STATE OF NEW MEXICO
DEPARTMENT OF FINANCE AND ADMINISTRATION
FINANCIAL CONTROL DIVISION

407 GALISTEO STREET
BATAAN MEMORIAL BUILDING, ROOM 166
SANTA FE, NEW MEXICO 87501
(505) 827-3682 FAX (505) 827-3692

Michelle Lujan Grisham
Governor

Olivia Padilla-Jackson
Cabinet Secretary

Donna Trujillo
State Controller
Director

MEMORANDUM

Date: August 16, 2019

To: All State Agency Human Resource Managers and Chief Financial Officers

From: Lakisha Holley, Central Payroll Bureau Chief

Subject: Payroll Phishing Fraud

The Central Payroll Bureau has received several notices within the last month from Human Resource Managers, other personnel authorized to make changes to employee direct deposit information, and state employees regarding payroll phishing attempts. Fraudulent email requests are being received that seek to change employee direct deposit information. The fraudsters use spoofed email accounts that seem to be from a known employee. In each case, the email was not sent from a State of New Mexico domain email address.

To protect employees from payroll phishing fraud, we encourage Human Resource Managers and Chief Financial Officers to set internal controls and preventative measures to ensure requests are legitimate. The following is a list of basic precautions and controls that are highly recommended by DFA and the State Personnel Office:

Once Human Resources receives the request, they should:

1. Check that any email received regarding a direct deposit authorization or change is from a state.nm.us email. If the employee hand delivers the form, check the employee's identification to confirm that the employee's name matches the form and bank statement or voided check.
2. Verify that all info is correctly entered on the form and above documentation was provided.
3. If the form was received by email:
    a. Call the employee to verify the change and advise the employee to expect an email that the employee will need to confirm.
    b. Email the employee back to confirm in writing the authorization or change.

c. Wait for the employee to confirm the change via email and then make the change.

4. Notify the employee by email or letter when the request has been completed and processed.

If there is suspected phishing and spoofing fraud, please notify DoIT and report fraud to the State Auditor (OSA) as soon as possible. Attached is a letter from OSA that was distributed on March 15, 2019 which provides further information regarding payroll phishing fraud.