資訊素養與倫理 高中職 5 版

編撰：臺北市立南港高級中學 陳哲雋 老師
臺北市立復興高級中學 陳　晉 老師

網路犯罪大挑戰

詐騙篇

網路犯罪大挑戰

詐騙篇

01 ▶ 一葉知秋 學思並進

1-1 學習目標

▶ 核心素養

- 科S-U-A2(普通高中)運用科技工具與策略進行系統思考與分析探索，並有效解決問題。
- 科V-U-A2(技術高中) / 科C-U-A2(綜合高中)具備系統思考與分析探索的能力，並能整合科學、科技、工程、藝術與數學等方法及工具，有效處理與解決問題。
- 科S-U-B2(普通高中) / 科V-U-B2(技術高中) / 科 C-U-B2(綜合高中)理解科技與資訊的原理及發展趨勢，整合運用科技、資訊、媒體及媒體， 並能分析思辨人與科技、社會、環境的關係。

▶學習表現

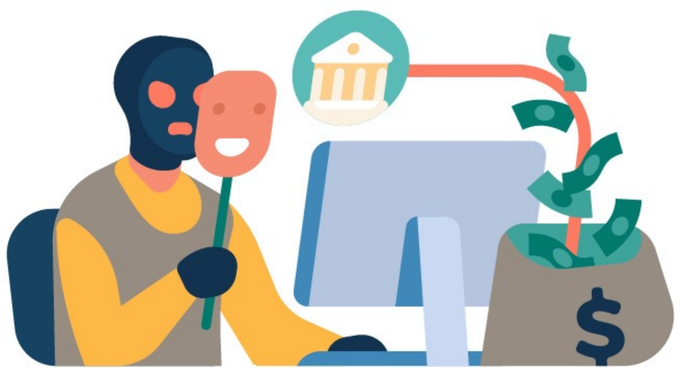
- 運t-V-1(普通高中)能了解資訊系統之運算原理
- 運p-V-1(普通高中、技術高中、綜合高中)能整合資訊科技進行有效的溝通表達。
- 運a-V-1(普通高中、技術高中、綜合高中)能實踐健康的數位公民生活。
- 運a-V-3(普通高中、技術高中、綜合高中)能探索新興的資訊科技。
- 設a-V-1(普通高中、技術高中、綜合高中)能主動控索科技新知。
- 設k-V-3(普通高中、技術高中、綜合高中)能分析、思辨與批判人與科技、社會、環境之間的關係。

▶學習內容

- 資H-V-1(普通高中、技術高中、綜合高中)資訊科技的合理使用原則。
- 資H-V-2(普通高中、技術高中、綜合高中)個人資料的保護與資訊安全。
- 資H-V-3(普通高中、技術高中、綜合高中)資訊科技對人與社會的影響與衝擊。

▶學習重點

- 能夠理解並實踐零信任原則。
- 能有效進行資訊判讀及網路連結安全檢視。
- 能認識網路來源及對資訊隱藏的風險有所認知。



1-2 引言

在當今資訊爆炸的數位時代，個人面對網路資訊時，應以「零信任」原則檢視內容。「零信任」原則強調對任何網路資訊均預設不信任，並主動進行批判性評估與驗證。網路資訊的快速傳播、易於製造以及無法有效確認來源的特性，使得不實資訊、假新聞、網路謠言及惡意連結氾濫，對個人判斷、人與人間的信任均構成威脅。提升全民數位素養，特別是媒體識讀能力、批判性思維以及網路安全意識，並善用查核工具，是應對此挑戰及預防相關風險的關鍵素養能力。

02 ▶ 兩全其美 觸類旁通

2-1 主題探索

2-1-1 網路零信任

數位時代的蓬勃發展，我們每天都被大量的資訊與無數的網路連結所包圍，使用者經常需要透過網路連結獲取資訊。然而這也潛藏著不容忽視的風險，透過惡意連結與假資訊進行網路詐騙時有耳聞，沒有足夠素養與安全意識的使用者可能難以辨識，容易經由惡意連結點擊偽冒的登入頁面、含有惡意程式的下載連結或被導向詐騙網站，也容易受假資訊誤導提供個人資訊或被詐騙，進而導致個人資料洩露、帳號被盜用、設備受入侵…等，甚至進一步造成財產損失。在2025年1月就發生過有多名臺北市教師收到假冒臺北市單一身分驗證服務之釣魚信件，信件中連結之網站也是仿照臺北市單一身分驗證服務登入頁（如圖1-1）。若使用者在釣魚網站嘗試輸入帳號密碼，就可能使帳號密碼被盜用，但其實利用網址就能發現該釣魚網站的網址並非正確的「ldap.tp.edu.tw」，藉此避免受害。

寄件者：[redacted]<adminsso@gs.tp.edu.tw>
日期：2025年1月8日 週三，19:04
主旨：【臺北市校園單一身份驗證服務】
收件者：<adminsso@gs.tp.edu.tw>

