Scams affecting the Agriculture Sector

Jane Richter

- The ACCC's Scamwatch has observed a rise in agriculture scams since the COVID-19 pandemic. According to the 2021 targeting scams report, farmers and small businesses lost over $1.5 million to scammers targeting the agriculture industry in 2021.
- An estimated one third of victims do not report scams to the ACCC and therefore the actual losses are believed to be higher.
- Scams cause great emotional distress and trauma. Anyone who suspects they have given money or details to a scammer should talk to someone they trust or seek professional support.

Australian farmers and agri-businesses are the targets of tractor scams.

Between January 2021 and August 2022, the ACCC's Scamwatch has received 533 reports about tractor and heavy machinery scams, including total losses of $2.6 million.

These scams were for new tractors, with scammers creating fake websites, and for second-hand sales on marketplace websites such as Facebook and Gumtree.

How tractor scams work

Fake tractor website scams

Scammers create fake websites that look like genuine online shops selling agricultural machinery.

They may use sophisticated designs and layouts, photos and brand logos taken from other websites, a '.com.au' domain name and even an Australian Business Number (ABN) taken from a legitimate business.

The websites often have a physical business address listed on the website which are vacant blocks or belong to another business.

Second-hand tractor scams

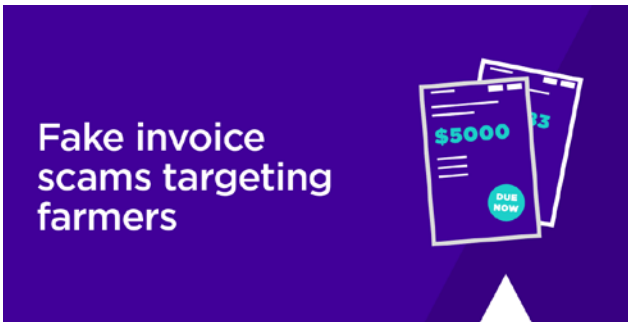
Scammers will pose as genuine sellers and post fake ads on classifieds websites, in print classifieds, and on online platforms such as Gumtree and Facebook Marketplace. However, once a deposit is paid, the scammer usually 'disappears' and delivery is never made.

7 tips to avoid being scammed

1. **If it seems too good to be true, it probably is**
   Scammers advertise machinery at much lower prices than what the market rate is.
2. **Don't purchase machinery if you haven't seen it in person**
   Scammers will always come up with an excuse as to why you can't inspect the machinery in person, or they will ask for a deposit first.
3. **Beware if they offer a 'free trial' or an 'escrow' service**
   Scammers may offer a 'free trial' in an attempt to earn your trust. However, they would ask for a deposit to be paid first.

   Scammers may also reassure customers that the deposit is paid into a third party or 'escrow' account, but the 'escrow' service is also fake and part of the scam.
4. **Don't rush into a purchase**
   Be cautious if the seller tries to make the sale feel urgent. For example, scammers often say that they need to sell quickly because they are in the army and about to be deployed overseas, or that their father has passed away and they need to get rid of machinery from their parent's farm.
5. **Do your own research**
   Look for online reviews to see other people's experience with the business. Do your research beyond the website itself, as those reviews may be fake.

   Scammers may also steal other businesses' names and ABN details for their website. If a physical address is listed, look it up online and see if it is the correct business on Google Maps. You could also call a neighbouring business to verify the seller.
6. **Be careful what personal details and information you provide**
   Be careful if you are asked to provide a driver's licence, passport or home address, which may be used for identity theft. Where people reported losses as a result of a scam, more than half of them lost personal details.
7. **Speak to someone you trust**
   If you think the sale might be a scam, get a second opinion from a family member or a friend to see what they think.



Fake invoices

Agri-businesses may be unknowingly paying fake invoices

Did you know that scammers sometimes send invoices that appear to be from real business suppliers, and you could pay them, not realising they are fake invoices until sometime later?

These are known as 'fake invoice scams' and between January and August 2022, the ACCC's Scamwatch received 19 reports from farmers and agricultural businesses, with $320,572 in reported losses.

