November 2019

RISK ADVISORY

HACKED! RANSOMWARE DEFENSE

TIPS TO LESSEN EXPOSURE

- ⇒ Change passwords frequently and use different passwords for all websites.
- ⇒ Take proactive measures to ensure all software is up to date.
- ⇒ Utilize pop-up blockers and close unwanted pop-ups by using keyboard command strokes (Ctrl + X) instead of clicking on the dialog box.
- ⇒ Ensure reliable antivirus software is in place and that it protects against spyware.
- ⇒ Safeguard important files by ensuring they are securely, properly, and frequently backed up.
- ⇒ Exercise caution when clicking on links or downloading attachments and be cautious of suspicious emails.
- ⇒ Ensure controls are in place that prevent the launch of executable files from emails. Executable files have the ability to run code when opened. Common executable files are: .BAT, .EXE, .BIN, and even .COM
- ⇒ If faced with ransomware, agencies should not send money; and they should immediately report the incident to local law enforcement and inform the OSA.

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

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

The Office of the State Auditor (OSA) has issued this Risk Advisory to alert the public, business owners, and governmental agencies in the State of New Mexico of risks related to the dangers of ransomware. The OSA strongly advises its stakeholders to be aware of the potential risks associated with cybersecurity threats, such as malware, in which the victim's data is encrypted and payment is demanded for the release or decryption of data. The OSA further advises reviewing internal controls and developing procedures to aid in the prevention and detection of cybersecurity threats that may lead to waste, fraud, and abuse associated with ransomware.

What is ransomware?

Ransomware is a serious cybersecurity threat caused most often by malicious links, spam email, compromised websites, and other malware.

Red flags include: receiving emails with irrelevant headers and/or subject lines or no subject at all; being CC'd/BCC'd on an email from a sender or other receivers that are unknown; attachments that don't make sense or are executable files; or hyperlinks embedded that link to a different site.

Be Aware! Report Suspected Ransomware and other cybersecurity threats.

The OSA has received reports of potential criminal violations and suspected fraud associated with ransomware from school districts with encumbrances that totaled over $1.3 million in recovery and repairs.

Reports of instances related to this and other cybersecurity threats should be made to the OSA as soon as possible. In accordance with 2.2.2.10(N)(2) NMAC, and NMSA 1978, Section 12-6-6, an agency or 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.

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