臺北市校園單一身分驗證服務

嗨！因為系統接收到賬號驗證要求，所以寄這封信件給您！

請點選以下連結登錄單一身份賬號驗證

請點選此處確認賬號

請於114-3-1 23:59 前完成賬號驗證，謝謝。

臺北市校園單一身分驗證服務 敬上

********** **********

请注意：本邮件系统自动传送，请勿直接回覆此邮件！

********** **********

© 2024 臺北市校園單一身分驗證服務 版權所有

臺北市校園單一身份驗證服務

帳號

請輸入帳號

密碼

請輸入密碼

忘記帳號/密碼

登入

尚未有帳號？親子帳號申請

台北通登入

常見問答

加入好友

圖1-1 2025年1月曾有多名教師收到假冒臺北市單一身分驗證服務之釣魚網站

伴隨數位時代而來的資訊真偽與網路安全威脅辨識是資訊素養的重大課題，在資訊判讀的脈絡下，應抱持「零信任」原則，對所有網路的來源資訊及連結均抱持不輕易相信的態度。這項原則的核心概念是「永不信任，總是驗證」，這意味著使用者在接受及使用任何網路資源、接收網路資訊或進行網路活動時，應先思考其潛在威脅並且養成謹慎查證的習慣。

在接收網路上的資訊前應先假設其可能為不實或片面，並主動採取查證措施，幫助我們在複雜的網路環境中，做出更明智、更安全的判斷。這包括：

- 注意網站類型：

檢視網址中的「網域」來判斷其網站類型，藉由網址我們可以先嘗試了解網站類型（可參考表1-1及表1-2內容判斷）。一般說來，政府單位、教育學術及研究機構和非營利機構等組織的相關資訊較為可信，另外從網址上也能看出網站來源，能用以判別釣魚網站，如前面釣魚網站案例中，可以藉由檢查網址是否為「ldap.tp.edu.tw」來進行判斷（如圖1-2）。

圖1-2 能利用網址列顯示的網域於辨識網站是否非釣魚網站，以單一身分驗證服務為例，正確網域應為ldap.tp.edu.tw，非此網域就是釣魚網站

表1-1 各類型網站特徵 資料來源：取自吳清基、林宜隆（2009）

類 型	特 徵
個人網站 .idv	1. 網站多是用於宣傳或分享個人的信念及所得。 2. 網頁資料可能缺乏編審標準來保證其可信度、正確性及客觀性。
商業性網站 .com	1. 網站主要目的是販售商品。 2. 廣告及公共關係是促銷商品的主要方式。 3. 有時使用者可在網站上找到與相關領域有關的、有價值的資料。
學術教育網站 .edu	1. 網站上的資訊通常比較嚴謹、可信度高。 2. 使用者可以在網站上找到和教學相關的資料、教育性的研討會論文集，以及來自於電子期刊的學術性文章。
非營利性網站 .org	1. 網站多是由專業組織主持。 2. 主要目的是提供專業推廣及意見交流。 3. 使用者可找到學術性的研究報告。
政府官方及國防軍事單位 .gov / .mil	1. 政府各部門（含軍方）提供政務與公共服務的資訊。 2. 使用者可找到學術性的研究報告。

表1-2 網域屬性及其網站類型

網域屬性	網站類型	網域屬性	網站類型
.com	商業團體或組織	.aero	航空業界使用
.edu	教育學術及研究機構	.coop	合作機構用
.gov	政府單位組織	.ebiz	商業機構使用
.info	一般資訊用	.idv	個人網頁
.int	國際性組織	.jobs	就業相關網站使用
.mil	國防軍事單位	.museum	博物館使用
.net	網路管理或服務機構	.name	個人登錄
.org	民間組織	.pro	專業人士或機構登錄

- 檢視來源：

  查明資訊的原始出處、作者背景及發布機構的可信度。了解資訊來源是否權威，是否有偏頗立場，是評估其可信度的重要依據。

- 交叉比對：

  從多個不同來源獲取資訊，比較其一致性與差異性，有助於我們拼湊出更完整的真相。

- 分析內容：

  檢查資訊的邏輯性、證據支持及是否存在偏見或情緒性語言。同時，留意資訊的發布日期，避免引用過時的資訊。

- 辨識意圖：

  思考資訊發布者可能的動機，他們是為了單純地告知、說服讀者、提供娛樂，還是有誤導或傳播錯誤資訊的意圖？理解發布者的潛在目的，有助於我們更客觀地判讀資訊。

在進行網路活動時，保持「永不信任，總是驗證」態度，將所有網路活動視為潛在威脅，即使是來自內部網路的連線也不例外。我們在對網頁連結進行點擊行為前，不應預設任何連結是安全的，而應在點擊前主動進行查證：

