

## Avoiding online scams

Lately I have received a number of emails supposedly from the Commonwealth Bank. I eventually opened one of these emails, which I don't encourage you to do. The email said I had one unread message in my online banking inbox. I don't bank with the Commonwealth. These emails are obviously a scam trying to obtain my bank details.

Scam emails often look legitimate with the correct logos, phone numbers, dates and even ABN's. They are designed this way to lull you into a false sense of security. Scam emails often ask you to open a link to NetBank and ask you to enter your banking details. You should never open a link in an email unless you know what the link is and who it is from, as sites may steal your details and your money. This is known as phishing. If your bank sends you an email it should never have a link to a website. If you are concerned about the legitimacy of a bank email, telephone your bank to confirm if they really sent it. If you get emails from banks you don't deal with, delete them immediately.

It's not only emails from banks that can disguise phishing emails. I have seen fake emails from PayPal and eBay, where logos make the email look legitimate. Yet the email is still just trying to obtain your banking details.

There are ways to tell if a website is legitimate. If you get an email from PayPal and the link takes you to a page where you need to enter your username and password make sure the page starts with <https://www.paypal.com>. If you get an email from eBay where you need to enter your username and password, be sure the address starts with <https://signin.ebay.com.au/>. If you are using Internet Explorer 7 or higher, it has a built in phishing filter which can usually identify if you are about to visit a known phishing site.

If you find you are getting a lot of unsolicited or spam emails you can download and install a free version of Mail Washer from <http://www.mailwasher.net/>. Mail Washer is used to identify and block spam emails. The program will remember which emails are spam the next

time you open your email. If you purchase the professional version of Mail Washer the spam emails identified will be deleted immediately.

Another way to reduce spam emails is setup a second email account with Hotmail or Yahoo which are both free. By having a second account you only use your preferred email address for important communication from friends, family or work. Use the second address when you need to sign up for things on the internet. Some websites will sell your email address to spammers, so if they sell your second email address which you hardly ever visit, this will prevent a lot of spam from entering your preferred email account. You do need to occasionally check the second account to keep it active.

Another scam which is increasingly common is fake antivirus programs. Programs look legitimate with plausible sounding names such as Win Antivirus and Win Defender, which can be easily confused with a real program called Windows Defender. Fake virus programs tell you that your computer has a virus, which it may not necessarily have, and that you need to purchase their program to remove the virus. You then pay for a program that you didn't need that doesn't work anyway. Some fake antivirus programs even load viruses, spyware and adware onto your computer, slowing down your computer and internet connection. Fake antivirus programs may even cause you to lose files, personal data or allow hackers to access your credit card or banking details.

If you see any emails that promote unrealistic promises such as telling you have won a prize or that you are going to inherit a large sum of money, there is a good chance these are a scam. These scams are often used to access your email address and other personal details enabling identify theft or tricking you into giving away your life savings.

A free eBook can be downloaded from <http://www.scamwatch.gov.au> which helps you identify many different scams.

If your computer is running slow or you think you may have a fake antivirus program, pop in and see me at the Grenfell Internet Centre or phone 6343 1720. I can remove the fake

antivirus and install AVG 8.5 Internet Security on your computer to stop future fake antivirus and viruses from being loaded on your computer.