資訊素養與倫理 國中 5 版

編撰：臺北市立北投國民中學 邱森德

網路犯罪大挑戰

網路世界不迷航．資安素養來導航

網路犯罪大挑戰

網路世界不迷航，資安素養來導航

01 一葉知秋•學思並進

1-1 學習目標

- 認識網路犯罪的常見型態及其潛在風險。
- 瞭解性私密影像的保護重要性與相關法律責任。
- 辨識及預防生活中常見的網路詐騙手法。
- 具備基本的網路安全知識，例如零信任架構與加密技術。
- 培養資安風險意識，具備處理網路風險的能力與正確態度。
- 同理及協助網路犯罪受害者，理解正確處理方式。

▶核心素養

- 科-J-A1 具備良好的科技態度，並能應用科技知能，以啟發自我潛能。
- 科-J-B2 理解資訊與科技的基本原理，具備媒體識讀的能力，並能了解人與科技、資訊、媒體的互動關係。
- 科-J-C1 理解科技與人文議題，培養科技發展衍生之守法觀念與公民意識。

▶學習表現

- 運a-IV-1 能落實健康的數位使用習慣與態度。
- 運a-IV-2 能了解資訊科技相關之法律、倫理及社會議題，以保護自己與尊重他人。
- 運a-IV-3 能具備探索資訊科技之興趣，不受性別限制。

▶學習內容

- 資H-IV-1 個人資料保護。
- 資H-IV-2 資訊科技合理使用原則。
- 資H-IV-3 資訊安全。
- 資H-IV-4 媒體與資訊科技相關社會議題。
- 資H-IV-5 資訊倫理與法律。
- 資H-IV-6 資訊科技對人類生活之影響。

▶學習重點

- 法律知識：瞭解散播他人性影像可能涉及的法律責任。
- 網路行為倫理：不製作、不散播、不儲存他人私密資訊。
- 詐騙辨識能力：練習查證資訊、分辨詐騙語氣與假訊息。
- 資訊素養與自我防衛：學習設定安全密碼、辨識可疑連結與網站。
- 數位同理心：建立對網路犯罪受害者的理解與支持態度。

1-2 引起動機

網路犯罪泛指透過電腦、網路或相關科技工具，進行非法的犯罪行為活動，常見的類型有：

- 網路色情：散布或販賣不雅圖片、散布性交易訊息。
- 網路詐騙：以假投資、假親友、假購物等方式，誘使被害人提供財物或個資。
- 網路誹謗：惡意散布不實言論，或冒用他人名義，傷害他人名譽。
- 線上遊戲相關犯罪：竊取他人遊戲帳號、虛擬寶物、裝備、貨幣等行為。
- 侵害著作權：在網路販售盜版軟體、未經許可張貼散佈他人著作。
- 網路駭客：以非法手法入侵或攻擊網站，惡意竊取、刪除或修改相關資料。

網路世界無遠弗屆，打破時空隔閡，蘊涵無限可能，隨著資訊科技的演進，以及AI工具的使用，為現代生活及人際互動帶來嶄新面貌。而科技始終來自於人性，我們身為數位時代的公民，享受科技所帶來的便利生活，不能忽略網路所衍生的新型態犯罪問題，要具備正確的素養與態度，才能適時保護自己，也要學習尊重他人。

03

這叫『深偽技術』，用 AI 模仿聲音或影片來騙人，很難分辨真假！

04

記住喔！遇到可疑來電要『冷靜＋查證＋報警』！

動動腦，想一想

- 你曾經接到陌生人或週遭的親友來電嗎？若對方開口借錢，該如何確認對方的身份與真實意圖？

02 兩全其美•觸類旁通

2-1 主題探索

一、性私密影像的保護

①什麼是性私密影像？

性私密影像一般泛指私下未公開的裸照、性愛影片、私密自拍等含有性感或私密資訊的圖像與影片。雖然這些內容是私人資料，可能因信任對方或受到脅迫而分享，一旦這些影像落入有心人士手中，可能會被惡意散布、販賣，甚至被用於網路勒索，將對當事人造成無法逆轉的嚴重影響。

現今社群媒體與即時通訊軟體的普及，使得私密影像的傳輸變得快速且難以控制。一旦影像被分享，便可能無法完全刪除，即便當事人或上傳者於事後進行刪除，仍可能早已被轉存或再次散布，這樣的行為存在著極大風險。

