AUSTRALIAN COMPETITION & CONSUMER COMMISSION

SCAMWATCH

Scams Awareness Week 2021

SCAMS AWARENESS WEEK

Activity: real or fake?

- Pulse check – how is your scam radar?
- We’re going to show you 3 images and ask you to pick whether each image is real, or a scam.
- You’re not being graded – just have a go!

Image A – real or fake?

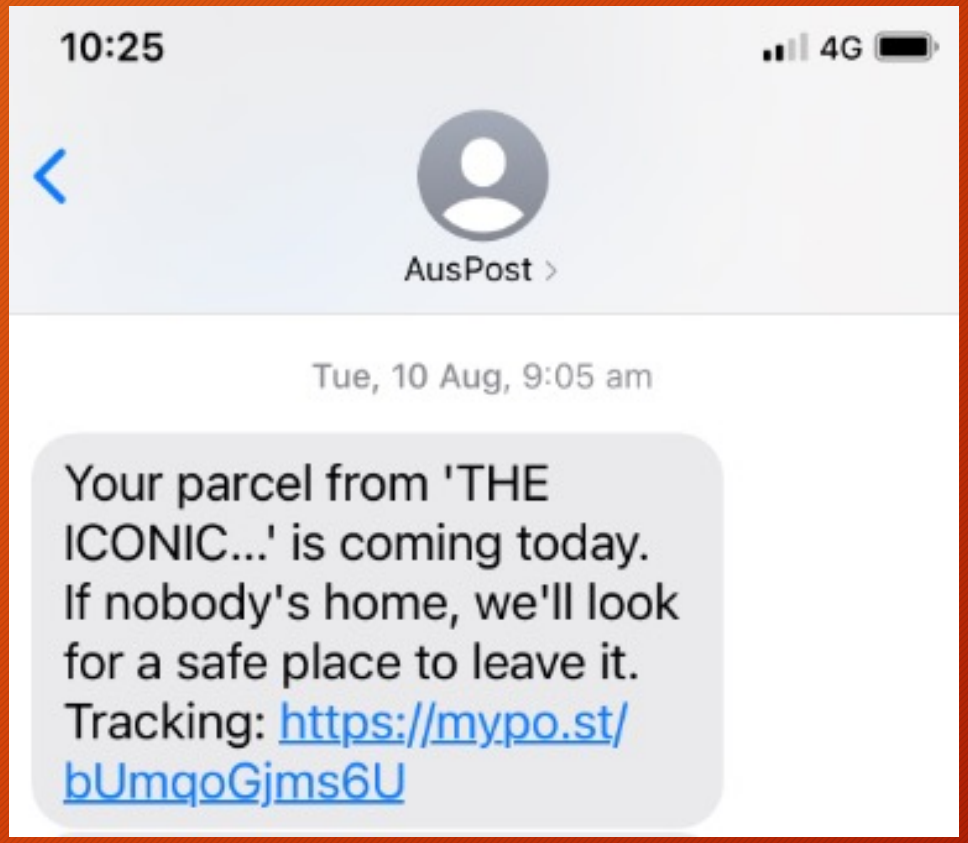


Image B – real or fake?

