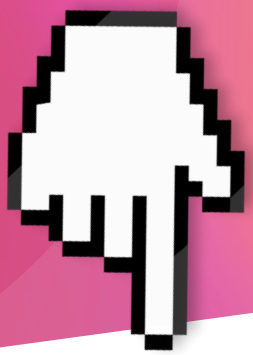
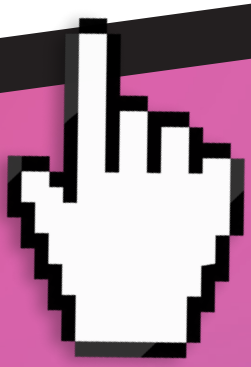
tinder®



Romance Scam Awareness Guide

How to protect yourself online



with Tracy Hall and
Professor Monica Whitty

Contents

Introduction and AU Scam Numbers

Dating apps have made finding a connection with someone easier than ever. Yet, as is the nature of the internet, it's also created an opportunity for criminals. Romance scammers prey on individuals who are hopeful, looking for genuine connection and love, and can be hard to spot. These types of scams are some of the most personally and psychologically devastating for victims as they are betrayed on multiple levels - trust, love, intimacy and financially.

Sometimes a criminal will adopt a fake persona (catfishing), but others may even use their real identity to impose the illusion of a romantic or close relationship to manipulate and steal. You can protect yourself by familiarising yourself with the psychological tactics and 🚩red flags🚩 we're sharing in this syllabus/module.

Some of these criminals belong to, or work for, large scale, sophisticated, scammer businesses with access to technology, resources and playbooks - so it's more important than ever to be aware and to be vigilant.

Australians reported losing **$201.1 million** in romance scams in 2023, according to the ACCC's Targeting Scams Report - that's a staggering **$23,000 per hour.** IDCARE has also reported helping Australians recover from losses in excess of $585 million in 2024.

We have partnered with Tracy Hall, a victim survivor of intimate fraud, along with Professor Monica Whitty from Monash University, to create this comprehensive romance scam factsheet. Designed to empower users, it provides valuable insights and actionable tips to help navigate online dating and recognise potential risks.

Psychology of Scamming

by Professor Monica Whitty, Head of Department for Software Systems and Cyber Security at Monash University.

Romance scams are a manipulative form of online fraud where perpetrators create fake profiles to lure victims into emotional and financial exploitation. These criminals, often part of organised networks, develop what I term a “hyper-intimate” relationship, moving victims off dating platforms to avoid detection.

Using advanced tactics like artificial intelligence and deepfake technology, scammers appear genuine in video calls and sound convincing in phone conversations.

Although middle-aged women are often targeted, victims span all genders and sexual orientations. Contrary to stereotypes, they are not desperate or overly lonely but are typically well-educated and trusting individuals. My research shows that victims may hold romantic beliefs that cloud their judgment and can see them act impulsively. Scam profiles are increasingly challenging to detect, even by sophisticated automated tools. Those who successfully identify scams often take their time verifying profiles, performing background checks, and approaching relationships with some scepticism.

My stage model outlines the progression of romance scams. First, scammers create attractive profiles to draw in victims, often using minimal but relatable details. They then “groom” the victim, fostering trust and forming an intense emotional bond. Once trust is established, scammers test the waters with small financial requests, such as gifts, before escalating to urgent demands like medical expenses or business crises.

This manipulation continues until the victim either realises the scam or the criminal is apprehended. Scammers sometimes return to victims, claiming to have fallen in love, only to continue exploiting them.

The psychological toll is immense. Victims face financial loss, emotional trauma, and shame, often becoming socially isolated as scammers discourage them from seeking advice from friends or family. Some victims are even unknowingly drawn into criminal activities, such as money laundering or drug trafficking.

Although awareness of these scams is important, it is insufficient as scams become more sophisticated. My main advice is to avoid any online relationships where excuses to meet face-to-face persist. From the outset, consulting trusted friends or family can help identify red flags and safeguard against exploitation.

