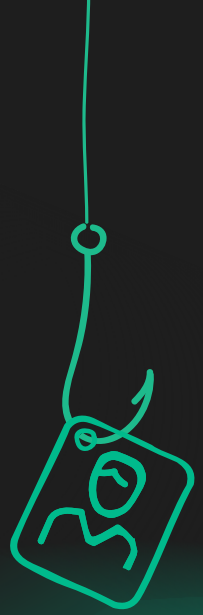
# 防範社交工程攻擊入門指南：國民及學前教育

jamf

**學校不只是供孩子學習知識的場所，也是他們學習人際互動、培養自信與成就感，並從同儕或他人身上獲得認同的重要場域。然而，這段歷程往往充滿變動與挑戰，且孩子的判斷力也尚未成熟。**

攻擊者正是看準這點，才會鎖定學校發動社交工程攻擊。

引發急迫感搭配施壓手段，加上學生的單純與經驗不足，便可能帶來各種遭受惡意利用的風險。



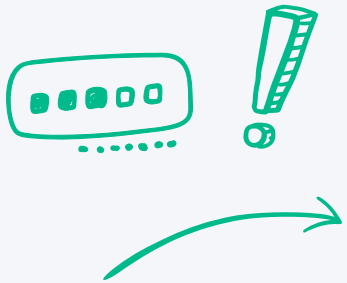
**本電子書將帶您瞭解：**

- **什麼是社交工程**
- **常見的攻擊手法**
- **社交工程在國民及學前教育校園中的真實樣貌**
- **預防攻擊的工具與實際作法**

# 什麼是社交工程？

**社交工程會利用心理操控手法，誘使使用者透露敏感資訊。它可以單獨進行，例如架設一個仿冒網站，顯示熟悉的登入頁面，實際上卻是用來竊取憑證；也可以與其他攻擊手段搭配，例如用來散佈惡意軟體。**

社交工程攻擊鎖定的是安全狀況中的「人」這個環節。這類攻擊極為常見，**其發生比例至少高出其他攻擊方式 45%**，這是根據**《2025 CIS MS-ISAC K-12 網路安全報告：教育與社群韌性》所指出。**



# 為什麼社交工程對 IT 團隊很重要？

**簡而言之，它讓校園更容易遭受攻擊。**
請思考以下幾點：

### 攻擊者可能繞過既有防護措施：

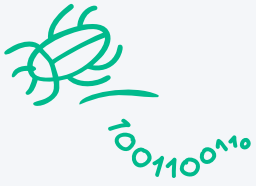
如果 IT 組態與防護機制未考量來自社交工程的風險，就可能被攻擊者加以繞過——畢竟在缺乏適當偵測工具的情況下，一旦攻擊者取得憑證，其登入看起來完全合法。

### 橫向移動（攻擊者從系統內部的某個帳號進一步擴散至其他系統）的風險：

只要一個帳號遭到入侵，就可能讓整個系統門戶大開，使攻擊者進而橫向移動至權限更高的系統，擴大受害範圍。

### IT 團隊必須承擔後果：

社交工程攻擊會增加 IT 團隊的負擔，使日常作業更加混亂。一旦攻擊奏效，雖然洩露資訊的是使用者，最終責任仍落在 IT 團隊身上。即使使用者再謹慎，也難保萬無一失——IT 團隊仍需介入，補強防護機制。




# 常見的社交工程攻擊手法

### 網路釣魚

網路釣魚是最常見的社交工程攻擊手法之一。攻擊者可能假冒校內人員或偽造校內服務系統，架設看似合法的網站，再利用急迫性誘使使用者交出個人資訊。

### 惡意廣告

惡意廣告係指利用線上廣告誘騙使用者下載惡意軟體，或竊取其憑證。

### 預設情境詐騙

假借情境詐騙形式多樣，但核心均為建立使用者的信任。攻擊者可能 冒充上級或同儕，讓使用者放下戒心，進而透露敏感資訊。

### 誘餌攻擊

誘餌攻擊透過難以抗拒的誘因吸引使用者，例如金錢回饋、獎勵、獨家內容等。一旦點選相關連結，就可能讓使用者同意安裝惡意軟體，或被導向釣魚網站。

### 搜尋引擎最佳化（SEO）中毒

攻擊者透過在搜尋引擎投放廣告，使其架設的仿冒惡意網站出現在搜尋結果前端，誘使毫無防備的使用者點選。

### 提示轟炸

攻擊者反覆發送多因素認證要求，藉由不斷干擾與施壓，讓使用者感到疲乏時或一時疏忽下同意存取。

這些手法其實早已存在一段時間，真正帶來改變的是 AI 造成的影響，AI 正徹底改變整個局勢。IBM 的**《2025 年資料外洩成本報告》（Cost of a Data Breach Report）**指出，每 6 起資料外洩事件中，就有 1 起攻擊是由 AI 驅動。