- 仔細檢查連結網址：

  我們在點擊任何連結之前，可以先將滑鼠游標停留在連結上（不要點擊），查看左下角或工具提示中顯示的實際網址，並留意是否有拼字錯誤、不尋常的字元，或與預期網站名稱不符的網址。詐騙網站常常會使用與合法網站非常相似的網址來欺騙使用者。

- 確認傳送者身分：

  當我們收到藉由電子郵件或訊息傳送的連結，務必確認傳送者的真實身分並留意可能的假冒行為。我們可以嘗試透過其他管道（例如電話或面對面）與對方確認該訊息是否為其本人發送。

- 對異常要求提高警覺：

  當我們收到任何來源要求提供個人資訊、帳號密碼，或點擊連結下載檔案的訊息都應提高警覺。正規的機構通常不會透過非官方網站或私人管道來要求這些敏感資訊。

- 使用瀏覽器安全功能：

  大多數現代瀏覽器都內建了惡意網站偵測功能，我們應確保這些功能已啟用，並且注意瀏覽器的警訊，同時定期更新瀏覽器，以獲得最新的安全防護。

- 小心非預期出現的各種警訊與檔案：

  如果我們在瀏覽網站時畫面上彈出奇怪的視窗及警訊，或突然開始下載檔案，要小心這可能是駭客藉由暗藏惡意的程式碼到網站中，當使用瀏覽網站時自動觸發執行，應立即關閉網站並刪除下載內容，同時可藉由防毒軟體掃描電腦確保安全。

「零信任原則」並非單純要求我們對所有事物都抱持懷疑，而是一種負責任的資訊素養與倫理習慣，提醒我們在享受網路便利的同時，仍需具備風險意識。透過在資訊判讀與網頁連結點擊上實踐這項原則，我們能保護個人隱私與資產安全。

2-1-2 網路陷阱多，法律來把關：案例中的智慧

在前面我們已經理解了「零信任」——也就是對網路上的任何資訊來源都先抱持懷疑、謹慎查證的態度。那麼，如果我們忽略了這些原則，不幸成為網路犯罪的受害者，或者更糟的是，無意間成為他人犯罪的幫兇，我們可能會面臨哪些法律問題呢？

透過真實的法院判決案例，帶領大家一窺網路犯罪的樣貌，並了解相關的法律規定。讓我們從這些案例中學習，不僅保護自己，也更懂得尊重他人的權益。

案例一：釣魚簡訊的誘惑－「國泰世華銀行」也遭殃！

（改編自：臺灣臺北地方法院113年度訴緝字第53號刑事判決）

週末下午，小陳正在和朋友用通訊軟體熱烈討論下週校慶園遊會的攤位佈置，手機突然「叮咚！」一聲，跳出一則簡訊。寄件人顯示為「國泰世華銀行」，內容寫著：「【國泰世華】您的網路銀行帳戶因系統升級，為確保帳戶安全，請立即點擊下方連結進行驗證，否則帳戶將暫時凍結。」簡訊末尾還附上一個看起來很像官方網址的短連結。

小陳心頭一驚，他平常有用國泰世華的網銀繳手機費和買遊戲點數，要是帳戶被凍結就麻煩了。他一邊想著園遊會的事，一邊也沒多想，手指便自然地按下了簡訊中的連結。

連結打開後，出現了一個和國泰世華銀行官方網站幾乎一模一樣的登入頁面，連Logo、排版、色調都做得維妙維肖。小陳不疑有他，迅速輸入了自己的網路銀行帳號和密碼，接著又按照頁面指示，輸入了手機收到的「驗證碼」。頁面顯示「驗證成功，感謝您的配合！」後便自動跳轉回銀行的官方首頁。

小陳鬆了一口氣，繼續和朋友討論校慶的事。直到傍晚，他想用網銀轉帳買園遊會要用的材料時，才赫然發現自己帳戶裡的幾萬元存款竟然不翼而飛！他急忙打電話給銀行客服，客服人員查詢後告訴他，他的帳戶在下午被人從不同的IP位址登入，並將款項轉出到數個陌生帳戶。客服人員也確認，銀行並未發送那樣的系統升級簡訊。小陳這才恍然大悟，自己點進的是詐騙集團精心製作的「釣魚網站」，個資和錢財都被騙走了。

法律小教室

在上述案例中，詐騙集團的行為可能觸犯了以下法律：

- 加重詐欺罪（刑法第339條之4）：

詐騙集團「意圖為自己不法之所有」，「施用詐術」（製作假的銀行簡訊和網站），使被害人「陷於錯誤」（誤以為是真實銀行要求而輸入帳密），進而「交付財物」（帳戶內的錢被轉走）。而且，他們是利用「網際網路」這種傳播工具對「公眾」散布詐騙訊息，因此刑責會比普通詐欺更重。

