2018 Scams Awareness Week campaign toolkit
Threat-based impersonation scams
Monday 21 – Friday 25 May 2018

Background

Since 2011, the ACCC, as chair of the Australasian Consumer Fraud Taskforce (now known as the Scams Awareness Network or SAN) has led a major annual scams awareness campaign, the National Consumer Fraud Week (now known as Scams Awareness Week).

This campaign has a different theme each year and provides an opportunity for SAN members to continue to raise public awareness and disrupt scam activity by equipping people with the knowledge to identify and avoid scams. Scamwatch data from the previous calendar year is referred to in these campaigns.

This year's campaign will run from Monday 21 to Friday 25 May 2018 and will focus on threat-based impersonation scams with the slogan 'Stop and check: is this for real?'.

Threat-based impersonation scams include a number of approaches where scammers impersonate a government agency or trusted company and make threats of fines, arrest, court action, and even deportation to scare victims into making payments to them or giving them their personal information.

The ACCC releases its annual *Targeting scams* report on the first day of Scams Awareness Week every year. This report discusses scam trends, statistics and the activities of relevant organisations to combat scams in the previous calendar year. The ACCC's 2017 *Targeting scams* report will be released on 21 May 2018.

Aims & objectives

The primary aim of these annual campaigns is to raise awareness of particular scams targeting Australians.

A secondary aim is to inform people about the resources available to help them and what they can do if they think they have been contacted by a scammer or fallen victim to a scam.

In this year's campaign, these aims will be accomplished by completing the following objectives:

- raising awareness of threat-based impersonation scams amongst the target audiences
- promoting Scamwatch (www.scamwatch.gov.au) as a reliable source of information and guidance on scams as well as a place to report them
- attracting media attention for the campaign through the release of the ACCC's 2017 *Targeting scams* report on 21 May 2018.

Target audiences

The target audiences for this campaign are

- consumers, and particularly vulnerable consumer groups, and their relevant key intermediaries
- mainstream media.

Campaign slogan

Stop and check: is this for real?

Campaign webpage

The campaign webpage on the Scamwatch website – www.scamwatch.gov.au/scamsweek2018 – will go live on 21 May and will include information about this year's theme, links to the campaign resources and the ACCC's 2017 *Targeting scams* report, which is also being released on 21 May.

Key messages

All key messages are suggestions only, and key stakeholders and campaign partners are welcome to produce their own messages in line with their audiences and the broader campaign theme.

High-level key messages

- This Scams Awareness Week, which runs from 21–25 May 2018, Australians are urged to be on the lookout for threat-based impersonation scams by taking a moment to 'Stop and check: is this for real?'
- In these scams, scammers pretend to be from a government agency or well-known company. Their aim is to scare you into parting with your money or personal information and if you don't, they threaten you with fines, disconnecting your internet, taking you to court, arrest or even deportation.
- The ACCC's Scamwatch received almost 33,000 reports of these scams in 2017. Over $4.7 million was reported lost and more than 2800 people gave their personal information to these scammers.
- If you're contacted unexpectedly and threatened by someone who says they're from a government agency or trusted business, always consider the possibility that it may be a scam – then stop and check if it's for real.
- For more tips and information about these scams, where to get help or to report a scam, visit the Scamwatch website (www.scamwatch.gov.au/scamsweek2018).
- Scams Awareness Week is an initiative of the Scams Awareness Network, a group of Australian and New Zealand government agencies with responsibility for consumer protection and policing in scams, cyber safety and fraud.

Detailed key messages

These detailed key messages cover three main aspects of threat-based impersonation scams – how these scams work, how people can protect themselves and what people can do if they think they've been scammed.