References

Whitty, M. T. (2023). Drug mule for love. Journal of Financial Crime, 30(3), 795-812. https://www.emerald.com/insight/content/doi/10.1108/jfc-11-2019-0149/full/html

Whitty, M. T. (2019). Who can spot an online romance scam? Journal of Financial Crime, 26(2), 623-633. https://www.emerald.com/insight/content/doi/10.1108/jfc-06-2018-0053/full/html

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. Cyberpsychology, Behaviour, and Social Networking, 21(2), 105-109. https://www.liebertpub.com/doi/full/10.1089/cyber.2016.0729

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. Criminology &Criminal Justice, 16(2), 176-194. https://journals.sagepub.com/doi/abs/10.1177/1748895815603773

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating scam. British Journal of Criminology, 53(4), 665-684. https://academic.oup.com/bjc/article-abstract/53/4/665/396759?login=false

AI and Scams

Advances in AI technology are making it increasingly harder for the average person to determine what is real and what isn't. In addition, if your new connection is not located in your city or area and you can't meet face to face, be extra wary of what could be a fake profile or person generated by AI.

AI-Generated Conversations

Are your questions being avoided? Or is it all too perfect and not as conversational as you'd expect? These are all signs that a bot or AI is being used to generate conversations and content.

Voice Cloning

Phone calls that use someone else's voice to disguise a foreign accent or make the person seem more sophisticated are ways that voice cloning is being used in romance scams. Real-time voice converters can be used in both calls and videos to fool the victim into believing the conversation is authentic and real.

Deep Fakes

Reverse image searches can help you determine whether the images you are being sent are genuine or not - they could either be from a stock image library, AI-generated or in fact stolen identities of someone else.

Video Clones

Even video calls can be faked these days. If you're not sure, look for unusual facial gestures or expressions or hair that doesn't look real, as that could be an indication of a deepfake. Quite often only the mouth, eyes, eyebrows and a few other facial movements will be generated.

Things to be Aware of and Potential Red Flags

These criminals are professionals. They may appear authentic, engaging and affectionate - they may even have a real Instagram account. Sadly there are playbooks and scripts that are available and used by criminal organisations to deceive innocent victims and intentionally defraud them.

It's also important to realise that romance scams can be long-term, where scammers build trust and maintain relationships for months or even years before the person is aware it is a scam. This all might seem innocent, but there are some common telltale signs that something nefarious is lurking:

🚩

If they quickly ask you to leave the dating platform to communicate directly.

This could indicate that they are attempting to remove traces of the interaction and get more of your personal information like your phone number, which can be lucrative for a scammer. Not all scammers want money. Data is valuable too as it can be sold or used to access other personal accounts. Be aware of how much information you give to ‘strangers’.

If it seems too good to be true.

Frequent, immediate, or over-the-top displays of affection or attention - or “lovebombing” - is a red flag. A scammer wants to establish a relationship as quickly as possible, so be wary of anyone who says your introduction was “fate,” makes grand promises or even proposes marriage very quickly.

If they avoid meeting up IRL.

Scam artists will often make plans and cancel at the last minute due to unforeseen, often serious circumstances. These excuses - like a medical or family emergency, or something keeping them overseas - often become the reason they ask for financial support.

If they ask for personal information.

A connection shouldn’t ever require the sharing of a passport, driver’s license, identification number or any other information that is otherwise considered to be private. Personal data is very valuable to these criminals. Be aware of how much you disclose. Hot Tip - don’t disclose any of these things.

If they emphasise financial obstacles or challenges.

Figuring out who prefers to pay the bill at dinner is one thing, but being pulled into someone’s personal financial woes or needs is another. If this happens, particularly early on, it may be a sign of deeper deception. No matter how much you love them, embrace your main character energy and put your financial security and future first.

Reminder - even meeting IRL requires some vigilance.

