




Social media – suggested tax time posts





Social media is a great way to spread the message on how to protect yourself online at tax time. Here are some suggested Facebook posts that are ready to use. These are just thought starters – if you would like to adapt them for your audience or channels, please do.

You can also visit Stay Smart Online on Facebook and like, comment or share our content. The campaign hashtags are #StaySmartOnline and #TaxTime.

The social media tiles below, along with a Facebook cover, website banner and case studies to share, are available on the Stay Smart Online website:

www.staysmartonline.gov.au/taxtime19

Image	Post
	<p>Watch out for scammers at #TaxTime! Scammers often impersonate the @atogovau and demand payment for fake tax debts.</p> <p>Remember, the ATO will never ask you to pay your tax debt with pre-paid cards or with cryptocurrencies like Bitcoin. For electronic payment of tax debts, the ATO accepts payment into an account held by the Reserve Bank of Australia only.</p> <p>For more info about ATO payment options, visit www.ato.gov.au/General/Paying-the-ATO/How-to-pay/</p> <p>More tips to protect yourself online a tax time: https://www.staysmartonline.gov.au/taxtime19</p>
	<p>Cybercriminals may use business information such as your AUSkey to commit tax fraud in your name.</p> <p>Beware of anyone asking you to 'confirm' your business details. And don't share your details unless you've checked the person you're dealing with is who they say they are.</p> <p>Learn how to keep your business safe from scammers this #TaxTime https://www.staysmartonline.gov.au/taxtime19</p>
	<p>Stay one step ahead of scammers at #TaxTime!</p> <p>Sign up to the free @StaySmartOnline Alert Service to receive information on the latest online threats and how to respond – https://www.staysmartonline.gov.au/alert-service</p>

	<p>Scammers can be really convincing. If you receive a message claiming to be from the @atogovau, think twice before downloading attachments or clicking links in emails or text messages, even if they appear to come from someone you know.</p> <p>More tips to avoid suspicious messages https://www.staysmartonline.gov.au/taxtime19</p>
	<p>Always check your tax through ATO online services via myGov – and manually type the URL into your browser https://my.gov.au</p> <p>Scammers often impersonate the @atogovau in emails, text messages, phone calls and over messaging services or social media. The best way to avoid falling victim is to ignore these approaches and only log into your myGov account to check if you owe a debt or are due a refund.</p> <p>For more advice head to https://www.staysmartonline.gov.au/taxtime19</p>
	<p>Using a security code sent to your mobile phone to sign into myGov, https://my.gov.au, is a quick and secure way to access ATO online services.</p> <p>To set up your security code, sign in to your myGov account then select 'Account settings' at the top of the page. Choose 'Sign-in options' and turn on 'Receive a code by SMS'.</p> <p>Be cyber safe at #TaxTime: https://www.staysmartonline.gov.au/taxtime19</p>
	<p>Stay alert for scammers this #TaxTime! Scammers often impersonate the @atogovau and demand payment for fake tax debts.</p> <p>Remember, the ATO will never ask you to pay your tax debt with pre-paid cards or with cryptocurrencies like Bitcoin. For electronic payment of tax debts, the ATO accepts payment into an account held by the Reserve Bank of Australia only.</p> <p>For more information about ATO payment options, visit www.ato.gov.au/General/Paying-the-ATO/How-to-pay/</p> <p>More tips to protect yourself online a tax time: https://www.staysmartonline.gov.au/taxtime19</p>