# Be wary of fake parcel delivery emails

12 December 2016
You are advised to be wary of fake parcel delivery emails after the Australian Competition and Consumer Commission (ACCC) warned the number of complaints about this scam more than tripled in 2016.

The ACCC says it received more than 4,300 complaints about the scam in 2016 – up more than threefold on 2015 – and 350 people reported providing personal information such as bank account details to scammers.

"Unfortunately this scam is particularly effective during the holiday season with so many Australians going online to buy Christmas presents," ACCC Deputy Chair Delia Rickard says. "There is nothing festive about this scam - scammers will use it to steal your personal information and lighten your wallet."

The scammers will typically send fake emails that purport to be from legitimate parcel delivery businesses such as Australia Post or FedEx. These emails may claim the recipient has an 'undeliverable package' and threaten to charge a fee for holding an undelivered item. The email then directs the recipient to open an attachment, click a link or download a file to retrieve the parcel.

However, recipients who follow these instructions are likely to inadvertently infect their computer or network with malicious software (malware). They may find a type of malware known as ransomware has locked their files and the scammers are demanding payment for the software to unlock them.

The ACCC recommends people take the following steps to help protect themselves against these scams:

- Be aware of phishing campaigns and if you do receive a suspicious email purporting to be from a reputable Australian organisation, such as Australia Post, please err on the side of caution. If concerned, contact the organisation for verification (for example, for Australia Post related emails, you can contact scams@auspost.com.au)
- Do not click on links or download files in emails you receive out of the blue - especially if they are executable (.exe) files or zip (.zip) files. These files are likely to contain malware or ransomware viruses.
- If you are suspicious about a 'missed' parcel delivery email, call the company directly to verify that the correspondence is genuine. Independently source the contact details through an internet search or phone book – do not rely on numbers provided in the suspicious email.
- Regularly back up your computer's data on a separate hard drive. If your computer is infected by malware or ransomware you can restore the factory settings and easily re-install all of your software and data
- Buy yourself (or your business) a standalone hard drive for Christmas. These have become relatively inexpensive and can save you a lot if your computer is infected by malware or ransomware.