Business Email Compromise

Malicious cyber activity varies; the diagram below is one example of how cyber actors use BEC to scam victims.

Cybercriminals compromise the email and IT systems of legitimate businesses.

Cybercriminals observe transactions and identify opportunities to divert money to their own accounts.

Cybercriminals will either impersonate known recipients (whether a customer or a CEO), using spoofed accounts or compromised accounts to appear legitimate.

Many businesses only realise they have been caught out once it is too late, usually after the intended recipient complains they never received the payment.

The victim updates the payment details and pays the cybercriminal instead of the organisation that was meant to be paid.

Cybercriminals will send emails advising of changes to payment details.

More than 4,600 BECs reported

Over $81 million (AUD) lost due to BEC

Increase in average financial losses per BEC report ▲54%