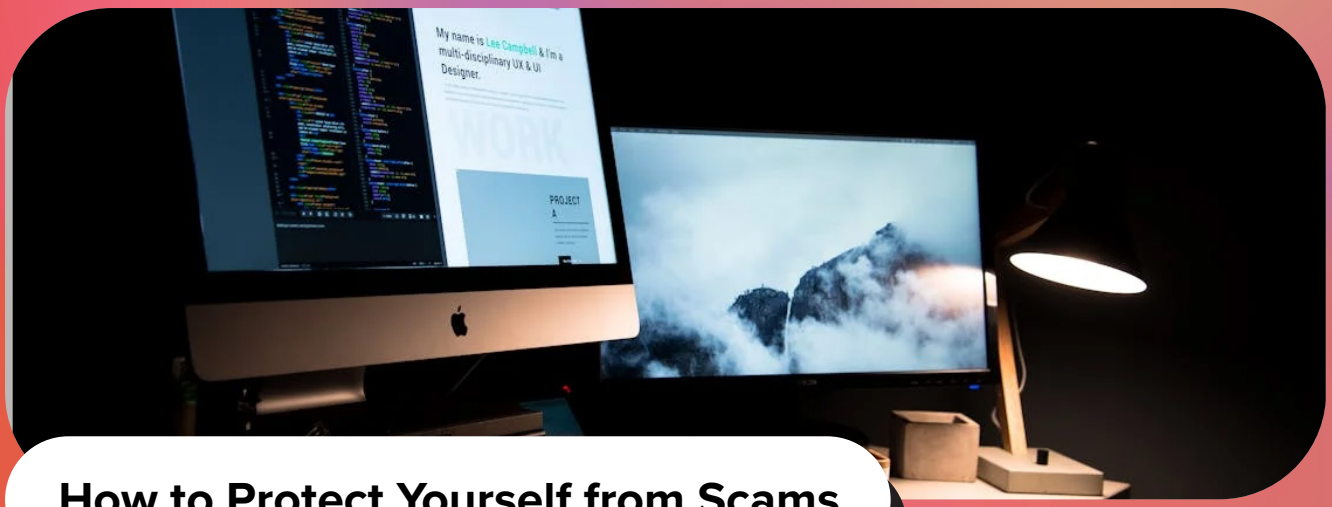
Some scammers are actually skilled con artists who are adept at earning trust quickly. These individuals may mirror your values, morals and future desires to make it seem you're 'on the same page' and want the same things. If they're acting suss, do your research - trust, but verify. Be skeptical, not cynical and ensure you take off your rose-coloured glasses.

They don't have a digital footprint.

If the person you're dating doesn't have a digital footprint - this should be a red flag. Verify things they tell you, don't be afraid to ask pointed/bold questions and be aware of vague answers or avoidance. It is ok to be cautious. If you're feeling suss - talk to a trusted friend - quite often they will see something you don't.

They avoid/refuse to introduce you to family and friends.

If you are communicating with someone and building more than just a casual relationship for longer than a few weeks, it's not out of the question to ask to meet their friends and family relatively quickly. If they avoid the question, or flat out refuse - this is a red flag. Verifying people through their friends and family is a great way to get a sense of their vibe and check they are who they say they are.



How to Protect Yourself from Scams

Beyond spotting a scammer in action, there are a number of things you can do to take control of your safety and protect yourself from a scam.

Protect Yourself

Protect what's yours.

Never share ANY personal information with people you don't know. Your personal identifying information (PII) address, and details about your daily routine (e.g., that you go to a certain gym every Monday, or always go to the same yoghurt bar with friends) along with any info about your family and friends should be kept private. This includes identifiable data including your government issued ID's like passport or driver's licence. Data is valuable and should be protected at all costs.

Be careful about what you post and make public online.

Scammers can use details shared on social media and dating sites to better understand and target you. They will find a way to leverage this information to build trust and rapport with you. Avoid sharing personal details about family and friends, your home or work address, or your daily routine.

Keep it secure.

Your Tinder password should be stronger than the chemistry with your match, and that's saying something. Make sure you're careful when logging in from a public/shared computer and beware of any Tinder emails that ask for your username and password information (we wouldn't send emails like this). If you receive an email asking for account info, report it immediately! You can find details on how to write to us to report this type of behaviour in the in-app safety centre.

Don't rush it.

Before you shift things to IRL, take your time and get to know the other person. Want to snuff out the red flags? Don't be afraid to ask questions or get on a video chat to screen your match before meeting them! Tip: Meet in a populated, public place. Good Spots: Happening bars, good restaurants or chill cafes. Bad Spots: Your home, your date's home or any secluded or private location.

Trust your gut (or your bestie).

