STAYSMARTONLINE Partner Resource Kit

# National Scams Awareness Week

## 21 – 25 May 2018

#IsThisForReal #StaySmartOnline
#ScamsWeek18

An Australian Government Initiative

# National Scams Awareness Week 2018

National Scams Awareness Week is an annual awareness-raising week run by the Australian Competition & Consumer Commission. This year, we are urging Australians to be on the lookout for threat-based impersonation scams by taking a moment to ask - 'Is this for real?'

## What is a threat-based impersonation scam?

Threat-based impersonation scams are common and can often be traumatic for the victim. Typically, these scammers pretend to be from a government agency or well-known company. Their aim is to scare you into handing over your money or personal information and if you don't, they threaten you with fines, internet disconnection, arrest or even deportation.

## How can I get my organisation involved?

Scams Awareness Week is a great opportunity for Government, Stay Smart Online and our partners to join forces to educate Australians and encourage them to take simple steps to improve their resilience to scams.

Our goal is to help people identify and protect themselves from threat-based impersonation scams. We want to encourage people to talk more about the scams they come across, and to help others avoid them too!

We've developed a bunch of resources that make it easy for your team to be part of National Scams Awareness Week, and share the content with your own audiences.

**Here are some ideas to get you started**

- Share your #IsThisForReal story on social media to start the conversation
- Put up posters around the office, meeting and break rooms
- Use the social media material to share messages on your Facebook, Twitter, LinkedIn or Instagram accounts
- Publish a news article in your newsletter or on your blog/intranet
- Use our screensavers on your computers as a daily reminder for staff
- Digital banners and web tiles are perfect for your website, intranet or even email auto-signatures!
- Share the case studies to help your colleagues understand that anyone can fall victim to a scam

You'll find plenty of resources that are ready to run with on our website.

## Need help?

If you have any questions about our resources or other ideas about how you can support National Scams Awareness Week, please get in touch with us StaySmartOnline@ag.gov.au

# Key messages

Scams Awareness Week, runs from 21–25 May 2018, and Australians are urged to be on the lookout for threat-based impersonation scams by taking a moment to ask - 'Is this for real?'

### How these scams work

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 2,800 people gave their personal information to these scammers.

### How you can protect yourself

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 ask - 'Is this for real?'

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. Don't use the contact details provided by the caller or in the message they sent to you.

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.

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.

### What to do if you think you've been scammed

If you've sent money or shared your banking or credit card details, contact your bank 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, Australia's not-for-profit national identity and cyber support service.

Scammers are often based overseas, so it's extremely difficult to track them down or to take action against them. So take the time to warn your friends and family about these scams.

To report a scam, visit the Scamwatch website (www.scamwatch.gov.au/report-a-scam).

### Where to go for more information

For more tips and information about these scams or where to get help, visit the Stay Smart Online Website (www.staysmartonline.gov.au/scams2018).

# Share your #IsThisForReal story

We know that people don't like to talk about the times when they have been scammed or nearly fallen for a scammers trick! But the more we share these stories the more we can help others from falling victim.

We know there are many people who have been scammed, or know someone who has been scammed. We'd love to hear from you if you have a story to tell that helps educate others!

## Instructions for your story board

On the poster board available from our website and in your own words please tell us your #IsThisForReal story (some examples on the next page).

Hold your answer on paper in front or next to you. Take a full colour photo with a background that represents your profession (this could be your organisation's logo).

Post your photo to social media (Facebook, Twitter, Instagram, LinkedIn) using the hashtags #IsThisForReal #ScamsWeek18 and #StaySmartOnline.

Please email your photo/s to us StaySmartOnline@ag.gov.au in a high resolution JPEG file so we can share them too!

## Here are some example answers. Please share your own stories.

1. I was recently emailed a traffic infringement for immediate payment, but thought 'Is this for real?' as I don't even drive.
2. My dad called me after receiving an email about a supposed tax refund. He said he hadn't submitted a tax return so I told him it was a scam!
3. I received a call from someone who told me my computer had a virus… after talking to them for a couple of minutes I began to think 'is this for real?'
4. I was contacted by an energy company who told me my account was in arrears and would be cut off if I didn't pay immediately. I use a different energy provider altogether, which made think 'Is this for real?'