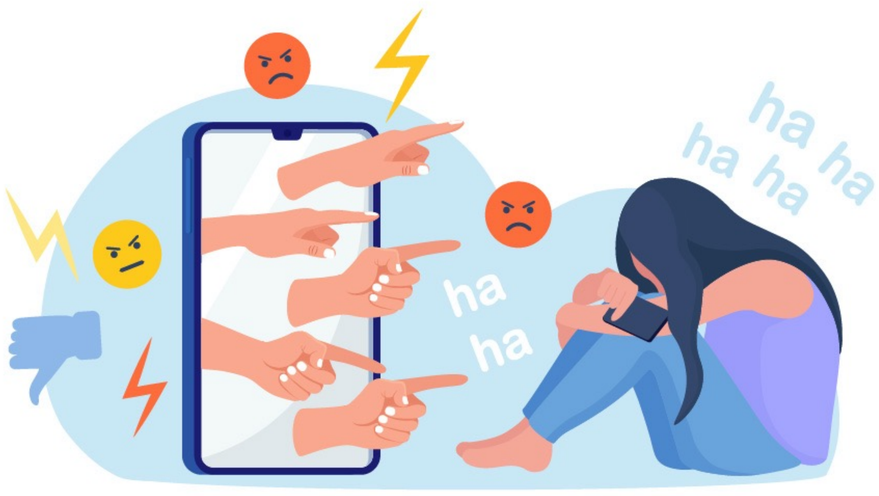
②非自願散布的影響

當性私密影像未經本人同意被公開，可能導致當事人心理與情緒的創傷、造成焦慮、難過與憤怒。同時因隱私被洩露，當事人因恐懼被他人嘲笑，而選擇逃避社交生活，將進一步影響其人際關係與心理健康。隨之而來的網路霸凌也可能進一步加劇當事人的心理壓力，而被貼上羞辱性標籤，或遭到同儕排擠。此外，污名化可能導致當事人未來在求學、求職、交友等方面遭遇困難，長期心理陰影難以消除，甚至因無法承受壓力而選擇自殘或輕生等偏激行為。

③AI深偽（Deepfake）技術的風險與應對

Deepfake（深偽）技術是一種人工智慧影像合成技術，可以讓一個人的臉部或聲音與他人的影片或音訊合成，製造出偽造的影音內容。這種技術若被不肖人士濫用，可能會製作成虛假的性私密影像，用來勒索或將相關影片販售謀利，並藉由網路快速散布，導致受害者名譽受損，或是衍生詐騙行為，造成精神上及財產上的損失，嚴重危害社會秩序。

所以我們應該避免將個人影像上傳至不明網站，並定期檢查個人社交媒體的隱私設定。此外，社群媒體平台與政府單位也積極發展相關技術，來識別與防範深偽內容，並確保個人隱私不受侵犯。



【 社交媒體的隱私設定 】

- 使用公用或借用他人電腦設備後，務必登出個人社交媒體帳戶，避免未經授權的存取行為。
- 適度調整隱私設定層級，選擇誰可以看到自己的貼文和個人資訊。
- 避免過度分享個人敏感信息，例如地址、電話、財務狀況。
- 定期檢視服務條款，了解社交媒體的隱私管理政策。

④法律責任與防制作為

根據《兒童及青少年性剝削防制條例》和《性侵害犯罪防治法》，任何人未經當事人同意，散布、轉傳、儲存或公開他人性私密影像，均可能涉及刑事責任，如果因好奇在網路上進行人肉搜索、談論遭散布被害人之身分隱私，也有可能因此受罰。

行政院性別平等處發布數位/網路性別暴力之定義、類型、及其內涵說明，教育部國教署也提出宣導「五不四要」防護原則：「不」違反意願、「不」聽從自拍、「不」倉促傳訊、「不」轉寄私照、「不」取笑被害；「要」告訴師長、「要」截圖存證、「要」記得報警、「要」檢舉對方。

學校、家長及社會應共同協助受害者走出陰影，提供必要的心理輔導與支持，並尋求相關法律協助。提醒大家不要成為網路犯罪的加害者及被害者，要適時保護自己，也要學習尊重他人。

二、網路詐騙的預防

①常見詐騙手法

網路詐騙手法多樣，最常見的包括：

- 假網拍詐騙：消費者在不明網站購物，付款後卻收不到商品，或收到與描述不符的劣質商品。
- 假投資詐騙：詐騙者會以「高獲利、零風險」為誘因，吸引受害者投入資金，實際上這些所謂的投資平台多為詐騙陷阱，最終無法取回資金。
- 假親友求助：詐騙者假冒親友的身份，聲稱遇到緊急狀況（如生病、臨時急用、投資周轉），誘使受害者匯款。
- 假愛情交友：詐騙者透過交友軟體或社群網站等管道，盜用帥哥、美女頭像照片，假冒他人身份，讓受害者誤入情網，再以境外寄送、禮物關稅、結婚基金、共同投資…等方式，誘騙被害人匯款。

