

Introduction

Scammers may impersonate employees or managers of small businesses in an attempt to trick staff into sharing sensitive information, transferring funds, or granting access to business systems. This impersonation commonly occurs via email. It is essential for small businesses to be aware of how to detect impersonation scams to prevent financial or reputational harm to their business.

Commonly impersonated people in a business:

1. Business Owners
2. Managers
3. Human Resource Managers
4. Administrative Assistants
5. Business Accountants

How to prevent employee impersonation

- Provide training to employees on how to identify impersonation attempts.
- Implement verification procedures for financial and information requests (such as the change of bank account details or requests for sensitive business or employee information).
- Be mindful of what information is publicly available and may be harvested for impersonation attempts (e.g. employee role titles and email addresses).
- Enforce multi-factor authentication (MFA) on business email accounts.
- Educate your clients about your payment procedures so they are aware of possible impersonation attempts.

Red flags to look for:

- ☐ A sense of urgency and time pressure: scammers will often put time pressure on the people they contact to minimise the opportunity to verify the legitimacy of the communication.
- ☐ Instructions to click a link: scam communications often emphasise the need to click on a link as part of the response actions.
- ☐ Request for payment: scammers may request payment urgently, often via gift cards.
- ☐ Requests to change payment details.
- ☐ Inconsistent language or change of tone: scammers impersonating employees may use language which is different from what would normally be expected of the employee.
- ☐ Scammers may ask that the details of their request are to remain confidential.

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

Employee email compromise:

- ☐ Reset password to something unique and strong.
- ☐ Ensure you enable multi-factor authentication.
- ☐ Log out of all devices on the account.
- ☐ Look for any changed account recovery methods you don't recognise.
- ☐ Check email forwarding rules and delete any rules you don't recognise.
- ☐ Check Sent and Deleted folders for unrecognised email correspondence.
- ☐ Notify relevant contacts to warn them of potential scam attempts as early as possible.
- ☐ Immediately contact financial institutions regarding any unauthorised transactions.

If the compromise has potential to cause serious harm, you may have obligations under the Privacy Act 1998. According to the OAIC (Office of the Australian Information Commissioner), serious harm may include serious physical, psychological, emotional, financial, or reputational harm. Please see IDCARE's fact sheet regarding what to do if your business has experienced a data breach [here](#).

Employee email impersonated:

Protect your domain

Contact the email provider of the fraudulent address

If the fraudulent email is using a common email provider (such as Outlook, Gmail, Hotmail) to impersonate the victim, you may be able to send an abuse report to the email service provider, where they may conduct an investigation or take action.

- ☐
 - For Gmail, submit an abuse report [here](#).
 - For Hotmail, Outlook, Live or MSN, report the email as an attachment to abuse@outlook.com
 - For other email providers, access their official website for abuse reporting methods.

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.

Contact the registrar of the fraudulent domain name



- You can find out the registrar of the domain by performing a whois lookup for .au domains at whois.auda.org.au and for international domains at lookup.icann.org.
- The lookup results may list a Registrar Abuse Contact Email to send takedown requests to. If there is no abuse contact email provided, perform an internet search to find the registrar's website and look for an abuse form or contact email there. Once you have the registrar's contact details, send a takedown request.
- Include in your takedown request information about the fraudulent domain name and how it is similar to your own. You can do this by taking note of the Registrant, Registrant Name and Registrant ID (which is typically an Australian Business Number (ABN) or an Australian Company number (ACN) for domains ending in .au). This is helpful because often scammers will use your details for these fields when creating the domain to make it appear more legitimate.



- Submit a complaint to the auDA for domains being used for impersonation.
 - The au. Domain Authority (auDA) is the official Australian authority and regulatory body for the .au domain name, such as ones ending in com.au, net.au, org.au.
 - You should submit a complaint to the auDA at auda.org.au if a scammer is using an Australian domain name which references your registered business name or is a misspelling of your domain name.

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.