

FACT SHEET: Relationship Scams

F
A
C
T
S
H
E
E
T

Relationship Scams involve a person developing a relationship (which may be romantic, a friendship, or based on a common interest) with an individual they believe is real and genuine, but who is actually motivated to:

1. Steal money
2. Acquire identity credentials
3. Commit other crimes, including involving the relationship scam victim in drug trafficking, money laundering, and investment fraud

Quick Facts

-  Anyone can become involved in a relationship scam, with reports to IDCARE from all ages, genders, cultural backgrounds, education and income levels.
-  Driver licences are the most commonly compromised credential in a relationship scam.
-  In the first quarter of 2021, almost half of all callers to IDCARE involved in a relationship scam had sent money to the scammer. The average amount sent was \$82,000, with individual losses up to \$2 million.

Detection – Is this a relationship scam?

The majority of relationship scams begin online. That is not to say that physical meetings or engagements do not occur. Common platforms used by scammers include social media (such as Facebook), relationship or dating websites and apps (such as Tinder, Bumble, Hinge or Grindr), and even email and SMS. IDCARE has seen investment fraud and employment scam attempts divert to relationship scams, and vice versa.

If you are concerned that you or someone you know may be involved in a relationship scam, this checklist provides some of the common elements of a relationship scam. The more times you answer “yes”, the more likely it is that this is a relationship scam.

- | | |
|---|---|
| <ul style="list-style-type: none"> <input type="checkbox"/> The relationship started online, not in person. <input type="checkbox"/> Communication quickly switched to a new platform, such as Facebook Messenger, Hangouts, WhatsApp, Viber, Skype or email. <input type="checkbox"/> You met during a difficult time in your life, such as following a breakup or the death of a loved one. <input type="checkbox"/> The person expresses strong feelings or interest soon after first communicating with you. <input type="checkbox"/> You have never met in person. <input type="checkbox"/> Video chats do not occur, or are of poor quality, or the person you are communicating with has no camera. <input type="checkbox"/> You have received no photos of the person you are communicating with, or they are of poor quality, or when doing a reverse-image search the individual uses a different name. <input type="checkbox"/> The person claims to be from Australia, New Zealand or another high-income country, but is currently located overseas (mostly likely for work). <input type="checkbox"/> The person claims to be an aid worker, military personnel, oil rig worker, or a professional working abroad. <input type="checkbox"/> Plans to meet in person never happen due to last minute problems, for example, they lack the funds, they or a family member becomes sick, or they encounter difficulties in their journey. <input type="checkbox"/> You are encouraged to keep the relationship secret from your family and friends. | <ul style="list-style-type: none"> <input type="checkbox"/> The individual requests personal information and/or credentials from you such as your passport, driver licence, or a photo of you holding these items. They might tell you that they have been scammed before and want to make sure you are real, or they need them for travel arrangements to meet in person. <input type="checkbox"/> The person requests money. This may be to cover travel or medical expenses, or to cover the postage or customs fees for an item. <input type="checkbox"/> The person wants to set up a business with you or gain employment in Australia/New Zealand and needs your help e.g. money or credentials to complete paperwork. <input type="checkbox"/> You are asked to receive or transfer goods or funds on the person's behalf. <input type="checkbox"/> You are asked to make any payments via money order, wire transfer, international funds transfer, pre-loaded card or electronic currency. <input type="checkbox"/> You confront the person about your suspicions that they are scamming you, and they reveal that although they have scammed you initially, they are now sincere about their feelings and want to continue the relationship. <input type="checkbox"/> You may have been contacted by another party claiming to be working in a hospital or a family member, because the person you have developed a relationship with is in hospital requiring urgent medical care. |
|---|---|

FACT SHEET: Relationship Scams

F A C T S H E E T

Response – What do I do now?

- Cease all communication with the scammer – phone, email and online.
- Tell a trusted person what has happened, and let them know you need their support as you work through your emotional and practical recovery.
- Contact your GP if you feel you need additional support to work through your grief over the financial and emotional losses.
- Contact and advise your banks and any other financial institutions of the relationship scam, and request increased security on your accounts.
- Notify the relevant document issuing organisations for any of the credentials that the scammer may have accessed. Common credentials include:
 - Driver licence
 - Passport (Australian passports contact [DFAT](#) on 131 232, for NZ passports contact [DIA](#) on 0800 22 50 50)
 - Medicare card (Australian residents contact Services Australia on 1800 941 126 or email the [Scams and Identity Theft Helpdesk](#))
 - ATO details (Australian residents call 1800 467 033) or IRD details (NZ residents call 0800 257 777)
 - RealMe details (NZ residents call 0800 664 774 or online at [RealMe](#))
 - Bank account details, including login information
- Contact your superannuation fund/s to increase security on your accounts.
- Contact all [Credit Reporting Agencies](#) for your free credit reports and to arrange credit bans.
- Update or add passwords, PINs, and multi-factor authentication to all accounts, apps, and websites requiring logins.
- Check if forwarding rules have been changed on your email accounts.
- Be aware that you may see an increase in scam attempts unrelated to the relationship (via telephone, email and SMS).
- Contact the police to report any misuse of your identity, and in order to gain a police report.
- If you have sent or received money or goods online, provided remote access to your computer, or shared credentials online that would enable identity theft and fraud, you can alert police through:
 - [ReportCyber](#) (in Australia)
 - Call 105 or go <https://www.police.govt.nz/105support> and choose “Report a Police non-emergency” (in New Zealand)
- If you are concerned that the scammer may have had access to your internet enabled devices, ask your IDCARE case manager about our free Cyber First Aid support service.
- For additional support or information, contact IDCARE by submitting a [Get Help Form](#) or call 1800 595 150 (Aus) or 0800 121 068 (NZ).

Prevention – How can I avoid a relationship scam?

- Try to remove emotion from your decision making no matter how caring, engaging or persistent the friend or prospective partner is.
- Do a reverse image search on their profile photos to check if they have been used on other sites with different names or locations (such as [Tineye](#) which is free, or [Social Catfish](#) where you will need to pay for an account).
- Be cautious when sharing personal pictures or videos, especially if you've never met the person before. Scammers are known to blackmail their targets using compromising material when the relationship is over.
- Be very careful about how much personal information you share on social network sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.
- Discuss your growing friendship with people you can meet face-to-face, such as friends, family or work colleagues. You would want to introduce a new friend or potential partner that you had met in person, so do the same with this online relationship.

Sharing & Disclaimer

IDCARE is Australia and New Zealand's national identity and cyber community support service. IDCARE is a not-for-profit and registered Australian charity. © 2021 Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person in respect to any actions performed or not performed as a result of the contents of the assessment or any accompanying data provided.