# HOW TO IDENTIFY EMAIL PAYMENT FRAUD.

The request claims to be urgent and/or confidential.

The request is made on behalf of the CEO or CFO.

You are requested to ignore standard payment authorisation processes.

The request includes grammatical and spelling errors.

The type of request, language or format are unusual.

The ‘reply to’ email address is different to the sender’s address.

## Protect yourself from Scams

1. Don’t open suspicious texts, pop-up windows or click on links or attachments in unsolicited emails – delete them
2. Don’t enter or provide your card number to unsolicited sites or callers
3. Don’t respond to phone calls about your computer asking for remote access – hang up
4. Keep your personal details secure
5. Choose your passwords carefully
6. Review your privacy and security settings on social media
7. Beware of any requests for your personal details or money

**If you think you have been a victim of a scam or email fraud, you need to let us know as soon as possible by calling us on 1300 660 550, or by attending your nearest branch.**

DelphiBank

1300 660 550
delphibank.com.au
@delphibank