

Introduction

Business email compromise, email phishing and false invoice fraud are among the most commonly reported incidents to IDCARE by small businesses. Effective email security is essential for preventing cyberattacks, protecting sensitive information and maintaining client trust.

This fact sheet provides practical tips to strengthen email security and help small business owners better protect their inboxes.

Common ways criminals target business email accounts

Business email compromise (BEC)

Business email compromise (BEC) is a targeted cyberattack in which a threat actor gains access to a company's email account.

Once inside the account, the attacker may:

- Manipulate financial transactions.
- Redirect payments.
- Steal sensitive information.
- Distribute phishing emails to your contacts.
- Impersonate employees, executives, or vendors.
- Obtain password reset codes to other online accounts, such as social media, or invoicing software, allowing for account takeover
- Automatically forward any received email to a different address.

False invoice fraud

False invoice fraud happens when a scammer sends fake invoices to deceive businesses or individuals into paying money. They may do this by compromising trusted email accounts or impersonating an email address.

IDCARE highly recommends checking for any exposures your business email address may have had by visiting haveibeenpwned.com and update any passwords that appear to be breached.

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.

Tips for securing your email

Forwarding rules

Email forwarding rules are settings in your email account that automatically send incoming emails to another address. If a scammer accesses an email account, they can create a hidden forwarding rule to receive copies of your emails. Additionally, these rules can also be set to delete emails once they are forwarded.

Check your email forwarding settings regularly. Unauthorised changes could indicate compromise.

Note you will likely need to login via a web-browser to view these settings, as forwarding rules aren't typically available directly via the settings page of the mobile app.

- ☐ **Gmail:** Please see Google's guidance regarding [email forwarding rules](#).
- ☐ **Outlook:** Please see Microsoft's guidance regarding [email forwarding rules](#).
- ☐ **iCloud:** Please see Apple's guidance regarding [email forwarding rules](#).

Multi-factor authentication (MFA)

MFA adds an extra layer of security, requiring a second, verifying factor beyond your password, such as a code sent to your phone or an authenticator app. Set this up to reduce unauthorised access risks.

- ☐ **Gmail:** Go to Security > 2-Step Verification and follow the setup steps to use SMS, an authenticator app, or a security key. [Please also see Google's guidance online](#).
- ☐ **Outlook:** Go to Security > Additional Security Options > Set Up MFA. [Please also see Microsoft's guidance online](#).
- ☐ **iCloud:** Enable two-factor authentication through your Apple ID at account.apple.com under Security. [Please also see Apple's guidance online](#).

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.

Password resets

Ensure that your password is strong and unique and update it regularly. Never use the same or similar password twice. Visit haveibeenpwned.com to understand if your password(s) have been involved in any known online breaches.

- ☐ **Gmail:** Access Google Password to change your password. [Please also see Google's guidance online.](#)
- ☐ **Outlook:** Go to Security > Password Security to update. [Please also see Microsoft's guidance online.](#)
- ☐ **iCloud:** Update your Apple ID password at account.apple.com under Sign-In & Security. [Please also see Apple's guidance online.](#)

Recovery emails

If you forget your password or are locked out, a recovery email allows you to receive a one-time password (OTP) to help you restore access. Ensure your recovery email is kept up to date so you can regain access to your account if you're locked out.

- ☐ **Gmail:** Go to Security & sign-in > Recovery email. [Please also see Google's guidance online.](#)
- ☐ **Outlook:** Sign into the Advanced security options page of your Microsoft Account (Outlook.com accounts are Microsoft accounts) to add a new way to sign in or verify sign-in using another email address. [Please also see Microsoft's guidance online.](#)
- ☐ **iCloud:** Update recovery information through your Apple ID settings. [Please also see Apple's guidance online.](#)

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 your signed-in devices

Regularly review devices signed into your email. If you see a device you don't recognise, it can be a strong indication your account has been compromised.

- ☐ **Gmail:** Visit Security & sign-in > Manage all devices to view and remove unfamiliar devices. [Please also see Google's guidance online.](#)
- ☐ **Outlook:** Check My Microsoft Account > Devices and remove any that you don't recognize. [Please also see Microsoft's guidance online.](#)
- ☐ **iCloud:** On account.apple.com, under Devices, review and manage all linked devices. [Please also see Apple's guidance online.](#)

Additional recommendation

If you use Microsoft Defender for Office 365, which is a paid service, you can enable [Impersonation Insight](#) to help reduce the risk of falling for an impersonated email address. You will receive warnings when you are sent emails from domains that are similar to yours but not quite the same. This means you will be alerted to someone potentially impersonating staff members or your clients.

What to check if your account has been accessed

1. Recent Activity

Look for any unusual logins from devices and locations you don't recognise.

- ☐ **Gmail:** Visit Security & sign-in > Review security events to identify unusual logins. [Please also see Google's guidance online.](#)
- ☐ **Outlook:** Check Security > Recent Activity for unfamiliar access points. [Please also see Microsoft's guidance online.](#)
- ☐ **iCloud:** Check your recent emails for recent security alerts.

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.

What to check if your account has been accessed cont.

2. Review security settings

Resecure and check for further suspicious activity.

- ☐ Ensure MFA is enabled
- ☐ Check your recovery methods are correct
- ☐ Look for any unauthorised forwarding rules
- ☐ Reset your password

3. Linked online accounts

Review all online accounts linked to your email, including both sensitive and lower-risk ones. Check accounts such as:

- ☐ Online banking
- ☐ Government accounts such as ATO and myGov
- ☐ Superannuation and insurance
- ☐ Business CRM, accounting or invoicing software and websites
- ☐ Social Media

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.