- 可能會面臨的處分：一年以上七年以下有期徒刑，得併科一百萬元以下罰金。

◆案例解析與省思：

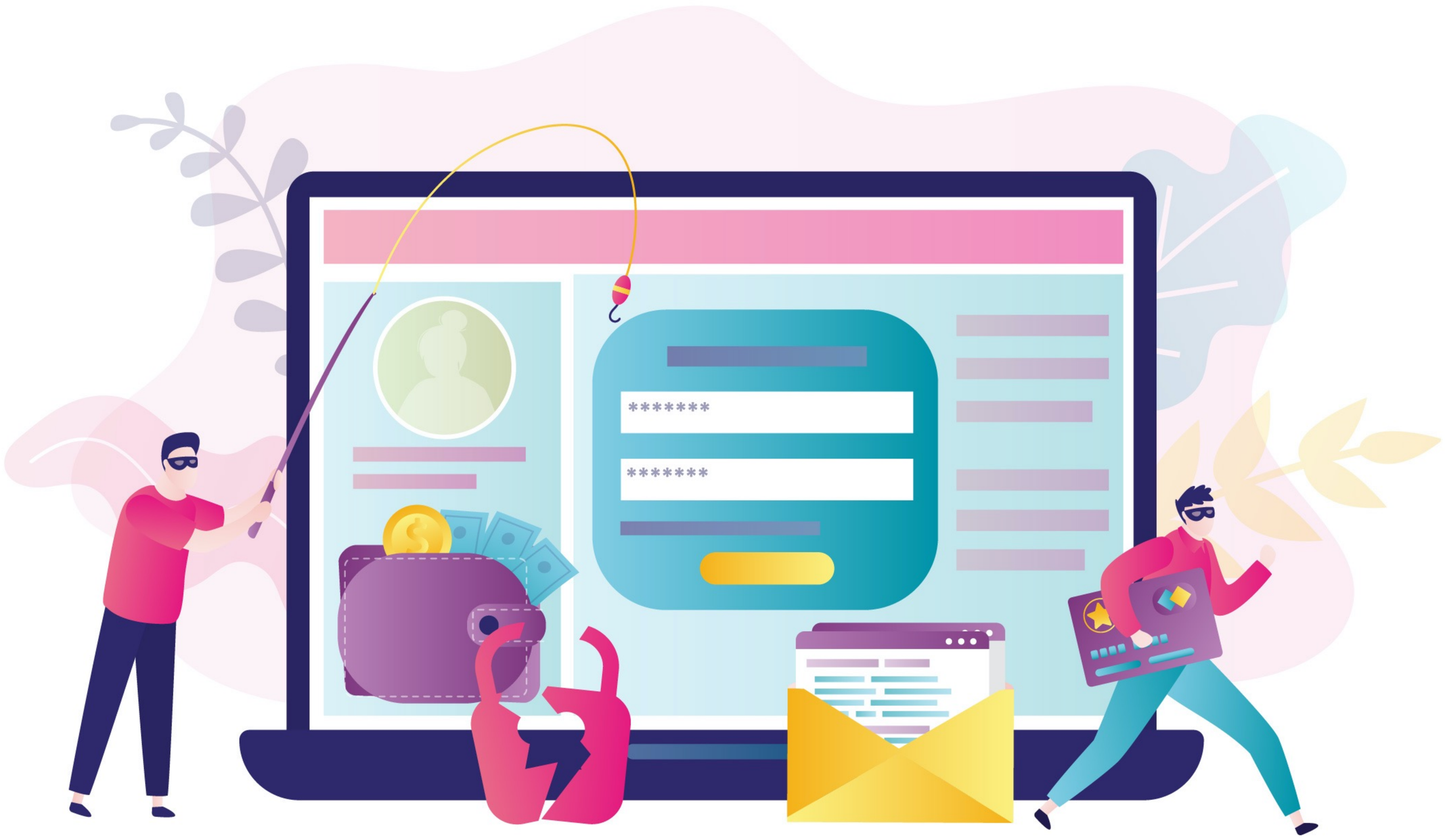
從「臺灣臺北地方法院113年度訴緝字第53號刑事判決」中，我們可以清楚看到，詐騙集團精心策劃的釣魚攻擊，正是利用了民眾對知名機構的信任感，以及一時的疏忽。

- 少了查證，多了風險：

如果小陳在收到簡訊時，能多一分警覺，不是直接點擊不明連結，而是主動透過官方App或官方網站查證，或撥打銀行客服電話詢問，就能有效避免損失。這正是「零信任」與「查證驗證」精神的具體實踐。許多時候，我們可能因為正在處理其他事情而分心，或因訊息內容的急迫性而慌了手腳，這時更要提醒自己「停一停、想一想、查證一下」。

