OLDER AUSTRALIANS' EXPERIENCES OF ONLINE SCAMS

2026

National Seniors AUSTRALIA

Contents

Executive summary 3
Prevalence of scams 5
Groups more affected by scams 6
Common scam types 7
Banks' actions to help victims recoup lost money 16
Take home message #1: Scammers are clever 17
Take home message #2: You can take actions that minimise risks 18
Methods and sample 19

Executive summary

National Seniors Australia, or NSA, is a member based, not-for-profit research and advocacy organisation representing Australians aged 50 and over.

Every year we survey thousands of older people on diverse topics relevant to lifestyle and wellbeing.

This report is based on two questions about online scams presented to around 4800 older Australians in a 2025 survey.

Online scams have become a commonplace part of our lives in the digital age.

The Australian government estimated Australians lost in excess of $318 billion to scammers in 2024 – and that only includes scams reported to the National Anti-Scam Centre.

Half that amount, over $159 billion, was taken from people aged 55 or over.

In this context, National Seniors Australia (NSA) has committed to an ongoing advocacy campaign against scams.

This document reports the results of a March 2025 survey which asked over 4800 older Australians about their experiences with online scams.

Two questions about scams were included in the March 2025 iteration of the National Seniors Social Survey (NSSS).

All respondents were asked: 'Have you ever been the victim of online fraud or a scam where you lost money or had your identity used fraudulently?'

Answer options were 'yes', 'no', or 'unsure', and 4766 people answered the question.

Just over 30% of respondents said they had been scammed and another 4% were unsure.

Greater proportions of people feeling financially tight rather than comfortable had been victims of scams, as had people with less funds in savings and investments, people in poorer health, and people with a religion that is important to them.

Perhaps surprisingly given the statistics, age was not a significant factor in the likelihood of being scammed, at least for this survey sample.

The respondents who said they had been scammed were then given a text box inviting them to write more about their scam experience if they wanted to, and three-quarters of them did so.

From their comments we were able to identify eight main types of scams and a few minor types.

Most commonly, almost half the commenters had simply had their credit card charged or funds removed from their account without engaging in any particularly risky activities themselves beyond ordinary electronic transactions such as using an ATM or buying something on card.

Other common scam types included:

- buying non-existent or poor-quality items from dodgy online sellers
- paying a fake invoice or responding to a cold call from a scammer pretending to be one's internet provider, electricity company, or another legitimate authority
- reacting to a fake computer warning by calling a fake helpline
- investing in a dodgy deal
- having a scammer hack one's email or social media profile for their own benefit
- having one's Centrelink, ATO or MyGov profile had been hacked and funds misdirected
- being duped into giving money to the scammer when they pretended to be a beloved family member or friend.

There are of course many types of scams, not just the experiences reported here. For comprehensive information and official advice go to scamwatch.gov.au.

Perhaps the most surprising and encouraging result from the survey was the extent to which scam victims had been assisted by their banks to recoup lost funds.

Around one third of commenters mentioned the response of their bank or other relevant authority when the scam occurred (other authorities including PayPal or the police).

In 70% of those cases, the victims recouped all the scammed money. Another 19% recouped some money or the authority acted positively to prevent further losses. Only 10% said their bank or other authority did not or could not help them.

Banks get a bad rap for the money Australians have lost to scammers, and NSA supports measures for banks to take more responsibility for scam prevention. But these results suggest that, contrary to public opinion, banks have by and large already done a lot of good in this space to support many of their customers.