**隨著生成式 AI 的出現，攻擊者「撰寫一封極具說服力的網路釣魚郵件所需的時間，從原本動輒 16 小時，大幅縮短至只需 5 分鐘。」**

AI 讓網路釣魚攻擊與產出深偽內容變得更快速、也更具說服力——學校必須積極因應這些變化，特別是在學生較易受影響的情況下，更應提高警覺，並採取對應措施。

# 社交工程在國民及學前教育校園中的真實樣貌

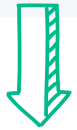
社交工程幾乎出現在各類網路攻擊中。根據 **Verizon 2025 年發佈的《資料外洩調查報告》（Data Breach Investigations Report）**，在教育服務產業中，其中 **17% 的攻擊與社交工程有關**。

真實樣貌因情境而異，因社交工程手法多變，且不斷演進。以下是幾種常見情境：

### 線上遊戲？其實是精心設計的陷阱。

某位中學生完成作業後，上網瀏覽遊戲相關內容。他／她無意間發現一個網站，宣稱可免費提供他／她最愛的線上遊戲虛擬貨幣！他／她忍不住點選連結，結果被導向一個竊取憑證的網站——對方承諾給予豐厚獎勵，但代價卻是交出登入資訊。

### 面對送上門的好事，更要仔細查證



一位新進教師急於在學校行政團隊前力求表現。某天，「校長」寄來一封電子郵件，要求提供禮品卡代碼，這位教師未加查證即依指示行事。這位教師還太資淺，並未察覺校長**平日的語氣**與這封郵件並不相符。

### 是或否：下載這個項目安全嗎？

（答案：不安全）

一名高中生正準備大學入學考試，於是上網搜尋備考資源。搜尋結果最上方出現一則贊助連結，標榜提供免費模擬試題。學生只需下載該備考軟體——但裡頭其實夾帶惡意軟體。

### 你有機會成為人氣王……代價是個資外洩到網路上。

一群小學生收到一封電子郵件，內文提到一項校內人氣票選活動——投票選出最受歡迎的學生，看看你是否會得獎！不過我們需要確認你確實是該校學生，請問能否提供你的個人資料？

# 防範社交工程攻擊

我們該如何阻止社交工程利用使用者，進而威脅資安？
關鍵在於兩個面向：**使用者與技術環境。**

## 使用者教育

對於使用者，尤其是年紀較小的學生，對網際網路世界的認識仍不完整。許多人也尚未養成對網路內容抱持懷疑與查證的習慣。理想情況下，應將數位公民素養納入課程。數位公民教育應著重於教導學生以負責任且安全的方式使用網際網路。

**這包括：**

- 教導學生常見的網路威脅有哪些（**需根據學生年齡設計教材**）
- **舉例說明**可疑網站／內容通常具備哪些特徵
- 鼓勵學生遵守網路倫理，並以負責任的**方式**使用網際網路

**此外，教師與學校人員同樣需要接受培訓。應納入考量的內容包括：**

- 網路釣魚電子郵件**模擬演練**
- 定期舉辦且全員需強制參與的合規**培訓**
- 建立**透明的溝通文化**——讓使用者在懷疑自己可能遭受社交工程攻擊時，願意主動向 IT 團隊反映

## 技術工具與政策：另一道防線

攻擊者之所以鎖定「人」這個環節，是因為這類攻擊所需的技術門檻較低，且更容易得手。因為人難免會犯錯，所以需要額外的防護措施來降低風險。

### 內容篩選

內容篩選可在使用者誤點惡意連結時，阻擋惡意內容。可透過允許／封鎖清單實作內容篩選，明確定義哪些網站可供存取（或禁止存取）。然而，這種作法仍有其限制：使用者不可能將所有實際需要使用的網站一一納入許可清單，也無法全面封鎖潛在的惡意網站。此外，學生離開校園後，接觸的網路環境並不像在校期間那樣受到保護。

更有效的作法是依「類別」進行篩選。這種作法不需 IT 管理員逐一列出特定網域，而是先將網站分類，再根據其類別決定是否予以封鎖。成人內容、賭博網站、檔案分享平台、社群網站，以及暴力或不當內容等，都可依設定加以控管。若再結合 AI 與機器學習進行智慧化篩選，防護效果將更為完善。

