

Cyber-Attack FAQs

1. What happened?
 - a. Travis Central Appraisal District was impacted by a cyber-attack. The cyber-attack was a ransomware virus. A ransomware virus encrypts data/locks files stored and keeps them in this state until a ransom is paid.
2. What was affected?
 - a. The cyber-attack encrypted files on many servers and included website property search, phone, email and computer assisted mass appraisal systems. Because the encrypted files were locked they were not accessible to the server and caused the system services to stop working.
3. Did the District pay the ransom and if so, how much?
 - a. No, the District did not pay any funds to decrypt our files. Law enforcement does not recommend victims of cyber-attacks pay any ransom. The District staff is working in conjunction with cyber security experts to remediate and restore systems functionality.
4. What have you done to fix the issues?
 - a. As soon as the virus was detected we implemented our security incident response and business continuity plan, we took immediate action to secure our system, infected systems were isolated, backup data was secure, appropriate state agencies were contacted, and cyber security experts were engaged to assist with remediation and restoration of system services. The District maintains comprehensive backup data at secure offsite locations that are being used to restore files and system services.
5. Was any confidential information affected by the cyber-attack?
 - a. No, the sole purpose of the cyber-attack was to encrypt and lock district files to hold them hostage for ransom.
6. Is there any evidence of a data breach?
 - a. There is no evidence that any data was breached during the attack.
7. Is there any evidence that this virus propagated to other systems?
 - a. There is no evidence that they virus propagated to other systems.
8. Was this related to the cyber-attacks on local government entities in August 2019?
 - a. While the District cannot say what variant of ransomware the other local government entities were infected with, the two incidents are similar in that they are both ransomware attacks on local government entities where funds were demanded for a decryption key to release the government data.
<https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault>
9. When will the system be back up?
 - a. Daily operations including appraisal protest and customer service are not being impacted. Identification and removal of the virus along with additional measures to prevent future attacks was the first priority. Website property search, phone, email, and computer assisted mass appraisal systems have been restored. Secondary systems will be restored within the next one to two days.
10. What efforts have been taken to make sure this does not happen again?
 - a. The District will continue to work with cyber security experts to conduct forensic analysis to identify the parties responsible for the cyber-attack and to implement future preventative measure.