以下資料由仁人服務社節錄及翻譯自官方網站，所有內容均以官方網站公布資料為準。
網站鏈接：https://spdblotter.seattle.gov/2020/05/08/criminals-exploiting-covid-19-to-commit-unemployment-fraud/

Criminals Exploiting COVID-19 To Commit Unemployment Fraud
犯罪者利用新冠病毒疫情涉嫌欺詐失業救濟金

西雅圖市、華州和聯邦執法部門目前正在調查大規模盜用他人身份冒領失業救濟金的詐騙活動。

詐騙活動的受害者沒有申請失業救濟金，卻收到其雇主人力資源部門或華盛頓州就業保障部的通知，被告知已經有人以他們的名義申請了失業救濟金。

西雅圖警察局的網路犯罪調查人員建議，如果知道或相信自己是失業救濟金欺詐的受害者，請採取以下行動：

採取以下行動保護你的財務身份和信用記錄：

第一步：聯絡人力資源部

- 聯絡所在單位的人力資源部，將情況報告給雇主。

第二步：聯絡華州就業保障部

- 撥打華州就業保障部電話 **800-246-9763** 或在線舉報詐騙行為
- 你需要提供以下資訊以核實身份
  - 社會安全號碼的最後 **4** 位數字
  - 出生日期和地址
  - 有效電話號碼
  - 你是如何得知有人以你的名義申請失業金
  - 或通過以下連結聯絡就業保障部：
  - https://fortress.wa.gov/esd/webform/ContactUS/

第三步：報告警方

- 向居住地管轄區相關機構提交在線或非緊急報告。
- 如果居住在西雅圖，則可以通過以下鏈接在線提交報告：
  https://www.seattle.gov/police/need-help/online-reporting
- 記錄並保存好所有與此相關的資訊和文件，包括案件編號。 身份盜竊受害者可以利用一些通常不向一般公眾提供的政府服務和設施，比如獲取某些已封存的公共記錄。

第四步：三大信用記錄局

- 在 www.annualcreditreport.com 上獲取 **Equifax, Experian** 和 **TransUnion** 的免費信用報告。 這些報告也可以通過致電 **1-877-322-8228** 獲取
- 向信用記錄局報告有人使用你的身份冒領失業救濟金, 並提供你報警的案件編號。 你可以要求信用記錄局對你的身份設置欺詐警示或者凍結你的信用記錄。 依照法律, 這兩種做法都是免費的。
  - 欺詐警示設置是免費的, 這使他人更難以你的名義開設新帳戶。 如果需要設置欺詐警示, 請聯繫以下三個信用記錄局中任何一家, 它必須將此通知給其它兩家。
  - **Experian 1-888-397-3742**
  - **TransUnion 1-800-680-7289**
  - **Equifax 1-888-766-0008**
- 每年至少檢查一次你的信用活動記錄。 作為身份盜竊的受害者, 你有權要求每月進行檢查。
- 信用凍結 –如果你近期內沒有大筆花銷 (例如購房), 你可以通過凍結信用以加強保護。 信用凍結是免費的, 你可以通過以下連結自行操作: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

第五步：聯邦貿易委員會 (FTC) 和國稅局 (IRS)

- 向聯邦貿易委員會 (FTC) 提交一份簡短報告, 並提供向當地警方報警時的案件編號 https://www.identitytheft.gov/ (有關詳細資訊,請造訪 www.ftc.gov/idtheft)
- 可以在國稅局 https://www.irs.gov/payments/view-your-tax-account 網站上開設一個帳戶。 用你的社會安全號開設帳戶可以防止犯罪分子使用你的身份開設帳戶。
- 另一個方法是在 https://www.e-verify.gov/employees 上鎖定你的社會安全號 (下一波網路攻擊可能是針對國稅局的稅務詐騙)。
- 以上這些報告看似多餘, 但這樣可以確保地方、州和聯邦政府將你列為受害者。 此外, 舉報的人越多, 就越有利於執法部門追蹤犯罪者。

第六步：保存記錄

- 將所有記錄、電子郵件副本等保存好。 如果將來遇到任何身份問題或在信用記錄中發現有不準確之處, 這些書面記錄將起到參考作用.

保護你的資料與身份

針對這次失業救濟金欺詐事件, 你已經採取了相應的措施, 但你還可以採取進一步的行動來保護自己免受網路犯罪的侵害。 以下是網路犯罪專家為那些想為自己和家人提供更多保護的人所推薦的方法和資源。

控制你自己的信息

- 鎖定信用資訊的服務會有所說明，然而你必須向相關公司提供個人數據，這可能會帶來更多的潛在風險。
- 有許多網站會引導你如何進行數據保護。 你可以在谷歌上搜索 "如何退出和凍結信用"，也可以使用下面這些第三方資源。 這些資源和西雅圖市政府沒有任何關係，但它們是其他受害者成功使用過的可信賴的資源。
  - https://Inteltechniques.com/links.html 該頁面右側連結的工作手冊將引導你完成信用凍結，並從數據代理和 "跟蹤者" 網站中將你的數據刪除。 "隱私清單" 是用於保護設備、帳戶和個人資料的可列印指南。 你無需在此頁面上購買任何東西，而只是使用他們的免費指南。
  - https://ssd.eff.org/en **EFF** 基金會有一些隱私和安全指南。
  - 大多數網路攻擊者使用的是以前在互聯網上盜取的連鎖酒店、娛樂服務行業及其它廣泛使用的數字化生產工具中的數據，這就是為什麼永遠不重複使用密碼的重要性。通過以下網站可以取得密碼管理器並使用多重身份驗證：
    https://thewirecutter.com/reviews/best-password-managers/
  - 在你最重要的帳戶上使用多重身份驗證 (輔助安全代碼)：
    https://authy.com/guides/
  - 最重要的是要保持警惕，留意釣魚電子郵件、虛假欺詐電話、甚至郵件/包裹盜竊等行為，這些都可能導致你的身份被盜竊。
  - 警惕那些免費應用程式或贈與，它們可能通過有關數據獲取你的資訊。
  - 更多指南
    - https://www.tripwire.com/state-of-security/security-data-protection/guide-digital-privacy-your-family/
    - https://protonmail.com/blog/coronavirus-email-scams/
    - https://lifehacker.com/s/dataprivacy
    - https://www.digitaltrends.com/computing/how-to-increase-your-privacy-security-zoom/
    - https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home