Your intuition is your greatest wingman. Always use your best judgment, and if the vibes are off, block and report. Be aware though - sometimes our rose-coloured glasses mean all the red flags are just flags - so it's always a great idea to chat to a trusted friend or your bestie about who you're talking to and interested in. Sometimes they can see things that you can't.....

Stick to Tinder.

Getting to know someone new? Staying on the Tinder platform is a great (and safe) idea! We only allow texts, emojis and video calls so don't worry about receiving any unwanted pictures. Be cautious and alert if your match tries to move the conversation to phone calls or other apps right away - they could be trying to bypass Tinder's Safe Message Filters.

Consider the types of pics you send.

It's important to consider the types of pics you send to others, as intimate photographs can often be used to extort money from victims by threatening to send explicit content to friends, family or more.

Do Your Homework

Check out their photos.

Scammers rarely use their own photos, so consider running a reverse image search to see if their profile photo is used elsewhere on the internet.

Ask (bold) questions.

Much like you would in getting to know a potential match, get to know people on a personal level by asking all of the questions. Look out for inconsistent facts and stories, or vague answers to very specific questions. Don't be afraid to probe further if something doesn't make sense. If they get agitated or avoid entirely, this is a red flag.

Educate yourself about scams.

Watch out for scammers who ask for financial help and anyone who won't talk on a phone/video call - they may not be who they say they are. If someone is avoiding your questions or pushing for a serious relationship without meeting or getting to know you first, that's probably a red flag.

Above all else, do not send money online.

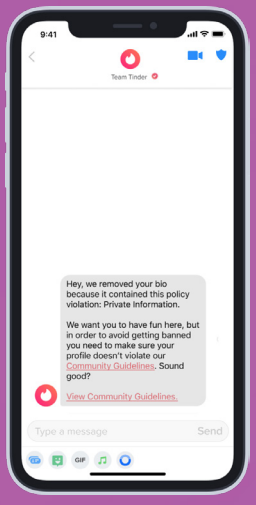
The ACCC advises to never send money to someone you meet online, including providing credit card numbers, bank account details, login credentials or any other personally identifiable information.

Your Safety Toolkit (Tinder's Features)

Every day, people trust Tinder to introduce them to new people. With this comes an essential responsibility, and the app is constantly evolving to help make every experience feel safe, respectful and positive. Tinder has invested in building a suite of safety tools so you can customise your safety toolkit when using the app. Here are some of the top fraud-fighting features on Tinder:

An invisible shield of machine learning (ML)

Using advanced ML systems, Tinder can identify patterns and ban bad actors from using the app before they interact with anyone. You'll never meet or match with these bad actors as they are blocked before they can do any harm.



Bio Guidance

Offering Bio Guidance is an additional step in ensuring members understand what's acceptable on Tinder, while also helping protect their personal information. For instance, one common mistake members make involves including personal information, like phone numbers, in their profile. Bio Guidance removes these details, and lets members know why and gives them another shot at writing their bio.

