SAN FELIPE DEL RIO CISD

Press Release – February 8, 2020

SFDRCISD TECHNOLOGY NETWORK SYSTEM ATTACKED BY RYUK MALWARE

SFDRCISD's Chief Operations Officer Les Hayenga announced that a portion of the District's technology network system was attacked by malware early Saturday morning. SFDRCISD's Technology team immediately discovered that some of our District's servers, which mainly provides storage for the District's network shares and print servers, were affected by the RYUK malware. While this attack made portions of these systems inaccessible to District users, it is not believed that any personally identifiable information of staff or students was exposed to risk.

Hayenga, who also serves as the coordinator between the District and the Texas Education Agency (TEA) in cybersecurity matters, set into motion the District's cybersecurity plan allowing the technology team to isolate the malware quickly and secure the District's cyber infrastructure against any further risk of cyberattacks. The SFDRCISD Technology team coordinated efforts with Dell cybersecurity engineers and response teams on Saturday to efficiently assess what was not working and collaborated with the FBI to identify whether a breach involving sensitive, protected, or confidential information had occurred. Once the issue was identified, all teams immediately began the full restoration process of the affected servers.

"Thanks to the quick assessment and prompt action taken by Mr. Hayenga and the Technology team, the impact could have been much worse, perhaps even disastrous," noted SFDRCISD Superintendent Dr. Carlos Rios. Dr. Rios explained, "Mr. Hayenga and the Technology team have been working over the past few months to refine the District's cybersecurity plan in the event of a cyberattack. Yesterday, our systems were attacked; and because of this team's superior depth of knowledge and their dedication to quickly resolve the issue this weekend, we can rest assured that they have been successful in limiting the potentially disastrous impact this virus could have caused within our systems.

In the third tier in the District's cybersecurity plan, the District immediately informed and reminded staff to implement safety protocols and cyber security practices to further protect and prevent the District's network system from being placed at risk of being exposed to any potential malware. District personnel are advised that while the Technology team is working effortlessly to restore the system to its full potential, some district campuses or departments may experience limited service or accessibility. "Full restoration may take a few hours or a few days," explained Dr. Rios. "We thank our staff and community for their patience and understanding while we safely and securely bring our impacted systems back online.