

# ATO related scams

## *What to look out for and how to protect yourself*



The ATO acknowledges that there are many different types of scams – online, phone, mail and face-to-face. Online scams, such as email ‘phishing’ scams are on the rise and are designed to trick you into giving away your money, passwords and/or personal details (such as your tax file number - TFN). You should never respond to an email requesting you to confirm, update or disclose confidential details like your name, date of birth, address, passwords, credit card details etc.

A new email scam claiming to be from the Australian Taxation Office is currently circulating.

This latest scam has a bogus ATO form attached to it, which asks for personal details including credit card details and ATM card PIN numbers. The email asks for the form to be completed, printed, and sent in to a genuine ATO address.

The email states that ‘after a recalculation of your fiscal activity, we have determined that you are entitled to receive a tax refund of AU\$ xxx’.

When the victim fills out the form and clicks the ‘print’ button, all of the personal details are instantly sent to a third party overseas.

After submitting personal details, victims are redirected back to the genuine ATO website.

These scams are predominantly designed to conduct identity theft and or credit card fraud.

From time to time, the ATO may amend your tax return (for example, because of a data-matching exercise). If this happens, we will send you an amended notice of assessment on paper to your postal address. It will never be sent by email.

Key indicators of this scam:

- the email asks you to confirm / update your personal details. You should always be suspicious of this
- poorly worded with spelling and grammatical mistakes
- includes an attachment (form)
- comes from an email address which is not a valid ATO email address
- asks for credit card and PIN numbers
- the ‘print form’ button sends all of the personal details to the scammers (as well as sending the form to your printer)
- the scam asks for the paper form to be sent to an authentic ATO address, to attempt to increase authenticity.

We recommend that if you receive a suspicious phone call or email you should contact the ATO immediately.



07 5443 4988

[www.accountingnorth.com.au](http://www.accountingnorth.com.au)