Protect your farm against cyber attacks

Security measures often focus on in-person property access, such as visitor logs, hiring practices, and keeping areas of the farm locked and secure. Cybersecurity is just as critical. Cyber-attacks are being carried out by animal activists and other groups that seek to expose, embarrass, or exploit farms and other organizations. Potential tactics include stealing data, publishing personal contact information to intimidate owners and employees, blocking access to crucial technology resources to disrupt business, or posting information online to embarrass a company

Ensure your systems and data are protected

1. Annually, have an IT security assessment conducted by a qualified security auditor who can identify IT infrastructure vulnerabilities. Though this may be expensive, it can prevent the costly loss of critical data.
2. Ensure all hardware and software is kept current with the latest updates. Identify all machines connected to the internet and assess associated security protocols. Regularly back up all files.
3. Update your emergency plan to include how to respond to a cyber-attack and distribute it to key personnel.
4. Train employees on how to avoid common attacks. See best practices below.
5. Learn about ransomware and how to avoid, or survive, a potential attack.

Signs that a system is compromised

Contact IT support immediately if the following occurs:

- The computer software is working oddly. Examples: a mouse cursor moves across the screen on its own, or internet searches are redirected.
- The internet is considerably slower than usual.
- There is a large increase in phishing emails.
- Operating software or antivirus programs cannot be updated.

Additional cybersecurity tips

Develop a company policy that no personal information will be requested from an employee via email or text. Make it clear to employees that unsolicited requests are not from the company.

Prohibit employees from using company computers and other devices for personal use.

Employee Training

- Never click on a link or attachment unless the email is from a safe sender and be on guard for a familiar sender with an unknown domain.
- Educate employees on catfishing (using a fake identity on social channels).
- Be cautious of people who seem too interested in their job and ask specific questions about their work or the farm either online or in-person.
- Never send company information to someone who is not an employee.
- Don’t open spam, including to unsubscribe. This confirms to the sender you exist. Delete it unread.
- Log-out and shut down computers and mobile devices when not in use.