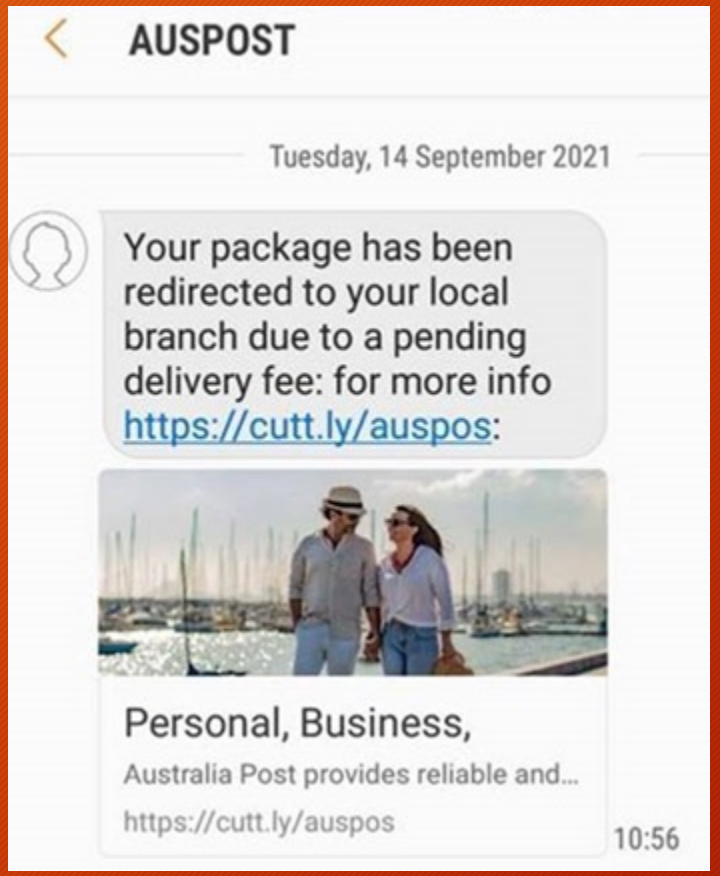
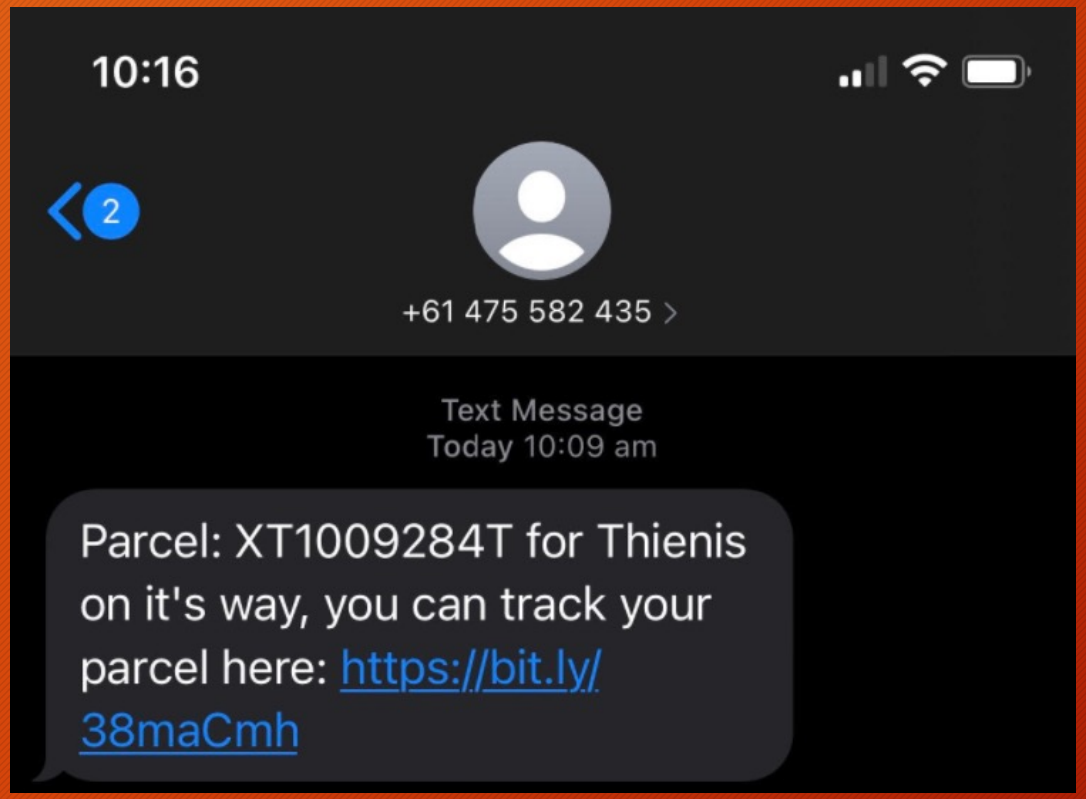


Image C – real or fake?



