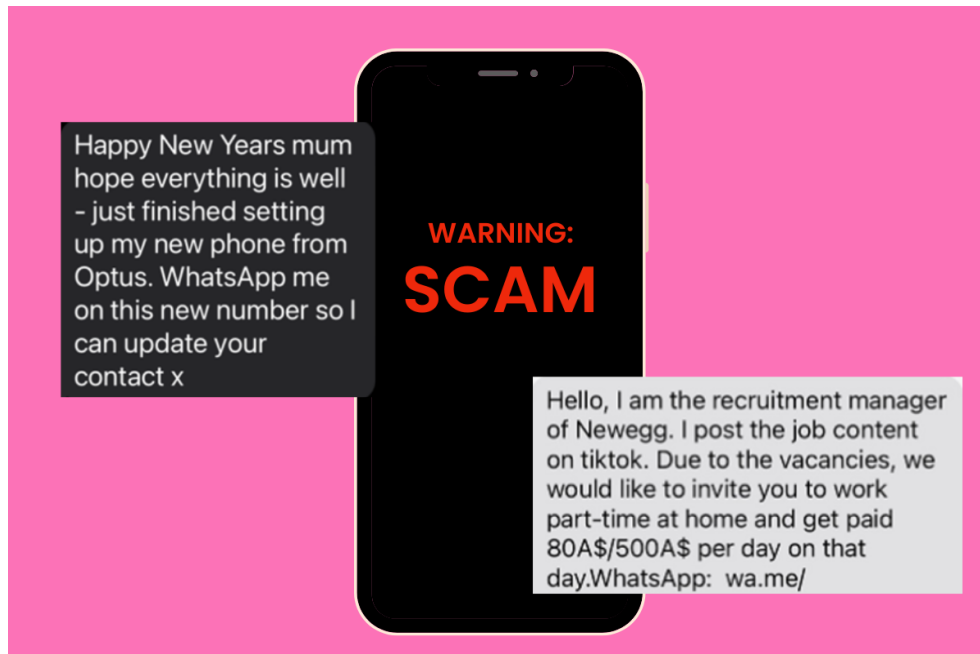


Send this to your parents and grandparents: The 4 things you need to know to avoid getting scammed.



"Please note that your toll invoice is past due."

That was the text message I received from a number last month telling me I'd need to visit a link or "my travel would be restricted".

"Great," I thought as I added it to the end-of-year to-do list in my head, under last-minute Christmas shopping.

It was only until I sat down the next day to deal with it, that I realised the message was quite obviously a scam.

If the questionable link wasn't enough, the fact that there was no information on who sent the message set alarm bells ringing.

Please note that your toll invoice is past due and you will need to visit: [REDACTED] to pay. Otherwise, your travel will be restricted.

Unfortunately, it's just one of thousands of messages that are cropping up on Aussie phones every month.

In fact, the Australian Competition and Consumer Commission's Scamwatch received over 200,000 reports of scams last year, costing Aussies over \$560 million.

And according to Katherine Mansted, Director of Cyber Intelligence at CyberCX, more of us are likely to fall victim.

"The reality is scammers have become more sophisticated," she told *Mamamia*.

"Back in the day, scammers didn't often bother to use proper English and proper grammar. They didn't have the same tools they do now, unfortunately."

"[Now], they might spoof your bank's numbers so it looks like a text is coming from your bank... We also see scammers investing in some pretty sophisticated business operations. So it might not just be an email or a text, sometimes it's an email or a text that prompts you to call a call centre. And you might even talk to a real person who is asking you to take a particular action that's actually a scam. So they're getting better."

As new scams continue to crop up, here are the four things that can help you avoid being scammed.

1. Tell your bank you'll call them back.

According to Mansted, one way to beat scammers at their own game is to take away their ability to fake trust.

If you receive a call from your bank or another institution, she recommends pausing before you provide any information and telling the person on the other line that you will call them back. Then you can validate the number is real by searching up your bank's number on their website.

"Sometimes my bank or the ATO [Australian Taxation Office] has called me and I break that form of communication and I start it again through a channel I trust, and we get on with our conversation."