②AI聲音詐騙與影像造假技術

隨著科技進步，詐騙手法不斷演變，有些詐騙集團會利用社群媒體假冒名人，或偽造官方認證，讓受害者誤信其合法性。加上現今AI技術不斷進步演進，詐騙手法變得更為精細。例如，詐騙者可以透過AI合成技術模仿親友的聲音，讓受害者誤以為真實親友在求助。此外，影像造假技術也能用於被用來製作假新聞，讓人們當下難以分辨資訊的真偽。

③識別詐騙及預防策略

識別詐騙：

- 檢查網址：確保網站網址是正確的，避免點擊不明連結。
- 反向圖片搜尋：使用Google反向圖片搜尋，檢查圖片是否被多次使用於不同詐騙案件。
- 識別語言錯誤：許多詐騙訊息含有文法錯誤或不自然的翻譯語意，這些都是常見的詐騙跡象。
- 人際雙重驗證：直接與家人或朋友聯絡確認，不要輕信來自社群媒體或訊息軟體的陌生請求。

預防策略：

- 網路購物應慎選優良有信譽的商家，透過面交或第三方支付平台，確保雙方權益，減少網拍消費糾紛。
- 「高獲利＝高風險」，民眾應深入瞭解自己的投資標的，不要輕信來路不明的網路社群或投資名師。
- 接到親友來電借錢，務必尋求其他人際管道再次確認，避免落入惡意陷阱。
- 與陌生人互加好友要謹慎，不要在言談間透露過多個人訊息，避免與網友間進行借貸往來，不要輕易將金錢交付他人。

三、零信任安全機制

①什麼是零信任架構

零信任架構是一種資訊安全策略，主張不應該預設信任任何人或設備，而無論該請求來自經許可的組織內部或外部，都應該對所有存取要求進行驗證。這種模式的核心概念包括「驗證所有人」、「最小權限存取」和「持續監測」，以降低內部與外部攻擊的風險。

②現代人該有的認知

網路詐騙的型態與手法日益演進，而資訊安全架構有其資源及設計限制，縱使是完備的零信任系統架構，只能降低資安事件的發生風險，無法絕對全面防堵所有漏洞。所以，現代人在使用各種資訊應用服務時，不能僅止於認識單純的功能應用，享受網路所帶來的便利，也必須建立良好的操作習慣及留意系統是否有異常活動紀錄，才得以在數位環境中優遊自得，保護自我安全，遠離網路詐騙的威脅。

③基本的資安素養

- 個人資料保護：減少社群中的公開個資訊息，留意網路服務及社交工具背後的數據收集行為，降低非必要的數位足跡，使用公用設備，記得清除使用紀錄。
- 做好裝置管理：個人電腦與行動裝置，不安裝非法破解的軟體、來路不明的APP、留意APP的非必要授權，避免遭有心人士植入木馬或開啟後門。
- 開啟系統驗證：啟用兩階段驗證（Two factor Authentication，縮寫為2FA）或生物辨識功用，提供額外的驗證程序，各項系統使用後務必正確登出。
- 定期更換密碼：使用強密碼，並定期更換，切勿在不同系統間使用相同密碼，以降低被破解入侵的風險。
- 檢視帳戶活動：定期檢視留意系統是否有異常活動紀錄。
- 留意社交攻擊：對於來路不明的訊息與連結，務必保持謹慎、適時查證，保護個人機敏資料，避免上當受騙。

