Fraudulent Employer Intrusion in Connecting Colorado Procedure

I. Purpose:

Intrusions are most frequently reported to local workforce staff by job seekers who have been approached with phishing scams. Others are caught by workforce system staff. This procedure provides steps to take when a fraudulent employer gains access to job seeker records in Connecting Colorado.

II. Scope and Goal:

A. Scope: This procedure applies to the Workforce Services Coordinator, the Business Services Executive Committee, MIS, local area business services staff, and local area Directors.

B. Goal: To standardize the process for handling intrusions into Connecting Colorado by fraudulent employers where the fraudulent employer gains access to job seeker contact information, including notification of job seekers.

III. Responsibilities:

A. WDP Staff Person: The Workforce Services Coordinator is responsible for managing this procedure.

IV. Procedure:

A. Definitions:

1. **Intrusion Detection:** The identification of a cyber intrusion by an attacker utilizing a fraudulent account established in Connecting Colorado. Intrusions are most frequently reported by Job Seekers who receive phishing attempts such as text messages, voice mail or email requesting google chat or google hangout.

2. **Phishing/Phisher:** The fraudulent attempt to obtain sensitive information, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

B. Notifications to CDLE Fraudulent Employer Email:

The Statewide Business Services Executive Committee will receive emails sent to CDLE_FraudulentActivity@state.co.us. The Executive Committee shall determine the lead point of contact for an intrusion. Generally, that person is the CDLE Workforce Services Coordinator.

C. Upon notification of a possible intrusion:

1. **Workforce center employee detecting or notified of the intrusion:**
When a Workforce Center employee is notified of or detects a possible intrusion, it is critical to complete the following steps and notify his/her immediate local area manager/Director and the State Business Services Executive team using the link to the “Fraudulent Employer and Phisher Intrusion Report” form” on the Connecting Colorado “Staff Information” page as quickly as possible.

2. Seek job orders where the job seeker's name, who reported the phishing, appeared. See p. 5 of this procedure for Connecting Colorado screenshots
    a. Use the information to identify the source Employer Account of the intrusion in Connecting Colorado. Seek support from experienced business services staff to help in the investigation.
    b. Investigate the employer account to determine if it is a fraudulent employer.
    c. If the employer is determined to be fraudulent:
        i. Inactivate the fraudulent employer account and store an FE "Fraudulent Employer" service code to the employer record.
        ii. Note: If the employer account is not in the local area, the area must be modified in order for the account to be inactivated.
        iii. Add detailed case notes to any employer determined to be fraudulent,
        iv. Note: Use the regular notes and not the confidential notes.
        v. Close all job orders associated with the fraudulent employer account,
        vi. Identify staff who approved employer account.
    d. Use the Fraudulent Employer AND Phisher Intrusion Report, complete as much information as possible on the form and copy all information from the completed form to the *Notes* of the employer record. Request as much information as possible, including:
        i. Name and Connecting Colorado Mask Number for the reporting job seeker
        ii. Any information used in contacting the job seeker by the phisher:
            - How contact was made
            - When contact was made
            - Actions requested by the phisher
            - Actions taken by the job seeker (did that person provide any personal information such as credit card numbers, bank information and social security number)
            - Copies of text messages, email and voice messages, and documents exchanged contracts, job application, bank information, checks, etc.
    e. Use the Job Referrals CSV Report to generate a list of people who are on the referral list for a fraudulent job order. Enter a Job Order Number and view the referrals in a CSV format. The CSV Report tab is available on the job order screen, under "View Referrals". Use the list of referrals, contact information for any/all job orders associated with the fraudulent employer account and share that information with the Director of the local area where the intrusion occurred.

3. **The local area manager/Director receiving the initial notification shall:**
    a. Review all information collected and actions taken by the workforce center employee.
    b. Managers will communicate the information and action taken with the local area Director email the cdle_fraudulentactivity@state.co.us email box, with a report of action taken.

4. **CDLE Workforce Services Coordinator (or designated lead) shall:**
    a. Determine who at the State level needs to be informed about fraudulent activity, such as:
        i. CDLE Management
        ii. CDLE Government Policy and Public Relations (GPPR)
        iii. State MIS/CSDC
        iv. Statewide Business Development and Career Services representatives and managers.
        v. Other officials as appropriate.
    b. Share information including the fraudulent employer information, any information received from job seekers, the local area where the intrusion originated, and the number of names on the employer account(s)' referral lists.

5. **The local Director of the area identified on the fraudulent employer account shall:**
    a. Use the approved template (Attachment A), send email to job seekers referred to any/all job orders associated with the fraudulent employer account. A list of job seekers referred can be pulled from the Job Referrals CSV Report available on each Job Order;; and communicate, using the cdle_fraudulentactivity@state.co.us email account, once the process is complete.
    b. Summarize actions taken and any known outcomes of an event.

