

WARNING ON FINANCIAL AND TAX CYBER CRIME

The Assistant Treasurer, Senator Nick Sherry, said today that an Australian Taxation Office (ATO) submission to a Parliamentary inquiry highlights the growing dangers of cyber crime to the financial and tax security of individual Australians and also to Government agencies.

The Assistant Treasurer also highlighted the wide range of actions underway to educate the community and crackdown on such illegal behaviour.

"There has been a 31%* increase in recent years in scammers and hackers targeting the Tax Office's computer systems," the Assistant Treasurer said.

"These incidents include attempts to phish for information and malicious software attacks, such as viruses and trojans."

"In addition, a number of email scams claiming to offer a Tax Office refund have been phishing for individual victims."

"More than 90 per cent of tax returns are lodged electronically and the use of the internet by taxpayers is continuing to grow - so everyone should be aware of the potential dangers."

The ATO provided an unclassified version of its response to the House of Representatives Standing Committee on Communications Inquiry into Cyber Crime last week.

"The Rudd Government considers e-security to be one of Australia's top national security priorities, as expressed by the Prime Minister in the Inaugural National Security Statement last year," the Assistant Treasurer said.

"The Rudd Government is committed to strengthening our e-security coordination arrangements and to ensuring that all Australians, including Australian businesses, have access to information to protect themselves against cyber crime and other online threats."

"Identity fraud is one of the fastest growing crimes in the world - with thieves using your bank accounts and credit card details to steal from you or to commit other crimes in your name."

"Some tax phishing scams are quite sophisticated - one recent case from a server based in the Ukraine lured victims by a bogus website that looked identical to the ATO website."

The Tax Office has put in place a wide range of initiatives to counter financial and tax cyber crime including innovative use of internet banner ads during relevant Google word searches and direct email advisories to domestic and international students.

Since 1 July 2008 the Tax Office has successfully finalised 35 prosecutions - resulting in 29 custodial sentences and \$1.5 million in reparation orders.

"The Tax Office is well resourced with specialist IT staff dedicated to the detection and follow-up of cyber crime," said the Assistant Treasurer.

"The Tax Office places a heavy emphasis on prevention of cyber crime and is actively involved in educating internet users about the potential risks."

Tax Office emails or SMS messages will never ask for your personal information, such as credit card details, tax file number, date of birth or passwords.

If an individual feels that they may have been the victim or attempted target of a financial or tax cyber crime, they should:

- delete suspicious emails immediately, and if you are unsure whether the email you have received is legitimate, check the Tax Office website for a list of genuine SMS and email activities and examples of fraudulent emails;
- contact the Tax Office on 13 28 61 as soon as possible if anyone has provided any personal tax information such as their tax file number;
- contact their bank or credit card providers immediately if anyone has provided personal bank information or credit card details; and .
- contact the Tax Office on 13 28 61 or the Tax Evasion Referral Centre on 1800 060 062 if they have any information on possible scams or any other fraud.

** 31% increase between 2007 and 2008*

CANBERRA
24 August 2009