【 如何清除使用紀錄？ 】

以Google Chrome瀏覽器為例：

- 進入「設定」→隱私權及安全性→刪除瀏覽資料→刪除歷史紀錄、cookie、快取及其他資料
- 可依個人需求，調整清除的時間週期、勾選清除的資料類別。

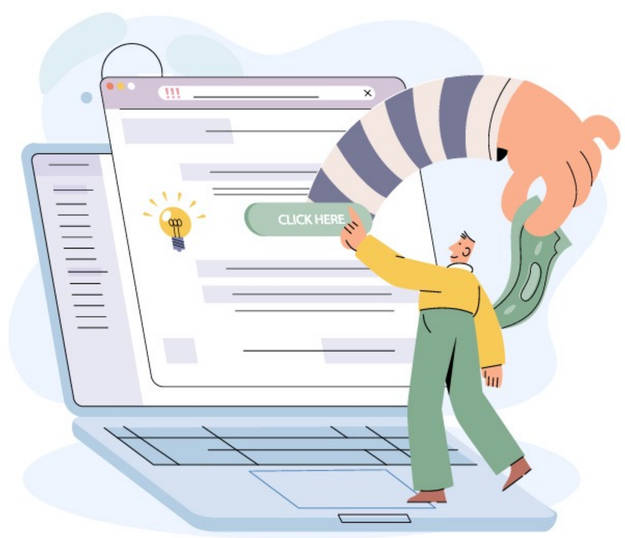
【 密碼設定原則 】

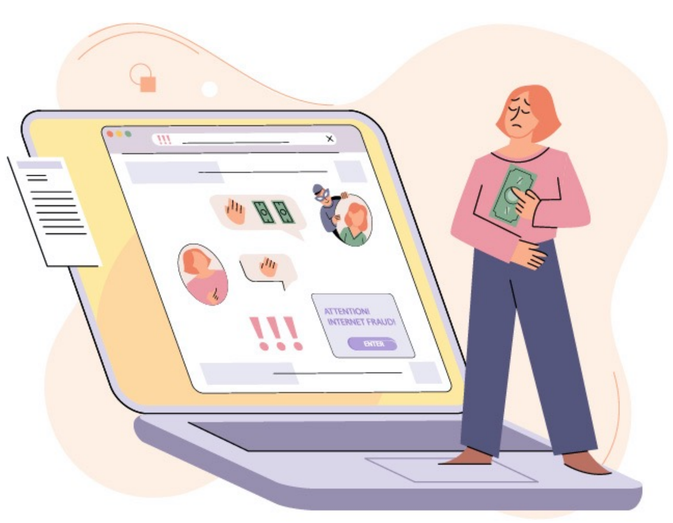
- 密碼的長度愈長愈好，字元數愈多，也會相對增加被破解的時間成本。
- 密碼的組成字元愈複雜愈好，在相同的字元數之下，使用數字、大小寫字母、符號組合的密碼，會比單純使用數字的密碼，大幅提升被破解的困難度。
- 避免使用連續性數字或有意義的單字，降低被暴力破解的風險。

