Cybersecurity and AI

Jane Richter, Communications & Marketing Manager, Berries Australia

Artificial intelligence (AI) is quickly becoming part of everyday farming and business, from marketing tools and record keeping to forecasting and customer communication. Many berry growers are already using tools like ChatGPT, Microsoft Copilot, or AI-powered farm software, often without thinking twice. These tools do save time, improve decision-making, and can help your business run more efficiently. But like any new technology, they also bring new risks, especially when it comes to cybersecurity and protecting your data.

The good news is that staying safe doesn't require complex IT knowledge. With a few simple practices, you can use AI confidently while protecting your farm business. The Australian Government's Australian Signals Directorate (ASD) has recently published a guide to ***'Artificial intelligence for small business'***, and this article draws from the information provided there to help growers understand the risks and set in place safeguards for their business.

Farms today are businesses that rely on large amounts of digital records (spray logs, picking data, payroll, financial transactions) and often use multiple online systems (email, cloud storage, harvest software platforms) to manage and share both customer and staff data. That makes them a target.

Cyber incidents aren't just a "big business problem" in fact small businesses including farms are often more vulnerable because they don't always have formal systems in place or tech experts on staff. When AI tools are added into the mix, the risks can certainly increase if they are not used carefully.

AI refers to software that can perform tasks like writing emails or reports, analysing data, answering questions or even generating content. Most AI tools are cloud-based, meaning the information you enter is processed online rather than on your own computer and this is where cybersecurity becomes important.

The ASD guide highlights three main cyber risks when using AI tools.

1. Data Leaks and Privacy Risks

AI tools often require you to enter information to get a response. If that information includes customer details, staff records, financial data or farm business information, it could potentially be exposed or reused.

Some AI providers may store or use data to improve their systems, depending on settings and terms of use, so the key message here is never assume information you enter into AI is private unless you've checked.

2. Incorrect or Misleading Outputs

AI tools can sometimes give incorrect answers (also sometimes called 'hallucinations'), can be manipulated by bad inputs and even sound really confident but be totally wrong!

For example, the guide highlights a real case where a professional relied on AI-generated information that turned out to be false, leading to serious consequences.

Remember that AI is a useful tool but should never be the final decision-maker. Always double-check important outputs and ensure that the facts are correct.

3. Third-Party and Supply Chain Risks

Most AI tools rely on external providers (software companies), and if those systems are compromised, your business could be affected. This includes risks like data breaches, system outages and weak security from providers.

Always remember that you are only as secure as the systems you use. Ensure your online access always uses strong passwords for all programs or apps, and enable two-factor authentication wherever possible.

You don't need to become a cybersecurity expert. Focus on a few practical habits.

1 Be Careful What You Enter into AI

- Don't upload personal, financial, or sensitive farm data
- Remove names and identifying details where possible
- Treat AI tools like a public space unless proven otherwise

2 Set Clear Rules for Staff

- Make sure everyone knows what can and can't be entered into AI tools
- Provide basic guidance on safe use
- Remind staff regularly

The ASD guidance stresses the importance of training staff on responsible AI use as this is a new area where accepted norms don't yet exist.

3 Check Your AI Tools Before Use

- Where is my data stored?
- Who owns the data?
- Will it be used to train the system?

4 Always Verify AI Outputs

- Double-check facts
- Don't rely on AI for critical decisions without review
- Use human judgement for anything important

5 Choose Trusted Providers

- Use reputable platforms
- Check for clear privacy policies
- Look for providers that prioritise security

6 Keep Basic Cybersecurity Strong

Outside AI, simple steps make a big difference:

- Strong passwords
- Multi-factor authentication
- Regular software updates
- Controlled access to sensitive information

A Simple Checklist for Growers

Before using AI in your business, ask yourself:

- Do I understand the risks and benefits?
- Do I know what information is safe to share?
- Have I checked how the tool handles my data?
- Do I verify the outputs before using them?
- Have I trained my staff on safe use?
- Do I know what to do if something goes wrong?

Where to Get More Help

- www.cyber.gov.au
  Small Business Cyber Security Hub
- www.cyber.gov.au/report
  To report incidents
- www.cyberwardens.com.au
  Offering free training for small businesses