以下信息由仁人服务社节录及翻译自官方网站，所有内容均以官方网站公布信息为准。
网站链接：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诈失业救济金

西雅图市、华州和联邦执法部门目前正在调查大规模盗用他人身份冒领失业救济金的诈骗活动。

诈骗活动的受害者没有申请失业救济金，却收到其雇主人力资源部门或华盛顿州就业保障部的通知，被告知已经有人以他们的名义申请了失业救济金。

西雅图警察局的网络犯罪调查人员建议，如果知道或相信自己是失业救济金欺诈的受害者，请采取以下行动：

采取以下行动保护你的财务身份和信用记录：

第一步：联系人力资源部

- 联系所在单位的人力资源部，将情况报告给雇主。

第二步：联系华州就业保障部

- 拨打华州就业保障部电话 **800-246-9763** 或在线举报诈骗行为
- 你需要提供以下信息以核实身份：
  - 社会安全号的最后 **4** 位数字
  - 出生日期和地址
  - 有效电话号码
  - 你是如何得知有人以你的名义申请失业金
  - 或通过以下链接联系就业保障部：
  - https://fortress.wa.gov/esd/webform/ContactUS/

第三步：报告警方

- 向居住地管辖区相关机构提交在线或非紧急报告。
- 如果居住在西雅图，则可以通过以下链接在线提交报告：
  https://www.seattle.gov/police/need-help/online-reporting
- 记录并保存好所有与此相关的信息和文件，包括案件编号。身份盗窃受害者可以利用一些通常不向一般公众提供的政府服务和设施，比如获取某些已封存的公共记录。

第四步：三大信用记录局

- 在 www.annualcreditreport.com 上获取 **Equifax**，**Experian** 和 **TransUnion** 的免费信用报告。这些报告也可以通过致电 **1-877-322-8228** 获取。
- 向信用记录局报告有人使用你的身份冒领失业救济金，并提供你报警的案件编号。你可以要求信用记录局对你的身份设置欺诈警示或者冻结你的信用记录。依照法律，这两种做法都是免费的。
  - 欺诈警示设置是免费的，这使他人更难以你的名义开设新帐户。如果需要设置欺诈警示，请联系以下三个信用记录局中任何一家，它必须将此通知给其它两家。
  - **Experian 1-888-397-3742**
  - **TransUnion 1-800-680-7289**
  - **Equifax 1-888-766-0008**
- 每年至少检查一次你的信用活动记录。作为身份盗窃的受害者，你有权要求每月进行检查。
- 信用冻结 – 如果你近期内没有大笔花销（例如购房），你可以通过冻结信用以加强保护。信用冻结是免费的，你可以通过以下链接自行操作：https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

第五步：联邦贸易委员会（ FTC）和国税局（IRS）

- 向联邦贸易委员会（**FTC**）提交一份简短报告，并提供向当地警方报警时的案件编号 https://www.identitytheft.gov/（有关详细信息，请访问 www.ftc.gov/idtheft ）
- 可以在国税局 https://www.irs.gov/payments/view-your-tax-account 网站上开设一个帐户。用你的社会安全号开设帐户可以防止犯罪分子使用你的身份开设帐户。
- 另一个方法是在 https://www.e-verify.gov/employees 上锁定你的社会安全号（下一波网络攻击可能是针对国税局的税务诈骗）。
- 以上这些报告看似多余，但这样可以确保地方、州和联邦政府将你列为受害者。此外，举报的人越多，就越有利于执法部门追踪犯罪者。

第六步：保存记录

- 将所有记录、电子邮件副本等保存好。如果将来遇到任何身份问题或在信用记录中发现有不准确之处，这些书面记录将起到参考作用。

保护你的数据和身份

针对这次失业救济金欺诈事件，你已经采取了相应的措施，但你还可以采取进一步的行动来保护自己免受网络犯罪的侵害。以下是网络犯罪专家为那些想为自己和家人提供更多保护的人所推荐的方法和资源。

控制你自己的信息

- 锁定信用信息的服务会有所帮助，然而你必须向相关公司提供个人数据，这可能会带来更多的潜在风险。
- 有许多网站会引导你如何进行数据保护。你可以在谷歌上搜索 “如何退出和冻结信用”，也可以使用下面这些第三方资源。这些资源和西雅图市政府没有任何关系，但它们是其他受害者成功使用过的可信赖的资源。
  - https://Inteltechniques.com/links.html 该页面右侧链接的工作手册将引导你完成信用冻结，并从数据代理和“跟踪者”网站中将你的数据删除。 “隐私清单” 是用于保护设备、帐户和个人数据的可打印指南。你无需在此页面上购买任何东西，而只是使用他们的免费指南。
  - https://ssd.eff.org/en **EFF** 基金会有一些隐私和安全指南。
  - 大多数网络攻击者使用的是以前在互联网上盗取的连锁酒店、娱乐服务行业及其它广泛使用的数字化生产工具中的数据，这就是为什么永远不重复使用密码的重要性。通过以下网站可以获取密码管理器并使用多重身份验证：https://thewirecutter.com/reviews/best-password-managers/
  - 在你最重要的帐户上使用多重身份验证（辅助安全代码）：https://authy.com/guides/
  - 最重要的是要保持警惕，留意钓鱼电子邮件、虚假欺诈电话、甚至邮件/包裹盗窃等行为，这些都可能导致你的身份被盗窃。
  - 警惕那些免费应用程序或赠与，它们可能通过有关数据获取你的信息。
  - 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