Well done!

- Image A – this message was legitimate
- Image B – this was a scam text
- Image C – this one was also a scam!

If you guessed these all correctly, well done! If you didn’t, don’t worry, you will be able to by the end of this presentation!

The role of Scamwatch

- Scamwatch is run by the ACCC.
- Provides advice to consumers and small businesses about how to recognise, avoid and report scams.
- Works with other consumer protection agencies to promote scams awareness.
- Scamwatch does not give legal advice or investigate individual cases, but it keep data about broad scam trends and works to disrupt scams.
- This year so far*, Scamwatch has received around 230,000 reports with over $225 million in losses.
- Some of the ways Scamwatch disrupts scams: intelligence sharing, consumer education, website takedowns.

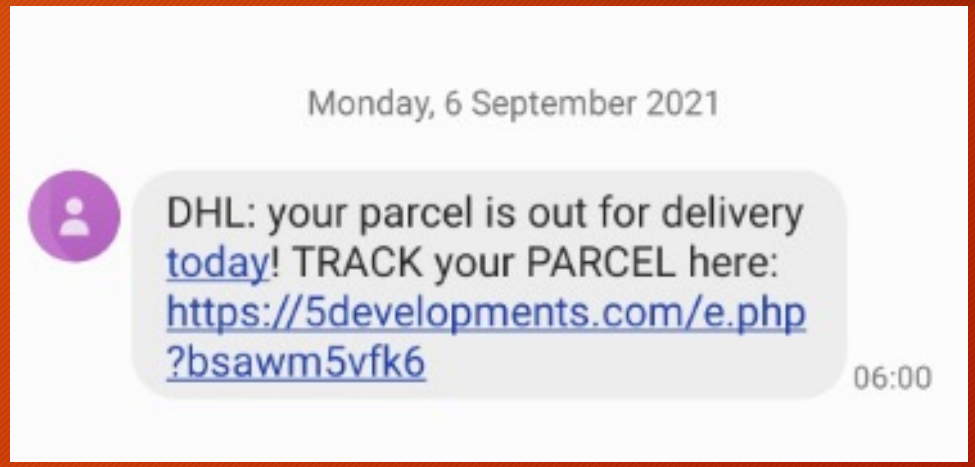
**data includes the period 1 Jan 2021 – 3 October 2021*

Latest scam trends

- Phishing: Scamwatch has been receiving a lot of reports about phishing scams. A driving factor is the inundation of ‘flubot’ scams.
- Malware scams that infect your phone using a dodgy link. Can steal your contacts and banking info.
- Have you received a message like this? Scamwatch has received over 18,000 reports with almost $11,000 in losses to these scams since August.*

*data includes the period 1 August 2021 – 12 October 2021

Poll – have you received a flubot message?



How flubot scams work

1. Phone owner gets a text message containing a php link
2. Clicks link and is invited to install software
3. Phone becomes infected with malware
4. Infected phone's contacts are added to central list of Flubot text recipients
5. Flubot can steal banking, contact and personal info from infected device

If your phone is infected, clean it with a factory reset after saving sensitive information

Latest scam trends cont…

- Investment scams: among the highest loss scams reported to Scamwatch. Losses to cryptocurrency investment scams are increasing. There has been 7,200 reports to Scamwatch with over $115 million in losses this year so far.*
- Dating and romance scams: not reported as much as other scams, but losses to dating and romance scams are usually very high. Scamwatch has received 2,500 reports of dating and romance scams with over $38 million in losses this year so far.
- The rise of ‘romance baiting’ – starts off as a dating and romance scam, but the victim is then lured into an investment scam.