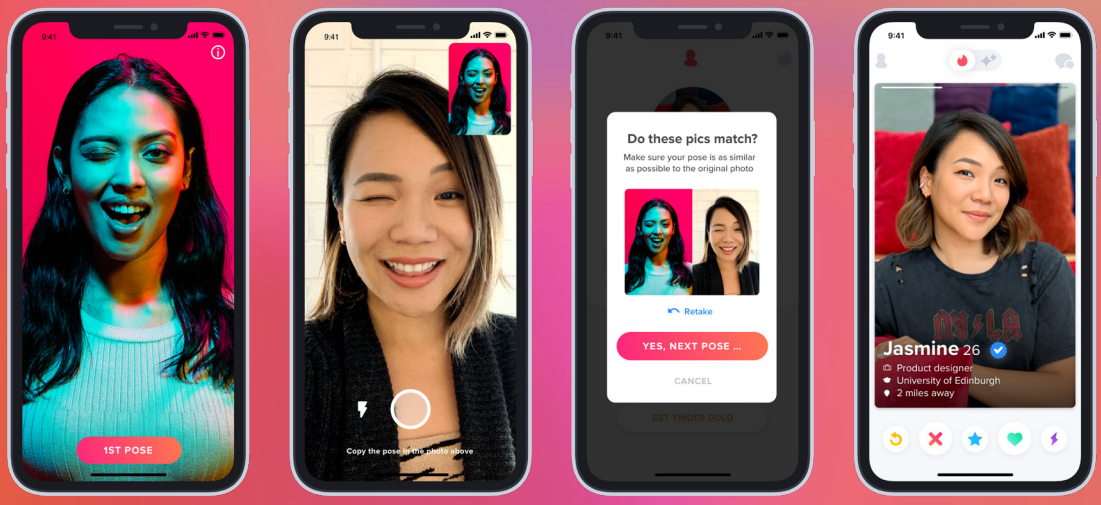
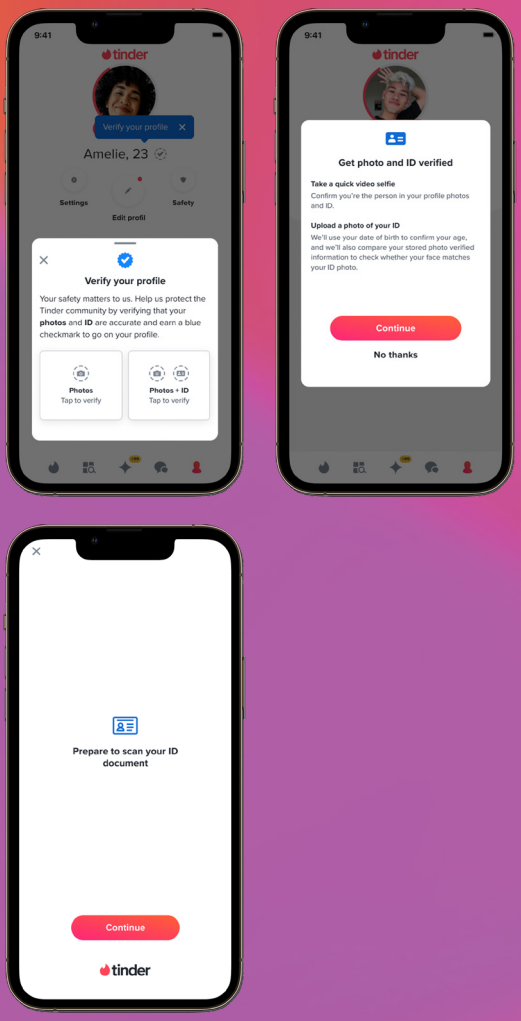


Photo Verification

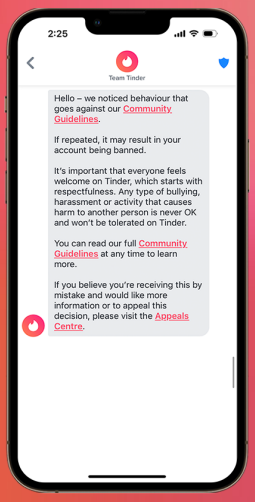
Once someone has created their Tinder profile, and added their photos during the sign-up process, they are encouraged to utilise Tinder's Photo Verification feature. It helps show possible matches that your photos are really you by comparing profile photos with a video selfie taken in-app in real-time. Within their Message Settings, Photo Verified members can also opt to only receive messages from other Photo Verified members.



ID Verification

ID Verification serves as an additional step for users to help confirm the authenticity of profiles. The enhanced process requires a video selfie and a valid Driver's Licence or Passport and will check to see whether the face in the video selfie matches both the photo on the ID as well as the person's profile photos. It will also check the date of birth on the ID. This can be done on the user's Profile page.

Users who only complete Photo Verification will now receive a blue camera icon badge and users who only complete the ID Verification will receive a blue ID icon badge. Users who complete both ID + Photo Verification will receive the blue checkmark.



