# 詐騙和網路安全術語須知

- **防毒軟體** - 用於預防、偵測，甚至移除惡意軟體的電腦程式。
- **自帶設備政策（BYOD）** - 由企業實施的政策，允許員工將自己的個人電子設備作公務用途。
- **常見漏洞與揭露（CVE）** - 羅列已發現資安弱點及漏洞的清單，並提供獨有的ID編號、描述和參考資料以便供公眾查閱。
- **加密貨幣** - 可像商品一樣交易的端對端去中心化電子貨幣。
- **網絡攻擊** - 對電腦系統、網絡、基礎設施或設備的惡意攻擊。
- **網絡事件** - 國家網絡安全中心（NCSC）定義為「違反系統安全政策以影響其完整性或可用性和/或未經授權訪問或試圖訪問系統的行為；符合《濫用電腦法》（1990年）」。
- **暗網** - 網路的其中一部分，但無法在搜尋器搜索出來，僅能透過特殊權限或軟體訪問。
- **數碼足跡** - 使用網路後留下的數據蹤跡，可能包括被動信息，如存儲的Cookie，或者被主動在網絡上發表的資訊，如社交媒體帖子。
- 加密 - 使用數學算法將數據打亂的過程。這些數據可以是靜態加密，例如儲存在硬碟中的數據，亦可以是傳輸中的數據，例如透過 HTTPS 從您的網頁瀏覽器傳送到銀行伺服器的資料。加密了的資料並不能代表網絡上的不法份子無法截取，只是已被轉換為無用的和無法理解的亂碼，讓不法份子得物無所用。
- 防火牆 - 根據特定規則，監控網路進出流量的網路安全系統。
- 駭客 — 專門從事電腦網路攻擊的人士。黑帽駭客進行惡意攻擊，而白帽駭客則進行有助於網路防禦的行動。
- 惡意軟體 — 以達成不法或惡意目標的程式，涵蓋多個方面，例如提供遠端存取、載入或植入其他惡意程式、竊取銀行資訊、加密並拒絕存取資料，或盜用設備的運算能力。
- 安裝補丁 — 安裝修補程式以更新現有軟體或硬體，修復已發現錯誤和漏洞的過程。
- 滲透測試（pen testing） - 機構利用駭客的攻擊手段來檢測自身網絡的安全性，通常由「紅隊」或專業的白帽駭客團隊負責。

- **釣魚 -** 通常透過電子郵件欺騙收件人洩露敏感資料、點擊惡意連結和/或打開惡意附件。不法份子常用釣魚以取得設備或網絡上初始入侵管道。
- **勒索軟體 -** 封鎖或限制使用者存取資料的惡意軟體，並要求受害者支付贖金才能解除限制。
- **短訊釣魚** — 透過短訊/簡訊傳送的釣魚訊息。
- **社交工程** — 操控他人的心理而作出某種行為，通常用於騙取個人資料。
- **魚叉式網路釣魚** — 針對特定人士或群體所發出的釣魚訊息。
- **特洛伊木馬** — 偽裝成看似無害的檔案或程式，讓受害者以為可安心開啟。特洛伊木馬十分常見，通常透過釣魚郵件傳送，或者由其他稱為「載體」的惡意軟體傳送。
- **雙重要素驗證（2FA）** — 一種要求用戶提供兩種身分識別要素的驗證過程，例如已知密碼和一次性密碼（OTP）。一般來說，這些要素可分為：「認知要素」（密碼）、「生物特徵」（指紋）或「持有物件」（密匙卡）。
- **虛擬私人網路（VPN）** — 允許在公共基礎設施上建立安全私人的連線，最初由機構開發，以對訪問內部網絡資源，例如電郵伺服器或共享文件夾等的員工進行身份驗證。現在，越來越多的人使用消費者VPN來作為建立及選取VPN伺服器的加密連線，並使用該伺服器連接到其他互聯網資源。
- **語音釣魚** — 透過電話進行並大量利用社交工程的釣魚攻擊。
- **零日漏洞** — 在補丁或更新發佈之前所發現到的漏洞。利用此類漏洞的惡意軟體通常被稱為零日漏洞攻擊。