**data includes the period 1 Jan 2021 - 3 October 2021*

Case studies

We’re going to look at some case studies of the types of scams you might encounter in your real life, that you may be able to learn from.

Poll – did you buy a pet during lockdown?

Case study 1 – puppy scam - $12,055 lost

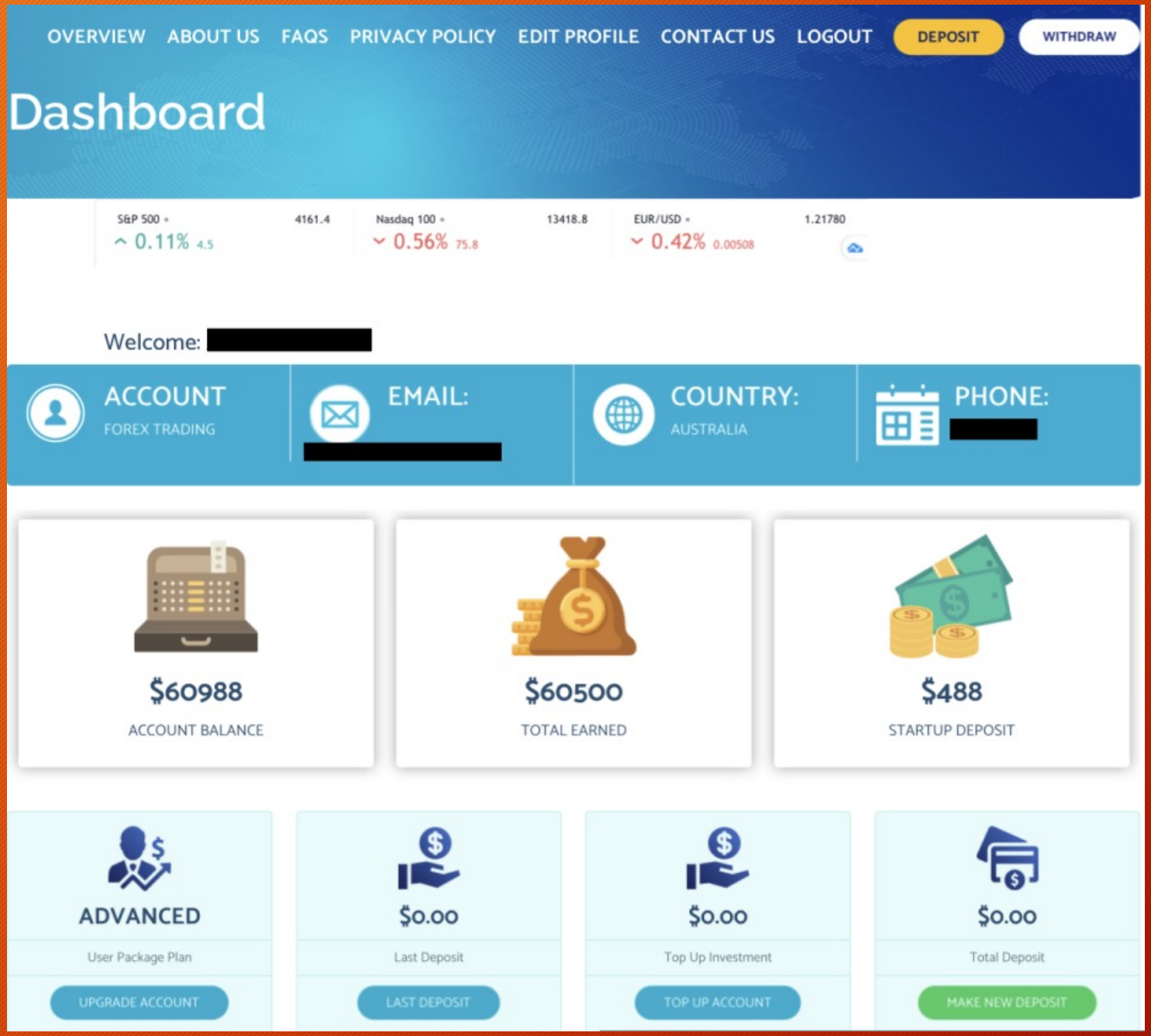
- Anonymous Scamwatch reporter came across a website selling puppies. The seller was based in Perth but said they could ship a puppy to the customer in Sydney.
- Made an initial payment of $1,850 for the puppy and shipping costs.
- Received “confirmation email” advising that the dog had been shipped and providing a tracking number.
- Began to receive continual requests for additional payments including a dog crate, pet insurance, pet vaccinations, state permits and coronavirus insurance.
- At this point, the victim realised the bank details they were being asked to pay into did not match the name of the logistics company they had been given details for.
- The victim lost $12,055 in total to this scam.