"If it's a scammer, then by doing that you've saved yourself... It also just gives you that bit of a slowdown, so you can have a think before you take any action."

2. Don't give into the fear.

One reason why scams are so effective is because they exploit our fear.

"Whether it's the 'Hi Mum' scams that are pretending that someone's child is being held hostage and being threatened with violence... [or] whether it's a recruitment scam saying, 'if you don't click this link, you'll miss an opportunity,' we need to be able to step back and break that fear of missing out or fear of harm and take the steps to validate what we're seeing," said Mansted.

Again, she recommends either establishing a trusted channel of communication or simply asking a friend or family member if the suspicious message checks out.

"[Scammers] are confidence tricksters. If we know how they work, how they operate, we can actually outsmart them."

3. Look out for the red flags.

Scammers are continuously evolving and switching up their tactics to try to trick us into providing our personal details.

However, according to Tessa Bowles, NAB Manager, Security Advisory Awareness, a common red flag to look out for is that scammers try to "create a sense of urgency" when they're talking to you over the phone or text.

"They may say things like 'you need to confirm your details', or 'your access to your accounts will be restricted', or 'you need to update or verify your details to continue banking'," Bowles told *Mamamia*.

"A bank will never pressure you to do that. If you are uncertain about the legitimacy of a call, we encourage you to hang up and call the bank back on the publicly listed number on their website."

4. Watch out for popular scams going around.

Investment, romance, and spoofing or impersonation scams, including the 'Hi Mum' scams, are the most common types of scams doing the rounds right now, according to NAB.

Their figures show that reported scams increased by 38 per cent year-on-year in 2022.

"Every day, we're seeing scammers directly targeting people through texts, emails, phone calls, computer messages and other sneaky tactics," said Bowles.

Recruitment scams.

If you're on the hunt for a new job this year, keep an eye out for recruitment scams that ask for a payment in exchange for a guaranteed income.

According to Scamwatch, Aussies lost over \$8.7 million to these scams last year, with scammers targeting young people in particular.

"One thing we're seeing a lot of and we saw a lot of 2022 coming out of a pandemic, as people are looking for a job change or a way to get rich quick, was recruitment scams," Mansted told *Mamamia*

That might be scammers posing as recruitment agencies, pretending to be headhunting... [or] a fake ad on social media offering paid product reviews."

"The easy way to avoid those is to again, stop and think before you take action. In particular, don't pay money to an organisation, or give them an upfront investment. And if someone's contacting you via an encrypted chat app like WhatsApp, it's a good chance that they're probably not a recruiter."



Bank scams.

Bank scams have also been on the rise recently.

Scammers will use software to spoof a bank's number and make the number they are calling or texting from appear as if it's coming from your bank, when it's not.

"Criminals can send messages with the sender's name set to 'NAB', or other organisations, which means their messages can appear in the same thread as other official texts sent from NAB," said Bowles.

"When a customer receives a text message or call impersonating NAB, it means a criminal has 'spoofed' our number and is impersonating us. NAB's systems have not been breached in any way."

'Hi Mum' scams.

'Hi Mum' scams have been going around for a while now, and will often see scammers pretending to be a child messaging from a new number and asking their parent for money.

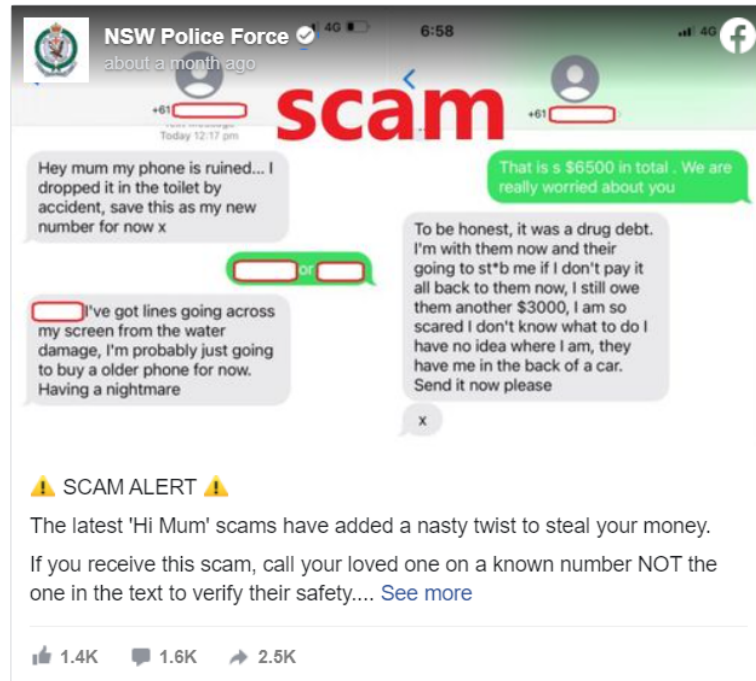
According to Scamwatch, at least \$7.2 million was stolen from 11,100 Aussies last year thanks to 'Hi Mum' scams, with two-thirds of these family impersonation scams targeting women over 55 years of age.



