Protect Your Business From Ransomware

AgTrust™ FARM CREDIT

What's happening?

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

What is Ransomware?

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.

What should you do?

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 multifactor authentication where 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.
PLANNING Implement a recovery plan in the event systems go offline and develop a plan to respond to a ransom request.	**PATCHING** Install updates and patch operating systems, software, and firmware as soon as available.	**TRAINING** Train team members to recognize phishing and ransomware scams on email and phones.

Ransomware Readiness Checklist:

- ☐ **Active anti-virus solution**- Have an up-to-date anti-virus scanning solution to detect incoming infected files
- ☐ **Active firewall protection**- Have active firewalls in place restricting port access on your network
- ☐ **Multi-factor authentication (MFA)**- Use MFA, where possible, to restrict unauthorized access attempts
- ☐ **Latest OS security updates**- Eliminate known vulnerabilities in the Operating System by applying available patches
- ☐ **Latest application security updates**- Keep applications updated to eliminate known vulnerabilities
- ☐ **Back up your data**- Keep at least two backups of your important data
- ☐ **Microsoft Office**- Turn off Macros in the Microsoft Office suite– Word, Excel, PowerPoint, etc.
- ☐ **Email safety**- Never open spam emails or emails from unknown senders
- ☐ **Attachments**- Never download attachments from spam or suspicious emails
- ☐ **Links**- Never click links from spam or suspicious emails