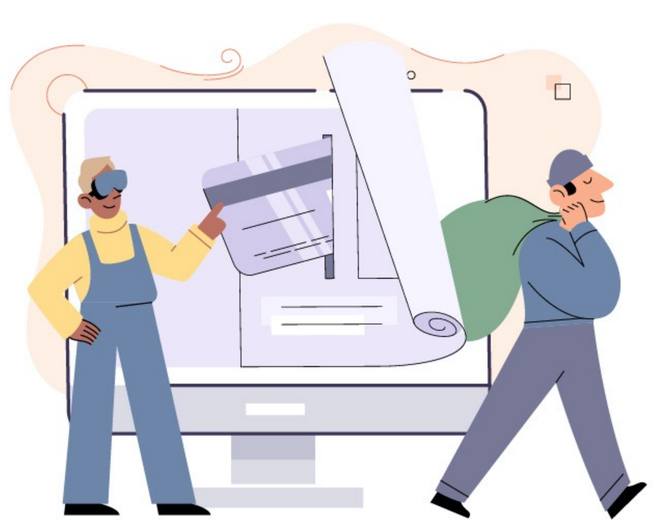
四、案例分析與討論

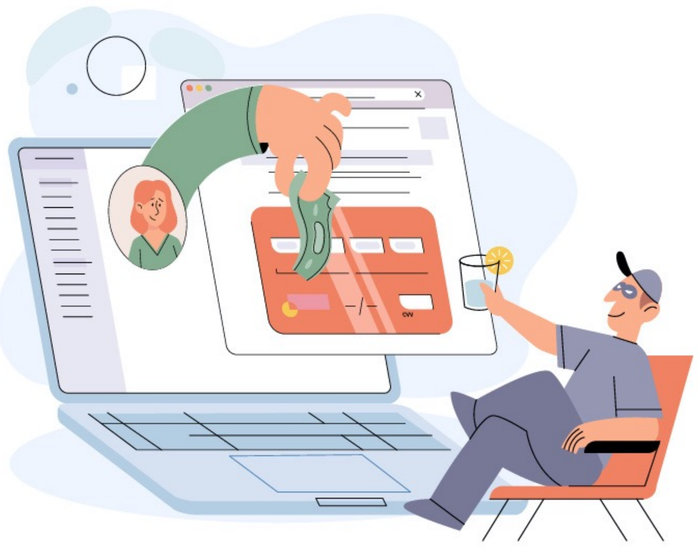
想一想，以下的網路犯罪手法，被害者為何受騙，這些案例有什麼共通之處？

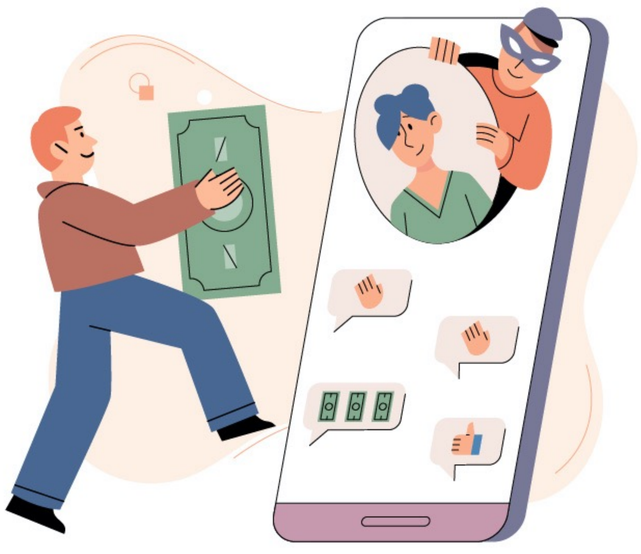
- 釣取個人帳號：以網路釣魚手法，利用手機APP、社群平台或通訊軟體，發送不明連結網址與訊息，謊稱當事人的帳號未驗證，需點入網址進行驗證，藉以盜取帳號或個資，甚至移轉金融財物。
- 變調異國戀曲：以交友軟體的跨國戀曲為糖衣包裝，先與當事人建立信任、培養感情，再以謊稱發生急難事件為由，騙取高額的匯款或資金協助。
- 坑殺投資小白：在網路社群平台或以通訊APP，成立投資社團與群組，謊稱掌握內線交易訊息，或以投資老師授課方式進行包裝，以低風險、高獲利情境，誘使投資者挹注資金，最後無預警蒸發失聯。

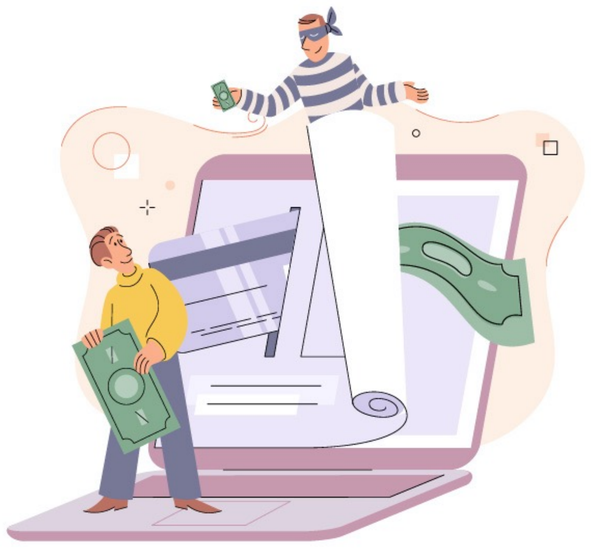












2-2 延伸學習

資訊安全素養：

- 趨勢科技(2024)。如何確保社交媒體隱私。
  取自：https://helpcenter.trendmicro.com/zh-tw/article/tmka-19375
- Fortinet(2025)。網路釣魚電子郵件分析的5個簡單提示。
  取自：https://www.fortinet.com/tw/resources/cyberglossary/phishing-email-analysis
- 中央通訊社(2024)。8字元密碼可在37秒內遭破解 專家建議愈長愈安全。
  取自：https://www.cna.com.tw/news/ait/202405130045.aspx
- security.org(2025)How Secure Is My Password?。
  取自：https://www.security.org/how-secure-is-my-password/
- Wilson說給你聽(2024)。雙重認證 二階段認證(Two factor Authentication)是什麼？有什麼好處？
  YouTube。取自：https://www.youtube.com/watch?v=iuqoerwYtJs

AI衍生犯罪：

- 雷光涵(2025)。日本3名國高中生用ChatGPT寫程式 註冊逾百組行動電話門號轉賣。聯合新聞網。
  取自：https://udn.com/news/story/6809/8577196
- CIB刑事警察局(2024)。冷靜想想反詐系列 EP9【AI深偽來電細分辨 講到匯款查證先】。
  YouTube。取自：https://www.youtube.com/watch?v=bLsaATEFIB0
- 台視新聞 TTV NEWS(2024)。AI深偽技術詐騙新招 淪犯罪工具【熱線追蹤】。
  YouTube。取自：https://www.youtube.com/watch?v=NyhJ1Ize-dk

社交工程攻擊：

- 啾啾鞋(2016)。路上撿到隨身碟，你會…? 超邊緣冷知識－第6集。
  YouTube。取自：https://www.youtube.com/watch?v=7jQF1xWgkrE
- TWCERT/CC台灣電腦網路危機處理暨協調中心(2020)。社交工程因應之道。
  YouTube。取自：https://www.youtube.com/watch?v=XNg8WNBySHs&t=10s

