New Mexico Office of the State Auditor

GAO
Government Accountability Office

1-866-OSA-FRAUD
www.saonm.org

State Auditor
Brian S. Colón, Esq.

Risk Advisory:
Don't Get Spoofed
Payroll Phishing Fraud Alert

March 5, 2019

The Office of the State Auditor (OSA) issues this Risk Advisory to alert governmental agencies and entities, the general public, and business owners in the State of New Mexico of risks associated with an email phishing scheme seeking users to change their direct deposit information for payroll utilizing spoofed email accounts. The OSA strongly advises individuals to be aware of the potential risk associated with responding to requests to change direct deposit information that appears questionable and to review their internal controls and processes for making any changes and updates to employee direct deposit information to prevent and detect fraud, waste, and abuse associated with the phishing and spoofing scheme.

Phishing and Spoofing Alert

The OSA has received several notices of state employees receiving email requests to change bank/financial institution account information of employees to redirect the employee's payroll direct deposit to a fraudulent account. In each instance, the phishing attempt to collect confidential information was sent by a fraudster using a spoofed email account, meaning the email account is an imitation or forgery of an email that appears to have originated from a known source, often another high-level state employee.

Red Flags

The phishing and spoofed accounts have been reported as follows:

- The domain of the sender imitates the real domain of a known individual to the recipient, be extra cautious of email that appear to be from managers, supervisors, and other high-level directors;
- The body of the email uses urgent language with a specific request, which places pressure on the recipient to expedite the request;
- The email requests the recipient change their bank/financial institution account information associated with their direct deposit to fraudulently redirect the recipient's payroll into an unknown and unauthorized bank/financial institution account.

New Mexico Office of the State Auditor

GAO
Government Accountability Office

1-866-OSA-FRAUD
www.saonm.org

State Auditor
Brian S. Colón, Esq.

Risk Advisory:
Don't Get Spoofed
Payroll Phishing Fraud Alert

March 5, 2019

Be Aware!

The OSA has received reports of potential criminal violations and suspected fraud associated with phishing and spoofed email requests for payroll changes from the Public Education Department, Santa Fe Public Schools, Clovis Municipal Schools, New Mexico Military Institute, Bernalillo County, and Central New Mexico Community College. We believe all State agencies and entities should be on high alert.

It's important to note that once a transfer of direct deposit funds is complete to the fraudulent bank/financial institution's account it can be difficult to get the funds back, causing a loss to the agency or entity. A swift response to an identified fraud is the best option at reactive remediation for recovery.

Reporting Suspected Phishing and Spoofing Fraud

Report fraud to OSA, as soon as possible. In accordance with 2.2.2.10(N)(2) NMAC, promulgated pursuant to NMSA 1978, Section 12-6-6, an agency or IPA (Independent Public Accountant) shall notify the State Auditor immediately and in writing upon discovery of any violation of criminal statute in connection with financial affairs. Include the following information in the written report:

- Estimated dollar amount involved; and
- Complete description of the violation, including names of persons involved and any action taken or planned.

To report fraud, waste, or abuse in any public entity in New Mexico:

- **Report online: www.saonm.org**
- **Hotline: 1-866-OSA-Fraud**

Risk Advisory:
Don't Get Spoofed
Payroll Phishing Fraud Alert

March 5, 2019

New Mexico Office of the State Auditor

GAO
Government Accountability Office

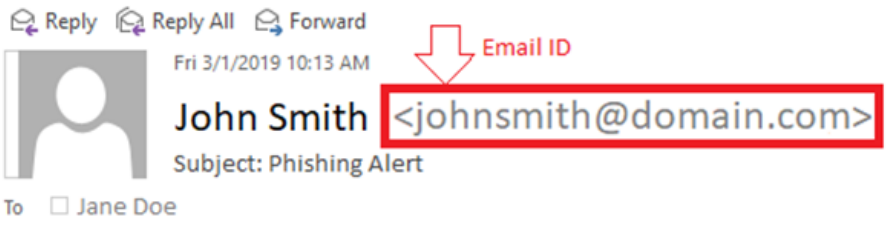
1-866-OSA-FRAUD
www.saonm.org

State Auditor
Brian S. Colón, Esq.

What Can You Do To Protect Yourself

Individuals are strongly encouraged to take the following proactive and preventative measures to ensure phishing attempts and spoofed emails are identified:

- If you are the recipient of an email request to change payroll distribution do not share personal bank/financial institution account information via email or make any changes to redirect employee payroll without validating the request or receiving prior authorization by the employee;
- Validate the domain of the sender as genuine. Enabling display of email ID will show you the domain of the sender to validate whether the email ID (including domain) matches with display name;



- Validate any suspected phishing attempts and suspected fraudulent requests through an alternate source; by phone or in-person with the sender. Call a known phone number for the individual listed as the sender, do not call an unknown phone number that may be listed in the potentially fraudulent email;
- Change passwords and never reveal your confidential information unless you are certain it is a legitimate request;
- Review internal controls and operational handbooks for how to report phishing schemes and alert appropriate IT professionals; and
- Conduct a special training and alert team members of phishing and spoofing schemes.

For further information or questions, on this or any Risk Advisory issued by the GAO, please contact the Government Accountability Office Director, Stephanie W. Telles at Stephanie.Telles@osa.state.nm.us

GAO
Government Accountability Office
New Mexico Office of the State Auditor