City, State and Federal law enforcement are currently investigating a widespread fraud campaign in which victims' identities are being used to file false unemployment claims.

Victims at the City of Spokane, who have not filed unemployment claims, have received notification from the Human Resources department, or the Washington State Employment Securities Department, indicating an unemployment claim has been filed on their behalf.

The City of Spokane is recommending the following steps for anyone who knows, or believes, they are a victim of **unemployment fraud**.

Steps to Protect Your Financial Identity & Credit History

- **Step One – Upon notification from HR or the Employment Securities Department about a fraudulent claim, contact WA State ESD employment Security Department:**
  - Toll free number to report fraud to ESD: 800-246-9763
  - Email: esdfraud@esd.wa.gov
  - Website: https://esd.wa.gov/unemployment/unemployment-benefits-fraud
    - You will need to provide the following information for identity verification:
      - Full Name
      - Last 4 of your SSN:
      - Your Address
      - Copy of your driver's license
      - Information on how you learned a claim was filed on your behalf
    - If you email please let ESD know: If an imposter-fraud claim was filed using your information, do you give permission to deny and cancel it?
- **Step Two – Crime Check**
  - File a non-emergency report with Crime Check, 456-2233
  - Start keeping a file folder or journal with the information from this incident, including any case numbers. Some government services and accommodations are available to victims of identity theft that are not available to the general public, such as getting certain public records sealed.
- **Step Three – The Three Major Credit Bureaus**
  - Obtain your free credit reports from Equifax, Experian, and TransUnion at www.annualcreditreport.com or call 1-877-322-8228
  - Report to the credit bureaus that the fraudulent claim was made using your identity and provide them with the case number from your police report. You can have a fraud alert put on your identity or freeze your credit. Doing either is free by law.

        - A fraud alert is free and will make it harder for someone to open new accounts in your name. To place a fraud alert, contact one of the three credit bureaus. That company must tell the other two.
        - Experian 1-888-397-3742
        - TransUnion 1-800-680-7289
        - Equifax 1-888-766-0008
    - Check your credit activity at least once a year. As a victim of identity-theft you have the right to check it monthly if you choose.
    - Credit Freeze – If you do not have upcoming large purchases, such as a home, you may want to freeze your credit for more protection. It is free and you can do it yourself. https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs
    - The Washing State Office of the Attorney General also provides security freeze procedures. https://www.atg.wa.gov/security-freeze-procedures
- **Step Four – FTC & IRS**
    - File a short report with the FTC and give them the case number for your local police report https://www.identitytheft.gov/ (good info at www.ftc.gov/idtheft)
    - Consider setting up an IRS account at https://www.irs.gov/payments/view-your-tax-account. If you create an account with your social-security number it will prevent criminals from creating an account using your identity.
    - Another option is to lock your social-security number at https://www.e-verify.gov/employees (The next wave of this cyber-attack may be IRS tax fraud.)
    - All of this reporting seems redundant, but we want to make sure you are recognized as a victim by the local, state, and federal government. Also, the more people who report it, the more support Law Enforcement agents will get to pursue the perpetrators.
- **Step Five – Keep Your Notes**
    - Hang on to any notes, copies of emails, etc. This is the paper trail that you can reference if you face any identity issues or locate inaccuracies on your credit history sometime in the future.

Protecting Your Data and Identity

You are done dealing with the fallout from this unemployment fraud incident, but may choose to further protect yourself from cyber-crime. Below are some steps and resources that the cyber-crime detectives recommend for anyone wanting additional protections for themselves and their families.

- **Control Your Own Information**

- Services that lock credit information can help, though you must provide companies with your own personal data, potentially creating more risk.
  - Most attackers use data obtained from previous internet breaches of hotel chains, entertainment services, and other widely-used digital productivity tools. That is why it is important to never use the same password twice.
  - Use Multi-Factor Authentication (a secondary security code) on your most important accounts.
  - Most importantly, be vigilant and watch out for phishing emails, vishing fraud calls, and even things like mail/package theft, which can lead to your identity being compromised
  - Be wary of free apps/offers, which could be mining your data.