“I met this guy through whatsapp and we started a relationship. After we had been talking for a while, he told me he was doing financial trading and he had an insider informer telling him when to buy or sell. He told me he had already made lots of money, and asked me to sign up so I could make money too. I gave him copies of my driver’s licence and bank card and he opened an account for me. I started to transfer funds into an overseas bank account he supplied details for, then I started to trade with him. I could see on my account that I was making money through my investment. Eventually I submitted an application to withdraw my profits. My application was refused and suddenly I no longer had access to my account and my boyfriend stopped replying to my messages. I realise now that I was scammed.”

Case study 2 – romance baiting scam - $500,000 lost

Case study 3 – website takedown

- Scamwatch received a number of reports about a website called TradeCapitalFX.
- People had been scammed after using the site to buy bitcoins.
- Victims were unable to withdraw their profits after making initial investments or were asked to pay additional fees in order to have their funds released.
- $9,000 in losses to this scam site were reported in May, so the Scamwatch team decided to take action.

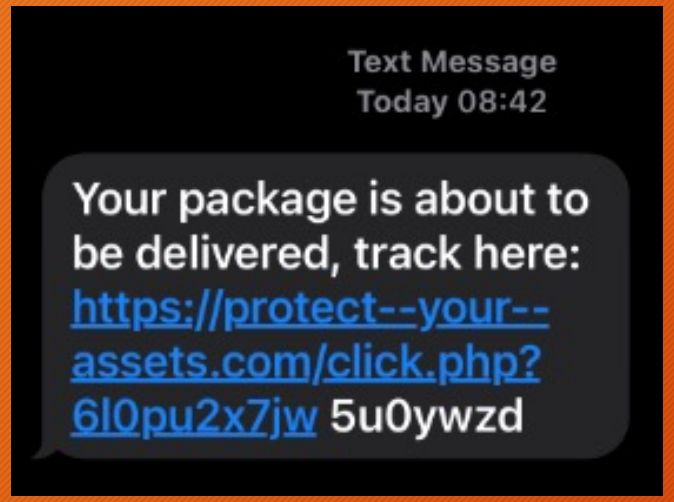

OVERVIEW
ABOUT US
FAQS
PRIVACY POLICY
EDIT PROFILE
CONTACT US
LOGOUT
DEPOSIT
WITHDRAW
Dashboard
S&P 500
4161.4
0.11% 4.5
Nasdaq 100
13418.8
0.56% 75.8
EUR/USD
1.21780
0.42% 0.00508
Welcome: [redacted]
ACCOUNT
FOREX TRADING
EMAIL:
[redacted]
COUNTRY:
AUSTRALIA
PHONE:
[redacted]
$60988
ACCOUNT BALANCE
$60500
TOTAL EARNED
$488
STARTUP DEPOSIT
ADVANCED
User Package Plan
UPGRADE ACCOUNT
$0.00
Last Deposit
LAST DEPOSIT
$0.00
Top Up Investment
TOP UP ACCOUNT
$0.00
Total Deposit
MAKE NEW DEPOSIT