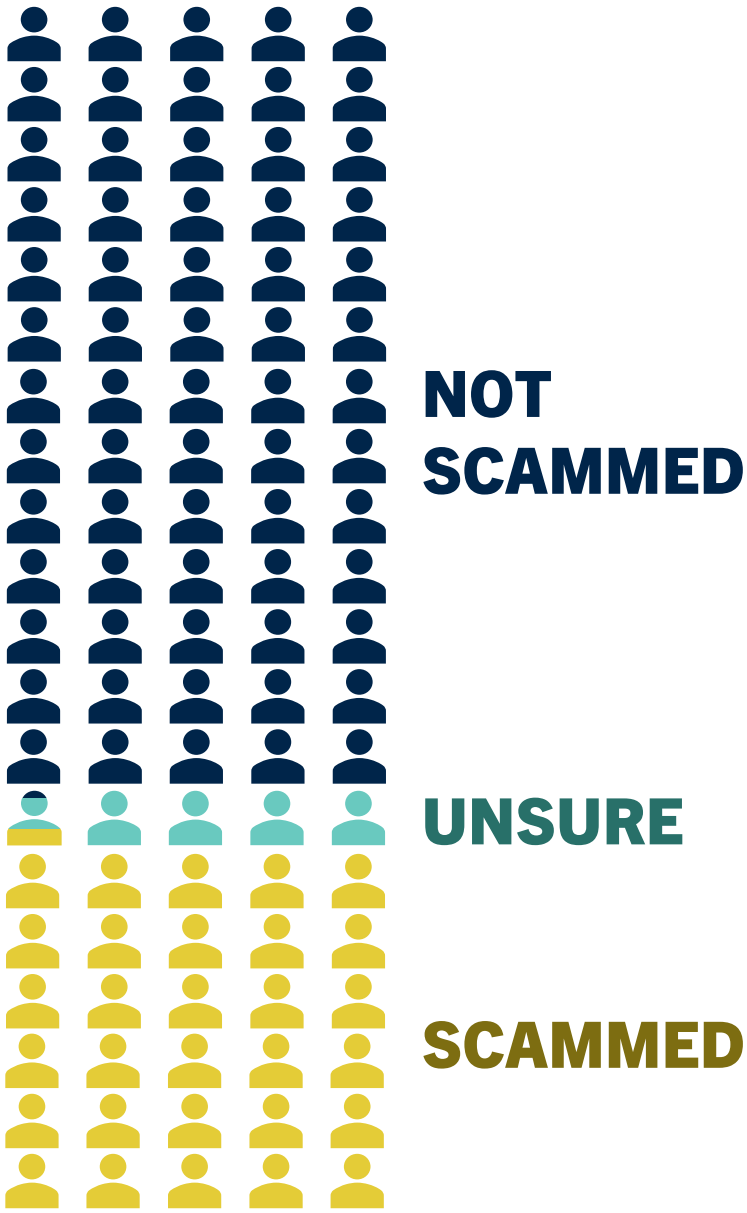
Prevalence of scams

One third of older Australians surveyed said they had been the victim of an online scam or were unsure if they had been.

Among the 4766 people who answered the question, 1447 (30.4%) indicated that they had been the victim of an online fraud or scam where they lost money or had their identity used fraudulently (yellow in the graphic).

A further 208 (4.4%) indicated they were unsure (teal in the graphic).

Among those who said they had been scammed, around 1080 wrote an informative comment about it.



Groups more affected by scams

Wealth, health, and religious beliefs were relevant to these older people being scammed. But age was not.

Statistical analyses of people who had been scammed showed that some socio-demographic factors were significant.

Wealth matters. A much higher proportion of people with less than $200k in savings and investments had been scammed (39%) compared to those with more (27-29%).

More strikingly, a greater proportion of people feeling the financial pinch had been scammed – whatever their actual wealth. Almost half of those feeling financially 'very tight' (47%) had been scammed compared to those feeling tight (38%), comfortable (29%), or very comfortable (24%).

Health also matters, with 43% of people in poor or very poor health being scammed. This compares to 37% in fair health and 29% of people who rated their health good or excellent.

In addition, larger proportion of people with religious beliefs that are important to them, and people from outside metro areas, had been scammed.

Notably, age was not significant for this group of survey respondents.

Common scam #1: Funds taken without authorisation

The most common scam type, reported by almost half the commenters, did not involve the victims taking any risky actions beyond ordinary electronic transactions.

Around 450 commenters reported a straightforward scam in which their credit card or bank account funds had been used without authorisation.

A few of these respondents speculated about a legitimate online purchase, ATM withdrawal, personal device hack, or mass data breach that likely led to their bank or card details becoming known.

However, most did not know (or did not mention) how the scammers obtained their card or account details.

A similar scam type, reported by around 13 commenters, involved scammers hacking into a non-bank payment account belonging to the victim, such as their PayPal, eBay, Amazon, iTunes, or frequent flyer account, and stealing from it.

> Some one gained access to my ANZ bank account over 10 years ago, changed the password and withdrew approx $70k and transferred it to a Betfair account and from there disappeared.

> My credit card was scammed after I bought articles online. 3 times.

