CyberWardens.

Protect your agribusiness from cyber criminals

The small business Cyber Security Guide for Agriculture

An initiative of COSBOA

cyberwardens.com.au

Cyber safety for your agribusiness

Micro and small agriculture businesses play a vital role in providing quality produce and products to local communities, creating employment and having an economic impact on all regions across Australia.

As you know too well, farmers and producers across livestock, cropping and horticulture have always faced diverse risks and challenges to overcome. And while the increasing use of internet-based technology has many benefits for agribusinesses, cyber security is a growing risk that needs to be managed.

In Australia, the agriculture sector is regularly targeted by cyber criminals. The latest data showed one in five agricultural businesses experienced at least one cyber incident a year[1]. From your automated machinery, drones and sensors on the farm, cameras scanning conveyor belts and batch tracking in production, and the digital finance management systems that agribusinesses rely on.

The latest COSBOA research shows that 8 in 10 small business owners/CEOs and employees have experienced a cyber threat at work or in their personal lives. Yet, 4 in 10 small businesses have little to no confidence in their ability to respond to a cyber threat.

Many small businesses consider themselves too small to be targeted by cyber crime which is simply not true. Recent data released by the Australian Signals Directorate clearly shows the frequency and financial impact of the threat is rising, as cyber criminals are increasingly targeting Australian small businesses. The average financial impact on small businesses from a cyber attack is $56,600.

Cyber criminals may target you to access a larger supply chain, and more often than not will be banking on you being underprepared and too busy to recognise the attack.

Your personal, customer and supplier data is valuable to cyber criminals. The impacts of cyber crime often extend beyond production delays and financial costs. Deteriorating personal health and legal issues are also harmful consequences.

This small business Cyber Security Guide is a quick reference tool that tells you what to look out for, and how to combat the increasing threats. This guide includes:

- Examples of cyber attacks in agriculture
- The most common small business cyber attacks
- How cyber criminals attack your business
- Stop hackers at the gate — top 8 tips
- Topline findings from the latest Cyber Wardens Research
- Cyber security checklist

After reading this guide, we encourage you and your workers to complete the free Cyber Wardens training program. It only takes 45 minutes and was designed by small businesses for small businesses, so you can be more confident and focus on growing your business.

Luke Achterstraat,

CEO, COSBOA

1 www.abs.gov.au/statistics/industry/technology-and-innovation/characteristics-australian-business/2021–22#cyber-security-incidents-impact-and-prevention

Cyber criminals are targeting agriculture businesses

Many small businesses believe they are too small for cyber criminals to target. This is especially true if their business doesn't involve sitting behind a computer all day.

Over the past few years, there have been numerous reports of cyber crime against agriculture businesses in Australia and around the world. Here is a selection:

- In 2020, ransomware impacted Australian wool sales and milk deliveries.
- In 2021, a cyberattack on a global meat processor impacted 47 facilities across Australia and thousands of workers.
- In 2022, a video went viral showing a tractor's display screen had been overridden with a video game.
- That same year, the FBI cyber division issued an alert to the food and agriculture sector that ransomware actors were targeting critical planting and harvesting seasons in the United States.
- In 2023, a satellite signal failure stopped GPS-guided tractors in NSW and Victoria in the peak sowing season — demonstrating the risk of GPS hacking on farmers.
- Also in 2023, a vineyard in New Zealand had its sensor system hacked and in Canada a ransomware attack on a pig farm paralysed cameras, accounting systems and feeding systems for a number of weeks.
- Drones are now used extensively by farmers and producers and are at risk of being hacked. Drones need to have the latest software updates and be set to return home to avoid them being stolen. In Australia, there are also numerous cases across several states of thieves scouting properties and machinery with drones.

> "I've come to terms with the fact a cyber attack will probably happen at some point, but you never think it's going to happen tomorrow."
>
> Micro agriculture business owner,
> regional NSW

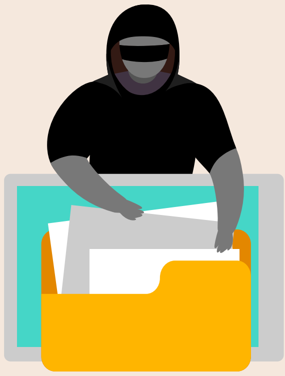
> "Being vigilant on cyber security is so important for our industry. It is vital that all agribusinesses, no matter their size, are taking the steps to protect their data and equipment."
>
> Elizabeth Skirving,
> CEO Rural Business Tasmania

The most common small business cyber attacks

1.