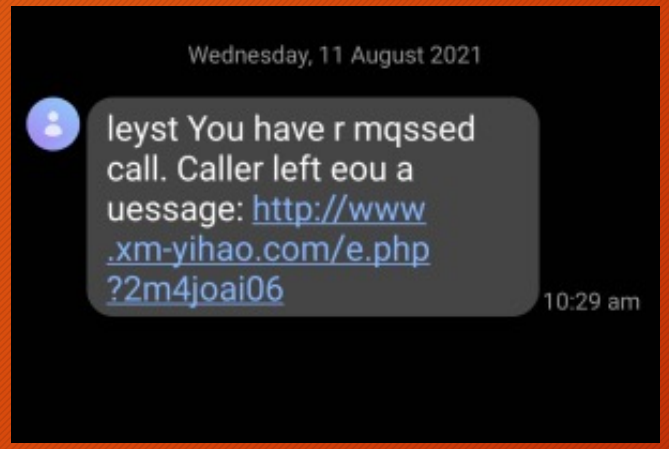
Case study 3 – website takedown cont…

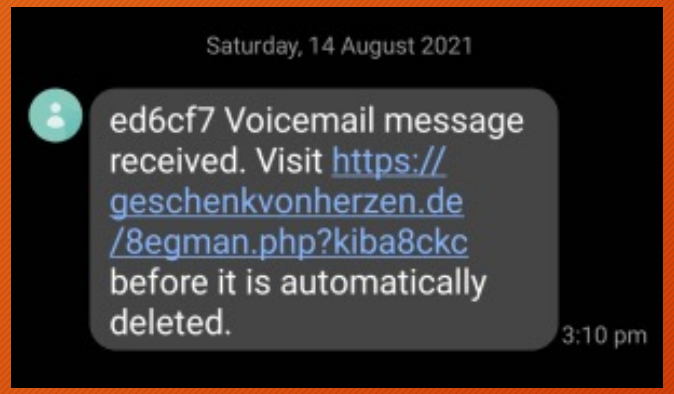
- Scamwatch investigated and confirmed the website was a scam.
- The evidence was submitted to the website's hosting provider and Scamwatch requested that the site be taken down to avoid further harm to consumers.
- The website hosting provider accepted the evidence and actioned the request – quickly removing the website.
- While this can't get the money back that was already lost, it does prevent others from getting scammed by this site.