> PayPal was hacked and over $2000 was fraudulently used for Booking.com.

> Credit card skimmed in an ATM while overseas

> Someone hacked my amazon account and items I did not order (sex toys) were charged to me.

> Lost $100 a decade ago via an unauthorised bank transfer. Had to close my bank account and open a new account as bank couldn't track overseas offender back to origin.

> I had over $500 taken from my CBA Travel Card. I hadn't given my card to anyone or shared the pin with anyone. I just used it for online purchases.

> My Visa debit card was used at Luna Park in Melbourne while I was living in Sydney.

Common scam #2: Sold non-existent, overpriced or dodgy item

In another common scam reported by around 175 commenters, the victims thought they were just buying something online, but it never arrived or wasn't as advertised, or they were charged too much.

Such transactions often took place on Facebook Marketplace or Gumtree, or via fake websites that had posed as known retailers.

Buying a non-existent item was reported most often, by around 120 respondents.

Approximately 20 respondents reported receiving an item that was poorer quality or different than that which had been described when they bought it, and the seller refused a refund or made it difficult to seek one or disappeared.

Around 20 people reported being charged multiple times for a purchase, being overcharged for something, or being signed up for a subscription rather than paying for an item once.

Around 15 were scammed by clicking links on dodgy websites that looked like the real sites. For some this occurred right after a legitimate transaction, so just seemed like a continuation.

Purchased goods online but never received them. Website was a scam.

Purchasing a visa for travel to USA. Paid a third party by accident and paid more than I needed to.

Did an online purchase and received a token cheap gift instead of what we ordered.

I purchased a mobile phone online and never saw which way they went.

Purchased dresses (two) online that arrived in a style not as pictured, unlabelled; and for return a stated requirement was that they be labelled. Overseas postage to be paid for return. All not part of pictured descriptor.

Purchased items from a non existent company

Purchasing a swimming pool for [exercise] and scammed just over $7000 deposit. It never turned up on delivery day and phone emails unanswered. Spent $3000 on a concrete slab in preparation

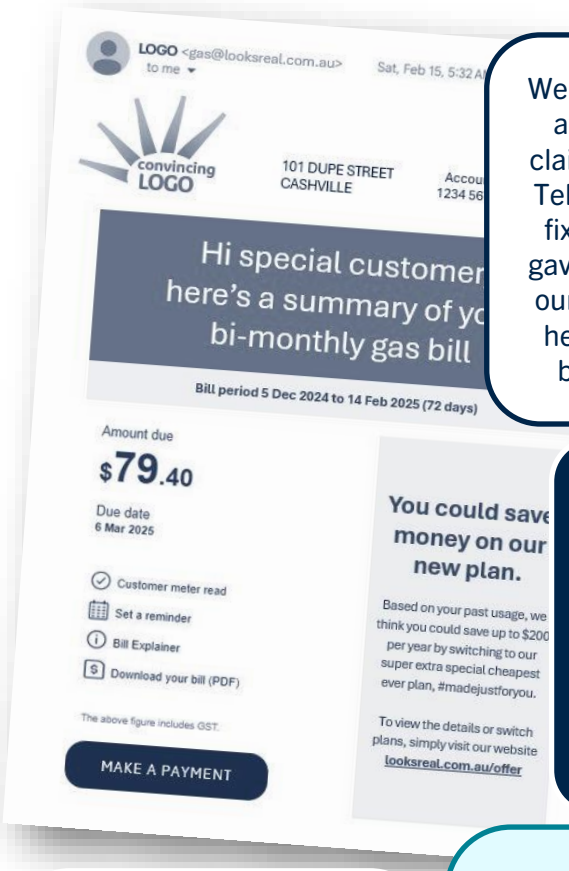
Common scam #3: Scammer pretended to be known business

Approximately 90 commenters paid a scammer or granted them access to their finances when the scammer pretended to be a government authority or known business.

Most of these scams were initiated by phone call or SMS. Often the scammer contacted the victim posing as their telco or internet service provider, offering technical help. Sometimes they pretended to be a bank calling to inform of a problem, their energy provider offering a deal, or Australia Post needing delivery payment. Two people reported scammers posing as law enforcement.

The victims often commented on how friendly the scammers were and how much they already knew about the victims. With these skills and knowledge, they were very persuasive in getting victims to open up their bank account.

