Scammers can disguise their number so it looks like your bank is calling — here are red flags to watch for

Unfortunately, the caller ID that comes up on your phone isn't always correct.

The ACCC's Scamwatch is warning people that scammers are using technology to trick victims by:

- making the call appear to come from the bank's legitimate phone number
- sending a text that appears in the same conversation thread as genuine bank messages.

It's called "**spoofing**" and it's a technique used in bank impersonation scams.

Last year, Scamwatch had 14,603 reports about bank impersonation scams, totalling more than $20 million in losses.

Scammers can also trick people with their dodgy ads for banks online.

When people type their bank's name into a search engine, they may click on the first link that comes up — and scammers can take advantage of that.

They might set up what looks like legitimate website for the bank, but it actually takes them to their dodgy impostor site instead.

What are the red flags to watch out for?

1. Pointing to the fact that they're calling you from an 'official' number to prove legitimacy (A would-be scammer tries to legitimise himself by telling the victim he's calling from the bank's number when he's not).
2. Building a sense of fear and urgency (A would-be scammer creates a sense of fear and urgency through the threat of a fraudulent transaction).
3. Using information collected elsewhere to prove their legitimacy (A would-be scammer states a victim's address in a bid to convince her the call is legitimate).
4. Asking the victim to repeat a code they claim was sent from their bank (A would-be scammer asks a victim to read out a 'cancellation code' while posing as a bank – the actual code is a password to complete an online purchase). NOTE: a bank will NEVER ask you to read out a security code, or send a code to cancel a payment

Another big red flag is a bank asking you transfer money to "keep it safe".

Never click on a link... your legitimate bank will never send you a message with a link to click

What should I do if I think I'm being spoofed?

- Hang up and call the bank back on its official, publicly-listed number.
- Dial that number yourself rather than just clicking a link you've search for online or tapping a link from a message claiming to be from your bank.

You don't have to answer all calls – the Communications Alliance recommends allowing unknown calls to go to voicemail. If they leave a message, you can listen to it to see if it's a genuine call.

https://www.abc.net.au/news/2023-03-31/banking-impersonation-scam-spoofing-disguise-phone-number/102159638?utm_campaign=abc_news_web&utm_content=link&utm_medium=content_shared&utm_source=abc_news_web

---

Recent Scams

NOTE: scammers can seem down to earth and genuine – always act with caution.

The 'Australia Post' scam

Scammer says: "I can pay through AusPost and arrange delivery right now," adding that an Australia Post courier would be in touch to arrange a time to pack and pick up the item.

Then, the scammer sends a link to "confirm order" and "receive your money".

DON'T click on the link as it will take you to what looks like a genuine Australia Post site.

Scammer will then ask for bank card details – not the bank account details, for payment.

Never give your credit/debit card details over the phone or by text message or email, and only provide it on-line when it is on a *genuine* secured site where you are purchasing an item/s from a *genuine* shop.

The overpayment scam

The scammer wanted to pay via PayPal and asked for the seller's email address – NEVER provide your email address – ALWAYS use the messaging system of the selling site (Gumtree, Marketplace) as it will hide your real email address to help prevent identity theft.

If you provide your email address, the scammer will send you a message asking if you received an email from PayPal. This will be a FAKE, and suggest that PayPal required them to pay more than the price of the item to expand the credit limit, so you will need to refund them the overpayment.

NEVER believe a text message or email on face value. If it looks like it is from your bank or PayPal, then directly login to that website using their genuine webpage and check your balance and messages. In the case above, you will see that no one had made a payment to your PayPal account, confirming it is a scam.

The 'missing payment' scam

The scammer will ask you to set up a PayPal account (if you don’t already have one).

Then the scammer will advise you that they deposited money into your PayPal account, "but it seems to have disappeared."

The scammer may also ask you to transfer money to their PayPal account for shipping, which they would refund you.

These are both red flags that you are being scammed.

How to spot a scam buyer

- The buyer is willing to purchase your item without having viewed it in person.
- The buyer makes a transaction that involves an overpayment and requests a refund.
- A buyer asks to pay via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency.