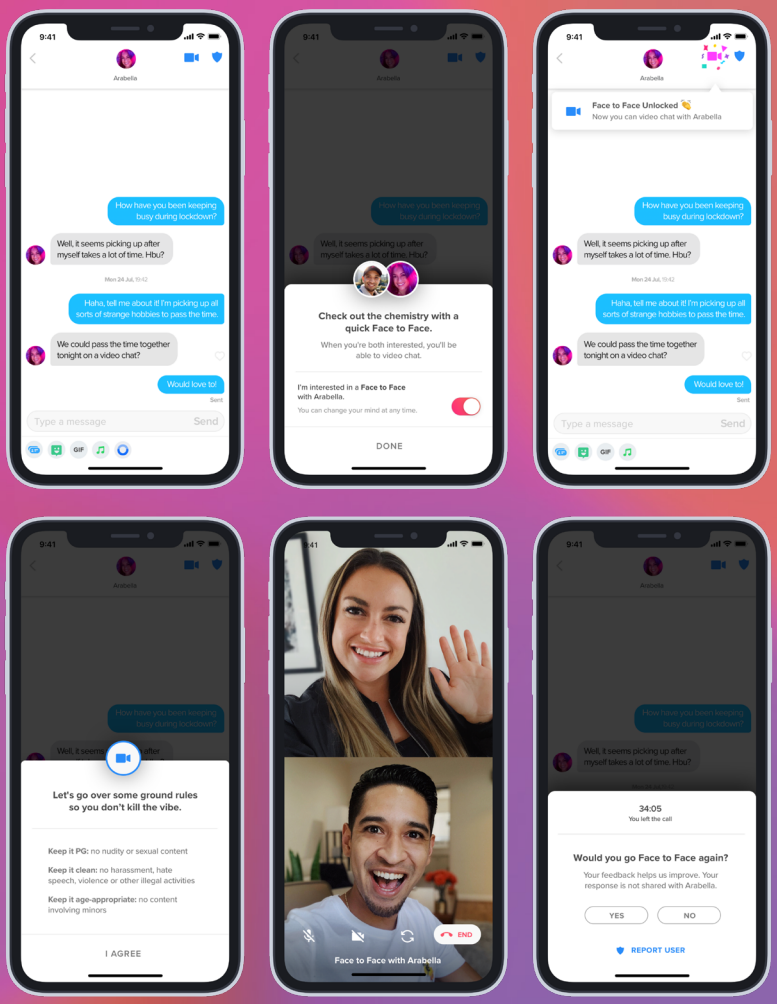
Warnings

In-app warnings aim to provide additional guidance to users by informing them of inappropriate behaviour, as well as offering an immediate opportunity to change their actions. The warnings are classified into three categories: authenticity, respectfulness, and inclusiveness. They cover behaviour such as harassment and protect users against advertising and impersonation.

Warnings are sent to users in-app within ‘messages’ from ‘Team Tinder’ with an explanation of what violation occurred, as well as broader information about expected behaviour and actions. When users receive a warning it will remain as a visible message that they cannot delete. Individual profiles are at risk of being removed if users continue to repeat the same violation.

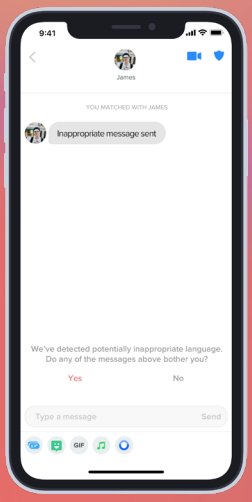
Video Chat

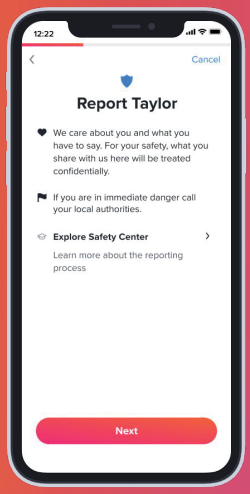
Tinder’s video chat feature was built with control and comfort as its first priority. The in-app video calling feature allows members to meet digitally, verify their match is genuine and better assess whether the chemistry is there before an IRL date - all without giving out personal contact details.

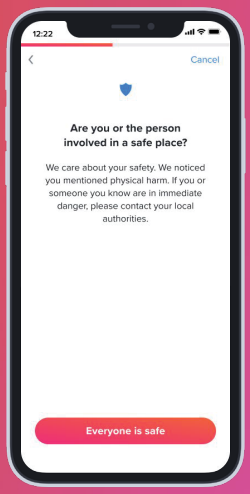


Does This Bother You?