## Here are some ideas for sharing your story on social media

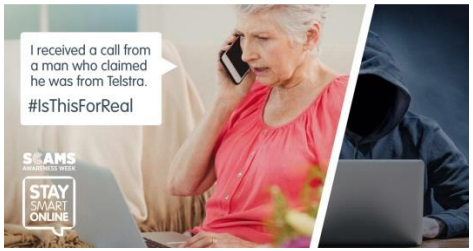
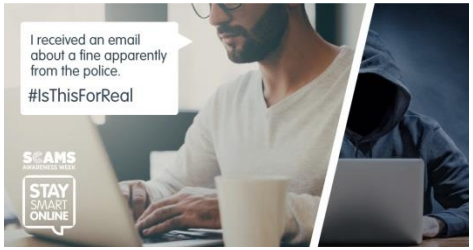
**Photo of you with your story**


**Facebook / LinkedIn / Twitter**

- Anyone can be the target of a scammer! Have you ever thought #IsThisForReal? Share your story to help others!
- Have you ever opened and email and thought #IsThisForReal. Our CEO shares his experiences!
- Your story can help others identify scams and better protect themselves.

# Social Media

Social media is a great way to spread the message of how to protect yourself from scams. Here are some Facebook posts and tweets that are ready to use. These are just thought starters, if you would like to adapt them for your audience, please do. You can also visit Stay Smart Online on Facebook and like, comment or share our content. The campaign hashtags are #IsThisForReal, #ScamsWeek18 and #StaySmartOnline.

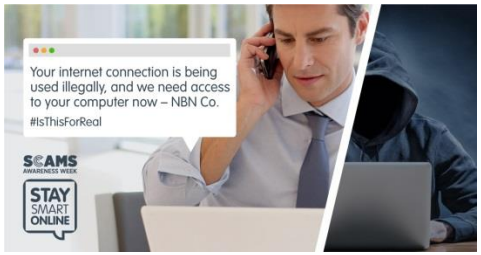
| Image | Facebook | Twitter |
|---|---|---|
|  | Scammers pretend to be from trusted companies - they email you fake bills or want remote access to your computer to 'fix the problem'. And they threaten to charge fees or cut-off your internet if you don't do what they ask! If you receive a call like this stop and ask yourself #IsThisForReal. For more tips visit www.staysmartonline.gov.au/scams18 | Scammers pretend to be from trusted companies. They threaten to charge fees or cut-off your internet. If you receive a call like this, ask yourself #IsThisForReal? For more tips visit www.staysmartonline.gov.au/scams18 |
|  | Australians lost over $4.7 million to scammers pretending to be from trusted companies in 2017, according to Scamwatch. If you get an email with an attachment or a link – ask yourself #IsThisForReal before opening it. For more tips visit www.staysmartonline.gov.au/scams18 | Australians lost over $4.7 million to scammers pretending to be from trusted companies in 2017, according to Scamwatch. If you get an email with an attachment or a link – ask yourself #IsThisForReal. More tips www.staysmartonline.gov.au/scams18 |
|  | Always remember – no government agency will threaten you to hand over your personal or bank details. If you feel threatened, it might be a scam! Always ask yourself #IsThisForReal. For more tips visit www.staysmartonline.gov.au/scams18 | Government agencies will never threaten you to hand over your personal or bank details. Always ask yourself #IsThisForReal. More tips www.staysmartonline.gov.au/scams18 |


Scammers work hard to make sure their threats seem genuine and frightening! They make you feel as if you've done something wrong and that you must do what they say immediately, or suffer the consequences. If you think it's a scam, it probably is! Always ask yourself #IsThisForReal. For more tips visit www.staysmartonline.gov.au/scams18

Scammers work hard to make sure their threats seem genuine and frightening! If you think it's a scam, it probably is! Always ask yourself #IsThisForReal. More tips www.staysmartonline.gov.au/scams18


If you get a random email from the Government demanding payment or asking for information they should already have, it could be a scam. Always ask yourself #IsThisForReal. For more tips www.staysmartonline.gov.au/scams18

If you get a random call from the Government demanding payment, it could be a scam. Always ask yourself #IsThisForReal. More tips www.staysmartonline.gov.au/scams18

