Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

EMAIL ATTACKS

EMERGENCY RESPONSE GUIDE

cyber.gov.au

What to do if your business has been targeted by email fraud or compromise

This guide has simple steps to follow if you are a victim of an email attack - whether that attack is hacking your email account or impersonating you by another method.

Maybe a friend, colleague, or service provider has received a suspicious email from 'you', but you didn't send it. The email may request payment for an invoice or ask to change bank account details.

Alternatively, maybe you noticed you are receiving unusual emails in your own email account. They may be about suspicious login activity or unexpected password resets. You might have also noticed emails have been deleted or moved to different folders.

These could be indicators of **business email compromise (BEC).**

Some of these steps may not be applicable to every situation, consider your circumstances to determine whether you should complete the relevant step(s).

Call if you need support

The Australian Cyber Security Centre has a 24/7 Hotline: 1300 CYBER1 (1300 292 371).

Call now if you need additional support and in the meantime, keep calm and read this guide. It steps you through what you can do right now to stop the attack and limit the damage.

Table of Contents

Step 1 - Report the incident

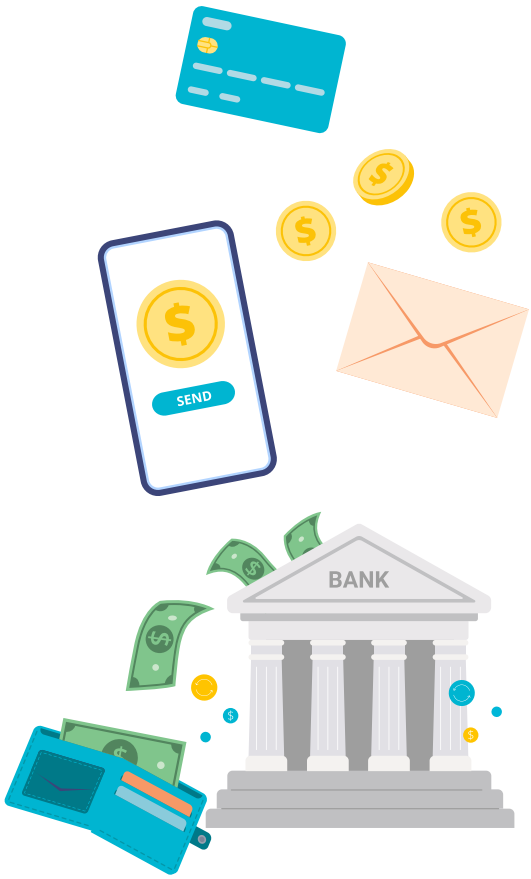
If you think your bank account or credit card details are at risk, contact your financial institution as soon as possible. They may be able to stop a transaction or disable your account. If one of your contacts has lost funds from the incident, encourage them to report to their financial institution.

You can report cyber security incidents to the Australian Cyber Security Centre (ACSC) through ReportCyber at **cyber.gov.au**.

Your report will go directly to the relevant police jurisdiction. By reporting early, you ensure the best chance of a positive outcome. Your report will also allow authorities to check for similar incidents that have occurred, assist with further investigations, and help others who have been affected.

When reporting an incident, make sure you:

- Include information in your report such as the method that was used to impersonate you, and the steps you have taken to resolve the issue (e.g. changing email password).
- Take note of your Report Reference Number (beginning with 'CIRS-') after submitting your report. This can be provided to other organisations (e.g. banks or insurance agencies).
- Remember to keep track of any further actions you take so that you can keep police and other relevant parties updated.



Step 2 - Check account security

After any email incident you should review your account security - even if you're not sure you have been hacked. Reviewing your account security will help you identify any intruders, regain control over your account, and help prevent you from getting hacked in the future.

Complete as many of the following steps as possible, or seek professional help:

1. **Change your password/passphrase**
   It's possible your old password has been compromised.
2. **Update your account recovery details**
   Cybercriminals could change the recovery details on your account to give them a back door to regain access.
3. **Sign out of all other sessions**
   Signing your email account out of all devices will remove the cybercriminal's access to your emails.
4. **Enable multi-factor authentication**
   Turning on multi-factor authentication is the most important defence against cybercriminals.
5. **Check account mail settings (including mailbox rules)**
   Check if your account has any email forwarding rules and delete any you don't recognise.
6. **Check third party application access**
   Have you ever linked your account to a third party service? Check if there are any apps or services that have access to your account and remove any that you don't recognise.
7. **Check login activity**
   Regularly review your login activity to check if your email account has been accessed at unusual times or from unusual locations.
8. **Check your email folders, devices and other accounts for suspicious activity**
   Check your email folders, specifically your sent and deleted items, to assess what actions a cybercriminal has taken.

Need further assistance?

