

Introduction

X is a virtual and public forum used by individuals, groups and businesses. This social media platform is designed for users to be able to share and discuss opinions and events. Posts on the platform are short and succinct, allowing for informal collaboration and quick information sharing. This guide provides simple steps you can take to protect your X account.

Prevention checklist

How to protect your information and account details when using X.

- ☐ Always use a strong & unique password on your account.
- ☐ Enable multi-factor authentication.
- ☐ X posts are public by default, however, you can choose to "[protect](#)" or make private selected posts.
- ☐ Backup your posts if they are important to you or your business.
- ☐ Regularly check for unknown third-party apps connected to your X account.
- ☐ Be careful of clicking links that take you away from the app, even from people you know.

Detection checklist

How can you detect if someone is attempting to access your X account?

- ☐ You have been signed out/locked out of the account.
- ☐ You receive verification codes and new login alerts randomly.
- ☐ Changes to account followers and following.
- ☐ Changes made to the profile contact information or recovery methods.
- ☐ New or unknown apps have been linked to your profile.
- ☐ Direct messages you don't recognise have been sent from your account.

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.

Response checklist

How can you respond to account compromise or a scam on X?

- ☐ Change your password immediately and ensure multi-factor authentication is enabled.
- ☐ Check login history.
- ☐ Delete any unknown trusted devices logged into the account.
- ☐ Delete any unknown posts, comments or direct messages made by the account when it was compromised (if a business account was used to distribute scam messages, consider notifying followers to not click on the link or follow the instructions).
- ☐ Inform X if you suspect there has been unauthorised access to your account.
- ☐ If you still have access to the account - see X's guide [here](#) on how to secure a compromised account.
- ☐ If you no longer have access to the account – complete X's help form [here](#)
- ☐ If your account is being impersonated, you can report it [here](#).

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.