

PROTECT YOUR VIRTUAL VALUABLES

5 TIPS TO AVOID BUSINESS
EMAIL COMPROMISE



1 SEEK SUPPLIER CONFIRMATION



If you receive a change of banking details from a supplier, always confirm by contacting the supplier on the trusted details recorded in your system. A phone call is usually best, particularly if your supplier's email system has been hacked.

2 TWO AUTHORISATIONS



Ask for two authorisations for payments to create an extra level of security, particularly for large transactions or those appearing sensitive or urgent.

3 SUPPLIER DETAIL UPDATE REVIEW



Implement or review your policies and processes for updating supplier details. Make sure everyone is aware of the new or updated policies.

4 BE ALERT TO PHISHING SCAMS



BEC (Business E-mail Compromise) scams are often initiated with a phishing attack. Avoid providing information about your company or its employees to unknown senders or callers.

5 CONTACT THE AUSTRALIAN CYBERCRIME ONLINE REPORTING NETWORK



If you are the target of a scam, contact your bank in the first instance and report any incidents to the Australian Cyber Security Centre (ACSC). By reporting the event, you may help others avoid them in the future.