03 三絶韋編•鑑往知來

【數位／網路性別暴力】

隨著網路應用服務的日益普及，現代的學生多數皆為「數位原住民（Digital Native）」，每個人的日常生活大小事已與網路緊密相連，而隱身在網路行為中的惡意文字或不當的圖片影音，若遭有心人士刻意操作，將造成當事人難以抹滅的嚴重傷害。

為重視此議題的影響，行政院性別平等會於110年明確定義「數位/網路性別暴力」，係指：「透過網路或數位方式，基於性別之暴力行為。即針對性別而施加他人之暴力或不成比例地影響他人，包括身體、心理或性之傷害、痛苦、施加威脅、壓制和剝奪其他行動自由等。」相關類型及其內涵整理如表1。

教育部國教署除了傳遞「五不四要」防護原則，也提醒學校師生若遭遇個人私密影像外流，應該儘快尋求「iWIN網路內容防護機構」（https://i.win.org.tw/）或「私ME-成人私密照申訴服務網」（https://tw-ncii.win.org.tw）協助下架，以保障當事人的權益及人身自由。

表1 數位／網路性別暴力之類型及其內涵說明

編號	類型	內涵
1	網路跟蹤	(1)對於他人反覆實施跟蹤騷擾行為，致令他人感到不安或畏懼，如：傳送攻擊或恐嚇性電子郵件或訊息；對於他人網路留言，發表攻擊性言論等。 (2)跟蹤或監視他人活動，如：透過手機GPS定位或電腦、網路使用紀錄等方法為之。 (3)監視或蒐集他人網路活動或資訊，進而違反他人意願與之接觸等。
2	惡意或未經同意散布與性/性別有關個人私密資料	惡意或未經同意而散布與性或性別有關之文字、聲音、圖畫、照片或影像等個人私密資料。
3	網路性騷擾	(1)未經同意逕將猥褻文字、聲音、圖畫、照片或影像等資料傳送他人，如：傳送具露骨性意味之電子郵件或簡訊；於社群網站或網路聊天室發表不適宜或具侵略性挑逗言論等。 (2)對於他人實施性別工作平等法、性別平等教育法或性騷擾防治法所定性騷擾行為。
4	基於性別貶抑或仇恨之言論或行為	(1)對他人之性別、性傾向或性別認同等，發表貶抑、侮辱、攻擊或威脅等仇恨言論。 (2)基於性別，對於他人之行為或遭遇，進行貶抑或訕笑，如：穿著性感、婚前性行為或遭受性騷擾等。 (3)鼓吹性別暴力。
5	性勒索	以揭露他人性私密資料（文字、聲音、圖畫、照片或影像等）為手段，勒索、恐嚇或脅迫他人。

