Question on Notice
No. 605
Asked on 10 May 2011

MS DARLING asked the Minister for Police, Corrective Services and Emergency Services (MR ROBERTS)—

QUESTION:

With reference to a recent *Courier Mail* story regarding cyber-attacks in the Sandgate area—

Will the Minister advise the House how residents can improve their safety online and protect their personal information?

ANSWER:

While the Internet is a powerful communication tool, offenders have adapted to it quickly and are now using it en masse to target victims via text message and email, or in cases like this, hacking into a system and attempting to steal personal information.

It is estimated identity theft costs the Australian community between $1.6billion and $3billion annually and this is expected to grow.

As well as potentially losing a great deal of money, victims can also be embarrassed and humiliated in the process.

There are three main areas where members of the public can take simple measures to improve their online security. They include computer security, online shopping and email management.

Firstly, with computer security, members of the public should ensure their computers have reputable antivirus software which has automatic updates. They should also ensure their computer is password protected and these passwords are changed regularly and never given to any other person. If the computer is connected to the internet through a wireless network, an appropriate level of encryption should also be installed.

The second area of concern is online shopping. Members of the public should ensure they only purchase items from trusted online vendors. Where possible, they should only use trusted payment methods or credit cards with online protection.

People should also be wary of calls or emails from people purporting to be from a financial or other institution seeking to obtain or confirm personal information. Members of the public should independently verify the contactors legitimacy before providing any such information.

The other area utilised by criminals to target individuals online is via email. Members of the public should adopt a few simple email management rules to ensure their safety online. Firstly, never open emails from people you don't know or forward or reply to any such emails. People should never click on any links or attachments in any such emails.

These emails should be deleted immediately. People should also be mindful of placing too much detail including email addresses in any online forum or site.

These straightforward rules can provide users of online services with a higher level of internet security and safety. People should seek professional advice from reputable companies in the computer industry in relation to antivirus software and other products available to enhance their safety online.

The Queensland Police Service (QPS) provides information in relation to online safety through a number of forums. There are also a number of QPS and other publications made available to the public which provide information and ways for members of the public to protect themselves from electronic crimes (E-Crime). These publications and other advice are also provided online through a number of state and federal government websites. The address of the QPS website is www.police.qld.gov.au.

The QPS's expert Fraud and Corporate Crime Group also has a number of initiatives aimed at preventing this crime and educating the public on how to avoid becoming a cyber crime victim.

At the end of National Consumer Fraud week (13 March 2011), there had been approximately two million hits on the QPS Facebook page in relation to information provided and promoted during the campaign, including detailed strategies to improve online safety. To access this information, go to the QPS Facebook page at www.facebook.com/queenslandpolice.