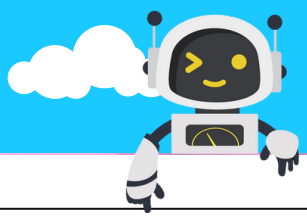

MY TRACTOR THINKS IT'S IN TEXAS

Use Strong Passwords

Ensure that all connected devices and accounts (like GPS systems, machinery software, or cloud storage) have strong, unique passwords. Enable multi-factor authentication wherever possible to add an extra layer of security.

Software Updates

Keep the software and firmware on your equipment up to date. Manufacturers often release updates to fix security vulnerabilities, so make sure you're installing these patches as soon as they become available.

Secure Your Network

Your farm equipment may rely on wireless networks for communication. Make sure your Wi-Fi network is encrypted and set up a firewall to protect your network from unauthorized access. Separate IoT devices from other network components to limit the impact of potential security breaches.

Educate and Train

Ensure everyone working on the farm understands cybersecurity risks. Conduct regular training on how to spot phishing attempts, suspicious emails, or social engineering tactics that scammers may use to gain access to your devices or data.

Monitor Access

Continuously monitor network traffic for unusual activity and implement intrusion detection systems to promptly identify and respond to threats. Restrict access to critical farm equipment and systems to trusted individuals only.

Backup Your Data

Protect your valuable farm data, such as operational data, GPS coordinates, and inventory records, by backing it up frequently. Use both local and cloud-based backup solutions so you can recover your information in case of a cyberattack or system failure.

Resources:

- cisa.gov/resources-tools/resources/food-and-agriculture-cybersecurity-checklist-and-resources
- foodandag-isac.org
- cyberhouserock.info