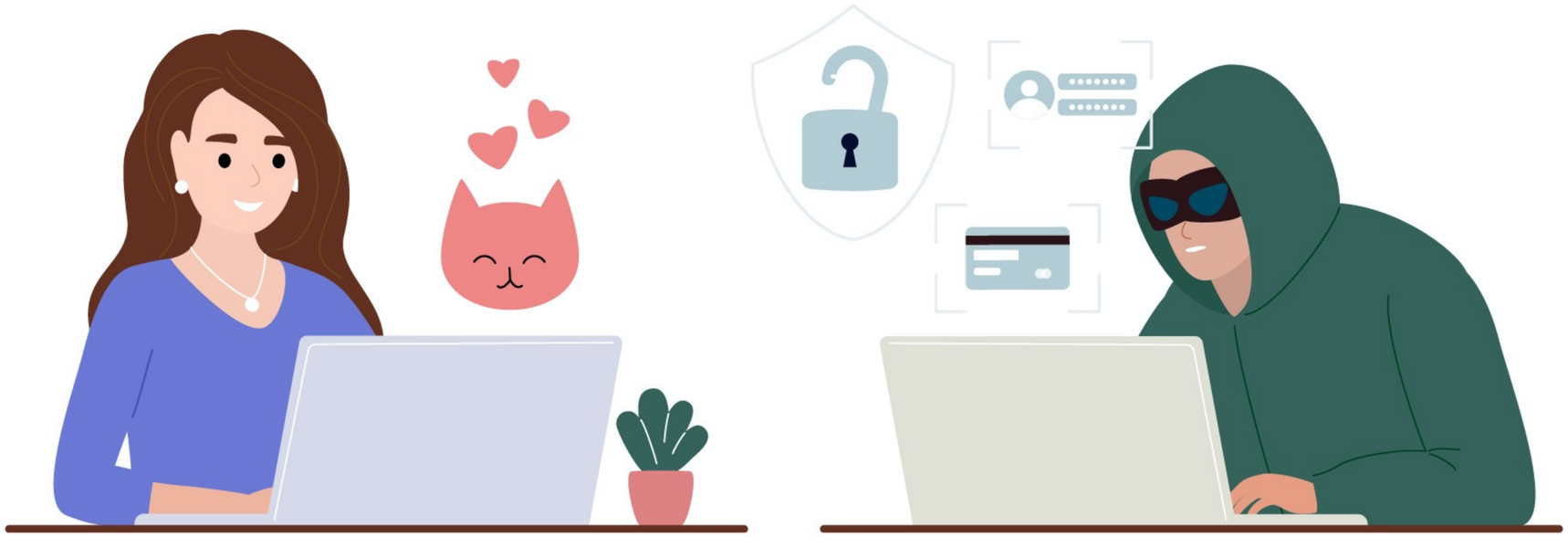


表1 數位／網路性別暴力之類型及其內涵說明

編 號	類 型	內 涵
6	人肉搜索	透過網路搜索取得與散布未經他人同意揭露之文字、聲音、圖畫、照片或影像等私密資料。
7	基於性別偏見所為之強暴與死亡威脅	基於性別偏見，以強制性交或加害生命之事恐嚇他人，使他人心生畏懼者。
8	招募引誘	係指運用網路或數位方式遂行人口販運，如：佯稱提供工作機會，或使用盜用之圖片、內容製作虛假廣告，引誘他人賣淫；抑或從事人口販運者，利用網路聊天室等傳遞人口販運訊息或進行廣告等。
9	非法侵入或竊取他人資料	非法侵入他人電腦或相關設備，以觀覽、取得、刪除或變更他人個人資料等，如：侵入網路攝影機取得他人影像資料等。
10	偽造或冒用身分	偽造或冒用身分，以取得他人個人資料、侮辱或接觸他人、損害他人名譽或信用、遂行恐嚇或威脅，或據以製作身分證件供詐欺之用等。

＊資料來源：行政院性別平等會（2021）。《數位/網路性別暴力之定義、類型及其內涵說明》。
取自：https://gec.ey.gov.tw/Page/ED8994F4EF5AD73E/2ab74b7e-0bdb-4067-b43a-4a3cfc9e2a1e

實踐活動

①「數位足跡模擬」：學生分析自己社群媒體上的公開資訊，思考是否可能被不當利用。
②「假新聞測試」：學生判斷某則新聞是否為深偽技術製作。
③「詐騙解碼遊戲」：老師提供多種詐騙訊息，學生分組找出詐騙特徵。
④「網路偵探」：學生使用Google反向圖片搜尋，檢查某些網購商品圖片是否來自可疑網站。
⑤「帳號安全測試」：學生檢查自己社群媒體的隱私設定，調整為最佳安全狀態。
⑥「釣魚郵件挑戰」：老師提供模擬釣魚郵件，學生找出可疑點。

【如何分辨釣魚郵件？】

- 看似正確但可疑的郵件位址或網域名稱。例如：username@g00gle.com。
- 郵件的主旨或內容，存在威脅性或緊急性字句。例如：謊稱網路銀行或社交媒體帳戶遭到入侵，誘騙使用者降低戒心，按下特定連結進行變更，藉此取得用戶帳密及個資。
- 夾帶非必要的可疑附件或安裝檔案。例如：要求使用者下載安裝來路不明的特定程式，藉機植入木馬，開啟後門。

創意挑戰

①「防駭密碼挑戰」：學生測試自己密碼的強度，並設計一個安全又易記的密碼規則。
②「網路安全海報設計」：學生設計一張宣導海報，提醒同學如何保護私密影像。
③「防詐騙短影音」：學生拍攝30秒短片，向家人或朋友解釋一種詐騙手法及應對方法。
④「法律守護者」：學生以漫畫或短篇故事形式，描述如何利用法律保護自己免受網路犯罪侵害。

