RANSOMWARE:
Protect your business

Ransomware is malicious software accessed network via an email attachment or a website that encrypts files on a computer network without user knowledge effectively locking that data. The only way to decrypt the data is usually paying a "ransom" to the criminals to release the data.

The FBI has recently warned of potential ransomware attacks specifically directed at agricultural cooperatives and timed to critical planting and harvesting seasons. This could disrupt your operations, cause financial loss, and negatively impact the food supply chain.

Cyber threat actors will continue to exploit network and system vulnerabilities within the food and agricultural sector. Implement the following to protect against ransomware attacks.

PASSWORDS

Use strong passwords and multi-factor authentication when possible.

BACKUPS

Regularly back up data and password protect backup copies offline.

ANTI-VIRUS

Install and regularly update anti-virus and anti-malware software on all systems.

TRAINING

Train team members to recognize phishing and ransomware scams on email and phones.

PATCHING

Install updates/patch operating systems, software, and firmware as soon as available.

PLANNING

Implement a recovery plan in the event systems go offline. Develop a plan to respond to a ransom request.

CENTRAL TEXAS FARM CREDIT