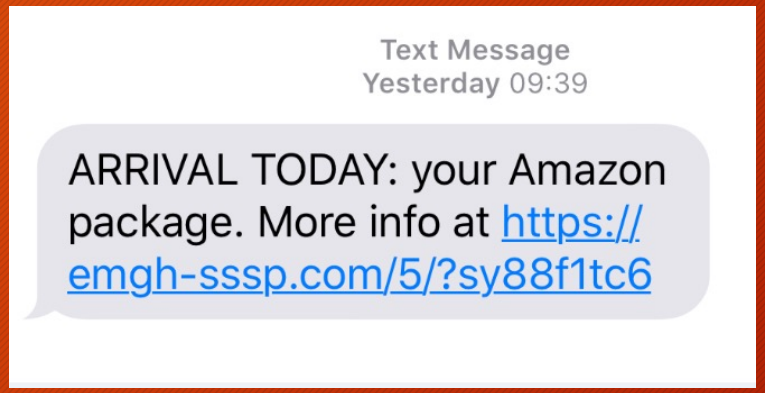
Some more real examples of flubot texts

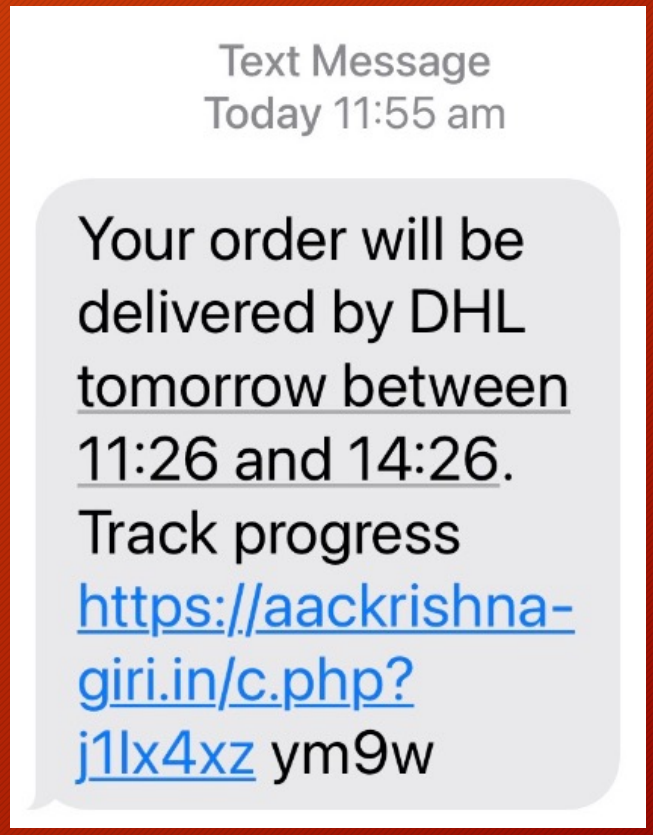
Watch out for these!











What Scamwatch is doing about scams

Scam disruption: intelligence sharing

Public sector sharing

- Government and law enforcement

Private sector sharing

- Telco, tech, banks, and more

What Scamwatch is doing about scams

Scam disruption: consumer education

- Scams Awareness Week
- Targeting Scams Report
- Scamwatch Radar alerts
- Little Black Book of Scams
- Media and social media

What you can do about scams

Use the T A L K method

- **T: Talk** to your friends, family, neighbours, colleagues about a scam you've come across, and share information.
- **A: Ask** a simple question, like "have you ever been scammed?" or "what's your top tip for avoiding scams?" to get the conversation started. You could even ask "have you received any of these flubot scam texts?"
- **L: Listen.** Sharing scam stories and experiences is helpful. Create a safe space for someone you know to talk to you about scams.
- **K: Keep talking!** Awareness is our biggest defence against scams. So TALK to as many people as you can about scams!

What you can do about scams

Reporting scams and where to get help

- Report to Scamwatch - https://www.scamwatch.gov.au/report-a-scam
- If you have lost money to a scam, contact your bank or financial institution as soon as possible - the Australian Banking Association provides a summary of steps for consumers when making a complaint to their bank. If you are not satisfied by the response from your bank, you can make a complaint to the Australian Financial Complaints Authority.
- If you have lost personal information and you are concerned your identity may be compromised, you can contact IDCARE for free support on 1800 595 160.
- Consider contacting the platform on which you were scammed to report the scam – https://www.scamwatch.gov.au/get-help/where-to-get-help#report-scams-to-facebook-services
- If you or someone you know is experiencing anxiety, emotional concerns or distress about scams, contact Lifeline on 13 11 14 24 or Beyond Blue on 1300 22 4636.

Scams Awareness Week 2021: 8 – 12 Nov

Overview

- Scams Awareness Week is a national campaign by the Scams Awareness Network, a group of Aus and NZ govt agencies with responsibility for consumer protection.
- Each year, Scams Awareness Week has a different focus and is delivered in collaboration with a large range of partners.
- Scamwatch provides activities and online resources that you can use throughout the week to raise awareness of scams.

Scams Awareness Week 2021
Get involved!

You can get involved by:

- Visit the Scamwatch website, download the campaign resources and participate in the activities. You could post some things around your office or host a scams awareness morning tea!
- Use the Scams Awareness Week background for your virtual meetings throughout the week. Great conversation starter.
- Follow Scamwatch on Twitter @scamwatch_gov for updates, and share the content.
- TALK to someone you know about scams!

Thank you!