About a third of the time, these scammers instead emailed a convincing fake bill from a service provider or a fake toll notice. Victims often simply paid these without realising or clicked a dodgy link. In some cases, an expected invoice from a tradie or other business was intercepted by scammers and the bank details changed, so the victim unwittingly paid the scammer instead.



We lost $55,000 to a fraudster. He claimed to be from Telstra and was to fix our internet. I gave him access to our computer and he cleaned out a bank account.

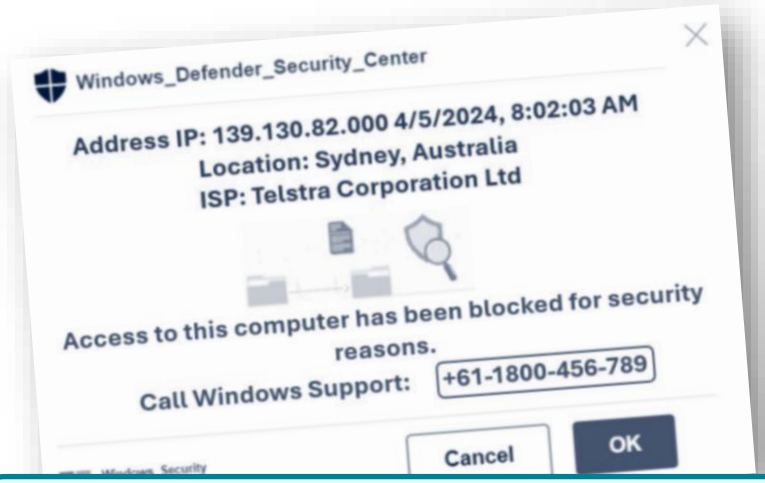
email intercept where they changed the bank info and we lost $30,000 in a business transaction.

A person posing as a policeman on a Saturday morning, letting me know that my bank accounts have been accessed. And Suggesting I phone the number on the back of my credit card to get assistance. This particular number I phoned had been intercepted as well so I thought I was following instructions from the bank but it was the scammer instructing me as to what to do, allowing him access to my bank account (which I did).

I was told that someone had used my PayPal account. I blame myself, I should have contacted PayPal. The conversation was hypnotic and I seemed to act automatically. I gave access to ID details and lost $2,000.

On a second email from a tradie sent a couple of minutes after the first, the attached invoice had been changed so that the bank account details were the scam. I paid $1,800

Common scam #4: Security warning popped up on screen



Around 45 people were scammed by a fake security warning popping up on their computer screen, sometimes with a voice speaking to them or a siren blaring.

This scam has affected computer screens in many countries around the world but adapted to deceive local people.

While browsing the internet, downloading software, or using social media, a warning message randomly pops up for users, telling them to call a help number disguised as Microsoft or a similarly legitimate company – but which is actually a hotline to the scammers. Sometimes the warning tells the user not to turn off their computer (though that's exactly what you should do to stop it – pull the plug at the switch).

In some versions of the scam the victim is asked to pay an amount to "fix the problem" or "remove the virus", and the scammer then "unlocks" the computer screen (though nothing is really broken).

In other versions, the scammer prompts the victim to go through a series of steps – clicking links or pushing buttons or even logging into their bank account – that ultimately feeds their money to the scammer.

There was a problem downloading an internet security program. I found an Australian number to call. They took over the computer and suddenly had red lines scrolling down at speed. They said it was a virus and it would cost me $500 to fix. At the time I was tired, irritated that the new program refused to be applied correctly, having a melt-down at what it would cost to fix. So I panicked and paid. That was 20+ years ago and a hard lesson, but I've never fallen for anything since.

I was working on my computer when something appeared on the screen saying that my computer had been infected by a virus and to ring Microsoft on the given number which I did. Later I realised that I was speaking to the hacker who got me to transfer money to an account in Vietnam to supposedly catch the hacker. Fortunately I only lost 6-7 thousand dollars and not my life savings, but as my only income is my War widows pension it still was a great loss.