And just like other scams, they have continued to evolve.

In December, NSW police noted the 'Hi Mum' scams have taken a 'nasty twist', with messages now referring to drug debt and kidnapping.

New scam messages include sentences like, "It was drug debt, I'm with them now. They're going to stab me if I don't pay it all back to them" or "I am so scared, I don't know what to do, I have no idea where I am. They have me in the back of a car."



ATO scams.

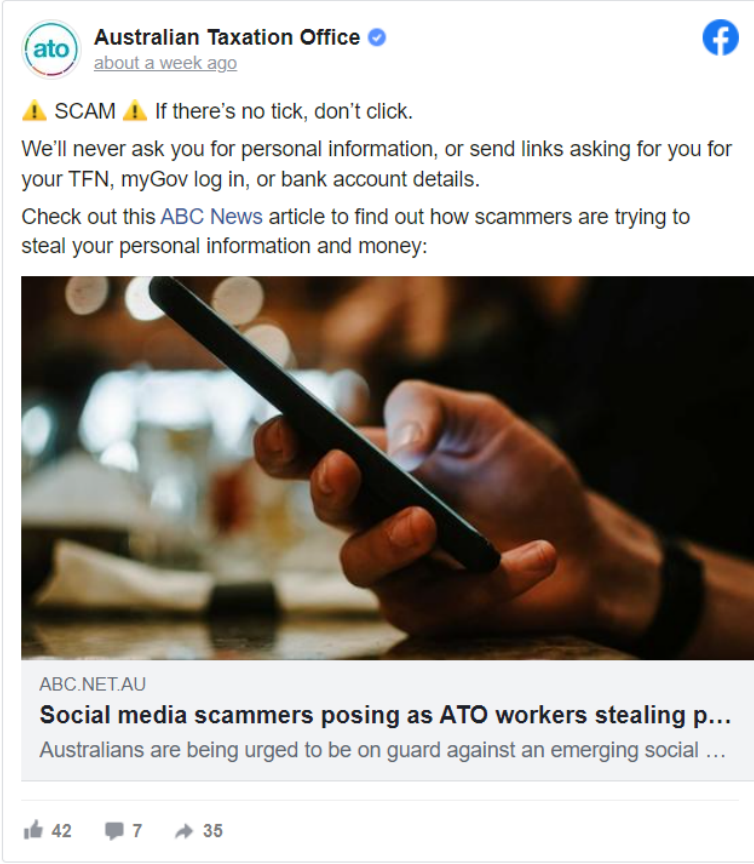
The most recent scam Aussies are being told to watch out for are those impersonating the Australian Taxation Office.

This week, the federal government warned scammers are impersonating tax office workers on Twitter, Facebook and other social media platforms, duping people out of money and personal information.

"They begin by scanning public conversations on social media where taxpayers ask questions or make complaints about the ATO," Assistant Treasurer Stephen Jones said in a statement.

"They then hijack the conversation using a fake ATO profile, contacting the member of the public directly with an offer to help resolve a complaint or follow up on a comment. After earning their trust, the scammer asks them to click on a link or provide personal details."

The ATO is currently working with social media platforms and other government agencies to help remove the accounts.



