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

互聯網是一種很好的在線交流方式，但它也暗藏危險。就像您離家出門需要鎖好門窗一樣，在使用互聯網之前您也應該採取防範措施，確保您和您的資料安全穩妥，避免成為網路犯罪的受害者。

如何在互聯網上保持安全

什麼是網路犯罪？

網路犯罪是在互聯網上發生的犯罪，受害者的個人資料或錢財會被盜用。許多人意識不到自己遭遇了網路犯罪，因此至關重要的是了解如何識別網路犯罪從而加強防範，或是獲取幫助以避免再次受害。

網路是公共空間

- 別人可以看到您瀏覽的網站，有時還能看到您輸入的資料。
- 您在互聯網上分享的任何資訊都可能被其他人看到。
- 如果不是出於正當的商業原因（例如辦理銀行業務），在互聯網上分享您的個人資料（例如社會保險號、銀行賬戶和醫療資訊）時要尤其謹慎。
- 使用商店和餐廳免費提供的公共 Wi-Fi 網路時，應始終保持警惕。
- 雖然使用公共 Wi-Fi 很方便，但安全性往往難以保證。也就是說您的個人資料（例如您的銀行帳戶的用戶名和密碼）可能會被其他人看到或竊取。

定期檢查隱私設置

- 隱私設置讓您能夠選擇將哪些資料與哪些人分享。
  - 在社交媒體（如 Facebook 或 Instagram）上，您可以使用隱私設置來控制與他人共享的內容。
- 請為手機上的不同應用程式設置不同的隱私選項，來限制與應用程式共享的內容（例如共享您的位置或數據權限）。
- 請確保您的在線帳戶的隱私設置需要輸入密碼才能更改。
  - 雙因素驗證是指，您每次登入在線賬戶（如銀行或信用卡公司）時，都會收到包含特殊代碼的短信、電話或電子郵件。這種驗證方式可確保是您登入了自己的帳戶。
  - 為在線帳戶設置雙因素驗證是個好主意。

健康和安全公告由發展服務部編制，旨在提醒個人及其家庭和其他人等留意在我們社區發現的特定風險。

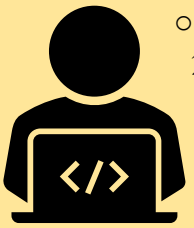
請接受以下調研，就本公告予以反饋，提出改進建議：公告調研

為在線帳戶創建強密碼

- 為您的帳戶設置強密碼，並定期更改。這有助於保護您的在線帳戶。
- 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。
    - **弱密碼示例**：password, YourName, 12345
    - **安全密碼示例**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs
- 避免使用容易猜到的密碼，比如您的生日或名字。
- 您的每個帳戶都應該有獨立的密碼。
- 不要把密碼列出來寫在紙上隨手放在一邊，尤其不要放在電腦旁邊。
- 密碼只能與您熟悉、信任的人共享，並且應該存放在安全的地方。

警惕病毒和惡意軟體

- ***惡意軟體*** 是一種對您的計算機有害的軟體。***病毒*** 是惡意軟體的其中一種。



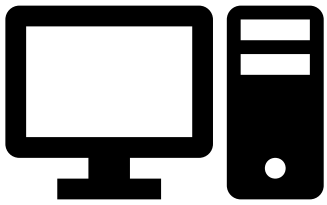
    - 病毒和惡意軟體能夠在未經您許可的情況下進入您的計算機系統，並造成其「感染」。
    - 病毒和惡意軟體能夠竊取您的資料、讓您的電腦速度變慢甚至崩潰，或者完全控制您的電腦。
- 如果一個連結或一封電子郵件已被感染，您點擊或打開它們時，病毒和惡意軟體就會侵入您的電腦。
    - 如果一個連結聲稱可讓您中獎或有免費禮物，請謹慎點擊。
    - 也許這些連結看起來就像遊戲、螢幕保護程式或可下載檔案一樣，但它們可能是惡意軟體或病毒。

點擊前請三思

- 留意您在線收到的電子郵件和消息的發件人。
    - 檢查他們的電子郵件地址，看看是否與您已有的地址匹配。

- 如果發件人催促您馬上回復或者讓您覺得出現了危機狀況，比如說您的銀行賬戶有問題，一定要提高警惕。這些類型的消息很可能是騙局。
- 網路釣魚是一種互聯網騙局，透過使用看起來真實的虛假消息，誘使人們分享自己的個人資料。

    - 在回復郵件之前，請檢查一下您是否熟悉發件人，信件是否存在拼寫或語法錯誤，是否有與內容不匹配的連結，是否有隨機的附件，以及是否要求您迅速採取行動。
- 如果您對附件或連結不熟悉，請不要打開或點擊。這些可能是仿冒的，會導致病毒安裝到您的電腦或手機上，損害您的設備或竊取您的更多資料。
    - 當您收到一封帶有連結或附件、內容出乎意料的郵件時，一定要聯絡發件人（透過電話或短信）確認是否真的是他們發送的。
- 國稅局只會透過美國郵政郵件向您寄送通知。不要回復自稱來自美國國稅局的電話、電子郵件或短信。



健康和安全公告由發展服務部編制，旨在提醒個人及其家庭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

弄清楚您在給誰發郵件或發短信

- 請記住，網路用戶的真實身分可能與他們宣稱的不符。
- 切勿向陌生人或素未謀面的人分享您的個人資料或發送自己的照片。
- 切勿向您最近才認識或從未見過面的人寄錢。
- 當您在在線表格或網站輸入您的社會安全號碼或任何帳戶號碼時，請提前核實要求您提供資料的人的身分。
    - 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。

- 別人可以複製徽標，使電子郵件看起來、聽起來都像真的一樣，所以請仔細檢查，看看是否存在拼寫錯誤、怪異的內容或模糊的圖像。
- 如果您不確定發件人身分是否真實，您可以透過您的在線賬戶聯絡其所屬公司或組織，或者直接打電話給他們。

如果成了網路犯罪的受害者，您該怎麼辦？

- 立即告訴您信任的人。
- 如果犯罪可能涉及到您的個人帳戶被入侵，請打電話給您的銀行或信用卡公司，讓他們能夠馬上了解情況。請停止使用任何已被入侵的扣賬卡或信用卡。
- 更改所有被入侵的帳戶或用戶名的密碼。
- 留意您的賬戶是否存在異常活動。

健康和安全公告由發展服務部編制，旨在提醒個人及其家庭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