# Bulletin

## Tasmanian Automotive Chamber of Commerce

**Reference No**. Scams targeting customers/mm-11-23

**Date:** 16/11/2023

## ACCC warns Australian Car Dealers on scams targeting customers. Let's not be a victim.

TACC has been alerted by the National Anti-Scam Centre, an operation of the Australian Competition and Consumer Commission (ACCC), of a rise in business email compromise scams targeting customers of car dealerships and used car traders. ACCC advised that intelligence reports indicate that the scam may be spreading to caravan dealerships also.

**What is the National Anti-Scam Centre?**

The ACCC runs the National Anti-Scam Centre which was established in July 2023. The purpose of the National Anti-Scam Centre is to make Australia a harder target for scammers. The National Anti-Scam Centre does this by facilitating cooperation and collaboration across industry and government. You can find out more, what the National Anti-Scam Centre is doing to stop scams on the ACCC website.

**About the current scam and what LMCTs need to know**

You will see below a summary of how the scam works and some ways that ACCC advice for businesses to protect themselves and their customers.

ACCC has also included this information in the Scams targeting customers of car dealerships and used car traders. TACC encourages you to print this advice and display it in a prominent position at your dealership.

**How the scam works**

ACCC advised that the scam typically involves the following:

- The legitimate business's email account is compromised, usually through an email phishing attack. The scammer can read emails sent and received by the business and can send emails from the account. The business may remain unaware that their email account is compromised for multiple weeks.
- The scammer emails customers from the compromised email account requesting payment of their deposit (or payment of a further amount if the deposit has already been paid), providing their own bank details rather than that of the trader or dealership.
- Alternatively, scammers may email customers from a different email address that looks similar to the actual email address used by the company.
- The customer receives the invoice from the scammer and transfers the deposit, thinking they are paying into the business's account.
- When the business notices they have not received a deposit, they email an invoice to the customer.
- The scammer sees this email sent by the business, and may send another invoice to the customer, requesting even more money. The invoices sent by the scammer appear identical to the genuine invoices, except for different bank account details.
- Because the scammer has access to the business email account, they know the names of staff and customers. The scam emails appear to be personally addressed to the customer and signed off by the trader's/dealership's staff.

**Warning signs**

- You don’t receive emails that people say they have sent you.
- Emails are classified as “read” without you having read them, or emails disappear from your Inbox.
- There are strange emails in your sent folder.
- You cannot access your email because the password is incorrect.
- You receive unexpected password reset notifications.
- Your email app reports sign-ins from unusual IP addresses, locations, devices, or browsers.

**Protect yourself and your customers**

The primary victims of this scam are your dealerships' customers, though the exploitation that comes via compromise of your business email account. ACCC recommends the following steps may help protect you and your customers:

- Check and secure your email systems as per the Australian Cyber Security Centre’s advice.
- Check your email system for unexpected ‘filter rules’. In Microsoft Outlook, click on the ‘File’ tab, then click the ‘Manage Rules & Alerts’ button. Scammers can use these to hide their correspondence from compromised accounts.
- Change email access passwords regularly, and always use a unique, complex password. Do not use the same or similar passwords for different services, apps, or websites.
- Let your customers know that they should contact you by phone or in person if they receive correspondence claiming you have changed your bank details. Ensure your public phone number is listed clearly on your website.
- Warn customers to be on their guard for suspicious emails. Request they advise you of any unexpected email contact from your business.

The National Anti-Scam Centre will continue to undertake disruption activities wherever possible, including by sharing intelligence with law enforcement and the financial institutions of alleged scam accounts.

ACCC are eager to hear about any initiatives Dealerships have implemented to reduce the impact of scams, or any intelligence you receive regarding scams and/or the impersonation of your business or staff. If you become aware of scam attempts, please report them to the National Antil- Scam Centre to help protect others.

You can contact the National Anti-Scam Centre at NASC@accc.gov.au.

**Michael McKenna MBA MBLaw**
Industry Policy Advisor