How these scams work

- Some scammers claim to be from government departments or trusted, well-known businesses and use threats to pressure or scare you into giving them money or your personal information.
- These threats are commonly received over the phone. Almost 85 per cent of reports submitted to Scamwatch about these scams identified that the scammer had contacted them over the phone. The remaining were contacted by email.
- The typical threats scammers use include that you will receive a fine, you will be charged additional fees, your internet will be disconnected, the police or debt collectors will be sent to your home or even that you will be taken to court, arrested or deported.
- Scammers impersonate government officials and say that you have an outstanding tax debt or that there are problems with your government benefits, immigration papers or visa status, and you need to pay the debt or other fees to fix the problems.
- Scammers also pretend to be from trusted businesses and organisations, including energy or telecommunications providers, Australia Post, banks and law enforcement agencies like the police. They may call and ask for remote access to your computer to fix a problem or they may email you fake invoices or fines, and threaten to cancel your service or charge you excessive penalty fees if you don't pay them immediately.
- If the scammer sends an email, it is likely to include an attachment or a link where you can download proof of the 'bill', 'fine' or 'missed delivery details' but opening the attachment or downloading the file could infect your computer with malware.
- Older people have been particularly vulnerable to these scams. People aged 65 and over submitted the largest number of reports to Scamwatch in 2017 and had the highest reported losses. Young people, people from non-English speaking backgrounds and people experiencing financial hardship have also been affected by these scams.

Protect yourself tips

- When dealing with uninvited contacts from government agencies or trusted businesses – whether over the phone, by email, mail, in person or through social media – always consider the possibility that it may be a scam.
- If you're unsure whether a call or email is genuine, verify the identity of the contact through an independent source, such as a phone book or online search, then get in touch with them to ask if they contacted you. Don't use the contact details provided by the caller or in the message they sent to you.
- Don't be pressured by a threatening caller. Hang up then check whether their story is real.
- Don't respond to threatening emails or voicemail messages asking for you to call someone back. If you do, the scammers may increase their intimidation and attempts to get your money.
- If you're still unsure, speak to a trusted friend or family member about what has happened.
- Never send money or give your bank account details, credit card details or other personal information to anyone you don't know or trust, and never by email or over the phone.
- A government agency or trusted business will never ask you to pay by unusual methods such as with gift or store cards, iTunes cards, wire transfers or bitcoin.

- Don’t open suspicious texts, pop-up windows or emails and don’t click on links or open attachments – just delete them.
- Never give anyone remote access to your computer if they’ve contacted you out of the blue – whether through a phone call, pop up window or email – and even if they claim to be from a well-known company like Telstra.

Have you been scammed?

- If you’ve lost money or given personal information to a scammer, there are steps you can take straight away to limit the damage and protect yourself from further loss.
- If you’ve sent money or shared your banking or credit card details, contact your financial institution immediately. They may be able to stop or reverse a transaction, or close your account.
- If you’ve given your personal information to a scammer, visit IDCARE (www.idcare.org), Australia and New Zealand’s not-for-profit national identity and cyber support service. IDCARE can work with you to develop a specific response plan to your situation and support you through the process.
- As scammers are often based overseas, it is extremely difficult for government agencies to track them down or for law enforcement to take action against them. So take the time to warn your friends and family about these scams.
- For more information about scams, where to get help if you’ve been scammed or to report a scam, visit the Scamwatch website (www.scamwatch.gov.au/scamsweek2018).

Scams Awareness Week logo & banners

A Scams Awareness Week logo has been developed which will help launch the new name of this annual campaign. It is expected that this logo will help build brand recognition over time as it will be re-used each year.

The versions of the logo and banners that are available are presented in **Attachment 1** and all versions have been emailed to you in a zip file.

These materials can be provided in other sizes on request. Please email your request to ScamsAwarenessNetwork@accc.gov.au.

Social media content

The ACCC’s primary social media platform for the campaign will be our @Scamwatch_gov Twitter account. The Scams Week campaign will also be supported by our @acccgovau Twitter account and our ACCC Consumer Rights and ACCC Your Rights Mob Facebook pages.

