞網路犯罪與法律

我們常遇到的網路犯罪議題有網路誹謗、網路霸凌、網路詐欺、網路駭客等等， 我們除了須做好自我保護以外，也要注意自身行為避免觸法。

回顧

網路詐欺是指在網路上，利用人性的弱點進行詐欺的行為。當我們透過網路進行交易時，在將金錢或其他物品交給對方之前，請務必再三確認真實性，以免自身權益受損。

駭客的原意是泛稱那些精通電腦知識的專家，主要目的是鑽研資訊技術或改善系統漏洞等。

THANKS!

Any questions?

簡報相關媒材來自於網路，
教材參考自南一、翰林及康軒，
本檔案使用屬學術非營利目的，
版權所有者得要求移除相關資料。