

# Staying Safe Online – BUSINESS EMAIL COMPROMISE

Scammers are accessing emails to change important information so they can take your money.

## How this scam works:

A *Business Email Compromise* or *Payment Redirection Scam* generally involves a scammer fraudulently accessing an email account of a genuine business.

Scammers intercept an invoice being sent from a business via email, changing the bank account details before sending the email on. The customer receives the invoice as expected and pays the invoice, however, the money goes into the scammer's bank account, and not that of the business.

Usually, the business and the customer are not aware this has happened.



### 3 warning signs

- 1 Scammers will often pose as staff members of a genuine business and send emails that look very real, requesting urgent or confidential payment often **in a way that differs from the normal process**.
- 2 Scammers could also impersonate a legal representative of a business and **request sensitive information** about an urgent matter, such as a large business transaction or a settlement.
- 3 Look out for a **change in bank account information from previous invoices** from the same business – this can indicate something isn't right.

### 3 ways to protect yourself

- 1 Always double check bank account details, even if you are familiar with the business or have used them before. Either refer to older invoices or contact the business directly to confirm.
- 2 Be wary of requests for payment that ask you to step outside normal processes, even from familiar sources.
- 3 Operate with extreme caution when transferring large sums of money and always double check bank account details with a trusted source.



Don't be afraid to contact the business you're paying to double check payment details.

## Think you've been scammed?



If you think you have been a victim of a scam it's important to call **Heritage on 13 14 22 (available 24/7)** promptly to limit any further loss and to see if the transactions can be reversed or disputed. If you are overseas please call +61 7 4694 9000.

**DO NOT** make further payments to the scammer.

Please ensure you change your passwords to secure your account and report the scam to [ACCC \(www.accc.gov.au\)](http://www.accc.gov.au) via the report a scam page. For more information on how to protect yourself from scam visit the [Scamwatch website \(www.scamwatch.gov.au\)](http://www.scamwatch.gov.au).



Go to our website to download more information about scams: [www.heritage.com.au/scams](http://www.heritage.com.au/scams)

**Heritage Bank**  
People first.