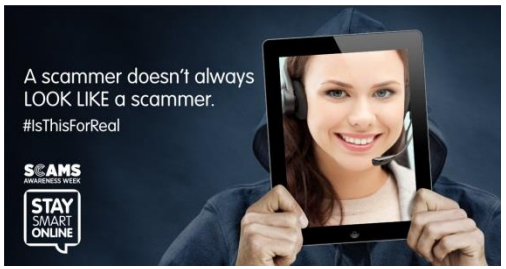



Last year almost 33,000 cases of threat-based impersonation scams were reported to Scamwatch! Always ask yourself #IsThisForReal. For more tips www.staysmartonline.gov.au/scams18

Last year almost 33,000 cases of threat-based impersonation scams were reported to Scamwatch! Always ask yourself #IsThisForReal More tips www.staysmartonline.gov.au/scams18


Anyone can say they are from the government or a company. If you're contacted unexpectedly by someone demanding payment or asking for information they should already have, contact the company via the number on their website & check if they really did contact you. Always ask yourself #IsThisForReal? For more tips www.staysmartonline.gov.au/scams18

Anyone can say they are from the government or a company. If you receive an unexpected call asking for information. Hang up and call them back on their main number. Always ask yourself #IsThisForReal More tips www.staysmartonline.gov.au/scams18




Do you know who you are REALLY talking to? Just because someone sounds friendly and professional doesn't mean they're who they say they are. Scammers can pretend to be from your bank, post office or telephone company. Always ask yourself #IsThisForReal. More tips www.staysmartonline.gov.au/scams18

Do you know who you are REALLY talking to? Scammers can pretend be for your bank, post office or telephone company. Always ask yourself #IsThisForReal. More tips www.staysmartonline.gov.au/scams18


Scammers use all kinds of tricks to disguise their true identity and get you to click on a link or give them money. If an organisation contacts you unexpectedly demanding payment, stop and consider whether they are who they say they are! For more tips www.staysmartonline.gov.au/scams18

Scammers use all kinds of tricks to disguise their true identity and get you to click on a link or give them money. If you think it's a scam, it probably is! Always ask yourself #IsThisForReal More tips www.staysmartonline.gov.au/scams18

# News article

## Stop and check – Is this for real?

*Sometimes scams are obvious, sometimes they're harder to spot. This week is Scams Awareness Week and we are urging all Australians to stop and check – 'Is this for real?'*

If you received a call out of the blue from someone saying you had a tax debt that you had to pay immediately or you'd 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 to help you, otherwise they would disconnect your service -what would you do?

These are good examples of threat-based impersonation scams. In 2017 the ACCC's Scamwatch received almost 33,000 reports of scams like these.

Typically scammers pretend to be from a government agency or a well-known, trusted business. They often use threats to pressure or scare you into giving them your personal information and your money. They also may threaten you with fines, disconnecting your internet, arrest, court action or even deportation.

The scammers work hard to make sure their threats seem genuine and frightening! They make you feel as if you've done something wrong and that you must do what they say immediately, or suffer the consequences.

Many people have fallen victim to this type of scam. In 2017, over $4.7 million was reported lost and more than 2,800 people were coerced into sharing their personal information.

### Protect yourself

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 'Is this for real?'

Here are some tips for you:

- When dealing with unexpected contact from government agencies or trusted businesses—whether over the phone, by email or through social media—always consider the possibility that it may be a scam.
- Don't be pressured by a threatening caller. Hang up then check whether their story is real. You can verify the identity of the contact through an independent source, such as a phone book or online search. Don't use the contact details provided by the caller or in the message they sent to you.
- Never send money, give your bank account or credit card details, or other personal information to anyone you don't know or trust.
- 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 that you know and trust.

### What to do if you have 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 bank 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, Australia'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 to track them down or to take action against them. So take the time to warn your friends and family about these scams.

## More information

Read more about threat based impersonation scams, including case studies and more tips on staying safe.

Read more tips about protecting yourself from all types of scams.

# Posters, screensavers & web tiles

You can put up posters around the office, or use our screensavers on your computers as a daily reminder for staff. Digital banners and web tiles are perfect for your website or intranet.