

Introduction

WhatsApp is one of the world's most popular messaging platforms, making it a common target for cybercriminals. Scammers use tactics such as phishing, impersonation, fake giveaways and account takeover attempts to steal personal information, money or access to accounts.

This fact sheet provides practical tips to help you avoid scams and account takeover, and to respond effectively in the event of unauthorised account access.

Protecting yourself against WhatsApp scams and account compromise

- ☐ Avoid responding to new unsolicited messages. If the message appears to come from a friend or family member, contact the person through another form of communication to verify the engagement.
- ☐ Do not click on links that people share as these can lead to malware and related phishing attempts. Verify messages appearing to come from known or legitimate organisations. Use their official contact channels to confirm whether they communicate with their clients/customers via WhatsApp.
- ☐ Add multi-factor authentication on your account (find out how with WhatsApp's [About two-step verification](#)).
- ☐ Review your [Privacy Settings](#) and consider reducing visibility about you (such as your status, profile picture, and live location sharing). You can run through the [Privacy checkup](#) to help strengthen your account.
- ☐ Set up a Screen Lock for WhatsApp on your Smartphone (such as FaceID or TouchID) under your device settings.
- ☐ [Control your group privacy settings](#)
- ☐ Never share your 6-digit code with anyone when you sign into WhatsApp.

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.

Detecting issues with your WhatsApp account

- ☐ Check "Linked Devices" in your WhatsApp settings to review all the devices linked to your account.
- ☐ Check messages that you have sent to see if you have any messages you did not send.
- ☐ Review your contacts. Often, hacked WhatsApp accounts can include contacts the legitimate user does not recognise.

Responding to WhatsApp account compromise

If you still have access to your account:

- ☐ Change the password and ensure that multi-factor authentication is enabled. Enable [strict account settings mode](#) to help reduce your vulnerability to account takeover by limiting functionality.
- ☐ [Log out of all computers](#) from your phone that is using your WhatsApp account.
- ☐ WhatsApp advises that as soon as you log back in to your account, all other sessions are logged out.
- ☐ Send a message to your contacts to let them know you are having issues with your WhatsApp account and that any requests from you should not be actioned.
- ☐ If you have shared sensitive information or documents in previous messages, contact IDCARE to speak about the risks associated with these credentials being exposed.

If you cannot access your account:

- ☐ Follow the steps recommended by [WhatsApp](#)
- ☐ If you have shared sensitive information in previous messages, contact IDCARE to speak about the risks associated with these credentials being exposed.
- ☐ Consider whether the compromise may have resulted from a specific event. There may be additional accounts that need to be secured, or further steps required to protect yourself. It may also be worthwhile contacting IDCARE for advice and recommendations on any actions you should take to reduce the risk of further compromise.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 160 (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.