Inbox break-ins

Email compromise attacks are a break-in to your inbox. Once inside cyber criminals gain access to important information and can launch more damaging attacks.



2.

Fake invoices and payment redirection scams

Business email compromise (BEC) fraud is a type of scam to trick you out of money or goods, usually by sending fake invoices that redirect payments to hackers.

3.

Banking burglary

Online banking fraud gives cyber criminals access to your bank accounts allowing them to transfer out your hard-earned cash.

From the latest Australian Signals Directorate's Annual Cyber Threat Report.

Report Cyber Crime

Every six minutes a cyber crime is reported in Australia.

If you have been the victim of a cyber attack, make sure you report it - cyber.gov.au/report-and-recover/report

This will help to protect other agribusiness owners.

Beware of the data breach!

Have you or a staff or family member had their data stolen in a previous cyber-attack?

Information stolen in previous attacks can be used to launch secondary attacks that target your business, especially if passwords are being re-used. This type of attack is called credential stuffing. You can learn more about it, and other cyber safety tips in our resource hub cyberwardens.com.au/resources.

CREDENTIAL STUFFING SHOPPING SCAMS

The National Farmers Federation (NFF) is urging all farmers to consider their data security and use software providers certified against the Australian Farm Data Code.

"As we become more reliant on digital technology, we also become more vulnerable if that data is misused. That could be in the form of a cyber attack, but also by not understanding the business model of the platform you're using and how they'll share and commercialise your data."

Gabi Ceregra, NFF Data Policy Manager

Top 8 tips to stop hackers at the gate

Technology is vital to your agribusiness but with it comes greater risk. Here are 8 things to look out for and what to do.

1. Cyber criminals will take advantage of how busy you are

It's harder to spot a scam, fake invoice or phishing attack when you're flat out and tired. Scammers exploit how busy you are and create a sense of urgency to manipulate you and your decisions.

What to do:

- Be careful whenever someone insists that you must act immediately, come back to it when you have more time.
- Stick to your usual banking and payment processes.
- Watch for red flags such as a strangely configured email address, unusual requests, unexpected invoices, "confidential" requests or unsophisticated language and typos.

2. Hackers will get a good yield from your poor processes and weak passwords

Bad and lazy habits make you vulnerable to cyber attacks.

What to do:

- Protect your email and important business accounts with multi-factor authentication.
- Set your apps, plug-ins and browsers to auto-update so you have the latest security updates.
- Shut down and restart regularly so your auto-updates are installed.
- Upgrade from passwords to longer passphrases on all logins, including cloud-based storage.
- Set a unique passphrase for every account (no double-ups and no shared passwords).
- Use a password manager to safely store passwords.

3. Scammers will send you fake invoices

Watch out for fake invoices, fake refund requests and fake links. According to Xero, nearly one in five small businesses has been a victim of invoice fraud, falsely paying out $15,500 on average.

What to do:

- Slow down and double-check every invoice and ensure they match previous ones.
- Ensure the business is legitimate.
- Check invoices with two people.

4. Scammers will try to access your computer

You protect your livestock, crops and vehicles, so don't let someone you don't know or trust access your digital assets — computers, tablets, or technology operating systems. A breach could result in regulator fines or legal action if customers or employee personal information is accessed.

What to do:

- If you're having tech issues, only trust your regular supplier or a business you can verify.
- If you're contacted and offered technical support or if you put out a call for technical help, be aware that not everyone who offers you assistance will be genuine.
- Never give out sensitive details to unverified providers.
- Never allow remote access to your devices if you have been contacted unexpectedly.

5. Scammers will pretend to be a customer or supplier requesting a refund

We know every small business loves its customers and is grateful for their support. That's why you might fall victim to a refund request scam. In cases where the initial transaction was made with a fraudulent card, you'll likely be obliged to return the funds from the original transaction. You will also be out of pocket for the money you refunded to the scammer.

What to do:

- Ensure the refund request is for a legitimate item or service.
- Refund scams occur when buyers purchase items and then ask for a refund or allege they have mistakenly overpaid you.
- Check every refund request to ensure the money is going back to the same card used for the original purchase.

6. Scammers will send you fake customer or supplier complaints

Fake complaints may be sent to your email, as a text, a private message on social media or through your website with a link to download a 'photo'.