Suggested template posts for Twitter, Facebook and LinkedIn throughout the Scams Week campaign are in **Attachment 2**.

Key stakeholders and campaign partners are also welcome to develop their own social media posts, in the context of this year’s campaign theme and using the campaign hashtags.

Campaign hashtags

The two hashtags to be used for this year's Scams Awareness Week are intended to highlight the campaign week and slogan:

- #ScamsWeek18
- #IsThisForReal

It is recommended that both hashtags are used, if space permits.

Social media infographics

A series of infographics have been developed for use on social media to accompany the suggested template posts or any posts developed by key stakeholders and campaign partners.

The infographics can be viewed in **Attachment 3** and all have been emailed to you in a zip file.

Videos

The videos being produced for the 2018 Scams Awareness Week campaign will be uploaded to the ACCC's YouTube channel on Monday 21 May (www.youtube.com/user/ACCCvideos).

Template articles

(These template articles are intended for use in blogs, emails, newsletters or online.)

Short article (about 300 words)

Warning about threat-based impersonation scams this Scams Awareness Week

If you received a call out of the blue from the Tax Office saying you had a tax debt that you had to pay immediately or be arrested, what would you think? If Telstra called you and said there were internet problems in your area and they needed remote access to your computer in order to help you otherwise they would disconnect your service, what would you do?

While it would be understandable if your initial reaction was fear or panic, this Scams Awareness Week, Australians are being urged to 'Stop and check – is this for real?'

These calls are examples of threat-based impersonation scams about which the ACCC's Scamwatch received almost 33,000 reports in 2017. About 85 per cent of these reports indicated the scammer had been in contact by telephone.

In these scams, scammers pretend to be from a government agency or well-known, trusted business and they use threats to pressure or scare you into giving them money or your personal

information. They may threaten you with fines, disconnecting your internet, arrest, court action or even deportation.

The scammers and their threats can seem genuine and frightening. They make you feel as if you've done something wrong or that there's some urgency and you must do what they say immediately or suffer the consequences.

And many people have believed these threats. According to Scamwatch, over $4.7 million was reported lost and more than 2800 people gave their personal information to these scammers in 2017.

If you're contacted unexpectedly and threatened by someone that says they're from a government agency or trusted business, always consider the possibility that it may be a scam – then stop and check if it's for real.

For more tips and information about these scams, where to get help or to report a scam, visit the Scamwatch website (www.scamwatch.gov.au/scamsweek2018).

Long article (about 700 words)

Warning about threat-based impersonation scams this Scams Awareness Week

If you received a call out of the blue from the Tax Office saying you had a tax debt that you had to pay immediately or be arrested, what would you think? If Telstra called you and said there were internet problems in your area and they needed remote access to your computer in order to help you otherwise they would disconnect your service, what would you do?

While it would be understandable if your initial reaction might be fear or panic, this Scams Awareness Week, Australians are being urged to 'Stop and check – is this for real?'

These calls are examples of threat-based impersonation scams, about which the ACCC's Scamwatch received almost 33,000 reports in 2017. About 85 per cent of these reports indicated the scammer had been in contact by telephone.

In these scams, scammers pretend to be from a government agency or well-known, trusted business and use threats to pressure or scare you into giving them money or your personal information. They may threaten that you will receive a fine, that you will be charged additional fees, that your internet will be disconnected, that the police or debt collectors will come to your home, or that you will be taken to court, arrested or even deported.

These scammers and their threats can seem genuine and frightening. They make you feel as if you've done something wrong or that there's some urgency and you must do what they say immediately or suffer the consequences.

And many people have believed these threats. According to Scamwatch, over $4.7 million was reported lost and more than 2800 people gave their personal information to these scammers in 2017.

Older Australians have been particularly vulnerable to these scams – people aged 65 and over submitted more than 5800 of the Scamwatch reports and reported losing almost $1 million last year.

