

Introduction

Scammers often impersonate businesses with the goal of deceiving clients, colleagues, or suppliers to respond to fraudulent requests, or to gain access to accounts, sensitive information, or money. Business impersonation scams can also result in scammers accessing client or customer information, putting them at risk of exploitation. This can significantly damage the business's reputation.

Types of Business Impersonations:

Website impersonation: Scammers often use duplicate websites to pose as an existing business. This occurs when scammers create a website that uses an address similar to the legitimate business. These impersonation sites often use the same or similar style of branding to look like the business they are impersonating. A legitimate business may use the website URL 'businessname.com', which a scammer can impersonate by slightly altering the domain name – for example, 'businessnameaustralia.com' (this is called typo squatting). Additionally, scammers can buy different extensions of a legitimate business website domain – the business may own 'businessname.com', but scammers could buy extensions like 'businessname.co' or 'businessname.org'. These websites can be used to gather sensitive information from business customers such as credit card details, or to sell fraudulent products, or promote malware.

Business email impersonation: Business email impersonation is a type of email scam that involves scammers exploiting employee, supplier or client trust in a business email, usually with the objective of obtaining information or money. Scammers use email impersonation for a variety of scams such as sending fraudulent invoices to clients of the impersonated business, requesting sensitive information from employees by posing as a colleague, administrator or management, or conducting phishing attacks.

There are two main methods for email impersonation, email spoofing & email compromise:

- **Email spoofing:** Scammers often use email addresses that closely resemble the legitimate email addresses used by a business. For instance, a legitimate business using the email domain 'millie@example.com' could be impersonated by scammers using the domain 'rnille@example.com' - these domains appear to be identical, but the scammer version uses an 'rn' to replace the 'm'. Alternatively, the display name of a legitimate business may be impersonated – scammers could use 'businessname@**gmail.com**' to impersonate 'businessname@**example.com**' but use the same display name.
- **Business Email Compromise (BEC):**
 Business Email Compromise (BEC) occurs when scammers gain unauthorised access to a business email account. Once compromised, scammers can view previously sent and received emails, allowing them to misuse this information. In addition, scammers may

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.

access sensitive information stored within the email account, including confidential documents or linked systems such as Xero, banking platforms, or social media accounts.

Unauthorised advertisements: Scammers use online advertisements to impersonate a business. These advertisements are often circulated on social media and promote fake products and/or services using the name of a real business. The advertisements are used to increase traffic to scam websites, phish for personal details or payment information, or distribute malware.

Social Media impersonation: Scammers may opt to create a fake business social media page with the aim of defrauding existing and new customers.

How to prevent business impersonation

There are several steps a business can take to help mitigate the risk of being impersonated by scammers.

- ☐ **Increase general scam knowledge:** Businesses can minimise the risk of clients falling victim to scams by providing general education on scams. This can be achieved by providing resources on good scam safety practices such as verifying the legitimacy of communications sent to them by double checking with the business directly, avoiding clicking on links, and recognising phishing attempts. Businesses should ensure that employees are well-equipped to recognise and respond to scam attempts.
- ☐ Businesses can additionally implement [DMARC & DKIM](#) to help prevent business email impersonation.
- ☐ **Enforce multi-factor authentication (MFA):** The use of MFA across a business should be mandatory. MFA adds a second verification step for online account access, in addition to a unique username and strong password or passphrase. MFA methods include one-time passcodes sent to a trusted mobile phone number or email address, or the use of an authenticator app. MFA adds an extra layer of security that can help prevent a business's accounts being compromised.

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.

How to prevent business impersonation cont.

- ☐ **Monitor the use of business name:** Businesses should actively monitor the use of their business name online to detect any impersonating websites or social media pages. Businesses should also consider buying like-domains and ensure they keep up to date on domain expiry dates to ensure scammers cannot buy the business domain if ownership is not promptly renewed. Businesses can also setup Google Alerts to notify them of any new search results or activity using their brand on websites.
- ☐ **Consider privacy protection:** Generally, businesses and individuals should limit the information they post online as scammers can misuse this to impersonate or spearfish a business or individual. Employees should be careful posting information that identifies their workplace, position, work email address, and personal email address this can make them easier to impersonate. Businesses should implement a policy of verifying email addresses before completing sensitive email requests.

Response

An effective response to business impersonation depends on the type of business impersonation and subsequent damage or harm done. General guidance is provided below and will apply in any events of business impersonation. Following this section is more specific information relating to the type of impersonation you may have experienced.

In **any event of business impersonation**, follow these steps:

- ☐ **Notify internal accounts receivable, accounts payable, and payroll team of the impersonation.**
- ☐ **Notify your customers:** Businesses should prioritise informing customers of any compromise so they can take the necessary steps to protect themselves. Public awareness of the issue should be encouraged through social media channels or other communications. Additionally, businesses should inform clients that if they are to receive invoices with any changed information, they are to contact the company through a different means of communication, for example a phone number on their website.