動動腦，想一想

隨著各種AI工具的快速崛起，網路詐騙的樣態也隨之演變。「水能載舟，亦能覆舟」，請討論我們可以如何應用AI工具學習知能，進而降低被網路詐騙的機會？

04 四通八達・小試身手

Q1 什麼是性私密影像？請舉出兩個例子。

Q2 如果有人未經你的同意散布你的私密自拍，會對你造成哪些心理與社會影響？

Q3 什麼是「深偽技術（Deepfake）」？這種技術可能會被用來做什麼壞事？

Q4 根據《兒少性剝削防制條例》，散布未成年人的性私密影像會有什麼法律後果？

Q5 如果你看到同學在傳播別人的裸照，你會怎麼處理這件事？
請說明你的行動與理由。

Q6 請寫出兩種你曾聽過的網路詐騙手法。

Q7 AI詐騙聲音是什麼？為什麼這種詐騙特別危險？

Q8 假如你接到一個語音電話，自稱是你媽媽，要求你轉帳，
你會怎麼處理？

Q9 請說明如何利用「反向圖片搜尋」來判斷網路圖片的真實性。

Q10 台灣曾發生過哪些網路詐騙案例？請簡述一個並說明詐騙手法。

Q11 什麼是「零信任安全」？請用自己的話簡單解釋。

Q12 為什麼「不輕信陌生人」是網路安全的重要原則？請說明原因。

Q13 什麼是兩階段驗證？請舉出你曾經使用過的一次驗證方式。

Q14 公共Wi-Fi有什麼安全風險？你使用公共Wi-Fi時會注意什麼？

Q15 請舉出三個安全使用密碼的好習慣。

Q16 你看到一則廣告寫著「一天賺10萬元」，而且附上LINE連結，你會怎麼做？為什麼？

Q17 如你朋友的IG帳號突然傳訊給你說他急需借錢，你要怎麼判斷這是不是詐騙？

Q18 你在YouTube上看到一段深偽影片模仿名人說話，你會如何判斷影片真偽？

Q19 如果你曾經在網路上分享過太多個人資訊（如住址、生日、學校），你現在該怎麼補救？

Q20 請寫下你認為在網路世界中最重要的安全守則，並說明理由。

參考資料

中文文獻：

- 教育百科(2023)。網路犯罪。民國112年6月11日，
  取自：https://pedia.cloud.edu.tw/Entry/WikiContent?title=網路犯罪

- 臺北市政府警察局士林分局(2025)。反詐欺犯預防宣導-防詐騙十招。民國114年2月27日，
  取自：https://sl.police.gov.taipei/cp.aspx?n=9C2331B90687BDBE

- 行政院性別平等會。數位/網路性別暴力之定義、類型及其內涵說明。
  取自：https://gec.ey.gov.tw/Page/ED8994F4EF5AD73E/2ab74b7e-0bdb-4067-b43a-4a3cfc9e2a1e

- 教育部(2022)。拒絕網路性暴力！國教署落實師生性平教育。民國111年6月15日，
  取自：https://www.edu.tw/News_Content.aspx?n=9E7AC85F1954DDA8&s=70631A3ABB17FF18

- 艾迪(2024)。AI深偽色情急增，如何才能制止新型性暴力？端傳媒。民國113年3月27日，
  取自：https://theinitium.com/article/20240328-whatsnew-international-ai-deep-fake-governance

- 內政部警政署刑事警察局(2025)。常見的詐騙手法語術解析與因應之道。民國114年6月2日，
  取自：https://www.cib.npa.gov.tw/ch/app/data/list?module=wg116&id=1909

- Google Cloud 線上支援。什麼是零信任安全機制。
  取自：https://cloud.google.com/learn/what-is-zero-trust?hl=zh-TW

- 王若桐(2025)。台灣最新詐騙手法「存款個資全被騙光」，這些平台一堆人受害。風傳媒。
  民國114年2月5日，取自：https://www.storm.mg/lifestyle/5318732

- 江雁武(2025)。七旬翁險遭「假交友」騙走積蓄，警30秒急奔攔詐。Yahoo!新聞-警政時報。
  民國114年2月24日，取自：https://tw.news.yahoo.com/七旬翁險遭-假交友-騙走積蓄-警30秒急奔攔詐-012735577.html

- 袁志豪、游明煌(2025)。不只中高齡，詐騙受害多年輕人。聯合新聞網。民國114年2月21日，
  取自：https://udn.com/news/story/7315/8561933

資訊素養與倫理 國中 5 版

出　　版 / 臺北市政府教育局
召 集 人 / 湯志民 臺北市政府教育局局長
副召集人 / 卓育欣 臺北市政府教育局資訊教育科科長
　　楊啓明 臺北市立明德國民中學校長
指導委員 / 賴阿福 臺北市立大學教授
　　盧東華 臺北市立大學助理教授
諮詢委員 / 曾文龍 臺北市立 育成高級中學校長
　　陳玫良 臺北市立北安國民中學校長
總 編 輯 / 黃耀祺 臺北市立明德國民中學教務主任
編審委員 / 邱森德 臺北市立北投國民中學主任
　　洪瑞甫 臺北市立龍山國民中學主任
　　林國星 臺北市立明德國民中學教師
　　陳柏亨 臺北市立北安國民中學主任
　　陳妤蓁 臺北市立明德國民中學教師
　　陳俊宏 臺北市立明德國民中學教師
　　郭怡君 臺北市立明湖國民中學教師
　　葛允文 臺北市立明德國民中學資訊組長
　　（按姓氏筆畫排列）
承辦單位 / 臺北市立明德國民中學
出版日期 / 中華民國114年6月

網路犯罪大挑戰

網路世界不迷航，資安素養來導航