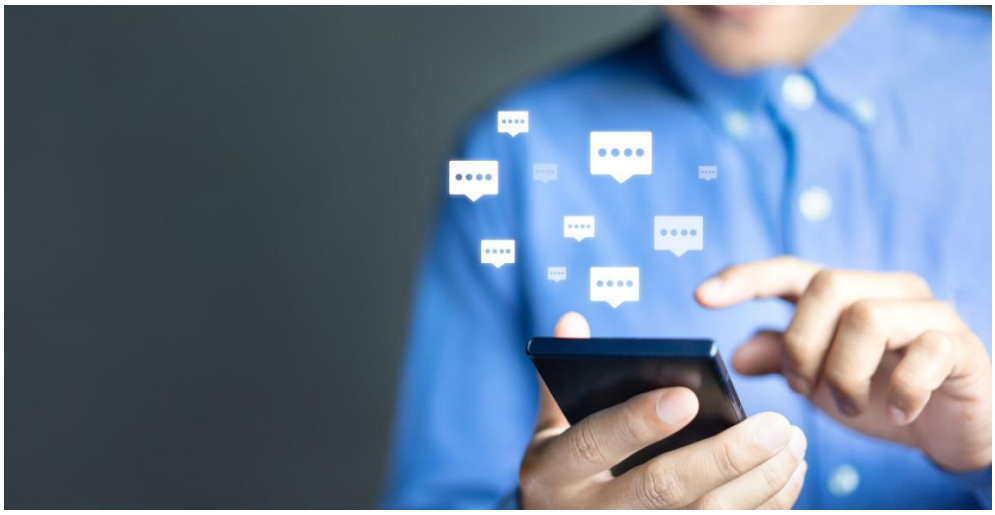
Stay Vigilant to Business Email Compromise Scams



What is a business email compromise scam?

A fraudster may impersonate a senior executive or business partner using a similar or hacked email address to ask for payments to be directed to a new bank account under their control; or to steal critical business information for future attacks.

Safeguard yourself and your business from this scam

As a business owner

- Instil awareness about cyber-security and email best practices in your employees.
- Conduct timely reviews to ensure that the current internet banking user listings are always kept up to date. Remove any users who have left the company.

As an employee

- Be suspicious of urgent payment requests, including those that are out of the ordinary.
- Carefully analyse all email request to transfer funds.
- Always verify changes in payment details with a call back to a known number.
- Do not click on hyperlinks and attachments from unknown sources.

If you have accidentally disclosed personal or banking information to a suspicious caller or if you notice unusual or unauthorised transactions, please call us immediately at **603-8317 5200.**

Besides calling the Bank, you can also perform self-service per below under such circumstances:

1. Suspend your access temporarily to OCBC Velocity.
2. Reset your OCBC Velocity password