Opened site, computer flashed a lot in a LOUD voice saying DO NOT SHUT DOWN FOLLOW INSTRUCTIONS, (automatically I don't know why, I went into auto mode) had to ring a number then transferred me, got into two bank account, had to follow instructions, hackers were 'tracking' me while driving to two banks to withdraw money & back to my home, Process took aprox 5 hrs. Following day went online noticed both accounts emptied, contacted Police, went into both different branches of different Banks, reported. Told nothing could be done, 'as I had the choice to follow their instructions' :(

Common scam #5: Investment too good to be true

Investments that proved fraudulent scammed just under 45 of the people surveyed, with more than a third of them related to cryptocurrency.

In these scams, older people invested in what looked like a good thing but never saw their money again.

In some cases, they could see their investment paying off, but they were ultimately prevented from withdrawing funds.

In many cases the whole operation simply up and disappeared. Others simply persisted with shonky practices.

Some commenters were taken in by phony celebrity endorsements.

Others were seduced by offers to help them learn investment skills – but they kept pumping money in with no return.

Around half these scams were related to cryptocurrencies including bitcoin.

Scam impersonating Australian Celebrity for Bitcoin investment

Crypto Scam, 12k loss, one in Court - but company went broke, so it seems.

Invested in companies that did a rug pull

Invested with Bitpairs $7500 account manager died COVID money went into Blockchain can't get it out believe still trading in my name

A 'boiler room' scam in 2017 - I bought 'shares' in a couple of companies that were not listed on the Australian Stock Exchange. They turned out to be worthless, although I have had subsequent contact from different companies offering to sell the 'shares' for me, so long as I paid various fees, of course

Online brokerage (highly reputable) used foreign company to acquire US shares and that company failed to handle a share split properly, costing us $40,000.

I was frauded by scammers selling digital investments - they pretended it was an investment but kept wanting more money to cash in my investment. I lost $25,000 before I realised it was a scam.

Common scam #6: Identity stolen to scam others

Around 40 people had scammers steal identity documents or take over their online presence, often to scam their contacts or draw credit in their name.

The victims of these scams were often unsure how the scammers obtained access to their identity, though some knew it was via a corporate data breach or even a hard copy identity document stolen from their home.

Some had their email address hacked, and the scammer emailed their contacts requesting payments, often in the form of untraceable gift cards.

Others had their social media profile taken over and the scammer used it for advertising or other nefarious purposes.

Some scammers took out loans or subscriptions in the victim's name, scamming the banks and other companies as well as the victims who were eventually sent the bill.

My email was hacked, and my niece gave 1 thousand dollars following an apparent message from me.

All my contacts were emailed (supposedly by me) telling them I was ill and unable to leave the house, so could they send me Apple gift cards.

Someone in USA hacked my Facebook account. They created a second user that was unknown to me and proceeded to use Facebook advertising to advertise their products.

Someone subscribed to Xbox with my details.

My identity was stolen twice to obtain credit from Latitude Finance 5 years ago and NAB 3 years ago.

Facebook, person impersonating me and posting kiddy porn

Someone opened a Samsung wallet in my name and spent $4000.

ID theft resulting in fraudulent credit card use and debts/loans/credit cards being set up in my name

Person pretending to [be] me stole photos from my house and used them on social media

Common scam #7: MyGov or Centrelink account hacked

Approximately 30 people had their MyGov account hacked so the scammers could redirect pension funds to themselves or file a false tax return.

One of these types of scams often occurred without the victims knowing it. Scammers would harvest their details from a fake message or a data hack, log in to their MyGov account and log through to their ATO account, and use their tax file number and details to file a fake tax return with the funds of course directed to their own account, not the victim's.

In the other scam type, the scammers would change the victim's bank details within their MyGov and Centrelink accounts. The victims' subsequent pension payments or any other Centrelink funds would then be directed to the scammer's account, unless the victims or the government got wise to it in time.

myGov

Acted on a fake MyGov email. Gave enough personal details for scammer to attempt to get money from the Australian Taxation Office

Centrelink Age pension website not secure enough so scammer accessed their site & gained access to my age pension account fraudulently altering my payment.

Through MyGov I had my bank details taken and used to submit a tax return in my name. Bank account details changed and the person received just over 4,000 from the ATO in a tax return. Apparently over 3,000 people were scammed at the same time as I was.

Someone got into my MyGov account and diverted my pension to another account and raised a pension loan against my account. I was never asked if I had done or approved this, and I was basically left floundering to largely sort and fix it on my own. Distressing and very hard in light of serious health issues at the time.

Common scam #8: Scammer pretended to be family or friend

Over 25 people were scammed by a text message or online contact they thought was from someone they knew and trusted.

