2022 年 10 月

健康與安全公告——防範網路犯罪

加州發展服務部

本公告是否有幫助？

請點擊投票。

防範網路犯罪

對於互聯網用戶來說，網路犯罪是一個日益嚴重的問題。雖然在網上保持聯絡非常便利，但如何安全使用互聯網也需要學習。網路犯罪分子將他們所認為的弱勢群體視為目標，其中就包括患有智力和/或發育障礙的人。每個人都應認識到遭遇網路犯罪的風險，了解網上衝浪時如何保持安全。

什麼是網路犯罪？

網路犯罪是利用移動設備（如手機）、電腦和公共 Wi-Fi 在互聯網上實施的犯罪。網路犯罪分子竊取敏感的或私人的資料以謀取經濟利益。

他們透過各種策略瞄準「獵物」，暗中收集個人資料。許多人在毫不知情的情況下上了網路犯罪的當，導致蒙受經濟損失（財務盜竊）、個人數據洩露和身分被盜。了解如何防範網路犯罪以及受害後如何尋求幫助，比以往任何時候都更重要。

網路罪犯是機會主義者，他們會尋找弱勢人群作為獵物。針對患有智力和發育障礙的人，犯罪分子可能認識他們，或故意接近他們，讓自己扮作熟人或值得信賴的人。

常見的網路犯罪類型

網路釣魚：利用電子郵件、短信和電話，讓受害者透露個人或財務資料和/或登錄憑證。

不送貨：利用互聯網非法索要電子支付資料，來為購買了卻永遠不會收到的商品和服務付款。

敲詐：透過冒充當局的人（如國稅局）恐嚇或威脅他人來獲取金錢或物品。敲詐方式可能包括人身傷害、刑事起訴或公開曝光等方面的威脅。它還可能涉及到鎖定受害者數據的訪問權限，以此要脅索要贖金。

個人數據洩露：竊取個人的私人資料和數據並將其分享給未經授權的用戶。

身分盜用：竊取和使用他人的個人資料進行欺詐或實施其他犯罪。

健康和安全公告由發展服務部編制，旨在提醒直接服務提供者、區域中心和其他人等，留意在我們社區發現的特定風險。

請接受以下調研，就本公告予以反饋，提出改進建議：公告調研

2020 年美國的網路犯罪情況

- 在 COVID 疫情期間，患有智力和發育障礙的人士成了網路犯罪分子的攻擊目標，以電子形式寄給他們的經濟影響補助金常遭犯罪分子挪用。
- 加利福尼亞州的網路犯罪投訴量居全美之首。
- 聯邦調查局收到了公眾的近 80 萬份網路犯罪投訴，比前一年**增加了 69%**。
- 網路釣魚是最常見的網路攻擊，報稱受害者超過了 **241,000** 人。
- 報稱損失超過了 **41 億**美元。
- 60 歲以上的人是所有年齡組中最易成為攻擊目標的人。

幫助保護您所服務的個人免遭網路犯罪侵害

網路是公共空間

提醒個人在互聯網上分享私人資訊（例如社會安全號碼、銀行賬戶資料和醫療資訊）之前要有警惕之心。

- **使用公共 Wi-Fi 時應始終保持謹慎。**
- 公共 Wi-Fi 在覆蓋範圍內對所有人開放，並且通常不要求用戶在加入前同意任何條款或條件。
- 雖然使用公共 Wi-Fi 很方便，但安全性往往難以保證。也就是說，其他人可能會在受害者不知情的情況下以電子方式查看個人資訊（如用戶名和密碼）。
- 安全的 Wi-Fi 網路通常要求輸入用戶密碼，並且可能需要付費或購買才能使用。

為在線帳戶創建強密碼

幫助您服務的個人創建強密碼。

- 建議個人不要使用常用密碼或容易猜到的密碼。
- 強密碼至少有 8 個字符，包括大小寫字母、符號和數字的組合。密碼越長越安全。
  - **弱密碼**：直接用 password、您自己的名字或生日，或 12345
  - **強密碼**：8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs

定期檢查隱私設置

幫助您所服務的個人檢查其移動設備和電腦上的隱私設置。向其解釋如何更改在線賬戶的隱私設置來設置雙因素驗證。雙因素驗證是指用戶每次登入在線賬戶時，都會收到包含特殊代碼的短信或電子郵件。

病毒和惡意軟體

- ***惡意軟體***是一種旨在損害移動設備或計算機系統的軟體。

- ***病毒***是未經許可進入計算機系統並將其「感染」的計算機代碼。它們會隱藏在以電子郵件或文本發送的檔案或應用程式中，一旦打開，計算機就會被感染。病毒是惡意軟體的其中一種。
- 病毒可以竊取用戶資料、降低計算機速度並使其崩潰，或者完全控制計算機或設備。
- 病毒不能自行傳播。人們在不知情的情況下分享它們，病毒就會傳播開來。病毒的傳播路徑通常是人們共享已感染的檔案或電子郵件。

成為網路犯罪的受害者後，應如何應對

向您的服務對象解釋，打電話給銀行、將受到網路攻擊的扣賬卡或信用卡掛失是何等重要。協助其更改在線帳戶的登錄信息。向被入侵的帳戶的機構發出警報，並詢問是否有任何已入帳的欺詐性消費。

DDS 健康工具包包含更詳細的資訊，可讓您了解如何幫助支持、保護您的服務對象。

有用資源

本地執法機構

網路犯罪投訴中心（IC3）

聯邦貿易委員會（FTC）

- 在 ReportFraud.ftc.gov 上報告欺詐行為
- 撥打 FTC 熱線：1-877-IDTHEFT (1-877-438-4338)
- 在 identitytheft.gov 上報告身分盜竊，了解詳細資訊

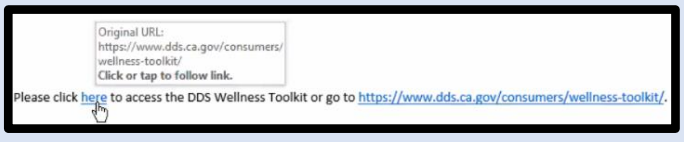
點擊前請三思

- 請勸告您所服務的個人不要打開來歷不明的附件，不要點擊無法識別的連結。這樣可能導致病毒或惡意軟體危害計算機。
- 提醒您的服務對象，如果一個連結看上去像是遊戲或承諾點開後即可獲得「免費」獎品，請提高警惕。
- 建議個人在收到電子郵件後檢查發件地址，確認發件人非假冒帳戶。如果收到一封帶有連結或附件、內容出乎意料的電子郵件，建議他們透過電話或短信聯絡發件人，確認真的是他們發送了電子郵件。
- 網路釣魚是一種常見的互聯網騙局，犯罪分子用看似逼真的假冒資料來誘使人們分享個人資料。
    - 在回復任何郵件之前，請留意是否存在網路釣魚詐騙的跡象：不熟悉的發件人、拼寫和語法錯誤、與郵件內容不匹配的可疑連結、隨機附件、具有緊迫感的電子郵件內容。

在回复或點擊電子郵件之前

鼓勵消費者核實發件人的身分。

- 將游標移到發件人的名字或連結上來檢查發件人的電子郵件地址，確保它看起來指向正確。



健康和安全公告由發展服務部編制，旨在提醒直接服務提供者、區域中心和其他人等，留意在我們社區發現的特定風險。
請接受以下調研，就本公告予以反饋，提出改進建議：公告調研