Overall, over the same period, Australians lost $15,006,570 to fake invoice scams.

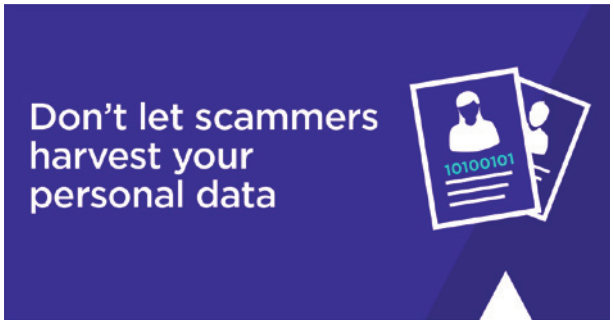
The scammers may hack into the email account of a business or supplier, and send you an email saying that their bank details have changed. These scammers can make invoices look almost identical to the real ones, with the only difference being the bank account details.

In one instance, a farmer paid a scammer's fake invoice of over $60,000, as they believed they were paying an invoice for the purchase of machinery.

Protect yourself. What can you do to avoid being scammed?

Be careful if a business tells you they have updated their bank details

- If you receive an email containing an invoice that says the supplier's bank details have been updated, you should call them to confirm this. Do not call the phone number on the invoice, as this may have been changed by the scammers. Instead, find the supplier's phone number from another source.
- You should also confirm via a phone call that you have the right bank details, if it is the first time you are paying money to that supplier's account, or for large purchases.



General scams awareness

Two common types of scams to look out for

Phishing scams

Phishing scams are attempts by scammers to trick you into giving out personal information such as bank account numbers, passwords, credit card details or personal information.

A scammer may contact you by email, phone call or text message and pretend to be from a legitimate business such as a bank or internet service provider. For example, they may pose as a bank seeking to 'verify' customer records.

To protect yourself from phishing scams, do not click any links or attachments in an email unless you are certain it is from a trusted organisation. If the email asks you to update or verify your details, this should be a warning sign.

Do an internet search using the names or exact wording of the email or message to check for any references to a scam. Many common scams can be identified in this way.

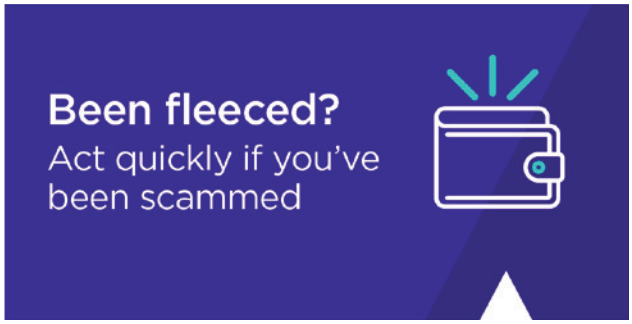
Remote access scams

A remote access scam happens when a scammer gets access to your computer after convincing you to download software to fix an internet or computer problem.

The scammer will usually phone you, pretending to be a from a large telecommunications or computer company such as Telstra, the NBN or Microsoft. They may also claim to be a technical support service provider.

Once they have remote access, scammers can access personal information stored on your computer, install malicious software or use your information for other crimes, such as identity theft.

To protect yourself from remote access scams, never give an unsolicited caller remote access to your computer. You should also never give your personal, credit card or online account details over the phone unless you made the call and the phone number came from a trusted source.



Report a scam

We encourage you to report all scams to the ACCC via the report a scam page www.scamwatch.gov.au/report-a-scam. This helps the ACCC to warn people about current scams, monitor trends and disrupt scams where possible. Please include details of the scam contact you received, for example, email or screenshot.

Scamwatch also provides guidance on protecting yourself from scams and where to get help. Find out more at www.scamwatch.gov.au

Find out more about scams

You can read more about these scams and other common scams on the ACCC's Scamwatch page at www.scamwatch.gov.au

ACCC AUSTRALIAN COMPETITION & CONSUMER COMMISSION

SCAMWATCH