What to do:

- Confirm you are dealing with a legitimate customer or supplier.
- Don't click on unusual file types and photos as the link may contain computer viruses or phishing attacks.
- Be alert to urgent requests pressuring you to transfer funds.

7. Scammers will target your casual workers and family

Cyber security needs everyone pitching in — everyone involved with your business can be a target, and everyone has a role to play in spotting and stopping attacks.

What to do:

- Talk to your family and workers about the heightened risk of cyber attacks on small businesses.
- Remind them to double-check anything suspicious and confirm invoice details directly with suppliers using a trusted contact number.
- If workers are being pressured to pay an invoice they don't recognise or have assumed is for the business owner or another colleague, tell them it's okay to think twice and check with you.

8. Scammers will look to access your old devices

Be careful when disposing of your devices and old equipment. Hackers could potentially access the data stored to access your emails, files, and other business-related information.

What to do:

- Ensure the protection of your data by performing a factory reset on your old devices.
- For highly sensitive information, consider enlisting the assistance of an IT professional or a specialised data destruction service.

How cyber criminals target your agribusiness

No matter how big or small your agribusiness, cyber criminals may target you. Recent research from the University of Cambridge highlights that the greater use of smart farming technology, combined with the power of artificial intelligence, increases the cyber security risks to farmers.

Hack and control smart farming equipment

Whilst smart farming technology can increase precision, yields and profitability in the hands of cyber criminals they can wreak havoc on your agribusiness.

Drones can be compromised sending pesticides onto the wrong paddocks, wifi gates opened releasing livestock, and smart irrigation systems drained. Temperature changes in smart greenhouses and misinformation feed into smart sensors.

Taking simple steps to ensure secure access, strong unique passwords, and back ups is essential to protecting your smart farming technology from cyber and ransomware attacks.

Inbox break in

Access your business email accounts to steal information or send fake invoices.

Fake invoices

Impersonate your customers or suppliers to redirect payments towards scammer accounts.

Cloud compromise

Gain access and control of important business records, client and priority business information.

Banking burglary

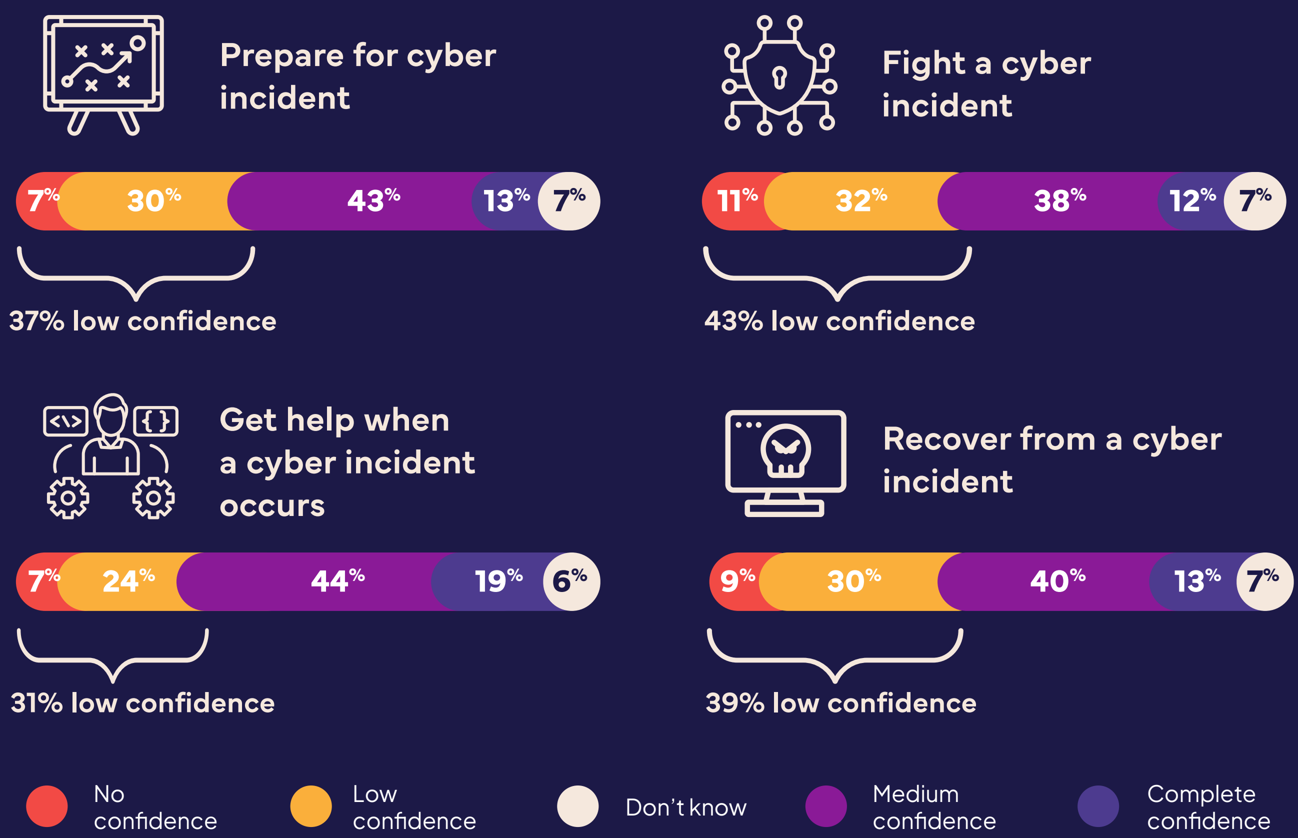
Access your business or farm bank accounts to steal money.