If you're contacted unexpectedly and threatened by someone that says they're from a government agency or trusted business, always consider the possibility that it may be a scam – then stop and check if it's for real.

Keep in mind the following tips to protect yourself:

- Verify the identity of the contact through an independent source, such as a phone book or online search, then get in touch with them to ask if they contacted you. Don't use the contact details provided by the caller or in the message sent to you.
- Never send money, give your banking or credit card details or other personal information to anyone you don't know or trust, and never by email or over the phone.
- Know that a government agency or trusted business will never ask you to pay them with gift or store cards, iTunes cards, wire transfers or Bitcoin.
- Don't open suspicious texts, pop-up windows or click on links or attachments in emails – just delete them. These could infect your computer with malware.
- Never give anyone remote access to your computer if they've contacted you out of the blue – whether through a phone call, pop up window or email – and even if they claim to be from a well-known company like Telstra.

But if you realise you've lost money or given your personal details to a scammer, there are steps you can take straight away to limit the damage and protect yourself from further loss:

- If you've sent money or shared your banking or credit card details, contact your financial institution immediately. They may be able to stop or reverse a transaction, or close your account.
- If you've given your personal information to a scammer, visit IDCARE (www.idcare.org), Australia and New Zealand's not-for-profit national identity and cyber support service. IDCARE can work with you to develop a specific response plan to your situation and support you through the process.
- As scammers are often based overseas, it is extremely difficult for government agencies to track them down or for law enforcement to take action against them. So take the time to warn your friends and family about these scams.

For more information about these scams, where to get help or to report a scam, visit the Scamwatch website (www.scamwatch.gov.au/scamsweek2018).

Case studies

(These case studies are from scam reports submitted to the ACCC's Scamwatch. All victims agreed to share their story when submitting their report and their personal details have been changed.)

Help Telstra catch the hackers

Olive received a call from a woman who claimed she was from Telstra. Olive was told her internet would be cut off within two hours as 'Telstra' had identified a number of unauthorised logins from overseas on her internet account – her computer had been hacked. Olive was then passed on to a technician named 'Chris' who made her log on to her computer and showed her the hackers'

supposed logins. ‘Chris’ told Olive that her bank accounts were in danger of being used by the hackers and that they had to be stopped. To help ‘Telstra’ do this, ‘Chris’ asked Olive for her bank account and credit card details and to log in to both of her accounts online, which Olive did. To catch the hackers, ‘Chris’ said he’d deposit $1600 into Olive’s bank account which she had to use to buy iTunes cards as soon as possible. Olive saw the money had been transferred into her account so she went and bought the cards. As instructed, she scratched the back of the cards and ‘Chris’ took a photo of them through Olive’s webcam. ‘Chris’ said he’d publish the codes online to help ‘Telstra’ track the hackers’ movements. He also instructed Olive not to use her computer until he called her back the next morning. Olive became suspicious at this point, so she contacted her bank and they confirmed that $1600 had not been deposited into her account and her account was now overdrawn. Her bank cancelled her credit card immediately.

Your NBN is being used illegally

Georgia received a phone call supposedly from Telstra and was told that her new NBN was being used illegally without her knowledge. This situation had been flagged as urgent by ‘Telstra’ and needed to be fixed immediately. Georgia was asked to download the Team Viewer software so a ‘Telstra’ technician could remotely access her computer and look at the security settings to fix the problem. ‘Telstra’ also said it would set up an additional password for extra security on Georgia’s computer. While in Georgia’s computer, the technician blanked the screen so she couldn’t see what he was doing but he stayed on the phone with her explaining every step. He accessed Georgia’s emails and hacked into her PayPal account, changing the settings so that a log-in would no longer be required each time a purchase was made. The technician purchased gift vouchers from the United States, telling Georgia the vouchers were for security programs needed on her computer and they would be fully refunded by Telstra. After the technician ended the call, several other purchases were made from gaming stores in the US. Georgia turned off her computer when she realised these unauthorised purchases had been made. But then ‘Telstra’ called her back asking her to switch her computer back on. Georgia is now receiving daily calls from ‘Telstra’ Security which is apparently another division of Telstra. She is also receiving calls from private numbers claiming to be PayPal and asking for her pin number. As well as the loss of some personal information, Georgia lost $600 from the unauthorised purchases.

