BE CYBER SMART
Think. Check. Connect.

# BE CYBER SMART

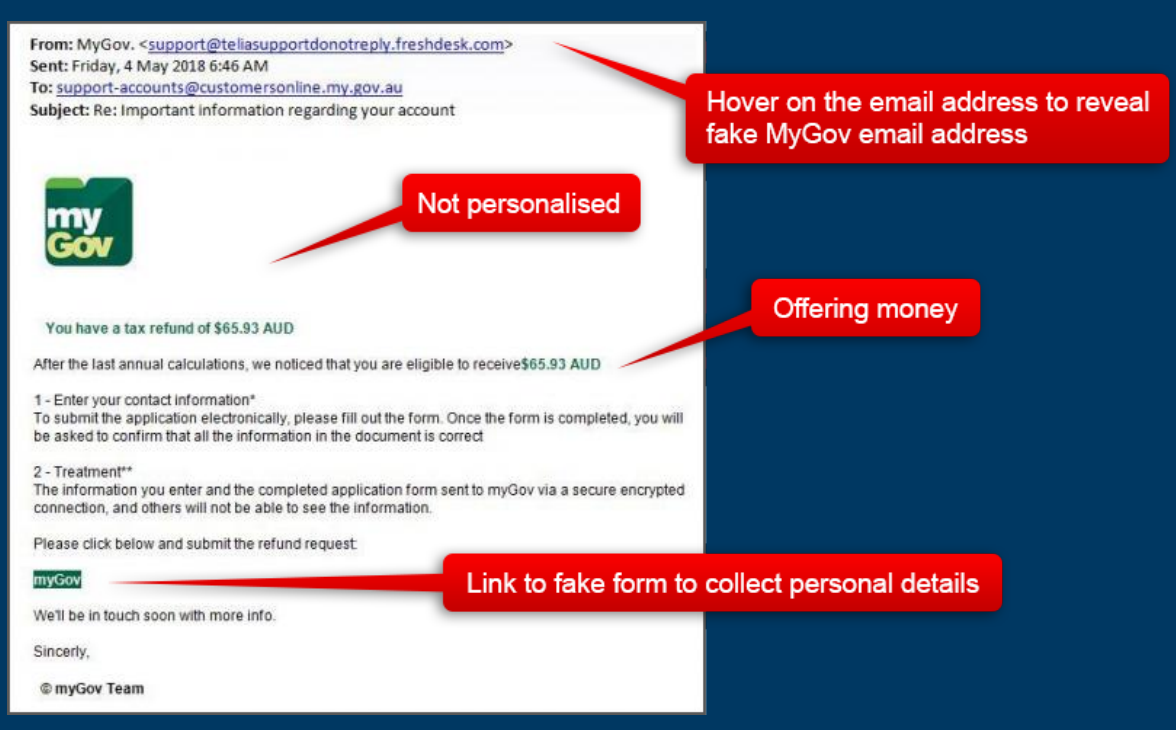
# DON'T BE PHISHED!

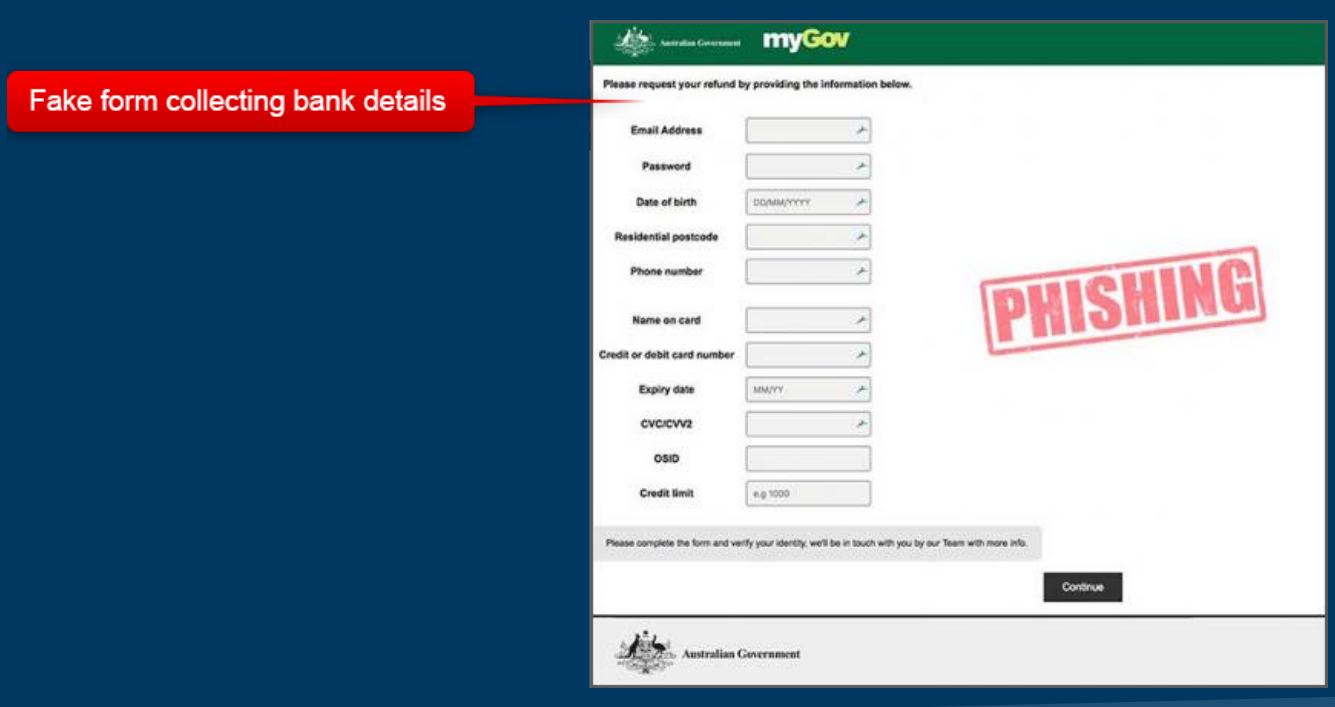
'**Phishing**' and '**spear phishing**' aim to lure you into providing passwords, banking details or personal information, or to download attachments or click on malicious links that contain malware to infect your device.

