NASC WARNS OF RISE IN BUSINESS EMAIL COMPROMISE SCAMS TARGETING DEALERSHIP CUSTOMERS

16 November 2023

To: AADA MEMBERS

The National Anti-Scam Centre (NASC) have contacted the AADA to advise members they have become aware of a rise in business email compromise scams that target customers of new car dealerships and used car traders.

The NASC is run by the Australian Competition & Consumer Commission and was established in July 2023 to combat the ever-increasing prevalence of scams. It aims to assist with collaboration across industry and government to achieve this.

NASC have provided the attached fact sheet for Dealers that details how the scam typically works, warning signs, and some short advice to protect your business and your customers.

More information about scams and what to do about them can also be found on the ACCC website.

Should you require further information or have a question regarding your business environment, the NASC can be contacted at NASC@accc.gov.au.

If you have any questions or need further information, please contact:

Brian Savage
DEPUTY CHIEF EXECUTIVE OFFICER
Australian Automotive Dealer Association Ltd.
E: bsavage@aada.asn.au
M: +61 418 377 594

Australian Government | National Anti-Scam Centre

15 November 2023

Scams targeting customers of car dealerships and used car traders

The Australian Competition & Consumer Commission (ACCC) runs the National Anti-Scam Centre which was established in July this year 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 about what we're doing to stop scams on the ACCC website.

We have become aware of a rise in business email compromise scams targeting customers of car dealerships and used car traders.

How the scam works

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 customers, though the exploitation comes via compromise of your business email account. The following steps can 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 take action against these scammers wherever possible, including by sharing intelligence with law enforcement and the financial institutions of alleged scam accounts.

We are eager to hear about any initiatives you 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 us to help protect others.

Up to date information about scams and how you can protect your business and customers from scams is available on the ACCC website.