- 保護個資，提防有詐：

除了金錢損失，個人資料外洩也是一大隱憂。銀行帳密一旦外洩，可能被用於更多非法用途。因此，妥善保管個人帳號密碼，不在不明網站輸入，是保護自己的基本功。



案例二：網拍撿便宜？當心「幽靈賣家」讓你血本無歸！

（改編自：臺灣新北地方法院114年度審金訴字第419號刑事判決）

小明是個熱血的高中動漫迷，尤其對某個偶像團體的「拉拉隊卡片」情有獨鍾，為了收集齊全套卡片，他幾乎跑遍了所有實體卡店，也時常在各大網路社團、拍賣平台尋覓。某天晚上，他在一個臉書二手交流社團裡，眼睛一亮！一位暱稱「Hao」、頭像是一隻可愛貓咪的賣家，竟然以市價近乎對折的價格，販售一套他夢寐以求、早已絕版的限量版拉拉隊卡片！

小明興奮不已，立刻私訊「Hao」表達強烈的購買意願。「Hao」回覆得很快，態度也很親切，但同時也強調：「這套卡片很多人問喔！因為價格很優惠，如果你要的話，可能要麻煩你先匯款全額到我的帳戶，我才能幫你保留，確認款項後我明天一早就幫你寄出。」對方還傳來幾張卡片細節的照片，看起來品項完美無瑕。

由於之前錯過幾次稀有卡片的經驗，小明深怕這次再猶豫就會被別人捷足先登。雖然心裡閃過一絲「會不會太便宜了？」的念頭，但想到終於能補齊收藏的缺口，他還是壓下了那一點點的不安。他迅速依照對方提供的銀行帳號，將自己辛苦存下的零用錢和打工錢，總共數千元，透過網路銀行轉了過去。轉帳完成後，他還開心地截圖告知對方。

沒想到，這才是惡夢的開始。隔天，「Hao」並沒有像約定好的那樣寄出卡片，反而開始用各種理由推託，一下說「臨時加班太忙，明天一定寄」，一下又說「包裝材料用完了，要去買新的」。幾天過去，小明越催促，「Hao」的回覆就越慢，最後甚至直接已讀不回。小明慌了，再點進對方的臉書頁面，卻發現帳號已經被註銷，或者自己被對方封鎖了。心愛的卡片沒買到，錢也討不回來，小明這才確定自己被騙了，心情沮喪又氣憤。

法律小教室

這位「幽靈賣家」的行為，最主要觸犯了：

- 詐欺取財罪（刑法第339條第1項）：

  賣家「意圖為自己不法之所有」，「施用詐術」（謊稱有商品要賣，並答應出貨），使小明「陷於錯誤」（相信真的能買到商品）而「交付財物」（匯款）。

- 可能會面臨的處分：五年以下有期徒刑、拘役或併科五十萬元以下罰金。

◆案例解析與省思：

「臺灣新北地方法院 114 年度審金訴字第 419 號刑事判決」揭示了網路購物中常見的詐騙手法。許多人，特別是學生族群，在購買自己喜愛的明星周邊、遊戲虛寶、限量商品時，很容易因為「稀有」、「低價」而失去戒心。

- 「查核商家」的重要性：

  在非正規的購物平台或社群（如臉書社團、IG、Dcard等）進行交易時，對賣家的背景查證尤其重要。

- 賣家評價與紀錄：

  該賣家是否有足夠的正面評價？帳號是否為新創立？是否有其他異常的交易紀錄？能否請對方提供更多元的驗證方式（如電話號碼、或其他平台的交易紀錄）？

- 商品價格合理性：

  價格是否低到不合常理？「一分錢一分貨」的道理在網路上依然適用。如果一個稀有商品價格遠低於行情，通常事有蹊蹺。

- 交易方式的保障：

  是否能採用有第三方支付擔保的交易方式（如蝦皮、PChome等平台的機制）？直接匯款給陌生人的個人帳戶風險極高。對於高單價商品，若情況允許，面交並當場驗貨也是降低風險的方式。

- 法律之前，人人平等：

  即使是網路上的虛擬交易，一旦涉及詐欺，同樣會受到法律的規範。判決中的被告，最終也為其詐騙行為付出了代價。

- 別讓「FOMO」心態成為破口：

  「FOMO」（Fear Of Missing Out，錯失恐懼症）是許多人，尤其是年輕族群在網路時代常有的焦慮。詐騙集團常利用這種心理，營造商品稀少、錯過不再的假象。保持理性，在按下購買或匯款按鈕前，先停下來花點時間質疑賣家是否刻意營造稀缺感、利用不合理的低價，或用話術催促你倉促決定，這種審慎的態度是避免受騙的重要一步。

透過以上兩個案例及相關法律的解析，希望能讓你更深刻體認到，在享受網路帶來的便利時，時刻保持警覺、落實查證，不僅是保護個人財產與資料安全的關鍵，也是身為數位公民應有的素養。在我們面對網路上的各種資訊與交易機會時，多一分思考與驗證，就能少一分受騙上當的風險。

