Losses to Car Ad Scams Climbing

Australians have already lost over $288,000 to vehicle scams in the first quarter of this year, more than all losses reported to Scamwatch in 2019, and scammers have now begun impersonating defence personnel to con their victims.

In a vehicle scam, scammers post fake online listings offering to sell in-demand cars at well below market value to lure potential buyers looking for a second hand vehicle. Scammers seek payment to secure the car for the buyer but never deliver the vehicle.

Vehicle scams are commonly hosted on sites such as Facebook Marketplace, Autotrader, Car Sales, Cars Guide and Gumtree.

“As second hand car sales increased during the pandemic, unfortunately so did vehicle scams. If current trends continue, Australians could lose much more to vehicle scams this year than the $1 million lost in 2020,” ACCC Deputy Chair Delia Rickard said.

“We want to raise awareness of these scams to reduce the number of people who may be vulnerable to them.”

A new technique we are seeing is scammers pretending to be defence personnel. In 97 per cent of reports received this year, the scammer claimed to be in the military (navy, army and air force), or to work for the Department of Defence, and said they wanted to sell their vehicle before deployment. This sought to create a sense of urgency with buyers and explained the unusually low listing price of the vehicles and why buyers could not inspect them prior to payment.

Email addresses that do not bear the legitimate the defence email format of @defence.gov.au may be an indication of a scam, but even the correct email format does not guarantee the car ad is not a scam, as scammers are able to spoof email addresses. It is best to look for all warning signs to avoid being scammed.

“A price that is too good to be true should be a warning sign for potential buyers. If a classified ad offers a vehicle at a very low price, the ad might not be legitimate. For example, one Scamwatch report noted a listing that advertised a car for nearly $10,000 below its market value to entice buyers looking for a bargain.”

Vehicle scammers often seek payment via a third party website. A large number of reports to Scamwatch mentioned the use of escrow agents, a third party who is supposed to ‘hold’ the money from the buyer until goods are received, before releasing the funds to the seller. Other commonly requested payment methods include eBay, direct bank transfer or international money transfers.

“If the seller claims to be unavailable and insists on payment before meeting the buyer or allowing them to pick up their new car, this should raise suspicions,” Ms Rickard said.

“It is relatively common for scammers to claim that they are travelling or moving away to avoid meeting buyers before payment.”

“Always try to inspect the vehicle before purchase and avoid unusual payment methods. If you have any doubts, do not go ahead with the deal,” Ms Rickard said.

In addition to losing money to vehicle scams, around 20 per cent of consumers who reported vehicle scams have lost personal information, after providing their address, phone number and copies of their driver's license to the scammer. To protect your identity, never provide your personal details to someone you have only met online.

"Fortunately, over 80 per cent of people who reported vehicle scams to us managed to avoid losing money by identifying the scam early. We encourage consumers to trust their instincts. If something seems too good to be true, it probably is," Ms Rickard said.

Further help for consumers

If you have been the victim of a scam, contact your bank as soon as possible and contact the platform on which you were scammed to inform them of the circumstances.

More information on scams is available on the Scamwatch website, including how to make a report and where to get help.

If you have experienced a loss online and believe the perpetrator is located in Australia, you can also report the scam to ReportCyber. ReportCyber triages reports and allocates them to the relevant law enforcement authorities for further action.

Victims of identity theft, or cybercrime can contact IDCARE, a free government-funded service that will work with you to develop a specific response plan to your situation and provide support. You can contact IDCARE on 1800 595 160 or visit www.idcare.org.

You can follow @scamwatch_gov on Twitter and subscribe to Scamwatch radar alerts for more information about current and emerging scams.

Background

Scamwatch received 346 reports of vehicle scams between 1 January and 31 March, with $288,459 in losses reported during this period.

This compares to over 1,000 reports and more than $1 million lost in 2020, and 330 reports and about $245,000 losses in 2019.

People aged 18-24 have lost the most money to vehicle scams in 2021 so far, $79,210, or 27 per cent of total losses. People aged under 35 lost 35 per cent of the total losses reported to vehicle scams so far in 2021. People aged 65 years and over reported lower losses than all other age groups.

New South Wales has the highest number of reports (114) and losses ($97,297) to vehicle scams, while reporters from the Northern Territory and Tasmania have not reported any losses this year to date.

Some examples of the fake Department of Defence emails that have been used in recent vehicle scams include:

- @airforce-raaf.org
- @royal-australian-defence-gov.com
- defence@royal-australian-air-force-gov-au.com