You owe the Tax Office

Eliza received a call from someone saying they were from the Australian Taxation Office and that she was being charged with tax fraud. The ‘Tax Office’ told Eliza she owed them $4900 and if she didn’t pay an initial instalment of $500, a warrant for her arrest would be issued and she could face jail. Eliza immediately panicked as she is a single parent from the UK with a 10-year-old son and no other family in Australia. She burst into tears and couldn’t think properly. The ‘Tax Office’ said she had to make a decision whether to pay now or be arrested within 24 hours. So Eliza gave the ‘Tax Office’ her credit card details. She was then told she’d receive a text message with a passcode which she had to provide so the arrest warrant could be stopped. Eliza was also told a taxation officer would visit her the next day with all the relevant paperwork advising how to pay back her full debt. However, as soon as Eliza gave the ‘Tax Office’ the passcode, she ran to the bank as she had begun to worry she’d been scammed. The bank teller confirmed that two withdrawals had been made from her account, totalling $4900. Eliza’s conversation with the ‘Tax Office’ lasted over an hour and in that time, she was in complete shock and disbelief at what she was being threatened with. When the ‘Tax Office’ mentioned the possible loss of her Australian passport and being deported back to England, Eliza simply panicked, otherwise she would never have provided any of her financial details.

You will be charged with tax fraud

Alex received a recorded message that the Australian Taxation Office had tried to contact him many times and that it had sent him letters which had been returned, unopened. Because of this, the 'Tax Office' was now taking legal action against Alex for tax fraud and evasion which would result in a warrant for his arrest. Alex called back the 'Tax Office' and spoke to 'James Ree' who provided his badge number and a case number. 'James' confirmed the 'Tax Office' had sent Alex letters to a particular address, but Alex said he hadn't lived there for about a year. 'James' told Alex he was about to be arrested and lose his assets as he owed taxes. 'James' said Alex could end up in jail for up to 10 years. Alex believed what he was being told. 'James' then told Alex that he could stop all of this from happening if he set up a tax debt repayment plan. All that was needed was an up-front payment of $500, then a regular payment plan could be organised with a taxation officer. Alex was also warned that this could be done in one of two ways – he could pay the 'Tax Office' privately, otherwise, the situation would become public knowledge and the 'Tax Office' would publish his name and offence in the newspaper. By this time, all Alex could think about was losing everything he had so he followed the instructions he was given. He went to Coles and bought $500 of iTunes gift cards. 'James' then said they would need another $500 of iTunes cards for the taxation officer's expenses so Alex bought these additional cards as well.

There's a problem with your immigration forms

Ali received a call on his landline from someone who worked at the Immigration Department to advise there been some changes to the immigration rules. Because of these changes, 'Immigration' needed new forms and because they hadn't received the required forms from Ali, they were now taking legal action against him. To stop this legal action, 'Immigration' told Ali to go to a store and buy 24 iTunes cards, worth $100 each, then scratch each of them and read out the codes immediately. The caller threatened that if Ali didn't follow the instructions, he would be taken into custody and face two years' imprisonment, along with an $88,000 fine. He was also threatened with deportation and told that his child would be taken away from him. Ali was told that he wasn't allowed to contact anyone, not even his wife, via any means of communication and to keep this discussion confidential. The caller gave Ali his name, badge ID and a case number, so Ali believed the call was genuine and bought the iTunes cards and recited the codes.

