Payment redirection scams cost Australian businesses $128 million in 2020

Payment redirection scams were the most financially damaging scams for Australian businesses in 2020 according to the ACCC's latest Targeting Scams report. Combined losses reported to Scamwatch, other government agencies, banks and payment platforms totalled $128 million in 2020.

Reports to Scamwatch show that Australian businesses lost $18 million to scams in 2020, a 260 per cent increase on losses reported in 2019.

"Small and micro businesses made most of the reports to Scamwatch and experienced an increase in losses in 2020, although larger businesses reported the highest losses," ACCC Deputy Chair Mick Keogh said.

Based on Scamwatch data alone, false billing scams were the most commonly reported scam by businesses and accounted for three quarters of total losses to businesses. Small and micro businesses accounted for almost 60 per cent of these false billing reports.

There are a range of false billing scams, but the most common type was payment redirection scams, also known as business email compromise (BEC) scams, with 1,300 reports and $14 million in losses. This is a substantial increase from the 900 reports and $5 million in losses reported in 2019.

In a payment redirection scam, scammers impersonate a business or its employees via email and request an upcoming payment be redirected to a fraudulent account.

Scamwatch also observed a new type of scam in 2020 that targeted farmers looking for a good deal on tractors and farm machinery. Scammers advertised equipment at prices well below market value, and told farmers that they couldn't view the tractors prior to purchase due to government restrictions from the pandemic. Farmers made payments to secure these special deals, when in reality the equipment never existed. Farmers were conned out of $1.1 million in these scams.

"One thing we know about scammers is that they will take advantage of a crisis," Mr Keogh said.

Businesses were also targeted by health and medical scams in 2020. About half of the $3.9 million in total losses reported to health and medical scams were from businesses, as they attempted to procure personal protective equipment for their staff to comply with government guidelines during the pandemic.

Other scam types that impacted businesses throughout the year included phishing, identity theft and hacking scams.

"It is so important for businesses to stay informed about scams so they can protect themselves," Mr Keogh said.

"The ACCC provides a range of resources for businesses on how to avoid scams on the Scamwatch website and in our media releases throughout the year."

Businesses that have been scammed should contact their bank as soon as possible. If the scam occurred on a platform such as Facebook, contact them directly to report it.

Businesses can also report a scam to ReportCyber, which is run by the Australian Cyber Security Centre and passes reports to law enforcement agencies for assessment and intelligence purposes.

The Small Business Information Network also provides details about new or updated resources, enforcement action, changes to Australia's competition and consumer laws, events, surveys and scams relevant to the small business sector.

Find out more in our media release.