“Does This Bother You?” is an in-app prompt that asks members this question when they receive a potentially offensive message on Tinder. When someone responds ‘yes’ to the prompt, they have the option to report the sender for their behaviour. This feature has helped increase the reporting of harassment. It has been enhanced to include more language that Tinder classifies as harmful or inappropriate, such as terms related to hate speech, sexual exploitation or harassment.







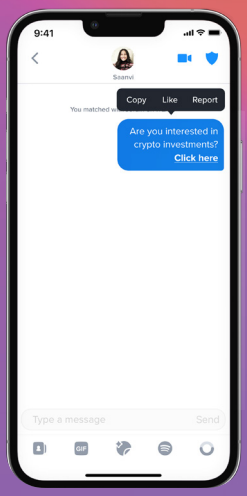
Reporting

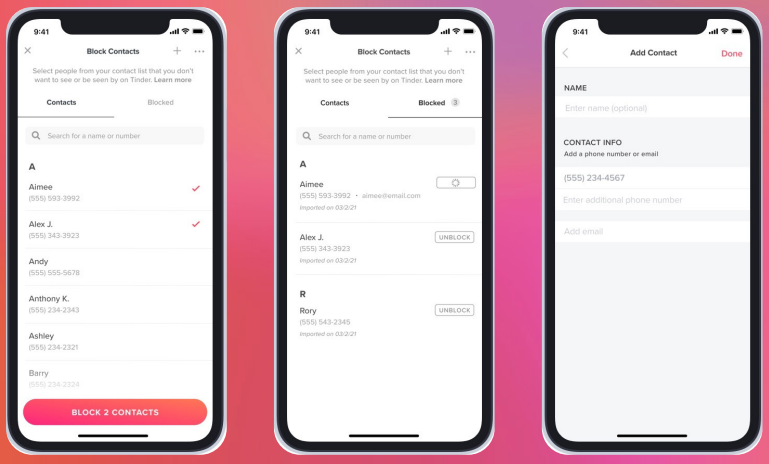
If someone approaches you on Tinder requesting money, please report them immediately. To report a match, go to your chat and select the safety centre badge in the top right corner. Select “report,” and choose a reason that best describes your experience. If you’ve come in contact with a scammer, you’ll likely select “fake profile” as the reason for reporting. Tinder will take it from there.

Tinder uses a robust reporting framework that combines technology and human review to swiftly evaluate member behaviour, ensuring it adheres to our Community Guidelines. Members can report someone directly from a profile or reach out through the Safety Centre in the app at any time. We take reports very seriously.

Long Press Reporting

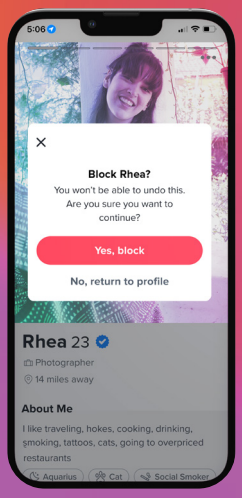
Tinder wants it to be as easy as possible for members to report bad behaviour. Long Press Reporting lets people tap and hold offensive messages, launching the reporting flow directly in the chat experience. By simplifying this flow, Tinder hopes more members will report bad behaviour, allowing it to take appropriate action against accounts that violate Community Guidelines.





Block Contacts

Block Contacts allows members to block personal contacts they'd rather not see nor be seen by, in the app – empowering them to confidently "like" their way to new connections without any unwanted surprises. Whether those contacts are already on Tinder or decide to download it later using the same contact info, they won't ever appear as a potential match.



Block Profile

Block Profile is an important step to give members the option to choose who they want to see on Tinder. When profiles are suggested, before matching, members can block the person so they don't show up again. It's an easy way to avoid seeing a boss or an ex. This new feature comes in addition to "Block Contacts" and blocking following making a report.

Resources

The ACCC: Little Black Book of Scams

The ACCC: Targeting Scams Report

Scamwatch: Romance Scams

eSafety: Romance Scams course

IDCare: Relationship Scams

What to do if You've been Scammed

1. Act fast and contact your bank or card provider to report the scam and to stop any pending transactions.
2. Change your passwords on all devices and online accounts.
3. Get help from IDCARE, Australia and New Zealand's national identity and cyber support service.
4. Report the scam to Scamwatch.
5. Talk to a trusted friend or family member and lean on them for emotional support.