These scams are particularly insidious because they prey on the victims' care for the people in their life by impersonating them and asking them for money.

Many commenters thought the scam message was from their adult child and willingly gave them funds.

Others received an email from a friend's (hacked) account asking to help them out or join them in a new venture, which again the victims happily did.

A few victims mentioned they were distracted at the time of receiving the scam communication so acted without thinking it all through.

I got scammed by the Hey mum scam - I thought it was a text from my daughter and I got scammed out of my savings

On Facebook. Scammer pretending to be a friend of mine and requested that I send a gift card. Was about $300.

It was a 'hallo Mum' text purporting to be from our son, asking for $4000 which he would pay back soon. When we rang him later it hadn't been him.

The Apple Gift Card scam where I purchased three gift cards purportedly for my NSA Branch President

Scammer masqueraded as a friend urgently requiring money and caught me at a busy time when I was distracted. I should have known better.

They called pretending to be my daughter who had dropped her mobile in the toilet & had urgent bills to pay. I was distracted at the time (involved in a card game with 3 others) & sent some money but finally realised it was a scam & did not send an extra larger amount

Someone impersonating my friend telling me to be a part of a scheme that I had been selected for. It required me to send money to various bank accounts. It was soon after my husband had died and I stupidly wasn't thinking properly.

Other kinds of scams

More than 50 commenters highlighted other scam types they had experienced.

Romance scam

a male who stalked me knowing my mother was dying and i was due to inherit --i fell victim to him and lost everything-- WHEN I WAS THEN BROKE he went back to his ex wife who was in process of inheriting from her mother too--so this man chases women with inheritances

Scammed by buyer

Selling something, person paying with PayID but instead my money was taken.

Sale of an expensive watch online where I stupidly did not receive the payment agreed in advance before sending the watch

Device ported

My mobile phone was ported to a different provider. Two and a half weeks later [...] my gmail account (with a very strong password) was taken over, and I had no way to prove my identity online.

Exchange rate scam

Many years ago our credit card was compromised from someone in Canada who was withdrawing money then returning it to account as exchange rate changed.

You won! scam

Received a "raffle" ticket in the mail saying we had a won second prize of a large sum of money in Hong Kong, which we had to send money for the exchange rate to complete, and it has continued on from there, us paying a large sum of money for "deposits etc". We have now stopped sending money but to no success of receiving anything in return.

Home for rent scam

When i sold my home a lady arrived at my door to get my Keys. She had met a lady outside a bank and signed a lease for my home and paid money for a bond and $400 for rent. She was told to come to my home and I would give her the Keys and she and her children could move in straight away. The poor woman had been scammed. The Scammers used the photo of my home for sale on the internet and interior photos from someone else, also probably from the internet. Still feel sorry for the lady and advised her to go to the police and her Bank

Scammed by friend

Ripped off $200k by a friend

... or family

grandson accessed my account and stole my savings

Banks' actions to help scam victims recoup lost money

The majority of people who were scammed financially did get their money back, usually with assistance from their bank.

Among the commenters who had money taken by scammers, 388 wrote about the relevant authorities' response.

With just a handful of exceptions, the authority mentioned was the victim's bank. The exceptions included PayPal, Centrelink, the police, and some major corporations.

In 70.4% of the 388 cases, the victim had all their stolen money returned to them.

Some commenters said it was their bank that identified a suspect transaction and alerted them about it. Others identified a problem and told the bank or other authority about it, and the authority stopped or reversed the transaction or otherwise retrieved their funds.

In another 19.3% of cases, the bank or other authority was able to supply a partial refund to the victim or took other actions to stop the victim losing more, or else it was unclear if all funds were recovered.

In only 10.3% of cases did authorities not help the victims recoup their funds.

I was targeted at night (as seniors often are - just when you are tired) by a bogus Telstra scam - early next morning I contacted my bank – [bank name] - the female manager [name] was amazing and sorted it all out (& cleared me with online E-First Aid) promptly without judgement about my 'stupidity' Consequently I lost 'face' but no money etc. I wish there were more [manager name]!!

It was a bitcoin scam, but fortunately the bank were able to get our money back.

Fell pray to a phishing email but my bank was proactive in discovering the event and retrieving my funds

My bank notified me that someone in USA was using my credit card details at a casino.

someone hacked my credit card but the bank refunded my money. I reported it within days.