The PayID scam

Similar to the PayPal overpayment scam, the scammer may request that you use PayID to accept the payment. If you setup a PayID account, the scammer will claim that PayID sent them an email saying they had to transfer an additional $500 to your PayID account to upgrade it to a "business account", in order to overcome a payment limit and allow the transaction to go through.

That fake email, will also be sent to you, saying that you need to reimburse that extra money before any of the cash would actually be able to get into your account.

The E-toll scams

Scammers posing as a toll roads operator to trick people into handing over personal information.

It starts with a message claiming to be from road toll operators like Linkt. Sometimes, people are asked to pay an unpaid toll, other times people are asked to update their account details for their e-tag. Sometimes the texts come from unknown mobile numbers, but Linkt says it's been made aware of scammers using a spoofing technique that makes the message appear as if the sender is Linkt. The message usually contains a short URL link, which takes people to a website with very convincing-looking branding. From there, they're directed to log in or enter personal information.

What to do to protect yourself

Never click any links that seem suspicious. Linkt says people should check for common signs of phishing sites, such as spelling errors and poor grammar and to be wary of URLs that don't start with https://www.linkt.com.au.

Scamwatch says you should contact the company directly if you think you have an unpaid bill, making sure you use the contact details you've found yourself online, in the phone book or on a previous bill, not the ones supplied by a suspected scammer.

The 'Hi Mum' scam

Scammers pretend to be the victim's child and ask them to transfer money or disclose personal information.

The scammer sends a message to the victim starting with something along the lines of "hi mum". The scammer says their phone has been lost or damaged and often asks the victim to replace their child's number in their contact list with the number they're messaging from. If the victim asks which child they're talking to, the scammer is careful not to name names and usually says they're the oldest child. There's often a bit of back-and-forth before the scammer asks the victim to borrow money for a replacement phone and directs them to transfer money. However, it's not just money — Scamwatch says there's been reports of scammers asking for personal information such as photos for their social media profile, so watch out for that too.

What to do to protect yourself

Check to make sure the person you're messaging really is who they say they are. Scamwatch says you can do that by calling the original number you have for that person and try a secondary contact method — so, maybe, send them a message over social media or send an email. Scamwatch also recommends telling another relative about the message. And you can always ask a question only your person would know the answer to or make up a fake question to catch out a potential scammer — so you could ask something such as: "How's the dog going?", knowing they don't have a dog.

The Threatening 'official' calls scam

Scammers call you up and try to scare you into thinking you've going to be fined or arrested.

Victims receive a phone call from someone claiming to be from a government department or authority threatening with serious consequences — some are told they're being fined; they have an unpaid tax bill or that there's a warrant out for their arrest. Sometimes, the call will tell the victim to pay a fee or fine to resolve the matter or ask for personal information, such as passport details, date of birth or bank information. Here's the script from an example of a scam call that Scamwatch shared — notice how they use the current threat of identity theft to legitimise their fraudulent claims:

> Investigation division of Department of Home Affairs. The reason behind this call is that there is a legal case being filed under your name and your identity is being used for several illegal activities. There is an arrest warrant issued under your name as well. To talk to a federal officer from the Department of Home Affairs press one now.

What to do to protect yourself

Stop and question whether the caller's story is true. Don't let them pressure you. Never use contact details provided by the caller, instead dig out those details yourself by looking at the organisation's official website. If you're unsure about who the person is or whether you can trust them, don't send money, give credit card details or disclose personal information to them.

The 'Suspicious' transaction scam

Scammers call victims, warning about a dodgy purchase, to trick them into handing over personal information.

Victims answer their phone or receive a voice message from someone claiming to be from their bank advising them of a suspicious transaction. Some may claim there was an issue because of the Optus data breach, some tell victims a specific amount as been charged to their account — it could be something like an Amazon or a Netflix account. The victim will be asked to "confirm" personal information or banking details, such as their credit card numbers. Here's the script from an example of such a scam call that Scamwatch shared with us:

> "We have received a purchase request of $299.99 and the same will be debited from your account within an hour automatically. If you have not placed the order, then please press one to speak with a representative to cancel the order or call us back at [redacted number]. Thank you."

What to do to protect yourself

Check your account independently via the organisation's secure app, log in to its website using your normal login or call them using a phone number you've dug up on your own, such as by looking at the Contact Us page on the organisation's official website.

