

## Introduction

Instagram allows individuals and businesses to share photo and video content with other users. Instagram, like Facebook and WhatsApp, is a part of the Meta brand, meaning users are able to link their Meta account.

Instagram's wide reach and usership as well as the advertising and messaging services embedded in the platform make it a valuable tool for criminals. By reviewing your Instagram security settings and being conscious of how you use Instagram you can mitigate against the risks posed by those who misuse the platform.

### Quick facts

IDCARE has seen a sharp increase in the number of clients seeking help with Instagram account issues. The most common issues reported to IDCARE regarding Instagram accounts are:

1. Account takeover (hacking)
  2. Responding to a post from a friend or business Instagram account that has been hacked, often leading to scams involving investments, grant applications or competitions
  3. Responding to an Instagram post or message about a competition or an investment opportunity
- Relationship scams that began on Instagram

## Prevention checklist

### How can I prevent Instagram account problems?

- ☐ [Instagram's Help Centre](#) provides information on how to [manage your privacy settings](#) and [improve your account security](#).
- ☐ Even if your account is private, don't post information, photos or videos you wouldn't want made public.
- ☐ Never post photos of your identity credentials, such as your driver licence or passport. If you do have photos of identity documents in direct messages, delete them as soon as possible.
- ☐ Always use strong and unique passwords and consider using a password manager to store these.
- ☐ Turn on [two-factor authentication](#) on all linked accounts.
- ☐ Never share your login information.

#### Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© 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 with respect to any actions performed or not performed as a result of the contents of this document.

### Prevention checklist cont.

- ☐ Be careful about [allowing access to your account to third-party apps or websites](#).
- ☐ Avoid clicking on links, even if they appear to be from a friend or business that you follow.
- ☐ Keep backups of your posts if they are important to you or your business.
- ☐ Unfollow and block users that you don't wish to interact with through Instagram.
- ☐ [Save backup codes](#) in case you lose access to your account and store these codes in a secure place such as a password protected word document.
- ☐ Disable geolocation on posts, tailored ads and others' ability to tag you in photos.
- ☐ If you meet someone through Instagram, be careful leaving the app to chat with them. Don't send money or provide them with identity credentials.
- ☐ [Report suspected fraud or scam posts and profiles](#) to Instagram.

### Detection checklist

**Common signs that there may be a problem with your Instagram account include:**

- ☐ You don't have access to your account anymore despite using the right password.
- ☐ Your account is leaving comments or sharing things that you haven't posted.
- ☐ Your account starts to follow people you don't know and also like their images.
- ☐ There are images on your account which you know aren't yours.
- ☐ Your account contact details, such as your email or phone number, has been changed.
- ☐ Accounts linked to your Instagram profile are removed or added.
- ☐ You responded to a message that you thought was from a friend or company you follow, perhaps regarding a competition or investment opportunity, only to later discover that their account had been taken over.
- ☐ You or your followers see another Instagram account using the same name (personal or business) and some of your photos, logos or posts.

#### Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© 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 with respect to any actions performed or not performed as a result of the contents of this document.

## Detection checklist cont.

- ☐ You do a reverse image search of one of your own photos and see it appears in a different Instagram account. When you go to that account, you see that it is claiming to be you or your business.
- ☐ When you try logging into your account, it displays a message saying that your account/s have been suspended or disabled.

## Response checklist

### How can I address problems with my Instagram account?

- ☐ Contact Instagram immediately if someone [has gained access to your account](#), is [impersonating your account](#), or [has created an Instagram account impersonating you or your business](#).
- ☐ Where possible, inform your friends, family and followers of any unauthorised access to your account. This will reduce the risk that they will engage with the criminal now controlling your account. You may choose to notify your customers on your website or an unaffected social media page of yours.
- ☐ If you are still able to access your account, Instagram advises that you confirm your email address and phone number are correct in the account settings, turn on 2FA, change your password and send yourself a password reset email, and remove any unauthorised linked accounts and access to your account from third party apps.
- ☐ If you have stored your credit card or other payment details on your Instagram account or any linked accounts, contact the issuer immediately to cancel the card and/or payment account.
- ☐ Notify the relevant document issuing organisations for any other credentials that may have been stored in your account.
- ☐ If your account has been suspended or disabled, you can follow Instagram's process to submit an appeal.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 170 (Aus) | 0800 121 068 (NZ)

#### Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© 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 with respect to any actions performed or not performed as a result of the contents of this document.