Nigerian romance scam 2015. They got given $ 20,000 of my superannuation. Police didn't have resources to help me then. Only 1 bank questioned my bank transfer of $14000 but I convinced them it was authentic. I was brain washed.

We didn't lose as much as some people but it was just as scary, they tried to change my banking details and the bank shut all our accounts down so they didn't get much.

We have had several significant fraudulent visa charges over the past 5 or so years, only one of which was not reversed.

My Visa debit card was used at Luna Park in Melbourne while I was living in Sydney. [Bank name] did not refund the amount

I had one of my bank accounts cleaned out when I was going through treatment for cancer and I wasn't thinking straight. The worse thing was the bank told me I was a silly old woman.

Take home message #1: Scammers are clever

Scams are diverse

The survey results described in this report demonstrate that there is no 'one size fits all' type of online scam.

Scammers are clever and constantly create new strategies for taking people's money.

But they also recycle old scams, simply updating them to fit in better with what's happening in the present day to be as convincing as possible.

We didn't ask survey respondents when they were scammed. But we do know that well known scams like the 'hey mum' texts (p. 14) or the virus warning pop-up (p. 10) have been circulating for years in different forms, and scammers still use them today.

It pays to always be vigilant. Don't assume that because a scam is old that it no longer applies. At the same time, don't assume scams will always take the forms you're aware of.

No shame in being scammed

It also pays to not blame yourself if you are scammed. It's not you being stupid – it's that scammers are clever.

The most common scam type in this report didn't involve the victims at all – their credit cards, bank accounts, or other accounts were simply hacked, and their money was taken. Often the victims didn't even know it had happened and don't know how the scammer sourced their account details.

This kind of scam can happen to anyone with a bank account.

The people who were scammed by dodgy sellers also did nothing wrong – they acted in good faith when wanting to buy an item and the seller ripped them off.

But even for other kinds of scams – where the victims responded to a fake invoice or warning, or invested in a dodgy deal, or got tricked by someone pretending to be their adult child or pretending to be in love with them – even in those cases where victims sometimes feel stupid afterwards, there is no reason to feel ashamed.

Successful scammers are very persuasive. Their scams are designed to tap into our better natures – the parts of us that want to help our loved ones, that want to see the best in people and trust them, that want to do the right thing and pay our bills diligently.

Scammers also take advantage of our desperation. Our analysis showed that almost twice the proportion of people who felt financially 'very tight' were scammed compared to people who felt financially 'very comfortable'. Scammers game us when we are financially vulnerable.

The comments showed that people often fell victim to scams when they were physically or emotionally vulnerable. Some were very sick, others were in mourning, and one person was scammed because they have dementia. Commenters mentioned being targeted at night when they were tired and not thinking straight.

Being scammed in these circumstances isn't on us, it's on the scammers. They are good at what they do, and they understand human nature.

The stigma of being scammed and feeling stupid can stop us from taking action or reaching out for help. So we need to remember it is not our fault, learn from the experience, and do something about it.

Take home message #2
You can take actions that minimise risks

Tell your bank

If there's one take home message from this report that rings loud and clear it is to report scams to your bank or other relevant authority as soon as they happen.

Doing so will give you the best chance of getting your money back, as many of the survey respondents did.

National Seniors supports policies that would force banks to reimburse scammed customers, to encourage them to invest in tech that prevents fraud transactions.

But we were surprised and delighted to see just how much banks have already done for older people who have been scammed.

Around 70% of commenters who mentioned a response by their bank or other authority received a full return of their stolen funds, and another 19% got back some of their funds or had other help from their bank to stop further losses.

It does no harm to ask and there's a good chance you'll get what you need.

Call out victim blaming

If your bank responds like one commenter's did and calls you "a silly old woman" or equivalent (p. 16), take these steps:

1. Remind them that there's no shame in being scammed and that scammers are clever and getting cleverer.
2. Tell them their remark is ageist (and possibly sexist, etc.). Remember that in this NSSS survey, age was not a statistically significant factor in who was scammed and who wasn't.
3. If it's warranted, don't be shy about reporting this kind of comment to the organisation. Blaming victims is unfair and feeds the stigma. Loading up comments with ageism or other offensive sentiments is completely unacceptable.