2-1-3 零信任與詐騙防範

面對網路世界時，我們應該保持「零信任」的態度，當接收到任何網路上的資訊或要求時，應該都先持懷疑態度，並主動且多方進行查證。即使這些訊息看似來自已知或信任的來源，例如朋友傳來的訊息或知名機構發出的通知，都不應直接輕信，我們應保持謹慎並進行查證。此外，應針對不同詐騙手法採取具體的防範措施，例如啟用多重認證、使用防護軟體、仔細核對交易對象與價格，或在視訊時要求對方進行特定動作以驗證身份…等。隨著科技的發展，詐騙手法也不斷在翻新，現今甚至可以偽造他人的臉孔及聲音。因此當收到任何要求提供個人資訊、點擊連結或進行金錢交易的訊息時，無論是簡訊、電子郵件、社群媒體訊息，甚至是電話，我們都應該先「停一停、想一想、查證一下」。尤其是當訊息內容具有急迫性或刻意讓人分心時，更需要提高警覺。只有這樣，我們才能有效地保護自己，避免成為網路詐騙的受害者。

對於常見的網路詐騙之防範，我們可以有以下作法：

1. 防範網路釣魚 (Phishing)

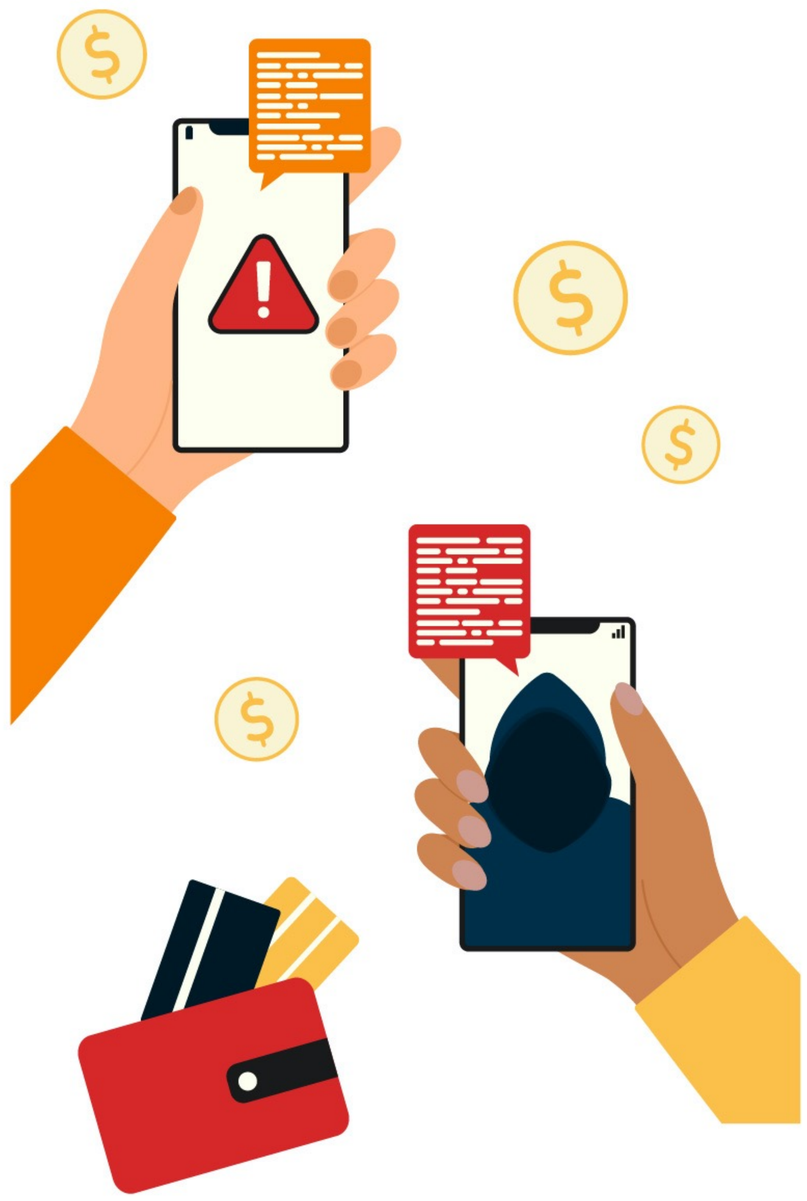
網路釣魚通常是指利用電子郵件、簡訊、社群媒體等社交工程技巧來騙取個人或企業資訊。攻擊之所以成功，常是因為受害者沒有意識到自己正面臨網路釣魚，以下是幾種常見的情況：

