



ASSISTANT TREASURER

<http://assistant.treasurer.gov.au>



BEWARE OF PHISHING SCAM PROMISING TAX REFUNDS

The Assistant Treasurer, Senator Nick Sherry, is warning Australians of a new email phishing scam using the lure of a tax refund to try to steal private information.

“This particular scam is quite sophisticated and uses convincing fakes of what could be easily mistaken for Australian Tax Office web pages,” the Assistant Treasurer said.

“The email claims to be from the Australian Taxation Office and shows a fake Tax Office email address as the sender.”

“Reports coming into the ATO suggest there is a high volume of these emails going out over the internet,” the Assistant Treasurer said.

The email uses the Tax Office logo and includes the words ‘Tax refund’ in the subject heading and the following text:

“General information about e-tax, including the demonstration, benefits of using e-tax, computer and eligibility requirements, and security.”

There may be other variations to the subject and text.

The email asks people to enter their email, name and date of birth to search for any refund owing, which then directs them to a bogus Tax Office website and asks for personal and credit card details. An example of this fake site is attached below.

“Anyone who receives the email should delete it immediately,” the Assistant Treasurer said.

“The Tax Office never sends emails asking people to provide personal information or credit card details. “

“You should always be wary of unsolicited emails claiming to be from the Tax Office, particularly those that encourage you to follow embedded links to other sites.”

“You should type internet addresses directly into your internet browser rather than following links in emails as an extra precaution.”

“Anyone who has already entered their credit card information into the bogus site should immediately report it to their credit card provider,” the Assistant Treasurer said.

More information on online security including examples of scam forms and emails is available at the Tax Office website, www.ato.gov.au

“Unfortunately, the incidence of cyber criminals, scammers and hackers is on the increase – with bogus emails targeting Australians from around the world,” the Assistant Treasurer said.

"Identity fraud is one of the fastest growing crimes in the world as thieves try to extract bank accounts and credit card details to steal or to commit other crimes using false identities.”

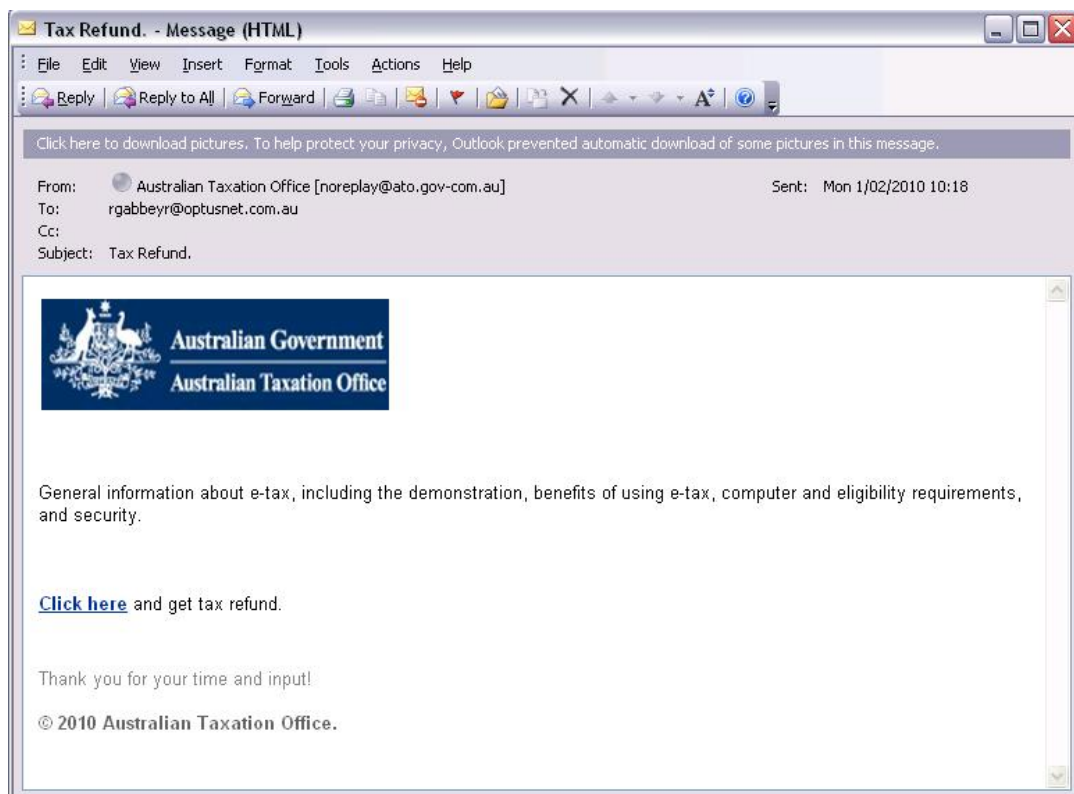
"The Rudd Government considers e-security to be one of Australia's top national security priorities and is committed to strengthening our e-security arrangements,” the Assistant Treasurer said.

CANBERRA

2 February 2010

Media Contact: Joe Scavo 0413 800 757

EXAMPLE OF FAKE EMAIL:



EXAMPLE OF FAKE WEBSITE WHEN “CLICK HERE” PRESSED:

The screenshot shows a website header for the Australian Government Australian Taxation Office. The main content area is titled 'Refund Status' and contains a 'Search Tax Refund Online' section. This section asks the user to enter their E-mail, Full Name, and Date of Birth, with a 'SEARCH' button below. The input fields are empty. To the left is a navigation menu with categories like 'What do you want to do?' and 'Tax topics A-Z'. To the right are 'Online Services' and 'Call Centre Top 5' lists.

FAKE SITE THEN SEEKS YOUR CREDIT CARD DETAILS:

This screenshot shows the same website, but the 'Refund Status' section has changed. It now displays 'Get Tax Refund on your VISA or MasterCard Now!' and shows a 'Refund Amount' of '\$ 210.75 AUD'. Below this, there are two sections: 'Enter Your Information' with fields for Address, City, State/Territory, Postcode, and Phone Number; and 'Enter Card Information' with fields for Card Type, Card Number, Expiration Date, and CVV/CNV. The input fields are empty. The rest of the page layout remains the same.