OFA FACT SHEET

August 2025

Why cyber security matters on the farm and how to protect yourself

Overview

Today's world is so connected that it's a matter of when, not if, a business will face a cyber security problem. Breaching incidents of all kinds, from compromised information to financial fraud or data held for ransom are on the rise, and agriculture is not immune to these threats.

The agri-food industry can be particularly vulnerable, especially at the farm level where many small, independent businesses have limited IT resources – and cyber security often tends to be one of those things that most people don't worry about until it happens to them or someone close to them.

Threats come from criminals, state-sponsored international hackers and activists.

Cyber security lingo

Computer virus: a type of malware that spreads between computers and damages data and software.

Data breach: private or sensitive information accessed, stolen, or shared without permission

Ransomware: malicious software that locks or encrypts your files and demands payment to unlock them

"Phishing" – a scam to trick people into giving away personal information, like passwords or credit card numbers, by pretending to be a trusted person or organization.

Key cyber security threats:

- **Outdated, unmaintained systems running old software**
  90% of farming systems haven't been updated*
  Most farms don't have a software patching or updating policy
- **No data backup**
  Data can't be recovered in security breaches, computer or server failures, or virus situations
- **Weak access control**
  Sharing passwords, using a single login for all users, and not removing access from former employees all compromise systems
- **Fake emails and text messages**
  Increasingly sophisticated but fake requests for banking or personal details can cause financial loss or data theft.

Ignoring cyber security = disruption, financial losses, decrease in customer trust

How you can protect yourself and your farm business

Cyber security isn't foolproof, but simple, consistent steps can greatly reduce risk—much like how we approach biosecurity. Here are some practical actions you can take:

Make sure hardware and software is kept up to date. Use strong passwords that aren't shared between employees and remove access from employees who no longer work for you.

Back it up. Copy your most important information regularly and store it in a safe place. Install valid anti-virus software, firewalls and malware detection systems that are kept up to date.

Never use public Wi-Fi to check your on-farm systems when you're away. Use a Virtual Private Network (VPN) or connect to your monitoring apps using the cellular data on your device.

Don't click on unverified links in emails or text messages. If you're not sure whether a message is legitimate, use a different method – like a phone call – to contact the supposed sender to verify the request.

Never reveal sensitive business or personal information to unsolicited callers. This is especially true if they say they are from a financial services provider.

Track your connected devices. Know which devices, sensors, computers, servers, mobile devices, automated equipment, environmental control systems, financial systems, and other hardware are connected in your on-farm networks.

Train yourself and your team. Establish basic rules to recognize where threats come from and what to do – or not do. Free online videos are available to help with training.

Excerpts from recent OFA Viewpoints

"Cyber security often tends to be one of those things that most people don't worry about until it happens to them or someone close to them. On our farm, we ended up bringing in some IT expertise to conduct an audit of all our systems, which we'd been piecing together for close to 40 years. Taking any kind of preventative action will reduce your risk in both the short and long-term."

Teresa Van Raay, Director, Ontario Federation of Agriculture
October 2024

"Ultimately, we need to think about cyber security on the farm like we do biosecurity – an investment into a best practice that, while not foolproof, will go a long way to minimizing or even avoiding risk. There is no such thing as 100% security, but with cyber criminals looking for weak or vulnerable targets, there are steps to minimize risk as much as possible."

Cathy Lennon, General Manager, Ontario Federation of Agriculture *May 2023*

Think of cybersecurity like biosecurity: it's not perfect, but every precaution counts toward protecting your farm's future.

For more information, including Viewpoints, resources, and a recorded webinar visit ofa.on.ca