- 對於已知或未知來源的文字簡訊、即時通訊電子郵件，只要是要求您點擊連結或詢問個人資訊的訊息，都應保持警覺，並注意附件可能包含惡意程式不應隨意下載。
- 小心任何彈出視窗或底部橫幅。
- 詐騙可能會假冒常見的服務或機構，例如銀行，聲稱您的帳號有問題，要求點擊連結驗證。這類連結可能酷似官方網站但實為惡意網站，藉此竊取您的登入資訊。
- 個人應於任何帳號盡可能啟用雙重認證 (2FA, Two-Factor Authentication)，並於電腦安裝防護軟體和防火牆。

2. 防範網路購物詐騙

詐騙集團常利用商品稀有、低價等誘因，以及買家怕錯過（錯失恐懼症，FOMO）的心理來進行詐騙：

- 購物前要先「查核商家」，尤其在非正規平台（如臉書社團、IG）交易時，務必查證賣家背景。
- 檢查賣家是否有足夠正面評價，帳號是否新創立或有異常交易紀錄。
- 可以請賣家提供更元化的驗證方式，如電話或其他平台紀錄。
- 注意商品價格的合理性，價格如果低到不合常理，通常事有蹊蹺，「一分錢一分貨」在網路上也適用。
- 選擇有保障的交易方式，盡量採用有第三方支付擔保機制的平台，直接匯款給陌生人的個人帳戶風險極高。
- 保持理性，在付款前「先停下來花點時間質疑」，思考賣家是否刻意製造稀缺感、不合理的低價，或用話術催促倉促決定。



3. 防範AI深度偽造（Deepfake）詐騙：

AI技術的發展也被詐騙集團利用於偽造聲音或影像來行騙。

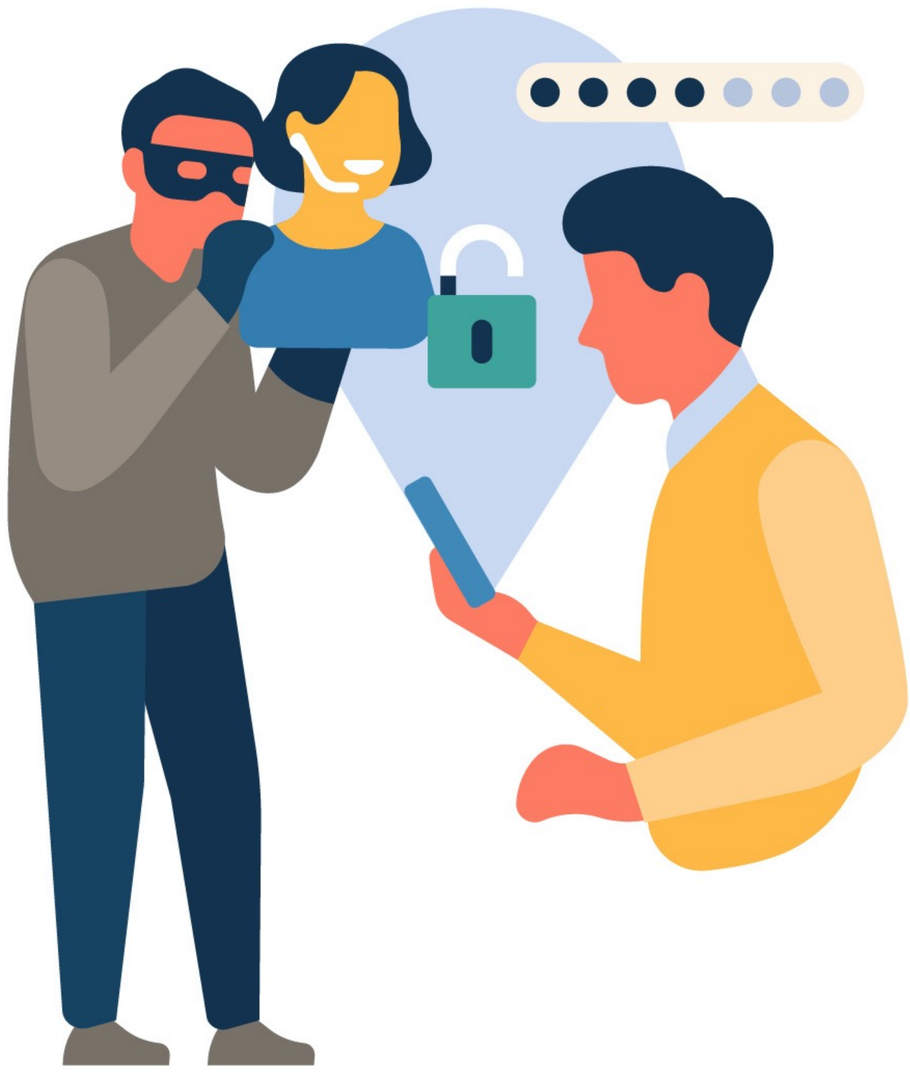
- 現在只要取得約 5 秒鐘的語音樣本，就能進行聲音偽造，因此詐騙集團可能透過不明來電或試探性電話（例如接通後無聲音並掛掉的電話）來收集聲音樣本，因此就算電話中聲音來自熟人 ，也應確認其說話習慣或使用只有彼此才知道的事情確認身分。
- AI變臉技術可以透過照片偽造出與本人極為相似的影像，在視訊通話中，可以要求對方進行特定的動作來辨別，例如請對方在臉部附近揮手或快速左右轉頭，如果是偽造的影像，可能會發現臉部有模糊或不協調的狀況。
- 可以與親友約定好「通關密語」，特別是在涉及轉帳等重要事項時，使用通關密語確認對方身份。