V. Quick Reference - Who to Contact:

Contact	**Name, job title, email, phone**
Tom Morgan	Workforce Services Coordinator 303-318-8191 tom.morgan@state.co.us

APPROVED EMAIL TEMPLATE FOR CUSTOMERS REFERRED TO FRAUDULENT JOB ORDERS

***** ATTENTION *****

This email is to inform you that we have become aware that you may have been, or could be contacted in the near future by a fraudulent employment phishing scam to obtain your personal information. We are informing you of this issue as a precautionary measure.

If you recently received a text message, voice mail, phone call or email concerning possible employment opportunities, please be wary.

Current phishing attempts come from company names such ****NAME**** or ****NAME****. If you receive communications from individuals claiming to be from these companies, be wary. The recent phishing communications use text messaging and contain typos and poor English. The HR manager often uses the title of "Dr." in their name.

Here are some recommendations on how to spot fraudulent activities:

- If you are called from an automated system and are asked to call your local Workforce Center at a fraudulent number. You should please call the number on the Workforce Center's website, not the one provided by the automated system.
- If you return a call, you may be asked for your social security number and date of birth. Please note that the Workforce system DOES NOT ask for your personal information such as social security number or date of birth over the phone, by text message or email.
- If the contact requires you to set up a Google Hangout account or contact through Google Chat.

To protect you from fraudulent activities:

- Be cautious about opening attachments or clicking on links in email.
- Use your favorite search engine to look up the website or phone number provided.
- Do not respond to any emails that request personal or financial information. This includes:
    - Social Security Number
    - Current Address
    - Date of Birth
    - Phone Number
    - Bank Account, Bank Card, or Credit Card Information
- If you think a company really does need your personal information, pick up the phone and call them yourself using the number on their website, not the one on the email.
- Always remain cautious, and if you ever feel suspicious about an email or phone call, do your research and ask questions.

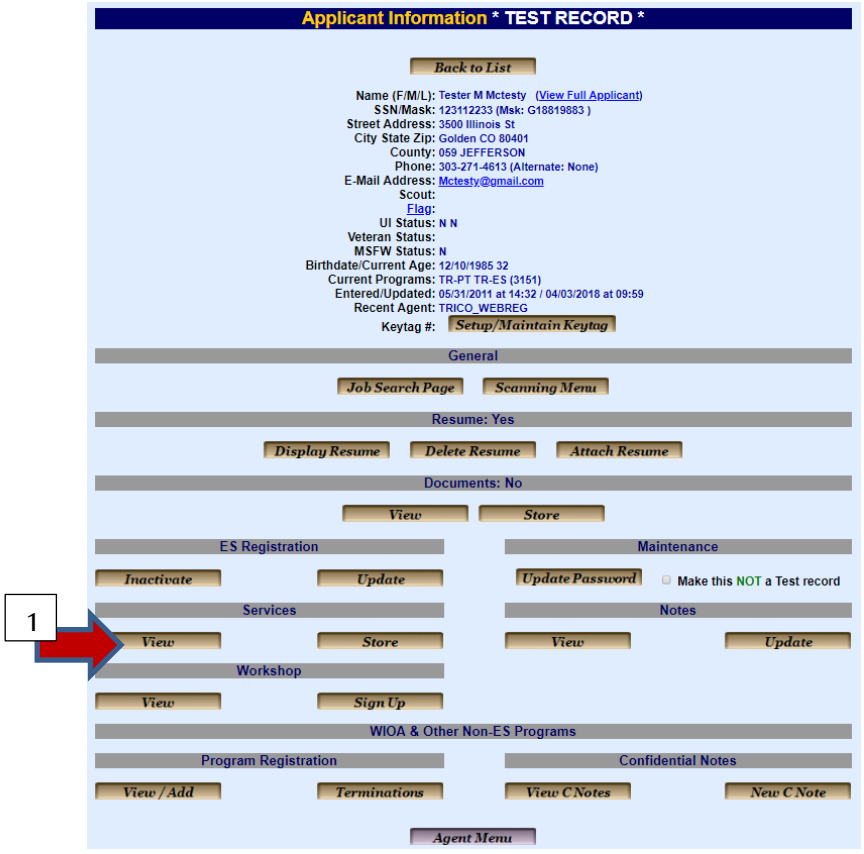
If you think you have been approached by a phishing scam, please contact your local workforce center to help us track attempts and better inform job seekers about these scams.