Topline findings from the latest Cyber Wardens Research

Almost 2,100 small businesses recently participated in our latest research. Here are some of the findings.

Many small businesses are unprepared to respond to cyber threats

On average, **4 in 10 small businesses** have little to no confidence in their ability to:



Make cyber-safety a top conversation in your business

Most small businesses (61%) are not talking about cyber security regularly, which further increases the risk they face. Read the full research report at cyberwardens.com.au/research/

Gaps in basic cyber safety create significant vulnerability

Simple cyber-safety strategies include; ensuring each account is protected with a virtual alarm via multi-factor authentication, up-to-date software, and strong password practices will protect your small business from most attacks.

50%

of small businesses have turned on a **virtual alarm** using **multi-factor authentication**

52%

of small businesses are able to defend against digital break-ins with **up-to-date software**

53%

of small businesses are **backing up** daily and would be ready to recover from attack

30%

of small businesses have **strong password practices**

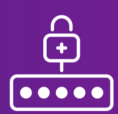
Bad habits can bulldoze your business

Bad habits are hard to break. Once observed, they become regular everyday behaviours adding risk. **Four in five small business owners** (78%) have everyday habits occurring which inadvertently make them more vulnerable to cyber crime.

Common risky habits increasing cyber risk in small business

Keeping a password document

'Sleep mode' avoiding software updates and patches



Re-using passwords

Snoozing software updates

Cyber attacks are more common than you think

Don't leave your agribusiness exposed

Cyber Wardens training, for you and your team, will help protect your agribusiness and help lock your digital doors.

In fewer than 45 minutes the free Cyber Wardens program will give your small business quick wins in cyber security.

Learn how to:

Defend against digital break-ins with **up-to-date software**

Set a virtual alarm system with **MFA (multi-factor authentication)**

Password like a pro by upgrading to **passphrases**

Bounce back with **backups**

Enrol today.

cyberwardens.com.au

Cyber security checklist

- [ ] **Complete** the free Cyber Wardens training
  cyberwardens.com.au
- [ ] **Encourage** your workers and suppliers to complete the Cyber Wardens training
- [ ] **Print** the Simple Steps Poster from the website for your shed
- [ ] Regularly **discuss** cyber security with your team and suppliers
- [ ] **Look** twice at invoices and emails
  (ask a colleague or trusted friend if you're not sure)
- [ ] **Follow** on social media for simple small business safety advice
- [ ] Each season **review** the simple steps in your Cyber Security Action Plan
- [ ] _
- [ ] _

CyberWardens.

Equip your business with Cyber Wardens training

It's a simple and free educational tool designed to build a cyber-smart small business workforce.

Cyber Wardens is an initiative of the Council of Small Business Organisations of Australia (COSBOA). By building the cyber capability of people who work in small business, Cyber Wardens helps businesses strengthen their cyber resilience, reduce the risk of cyber attacks and respond more effectively when incidents occur. Our goal is simple: make Australia a harder target for cyber criminals.

CyberWardens.

An initiative of COSBOA

Enrol today at **cyberwardens.com.au**