The Imposter bond investment opportunities scam

Scammers impersonate real financial companies or banks and claim to offer government/treasury bonds or fixed-term deposits.

Some victims are contacted by phone about offers of investment opportunities, while others search for investment opportunities online, find a fake but very convincing-looking, third-party comparison website and complete an enquiry form. From there, they're usually directed to transfer funds into a bank account or provide their credit details to make a deposit for their "investment".

What to do to protect yourself

Scamwatch recommends independently verifying the financial institution or bank issuing the bonds by calling them directly — and make sure you find that number on your own, rather than using any phone numbers or links provided by a suspected scammer. Check to see if the company is listed on government-run MoneySmart's "Companies you should not deal with" list. If you've been told you're dealing with someone from an institution, ask to speak to that person by name. Have an accredited financial or legal advisor check any potential investment opportunity. And, remember, bonds can be purchased via the ASX.

The Superannuation savings scam

Scammers have been cold-calling victims to set up self-managed super funds for them.

The scam used the names Invest Fast or Invest Quick and pretended to be a financial advice firm based in Melbourne. Scammers would cold-call victims and set up self-managed super funds (SMSF) for them so they could supposedly achieve high investment returns.

The scammers would then steal their victims' superannuation, either by getting them to agree to rollover their funds or forging the rollover documentation.

What to do if you've been scammed

The ACCC suggests taking the following steps if you've been scammed.

1. Contact your bank or financial institution as soon as possible (and cancel your card if you used it or provided your card's details).
2. Contact the platform on which you were scammed and inform them of the scam (e.g., block the scammer on Facebook and report them on Facebook Marketplace. Gumtree and Australia Post publish scam alerts and information on their respective websites, and you can contact them to report a scammer.
3. The ACCC encourages you to make a report on the Scamwatch website.
4. Finally, tell your friends and family – it helps to share your experience they can offer support and you can help protect them from scams.

https://www.abc.net.au/news/2023-01-04/selling-something-online-beware-the-scam-buyer/101824012?utm_campaign=abc_news_web&utm_content=link&utm_medium=content_shared&utm_source=abc_news_web

https://www.abc.net.au/news/2022-10-18/what-are-some-of-the-common-scams-going-around-the-moment-/101518706?utm_campaign=abc_news_web&utm_content=link&utm_medium=content_shared&utm_source=abc_news_web

https://www.abc.net.au/news/2022-10-19/scam-targeting-australians-superannuation-uncovered/101546098?utm_campaign=abc_news_web&utm_content=link&utm_medium=content_shared&utm_source=abc_news_web

AI scams on the rise

AI can replicate anyone's voice

The Guardian's investigation suggested the "voiceprint" security systems used by Centrelink and the Australian Tax Office (ATO) — which have used the phrase "In Australia, my voice identifies me" — could be fooled.

Last month the US Federal Trade Commission warned consumers about fake family emergency calls using AI-generated voice clones. The FBI has also issued warnings about virtual kidnapping scams.

These concerns have led experts to suggest a few basic tactics people can use to protect themselves from voice cloning:

- **Call friends or family directly** to verify their identity, **or come up with a safe word** to say over the phone to confirm a real emergency
- **Be wary of unexpected phone calls**, even from people you know, as caller ID numbers can be faked
- **Be careful if you are asked to share personal identifying information** such as your address, birth date or middle name

Scammers are using AI in phishing scams, which typically involve an email or text message that purports to be from a legitimate source but ends up using social engineering to obtain personal information. Some messages might also send you to a dangerous website using a link.

Cyber security company Darktrace said it had seen **a 135 per cent increase in sophisticated and novel social engineering attacks in the first months of 2023**, which it said corresponded with the widespread adoption of ChatGPT.

AI is also being **used to post fake product reviews online.**

Scammers can use AI to create malicious computer code and crack passwords… leading experts urge people to **strengthen their passwords and use two-factor authentication where possible**.

https://www.abc.net.au/news/2023-04-12/artificial-intelligence-ai-scams-voice-cloning-phishing-chatgpt/102064086?utm_campaign=abc_news_web&utm_content=link&utm_medium=content_shared&utm_source=abc_news_web