You will be deported in two hours

Sanjeet's wife, Maya, had arrived in Australia six months prior. Early one morning, Maya received a call from a 'David Wilson' who said he worked for 'Australian Immigration' in New Delhi. He said when Maya was leaving India, she gave the wrong date of birth on her immigration form, so she was going to be deported back to India within two hours. 'David' asked Maya to pay $930 which would mean she could be allocated a lawyer to fight her case while she remained in Australia. Maya was unsure whether to believe 'David' but he recited the details that she and Sanjeet had provided to the Immigration Department for a partner visa. He also told Maya to go to the Department of Foreign Affairs and Trade website and check the phone number there to see if she was receiving the call from the same number – and the numbers were the same. Maya became very scared and believed him. 'David' then convinced Maya to make a transaction via Western Union. He remained on the phone with her for about three hours and that entire time, prohibited her from putting his call on mute, calling Sanjeet or talking to anyone in a language other than English. After Maya transferred the $930, 'David' asked for payment of a 'case closing fee'. Maya said she couldn't do that because she didn't have any more money. 'David' made several more attempts but when he failed to get any more money from Maya, he admitted that he had just scammed her.

Pay a penalty or lose your pension

Danielle's mother-in-law, Rosa, was called by someone claiming to be from Centrelink. 'Centrelink' told Rosa she had not replied to their letters requesting information so she had to pay a $300 penalty. Of course, Rosa had never received any such letters. The caller spoke very quickly and told Rosa that her file had now been sent to the Canberra office and she would need to buy $300 of iTunes cards to cover the penalty for not responding to their letters. If Rosa did this, her file would be returned to her local Centrelink office. If she didn't, 'Centrelink' threatened to stop her pension altogether. Rosa didn't know what iTunes cards were so she asked if she could pay the penalty by cash or credit card. The caller said that wasn't possible and harassed Rosa into buying the iTunes cards by telling her where to go to get them and how to get there. Rosa finally agreed and was told that someone would call her back for the codes on the backs of the cards. Rosa was also given a number, supposedly in Centrelink's Canberra office, to call if she had any concerns. And she was told she had an appointment at her local Centrelink at 11:00 am the following Monday with a 'Sylvia Johnson' to discuss the situation. After talking to her daughter-in-law, Rosa realised this was a scam, however, she had given her pension number to the caller which she then reported to Centrelink.

You have an infringement notice

Anthony received an email apparently from the Australian Federal Police as it featured the agency's logo. The email said that he had been issued with an infringement notice for a violation such as speeding, illegal parking or toll evasion. It also stated that if Anthony didn't pay the fine within 28 days, enforcement action would be taken and he could be prosecuted in the Magistrates' Court. The email Anthony received included a file with the actual infringement notice and specific details of his violation which he tried to download. However, the file was corrupted. His computer security software alerted him there was a security threat and disabled the file.

Attachment 1
Scams Awareness Week logos & banners

Logos

There are four versions of the Scams Awareness Week logo.

Each version is available in Adobe, EPS and TIFF formats.

All of these versions have been emailed to you in a zip file.

The logos may also be available in other sizes on request. Please email your request to ScamsAwarenessNetwork@accc.gov.au.

POSITIVE

MONO

REVERSED

MON REVERSED

Banners

There are banners in six sizes available for the 2018 Scams Awareness Week campaign.

All of these banners, in TIFF format, have been emailed to you in a zip file.

These banners may also be available in other sizes on request. Please email your request to ScamsAwarenessNetwork@accc.gov.au.

