AUSTRALIAN AUTOMOTIVE DEALER ASSOCIATION

EMAIL COMPROMISE

PROTECT YOUR INFORMATION

WHAT IS BUSINESS EMAIL COMPROMISE?

Business Email Compromise (BEC) is a type of email fraud where scammers impersonate someone within or connected to an organisation, such as a company executive or trusted client, to trick employees into transferring funds or sharing sensitive information. These attacks are carefully targeted at employees with access to financial accounts or other valuable data, making BEC both highly specific and potentially costly.

Example: Imagine receiving an email that looks like it is from your CEO, urgently asking you to transfer funds to a new account. The email appears legitimate, but it is actually a fraudster trying to steal company money.

+61 2 5105 1022 | info@aada.asn.au | www.aada.asn.au/cyber-security-dashboard/

CULTURAL CYBER SECURITY

THREATS

BEC attacks are dangerous due to their targeted nature and potential for significant financial losses. Scammers often use email spoofing to make emails look like they are coming from familiar people or partners, which makes these attacks harder to detect. The global financial impact is substantial, with billions lost each year to BEC scams.

Key Risks:

- Australian businesses were scammed out of $227 million in "payment redirection" cons which includes business email compromise or BEC over the course of 2021. These scams often involve requests for large sums to be wired to fraudulent accounts.
- Some BEC attacks aim to obtain sensitive company information, which could lead to further security breaches or intellectual property theft.
- BEC scams create confusion within organisations, sometimes resulting in delays, extra verification steps, and strained internal processes.

TIPS

To prevent business email compromise it is important to:

- Always confirm any payment or sensitive information requests, especially those received by email. Calling the requester directly, is better than replying to the email. You can also ask for Purchase Order number which they usually can't supply.
- Enable Multi-Factor Authentication.
- Regular training helps employees spot red flags in emails, such as unusual phrasing, urgency that bypasses normal verification steps, or requests that deviate from normal procedures.
- Use advanced email filtering tools that can detect and block suspicious emails, as well as flagging external emails that might appear to be from internal sources.
- Attackers sometimes set up forwarding rules on compromised accounts to monitor communications. Regularly review and manage email settings to prevent unauthorised forwarding.
- Always check a senders email address and look for small alterations such as misspellings, grammatical errors or variations.
- Be cautious if someone asks for sensitive information, such as login credentials or financial data, through email.