## Does it look Phishy?

**Phishing emails are becoming more sophisticated and can include logos and links to fake websites.**

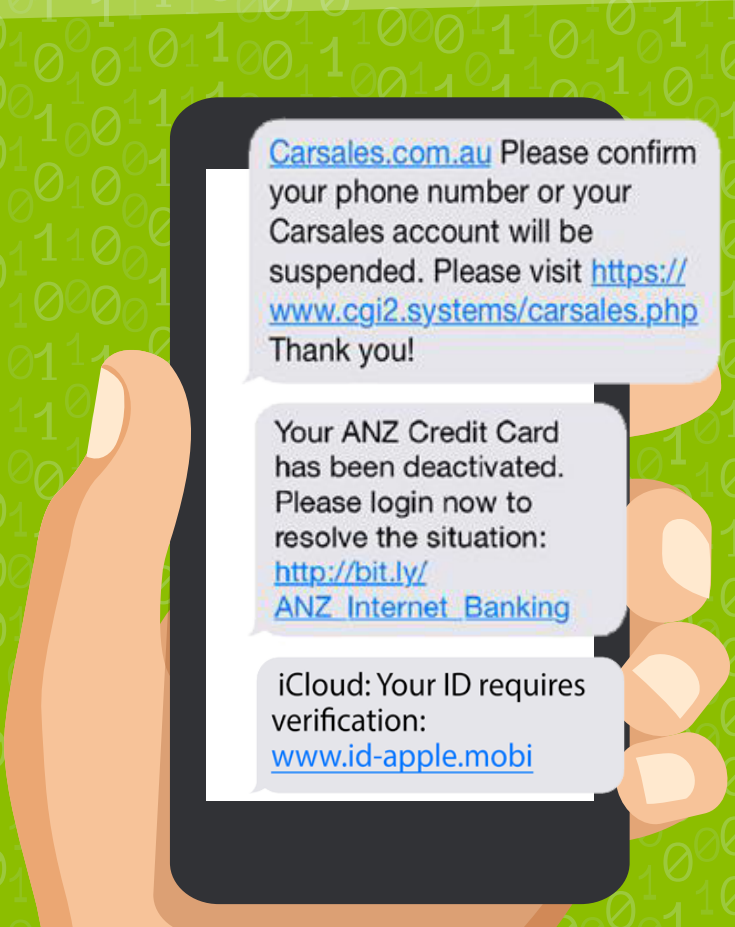
**Be alert to unexpected emails with links or attachments or suspicious requests.**




**Phishing** threats can be distributed by email, SMS, instant messaging or social media platforms.

**Spear phishing** is targeted phishing where personal information gleaned from other sources, such as social media, is used to make the email appear authentic.




## Don't be phished - Think, Check, Connect.

Hackers rely on you being busy and trusting

### THINK

**Be suspicious of emails – do not click on links you are not expecting.**

Think about what they are asking you to do. Don't share your user name or password and be careful about sharing your bank account details. Because of phishing, it is now standard policy for many companies to not call or email you to update or verify your personal or confidential details.

### CHECK

**Hover on the links and check the pop-up email and web addresses carefully to verify authenticity.**

Contact the sender to check authenticity only using legitimate published contact details, from a phone book or a website. Do not rely on contact details supplied in the email.

If you weren't expecting the email and the contents are suspicious **do not** click on any links or download attachments – report it to the **Australian Cybercrime Online Reporting Network (ACORN)** at **www.acorn.gov.au**

### CONNECT

**Only click on links you have checked and verified.**

Website links may look legitimate but check the URL. For example fake government emails or websites may use **.net** instead of **.gov.au**

**If you mistakenly click on a suspicious link – report it straight away to the Australian Cybercrime Online Reporting Network (ACORN) at www.acorn.gov.au and contact your IT provider.**

Monitor **www.acorn.gov.au** for cyber and scam alerts.

NORTHERN TERRITORY GOVERNMENT