Question on Notice
No. 518
Asked on 20 April 2005

Mr Livingstone asked the Minister for Tourism, Fair Trading and Wine Industry Development (Ms Keech)—

QUESTION:

With reference to Queenslanders who continue to be targeted by scammers, despite the best efforts of the Beattie Government to educate them to be scam-smart and as many of my constituents have recently received notifications that they have won prizes in overseas lotteries-

Will she advise how people can guard against falling victim to such scams?

ANSWER:

I thank the Honourable Member for his question and his keen interest in consumer protection.

The best advice for Queenslanders to avoid being ripped off by scam artists is 'if it looks too good to be true, it probably is'. This is the message the Beattie Government has been communicating to consumers since coming to office, and it is as true today as it ever was. I highlighted this message in Queensland Consumers Week 11-15 April 2005.

Two elements are common to all scams:

- first, the recruitment approach is something that looks plausible at first sight; and
- second, the main appeal is to greed or fear of loss.

The phoney lottery scam which the Honourable Member uses as an example seeks to gain consumers' trust through use of impressive letterheads and personalised mail merging. The recipient is encouraged to think they've received a personal letter, instead of mass-produced scam junk mail. The letters also include references to genuine foreign lotteries and websites the consumer can visit to confirm these lotteries actually exist.

The letter informs the recipient that they've won a substantial prize. To claim it, all they need do is send a small "handling fee", tax or the like, and the cheque will be despatched by return post. The amount the consumer is asked to send is also usually an odd amount (eg $27.82) to add to the perception that it is a legitimate fee.

Of course, there is no prize. The money sent by duped consumers goes into the pocket of the scam promoter. The fraudsters work on the principle that they only need one or two percent of recipients sending the "handling fee" to make a profit.

The internet makes the scam even more profitable, since there are negligible postage and printing costs. Internet schemes require only one person in 1,000 – or even one in 10,000 – to be duped, for the scheme to turn a dishonest dollar.

The internet has also spawned a whole new generation of scams. One scam Queensland consumers should look out for is 'phishing'.

'Phishing' scams involve a legitimate-looking email message from a financial institution, claiming that the institution needs to confirm internet banking details, such as account number and PIN or password. The consumer clicks on a link, and goes straight to a website.

The trouble is, of course, that the website is bogus – even though it may resemble the institution's site in every detail. Once the consumer enters the account and password information onto the phishing site, the fraudsters are able to use the information to transfer funds from the consumer's accounts into their own.

The key to avoiding internet scams is, first, to remember the advice 'if it sounds too good to be true, it probably is'. Second, remember the internet is just another communication medium like mail and the telephone. If you wouldn't do something over the telephone or by mail, don't do it on the internet. For example, you wouldn't give your bank account and PIN to someone who rang up claiming to be from the bank, so you shouldn't do it on the internet either.

Scams, phishing and other consumer frauds (such as the notorious Nigerian scam) are illegal throughout the world. Scam promoters rely on the challenges facing regulators in our global economy, and constantly change identities and addresses to avoid prosecution.

I have been working with my colleagues in other states and territories, the Commonwealth, and New Zealand through the Ministerial Council on Consumer Affairs (MCCA) to address these issues. A key to effective enforcement is sharing information among consumer protection agencies on a national and international basis. A new national consumer intelligence-sharing system called AUZSHARE, which was a Queensland initiative, was launched at MCCA on 22 April 2005.

When the Office of Fair Trading becomes aware of a new scam, information is posted on the national scam website www.scamwatch.gov.au and on the Office website www.fairtrading.qld.gov.au. It's a good idea to check on these sites, or phone the Office of Fair Trading on telephone 1300 658 030 for the cost of a local call. But remember: just because it's not on our websites doesn't mean it's not a scam. Scam promoters are constantly thinking up new scams and variations on old ones to ensnare the unwary.

Last, but by no means least, NEVER respond to something you think may be scam communication. A response tells the scam promoter two important things: you are living at the address, and you read the scam communication. If you respond, you may go onto a 'sucker list' database. These databases are swapped and traded by scam merchants. When you go onto a 'sucker list', you will most certainly receive more scam communications.