

Introduction

LinkedIn is a social networking tool for individuals interested in developing their professional network and find new opportunities to grow their careers. Whilst operating similarly to other social media platforms, on LinkedIn users invite “connections” to converse via private messages. While LinkedIn facilitates great opportunities to connect, it may also be used as a tool to facilitate social engineering by criminals.

Quick facts:

1. On LinkedIn you display your professional experience and achievements on your profile.
2. Depending on the account settings, corporate and personal email addresses and related contact details may be accessible.
3. LinkedIn has become a popular platform for recruitment, subsequently attracting employment scammers who use the platform to identify relevant targets.
4. LinkedIn experienced a data breach in 2016 in which LinkedIn usernames and passwords were exposed.

Prevention checklist

How to secure your LinkedIn profile and avoid scams

- ☐ Go to [LinkedIn's privacy settings](#) and review who can access your contact information.
- ☐ Ensure your email and LinkedIn account have strong and unique passwords.
- ☐ Enable two factor authentication on both your email and [LinkedIn](#) accounts. Do your research on individuals wanting to contact you about a job opportunity.
- ☐ Don't match with connections you do not know or do not trust.
- ☐ Review the type of information you post about yourself. You don't need to share your full name and date of birth. Never share credential information, such as driver licences and passports.
- ☐ Always use anti-virus and be careful to only access social media on trusted Wi-Fi.
- ☐ (If using the mobile app) Check and download LinkedIn updates to the app regularly.

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

Scams propagated through LinkedIn often take the form of:

- ☐ Invitations to connect with unknown people who send emails containing links aimed at directing you away from the LinkedIn in order to facilitate deceptive engagement.
- ☐ Fake jobs/money laundering where job opportunities are made by criminals that are administrative, requires a person to transfer money (often overseas), and may even demand an 'Application Fee' is paid.
- ☐ Receiving unsolicited emails with a .zip file attached that may contain malware/Trojans that can steal your data.
- ☐ Receiving unsolicited emails seemingly target towards your profession/interests which may be phishing emails.

Response checklist

- ☐ Forward or report any suspicious emails/messages received on LinkedIn using [this form](#).
- ☐ Download and run the latest anti-virus software on your devices.
- ☐ Change your LinkedIn password, preferably from another device.
- ☐ Remove or block the connection who sent the suspicious email/message.
- ☐ Delete suspicious emails from your account.
- ☐ Contact LinkedIn immediately if someone has gained [access to your account](#) or one of your connection's accounts.

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.