Familiarise yourself with Scamwatch tips

The government website Scamwatch outlines some basic steps we can all take to minimise the risk of being scammed. They have a three-part slogan to help us all remember:

- STOP. Don't give money or your information to anyone if unsure.
- CHECK. Ask yourself if the message or call is fake.
- PROTECT. Act quickly if something feels wrong.

There is more information about scams in Scamwatch's *Little Book of Scams*.

Report scams

Even if you can't get your money back or there have been other unalterable consequences for you, it is worthwhile to report all scams at Scamwatch's report-a-scam interface.

Your report can help others because it helps authorities take down scam websites or ads or act on other details.

It can also help warn the community of a new type of scam or of the prevalence of a known scam.

Methods

The information in this report comes from the iteration of the National Seniors Social Survey (NSSS) conducted in March 2025. Anyone aged 50 or older who resides in Australia is welcome to participate in the NSSS. The survey received ethics approval from Bellberry Ltd prior to implementation (approval 2023-11-1424-A-1).

The survey included a module entitled 'Engaging with digital technology', which included a question about scams and an invitation to comment, as described in this report. Comments were analysed for this report using the thematic analysis framework described by Braun and Clarke. We identified themes via inductive analysis guided by a critical realist approach that aimed for accuracy and objectivity in interpreting respondents' views. The number of comments comprising any given theme was estimated to give a sense of its prominence. The data were not cross-coded so numbers should be treated as estimates only.

Quotes from survey respondents were selected to illustrate some of the variety and prevalence of ideas expressed. Where possible they were reproduced verbatim, occasionally omitting or altering parts for clarity or anonymity (indicated with square brackets []). Minor typos were corrected for readability (no brackets). We retained all other phrasing idiosyncrasies.

When inviting people to participate, we strive for greater inclusivity and maximising participation, rather than numerical representativeness. This is especially relevant to open-ended questions because people's unique experiences are the focus, not statistical patterns, and some groups are more likely than others to write a comment.

Sample

The percentages below characterise the demographic traits of the 4766 respondents who answered the scams question. Note that this number excludes 43 survey participants who selected 'prefer not to say' for the scam question.

No question was compulsory, and unsure responses are not shown, so some rows do not add up to 100%.

Age group	50-64 years 12%	65-74 years 49%	75-84 years 35%	85+ years 5% (oldest 100)
Self-rated health	Excellent 12%	Good 55%	Fair 25%	Poor/very poor 7%
Savings including super	<$200k 33%	$200k-$500k 16%	$500k-$750k 8%	>$750k 24%
State or territory	ACT 3% SA 10%	NSW 24% TAS 2%	NT 1% VIC 19%	QLD 32% WA 10%
Not metro	Regional 27%	Rural 11%		Remote 1%
Gender	Female 56%	Male 43%		Non-binary 4 people
Education	School up to Year 10 15%	Year 12 or cert/dip 42%		Degree or higher 42%
Diversity groups	First Nations 1% Living with disability 6%	CALD background 3% Veteran 5%		LGBTI 2%
Religious	Have a religion important to me 32%		Don't have a religion important to me 58%	

**Survey data unweighted.*

The head office of National Seniors Australia is located in Brisbane/Meanjin but we represent older people from across this great continent.

We acknowledge the traditional custodians of the land and waters in which we operate, the Turrbul People, and all other First Nations, Aboriginal, and Torres Strait Islander people.

We honour and value their continuing cultures, contributions, and connections to Country, and pay our respects to Elders, past and present.

We extend our warmest thanks to the thousands of older people who participated in the 2025 National Seniors Social Survey, who so generously gave their time, thoughts and personal information. Without them this report would not be possible.

© National Seniors Australia 2026

National Seniors Australia (National Seniors) owns copyright in this work. Apart from any use permitted under the Copyright Act 1968, the work may be reproduced in whole or in part for study or training purposes, subject to the inclusion of an acknowledgement of the source. Reproduction for commercial use or sale requires written permission from National Seniors. While all care has been taken in preparing this publication, National Seniors expressly disclaims any liability for any damage from the use of the material contained in this publication and will not be responsible for any loss, howsoever arising, from use or reliance on this material. ABN 89 050 523 003.

Any correspondence may be addressed to research@nationalseniors.com.au.

1300 76 50 50 **nationalseniors.com.au**

National Seniors AUSTRALIA