### 多因素認證

多因素認證（MFA）可為登入流程增加額外防護。即使使用者憑證**遭到**外洩，MFA 也能降低攻擊者成功存取帳戶的機率。MFA 至少需透過以下兩種方式認證：

- **只有使用者知道的資訊**：例如密碼、PIN 碼或安全性問題
- **使用者的生物特徵**：例如指紋或臉部辨識
- **使用者持有的裝置或憑證**：例如另一台裝置或安全金鑰

## 技術工具與政策：另一道防線

### 單一登入

在技術環境中建置身分識別提供者（IdP），即可解鎖單一登入（SSO）：只需一組密碼，便可透過 IdP 解鎖使用者的**所有**帳戶。這代表使用者需記住的密碼更少，同時也能降低憑證遭受入侵的風險。但這是否代表攻擊者僅需取得一組密碼，就能登入所有系統？

其實不然，因為 SSO 通常會搭配 MFA。使用者可設定需透過生物特徵（例如學生的指紋）進行驗證。除了減輕密碼管理負擔與潛在的入侵管道，SSO 也有助於憑證遭到竊取。例如，當使用者誤入仿冒網站時，由於 IdP 無法辨識該網域，將不允許使用者登入，就能避免其憑證外洩。

### 裝置管理

前述工具固然重要，但若缺乏行動裝置管理（MDM），這些工具將難以有效部署。透過 MDM，IT 團隊可以：

- 掌握裝置的安全狀態
- 訂定安全政策與設定防護組態
- 訂定裝置限制與使用規範，例如強制要求設定密碼或限制特定應用程式
- 確保裝置更新至最新軟體版本
- 部署內容篩選解決方案

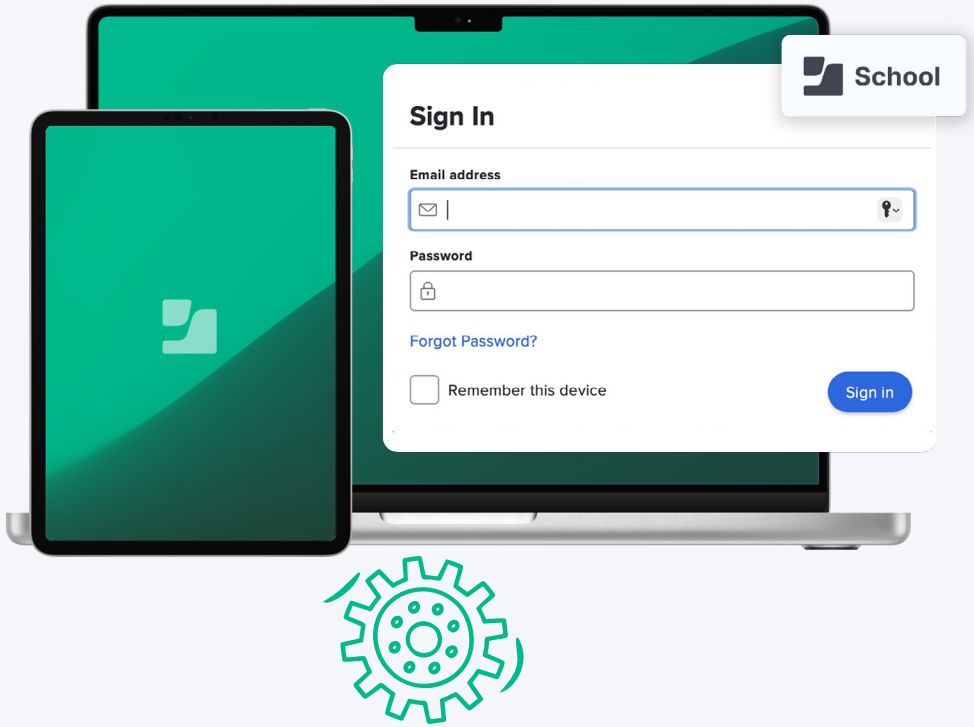
# 實際導入：Jamf School 與 Jamf Safe Internet

## Jamf School

Jamf School 是專為學校打造的 MDM 解決方案，
**主要功能包括：**

- **透過範本化裝置設定，**結合宣告式裝置管理
- **提供裝置清冊，**讓管理員便於掌握哪些裝置正在存取學校資源
- **掌握**裝置狀態，有助於迅速發現並處理問題
- 可為裝置套用各項**限制**與**設定**，包括強制要求設定密碼
- **支援 SSO**（需額外搭配身分識別提供者）
- **讓教師能輕鬆**提出應用程式申請，並交由 IT 團隊審核
- 還有**更多**功能！