2-2 延伸學習

- 中小學數位素養教育資源網。妨害電腦使用罪。
  取自：web.archive.org/web/20250317143858/https://eliteracy.edu.tw/Archive.aspx?id=283
- 公視晚間新聞（2023年8月27日）。防AI深偽變臉詐騙 警：可要求臉部揮手辨真偽。
  取自：https://youtu.be/6E6FvwVxyIw
- 公視晚間新聞（2023年12月12日）。疑AI深偽仿聲詐騙 專家：講話5秒即可擬真7成。
  取自：https://youtu.be/cU6vPOTHfxs
- 內政部警政署165打詐儀錶板。https://165dashboard.tw/

參考文獻資料

- 資訊素養與倫理－高中職版（第4版）。臺北市政府教育局
- 資訊素養與倫理－高中職版（第3版）。臺北市政府教育局
- 吳清基、林宜隆（2009）。資訊素養與倫理－高中版（2版）。臺北市：臺北市政府教育局。
- 趨勢科技。何謂網路釣魚？。民國114年6月1日
  取自：https://web.archive.org/web/20250427080901/https://www.trendmicro.com/zh_tw/what-is/-phishing.html
- 雷皓明律師（2023年5月18日發佈）。詐欺罪不是被騙就成立！律師帶你看 5 大詐欺罪構成要件。民國114年6月1日
  取自：https://web.archive.org/web/20250604145300/https://zhelu.tw/post/fraud
- 內政部警政署165全民防騙網。民國114年6月1日
  取自：https://165.npa.gov.tw/
- 臺灣臺北地方法院113年度訴緝字第53號刑事判決（113年11月22日）。民國114年6月1日
  取自：https://judgment.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=TPDM,113,訴緝,53,20241122,3
- 臺灣新北地方法院114年度審金訴字第419號刑事判決。民國114年5月29日
  取自：https://judgment.judicial.gov.tw/FJUD/data.aspx?ty=JD&id=PCDM,114,審金訴,419,20250529,1



04 ▶ 四通八達 小試身手

4.1 主題探討

Q1 在詐騙的案例中，如果受害者做了「查證」的動作，是否可以避免受騙？在案例中的受害者又可以怎麼進行查證來確認是否為詐騙呢？我們還能從案例中學到什麼教訓來保護自己或提醒其他人？

Q2 你是否也曾在忙碌或分心時，差點點入可疑的連結呢？當時是怎麼發現的？

Q3 零信任原則讓我們在面對網路來源要保持一份警戒，請找看看其他受詐騙的新聞是怎麼讓受害者放下心防，如果是你是否能維持「零信任」呢？

MEMO

資訊素養與倫理 高中職 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
　　林湧順 臺北市立大直高級中學校長
指導委員 / 盧東華 臺北市立大學助理教授
　　李啟龍 國立台灣師範大學附屬高級中學資訊室主任
總 編 輯 / 劉亦陞 臺北市立大直高級中學圖書館主任
執行編輯 / 魏仲良 臺北市立大直高級中學資訊組組長
編審委員 / 王鼎中 臺北市立建國高級中學老師
　　朱德清 臺北市立中山女子高級中學老師
　　侯莉莉 臺北市立內湖高級中學資訊組組長
　　孫晉忻 臺北市立景美女子高級中學老師
　　陳佳宜 臺北市立麗山高級中學老師
　　陳哲雋 臺北市立南港高級中學資訊組組長
　　陳　晉 臺北市立復興高級中學老師
　　陳瑞宜 臺北市立大同高級中學研發處主任
　　楊喻文 臺北市立第一女子高級中學資訊組組長
　　蔡志敏 臺北市立大同高級中學老師
　　蔡明男 臺北市立內湖高級中學圖書館主任
　　賴和隆 臺北市立中正高級中學老師
　　韓君尹 臺北市立和平高級中學資訊組組長
　　羅玗貞 臺北市立內湖高級中學老師
　　（按姓氏筆畫排列）
承辦單位 / 臺北市立大直高級中學
出版日期 / 中華民國114年6月

網路犯罪大挑戰

詐騙篇

臺北市政府教育局
DEPARTMENT OF EDUCATION
TAIPEI CITY GOVERNMENT