Investigating a Reported Fraudulent Employer Account (Job Posting) in Connecting Colorado

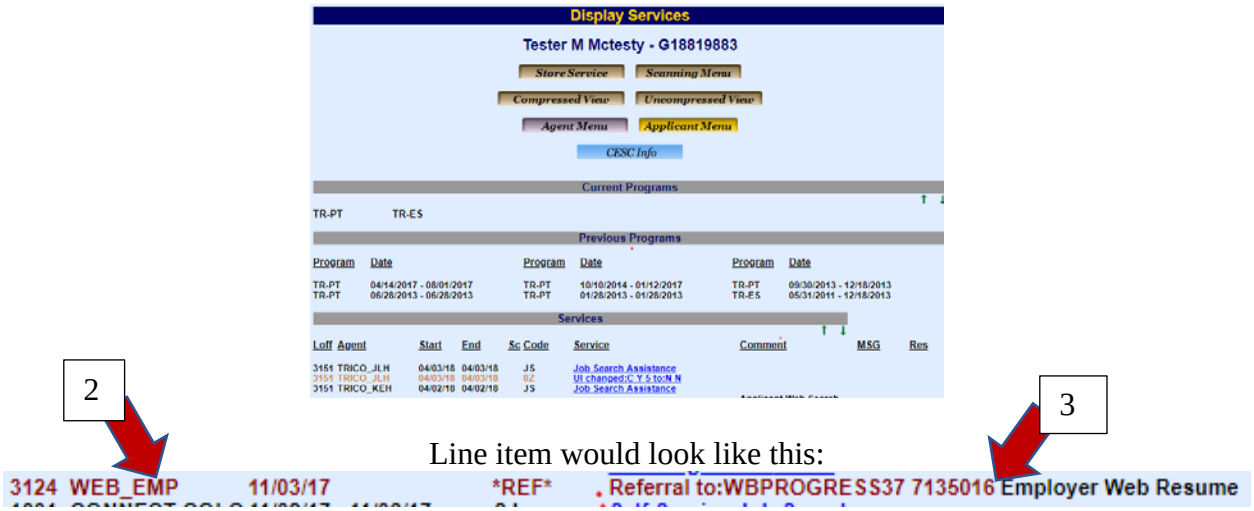
Situation:
You receive a report from a jobseeker that believes they have been contacted by a scam employer. Here is the information that you will need to have in order to find which account/job order in Connecting Colorado the scam employer used to obtain the Jobseeker's contact information.

- Name and Social Security Number of the Jobseeker
- Date of contact by scam employer (or as close as possible)

Note: Do not try to match the employer name from Connecting Colorado with the company name that was given to the Jobseeker. They will not be the same.
Go to the jobseeker profile and pull up their services (arrow #1).

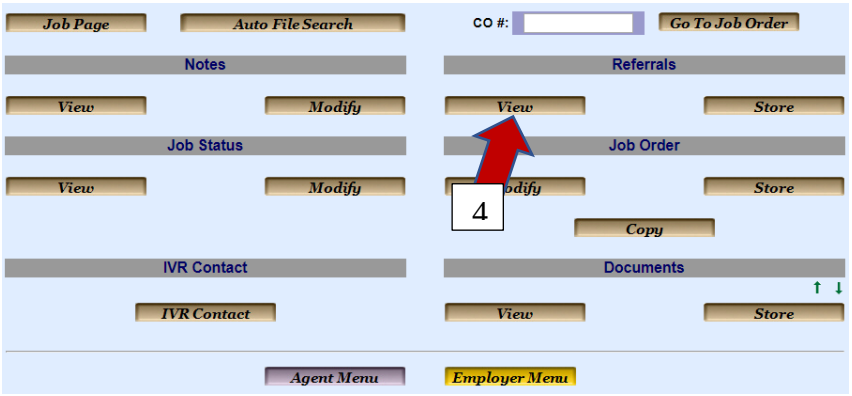


Look for the services that display the Agent as WEB_EMP. Find the date the referral was taken from Connecting Colorado and match the closest date to the date jobseeker was contacted.

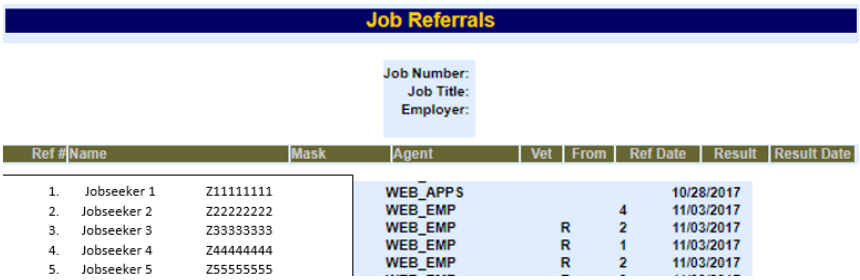


From the WEB_EMP line (arrow #2) look up the job number in the service column (arrow #3).

Go to the Main Screen and enter the job order number. From the job order go to the Referrals tab and select the View option (arrow #4).



Find the name of the jobseeker reporting the scam. This is the job order that the scam employer used to get jobseeker contact information. Other Jobseekers with WEB_EMP agent will be possible targets for the scam employer to contact.



Check out the job order and look for potential red flags. If job looks fraudulent, close all job orders on the account immediately and mark Employer record with **FE** (Flagged Employer).