

Introduction

LinkedIn is a social networking platform for individuals interested in developing their professional network and finding new opportunities to grow their careers. It operates similarly to other social media platforms: users invite “connections” and converse via private messages. While LinkedIn offers valuable opportunities to connect, it may also be used by online criminals to facilitate social engineering.

Quick facts:

1. On LinkedIn you display your professional experience and achievements on your profile.
2. Abuse Occurring via LinkedIn: Emails and related contact details are accessible on LinkedIn.
3. This may be influenced by the level of access afforded to users – for example, premium service recipients are able to send messages direct to a certain number of prospective connections.
4. LinkedIn has become a popular platform for recruitment, subsequently attracting employment scammers.
5. LinkedIn experienced a data breach in 2016 in which usernames and passwords were exposed.

Prevention checklist

How to secure your LinkedIn profile and avoid encountering scams

- ☐ Go to [LinkedIn's privacy settings](#) and review who can access your contact information.
- ☐ Ensure your email and LinkedIn 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 birth. Never share credential information, such as images of 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.
- ☐ See [LinkedIn Account Security Best Practices](#).

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 or money-laundering schemes, where criminals present administrative-style job opportunities that require you to transfer money (often overseas) and may demand an 'Application Fee'.
- ☐ 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](#).
- ☐ Change your LinkedIn password, preferably from another device.
- ☐ Remove or block the connection who sent the suspicious email/message.
- ☐ 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.