透過 Jamf School，學校可建立安全的裝置管理基礎，進一步強化對社交工程攻擊的防護。

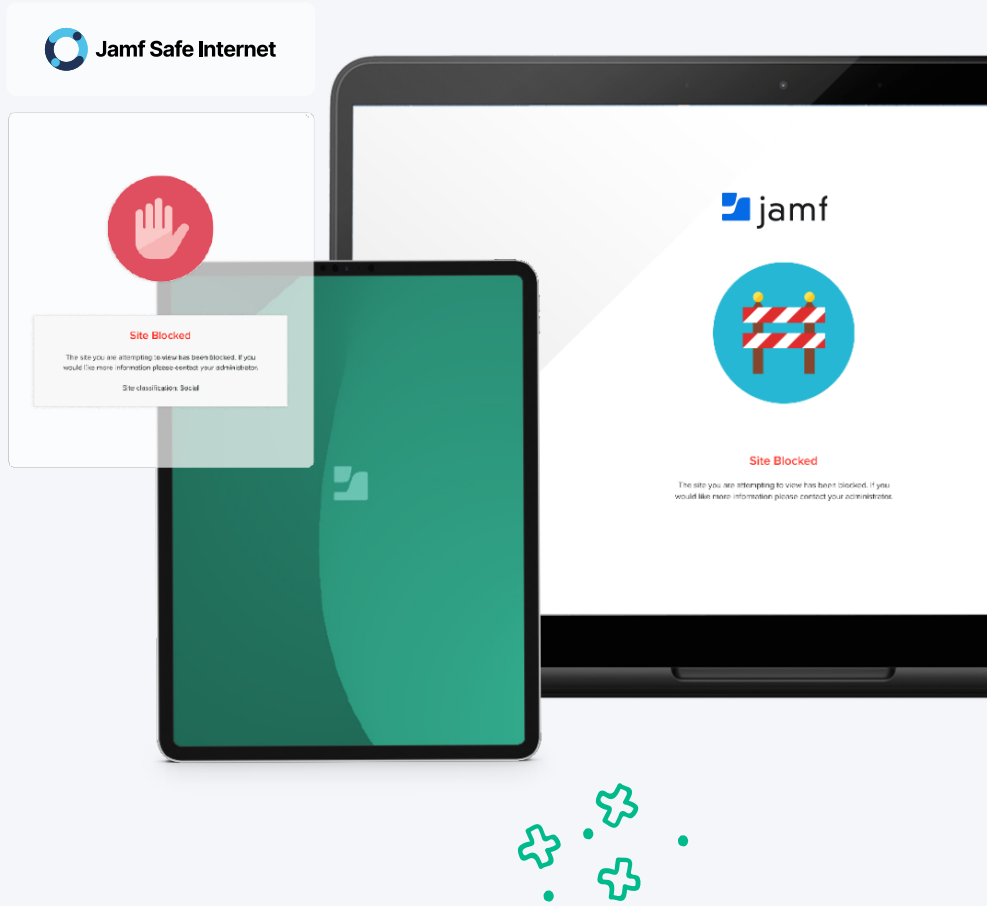


## Jamf Safe Internet

Jamf Safe Internet 支援 Apple、Chromebook 與 Windows 裝置，可進一步強化安全防護。Jamf Safe Internet 可靈活自訂，能依裝置的地理位置、類型或其他屬性，設定或調整各裝置群組的管理政策。無論裝置是集中存放於充電車並由學校以一對一方式配發，或為學生自有裝置皆適用。

為防範社交工程攻擊等威脅，**Jamf Safe Internet 提供：**

- 由 AI 與機器學習（ML）支援的**強大內容篩選機制**——即使釣魚網站尚未被系統辨識為惡意，也能先行阻擋使用者存取該網站
- 透過 **DNS** 與**網域名稱執行封鎖**，防範 DNS 偽冒攻擊
- 無論使用者身處何地，皆可**篩選 iPad 的裝置端內容**
- **內建網路防護機制**，在惡意網站影響裝置前即加以阻擋
- 強制啟用 **Google 安全搜尋**與 **Google Safe Browsing**，避免惡意或不當網站出現在搜尋結果中



即使不執行監控，同樣能提供完整的安全防護：學生可自由瀏覽網際網路、培養數位公民素養，亦不必擔心隱私遭受侵犯。安全可靠的課堂科技環境讓各方都能受益：

**教師**

能專注於教學，不再受登入問題與各種干擾影響。

**學生**

能在安全環境中自由探索與學習。

**IT 管理員**

能將重心放在其他任務上，無需擔心資安問題。

想進一步瞭解科技如何為貴校帶來改變嗎？

立即試用 Jamf