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.

- ☐ **Check other online platforms:** Businesses should check if their business name is being used on any other platform. A simple Google search can help determine if there are any scammers impersonating your business through social media pages, websites, or incorrect business listings (changed details).
- ☐ **Get support for handling the breach of sensitive information:** Businesses should consider whether there may have been unauthorised access to, or disclosure of, your customers or employees [personal information](#) through the compromise or impersonation event. The [Office of the Australian Information Commissioner](#) (OIAC) has information about what a notifiable data breach is, and IDCARE can provide support and advice in determining your next steps if an event has occurred.
- ☐ **Report to law enforcement:** Australian businesses can report impersonation scams to [ReportCyber](#). A reference number will be provided after submitting a report, which should be recorded.
- ☐ **Report a scam to the Australian Competition and Consumer Commission (ACCC):** If you have not already, you can report a scam to the ACCC through Scamwatch using their [online web form](#). Please note that the ACCC is unable to help you recover any money you have lost to a scam or assist in tracking down the scammer.

Additional guidance for different impersonation events:

In the event of **website impersonation**, follow these additional steps:

- ☐ Do not click on any links or images within the impersonation website, as they may be malicious.
- ☐ **Report the website to the registrar that owns the domain** (the domain registrar): To find the domain registrar for websites and where to report abuse, use [whois.domaintools.com](#). Include information about the fraudulent domain name and how it is similar to your business in the takedown request.

After submitting a report to the domain registrar, if the website ends in .au, you can also report the site to auDA. You may also use the [auDA Whois lookup](#) to find the domain registrar and where to report abuse.

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.

- ☐ **Report the website to WA ScamNet:** Businesses may be able to have the impersonating website listed on the [WA ScamNet](#) alert pages. Businesses do not have to operate in WA to be listed. WA ScamNet has information relating to trending scams, alerting customers of fraudulent sites. They can also offer further advice regarding small business compromises. WA ScamNet can be contacted on 1300 30 40 54.

- ☐ **Report fraudulent email usage to the relevant provider:** Businesses should determine if the impersonating email was an instance of email spoofing or compromise by checking the email address. Spoofed emails can be reported to the relevant provider. Please see instructions on how to do so for [Gmail](#) or [Outlook](#). For other email providers, refer to their websites for abuse reporting methods.

Business email compromise (BEC):

- ☐
 - Implement MFA on all user accounts.
 - Log off all machines and impose a password reset on all accounts immediately.
 - Check the affected accounts for changed account recovery settings - for example, unknown phone numbers and email addresses.
 - Check for any forwarding rules on any email accounts
 - Check other email folders to see if emails have been moved. Scammers will often store emails which they have sent or engaged with in lesser accessed folders such as RSS Feed (Outlook) or deleted items.
 - Review this [step-by-step guide](#) on email account security provided by ASD.
 - Additional information can be found on our [factsheet](#).

- ☐ **Contain affected computers and network systems:** Run an antivirus software scan and ensure that your business devices are up to date with the most recent security patches and system updates. Configure your settings to ensure that the antivirus scan automatically runs, at least daily, and that system and security updates occur automatically in future. Contact an IT professional to assist & remove any unauthorised access.

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.

In the event **unauthorised advertisements or social media impersonation**, follow these steps:

Report to the relevant social media platform: Most social media platforms have mechanisms in place to deal with reported impersonation scams. Businesses can report such content by using the in-built reporting mechanisms of platforms.

☐ **Facebook:** According to [Facebook Community Standards](#), the platform does not tolerate content that falsely claims to represent an established business for the purposes of scams and fraudulent activity. Please visit [this webpage](#) for directions on how to report a Facebook profile, post, or advertisement that is impersonating your business. Visit [this webpage](#) for guidance on how to report an impersonating account if you do not have a Facebook account yourself.

☐ **Instagram:** According to Instagram's [Terms of Use](#), the platform can remove or ban any content that is fraudulent, used for illegal purposes, or impersonates someone else. Please visit [this webpage](#) for directions on how to report an Instagram account, post, or advertisement that is impersonating your business.

☐ **X (formerly Twitter):** Impersonation is a violation of the [X Rules](#), and can result in accounts being permanently suspended. Please visit [this webpage](#) for directions on how to report an impersonation scam on X, and for further information on how X handles impersonations.

☐ **TikTok:** Please visit [this webpage](#) for directions on how to report an impersonation scam on TikTok.

☐ For all other social media platforms, visit the relevant platform's help centre for directions on how to report content.

☐ **Report to the hosting website:** If the unauthorised advertisement is on a site that is not a social media platform, then businesses should report the advertisement to the website that is hosting the advertisement. Please see information on how to report advertisements hosted on [Google](#) and [Bing](#).

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.