The image shows a Facebook post from the Australian Taxation Office (ATO). The post includes the ATO logo, the name 'Australian Taxation Office', and a timestamp 'about a week ago'. The main text of the post is a warning: '⚠️ SCAM ⚠️ If there's no tick, don't click. We'll never ask you for personal information, or send links asking for you for your TFN, myGov log in, or bank account details. Check out this ABC News article to find out how scammers are trying to steal your personal information and money:'. Below the text is a photograph of a person's hand holding a smartphone. Underneath the photo is a link preview for an ABC News article titled 'Social media scammers posing as ATO workers stealing p...' with a truncated description: 'Australians are being urged to be on guard against an emerging social ...'. At the bottom of the post, there are engagement metrics: 42 likes, 7 comments, and 35 shares.

ato Australian Taxation Office about a week ago

⚠️ SCAM ⚠️ If there's no tick, don't click.
We'll never ask you for personal information, or send links asking for you for your TFN, myGov log in, or bank account details.
Check out this [ABC News](#) article to find out how scammers are trying to steal your personal information and money:

ABC.NET.AU
Social media scammers posing as ATO workers stealing p...
Australians are being urged to be on guard against an emerging social ...

👍 42 💬 7 ➦ 35

Online shopping scams.

If you're a fan of online shopping, keep an eye out for fake websites.

Scammers can use the latest technology to set up fake retail websites that look scarily similar to legitimate businesses, right down to the design and logo.

Earlier this year, fashion chain Dotti shared a message to its customers, urging them not to purchase from a fake site replicating the real one.

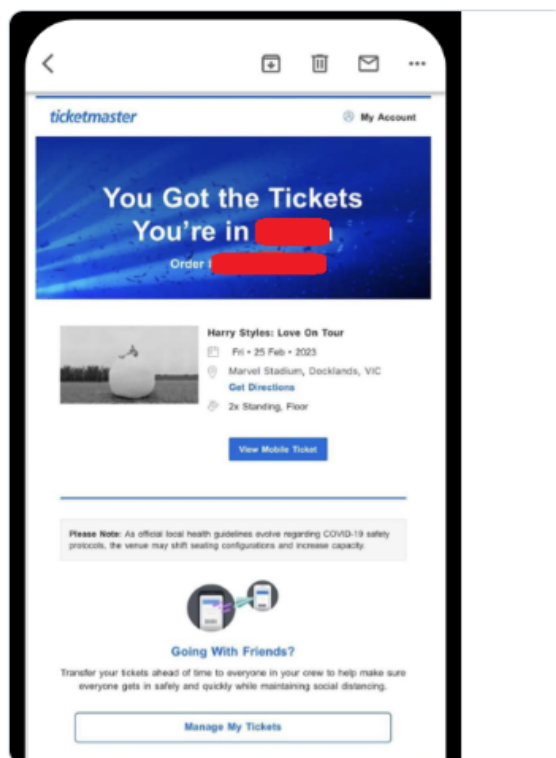
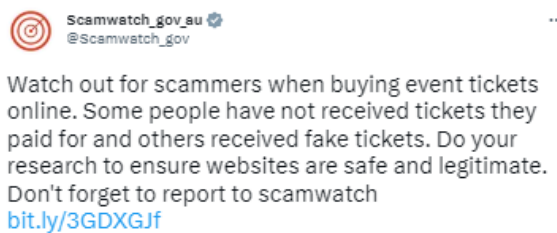
"We have been made aware that there are websites illegally using the Dotti name and logo in an attempt to scam customers and obtain personal information," a message sent to members of their 'Dotti Squad' and published on their website reads.

"Along with our retail stores, the only authorised websites that sell genuine Dotti products are dotti.com.au and dotti.co.nz. We strongly advise not to purchase from any other website due to the risk of fraud."

Concert ticket scams.

If you're looking forward to any concerts this year, make sure you only buy tickets from legitimate websites.

"Some people have not received tickets they paid for and others received fake tickets," Scamwatch warned in a recent Twitter post.



Feature Image: [Twitter@Scamwatch_gov/Mamamia](https://twitter.com/Scamwatch_gov/Mamamia).