Attachment 2
Social media content

Date	Twitter	Facebook / LinkedIn
Monday 21 May	#ScamsWeek18 starts today. This year we're warning you about threat-based impersonation scams where scammers aim to get your money or personal info by making threats and scaring you. To find out more, visit Scamwatch www.scamwatch.gov.au/scamsweek2018 #IsThisForReal	Scams Awareness Week 2018 kicks off today. This year we'll be bringing helpful info and tips on how to identify and protect yourself from threat-based impersonation scams. www.scamwatch.gov.au/scamsweek2018
	To get your money or info, scammers impersonate a government agency or trusted business & make threats that you'll be fined, have your internet cut off, be taken to court, arrested or deported. Don't be pressured by threats – just hang up or hit delete #ScamsWeek18 #IsThisForReal	
Tuesday 22 May	Scamwatch received almost 33,000 reports in 2017 of scammers impersonating government agencies, or trusted businesses like Telstra and Australia Post, and making threats. Always stop & check #IsThisForReal. For more info www.scamwatch.gov.au/scamsweek2018 #ScamsWeek18	Scamwatch received 33,000 reports of threat-based impersonation scams in 2017. Do you know what to look out for? www.scamwatch.gov.au/scamsweek2018
	Being threatened by someone who says they're from the government or a well-known business is scary. But just hang up. Get the organisation's number from an independent source like a phone book or online search & check if they did contact you #ScamsWeek18 #IsThisForReal	
Wednesday 23 May	Over $4.7 million was lost to threat-based impersonation scams in 2017 according to Scamwatch reports & more than 2,800 people gave their personal info to these scammers. Stop & check: is this for real? For tips: www.scamwatch.gov.au/scamsweek2018 #ScamsWeek18	More than $4.7 million was reported lost to threat-based impersonation scams in 2017. If someone claiming to be from a well-known organisation contacts you demanding money be paid to them in iTunes vouchers, bitcoin, or by wire transfer, it's a scam. www.scamwatch.gov.au/scamsweek2018
	Scammers impersonate government officials & say you owe a tax debt or there are problems with your government benefits, immigration forms or visa & you must pay the debt or other fees to fix the issues… or else. For more info www.scamwatch.gov.au/scamsweek2018 #ScamsWeek18 #IsThisForReal	More than 2,800 people gave their personal information to scammers posing as representatives of well-known organisations. Always remember - no government agency or trusted organisation will threaten you to try and get your personal information or bank details. www.scamwatch.gov.au/scamsweek2018

Date	Twitter	Facebook / LinkedIn
Thursday 24 May	Scammers pretend to be from trusted companies like Telstra. They email you fake bills or want remote access to your computer to 'fix the problem' & threaten to charge fees or cut off your internet if you don't do what they ask www.scamwatch.gov.au/scamsweek2018 #ScamsWeek18 #IsThisForReal	Telstra and the Australian Taxation Office are the two most frequently impersonated organisations used in threat-based impersonation scams. Make sure you know who you're dealing with before you share your personal information or bank details. www.scamwatch.gov.au/scamsweek2018
	Government agencies or trusted companies will never threaten you & ask you to pay them with iTunes gift cards, wire transfers or bitcoin. For more tips, visit Scamwatch www.scamwatch.gov.au/scamsweek2018 #ScamsWeek18 #IsThisForReal	
Friday 25 May	Most common contact method for threat-based scams? Phone calls, including pre-recorded voice messages. Even if overseas, scammers can make phone numbers look like a local number so you think the call is real. For more info www.scamwatch.gov.au/scamsweek2018 #ScamsWeek18 #IsThisForReal	You're more likely to encounter a threat-based impersonation scam over the phone. If someone calls you claiming to be from a trusted business or government agency and threatens you with a fine, court action or arrest, hang up. www.scamwatch.gov.au/scamsweek2018
	If you get an email with an attachment or a link to the details of your 'overdue bill', 'speeding fine' or 'failed delivery details' – don't open it. This could infect your computer with malware. Visit Scamwatch for more tips www.scamwatch.gov.au/scamsweek2018 #ScamsWeek18 #IsThisForReal	

Attachment 3
Social media infographics

These infographics can be used on social media to accompany the suggested template posts or any posts developed by key stakeholders.

These infographics have been emailed to you in a zip file.

01

02

03

04

05

06