For more detailed information on how to check your account security, read the ACSC's Guides: **Check Account Security for Gmail**, and **Check Account Security for Outlook**, available at cyber.gov.au/emailsecurity

Step 3 - Notify contacts and relevant third parties

If you have been hacked or impersonated, you should alert your contacts (such as customers, colleagues and suppliers). This will help them recognise suspicious activity and disregard fraudulent emails such as those that refer to changing of bank details, requests for large payments or unusual links or attachments.

If your email account has been compromised and has caused serious harm to your contacts, you may have further mandatory reporting requirements to your customers, as well as legal obligations to report a data breach to the Office of the Australian Information Commissioner (OAIC). For further information on the OAIC's Notifiable Data Breaches scheme, please visit the OAIC website.

Refer to the OAIC and seek legal support regarding mandatory reporting obligations: oaic.gov.au.

If you have been the victim of identity theft, contact IDCARE – idcare.org or 1800 595 160. It is a free government-funded service to assist you.

Step 4 - Send a takedown request

If someone has sent an email pretending to be you, check whether the email came from your exact email address. You might find there are slight differences in the spelling or the name of the business in the domain name (the bit after the @ sign in an email address). The use of a fraudulent domain name that looks similar to your own is known as **domain spoofing.**

If someone is using a domain name for malicious purposes or to target your business through impersonation, there are several options for you.

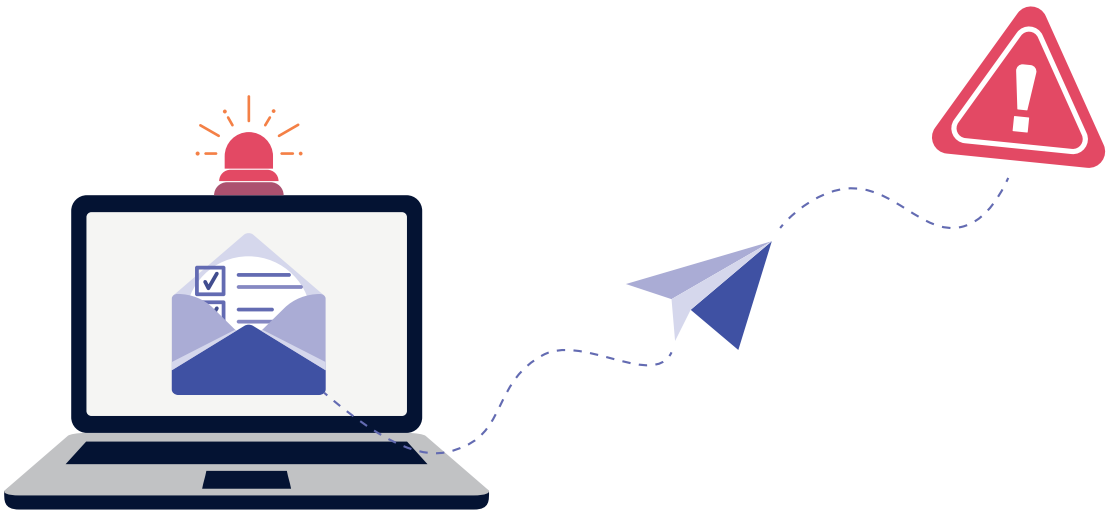
What do I do?

Submit a complaint to auDA for eligible domains.

- The **.au Domain Authority (auDA)** is the official Australian authority for domain names ending in .au, such as com.au, .net.au, and .org.au.
- If someone is using an Australian domain name that incorporates your registered business name or is a misspelling of your domain name, you can submit a complaint to auDA at auda.org.au for further advice.

Contact the registrar of the malicious domain name and request they take the domain down.

- To find out who the registrar is, you can perform a **whois lookup** for .au domains at whois.auda.org.au and for international domains at lookup.icann.org.
- If the lookup results also include a Registrar Abuse Contact Email, you can send your takedown request directly to that email address.
- If there is no abuse contact email listed, internet search to find the registrar's website and look for an abuse form or contact email there.
- Also take note of the Registrant, Registrant ID (typically an Australian Business Number (ABN) or an Australian Company number (ACN) for domains ending in .au), and Registrant Name. If someone is impersonating you, they will sometimes use your details for these fields to make the domain appear more legitimate.
- Once you have the registrar's contact details, send a takedown request with information about the fraudulent domain name and how it is similar to your own.



Step 5 - Contact the email provider

If someone is using a common email provider (such as Gmail) to impersonate you, this is known as **display name spoofing**.

Display name spoofing is a targeted attack where cybercriminals send emails using a fraudulent display name on their email account. Emails will look like they came from you, but closer inspection of the email address will show that it's incorrect.

These spoofed email addresses typically originate from Microsoft's email services (Outlook, Hotmail, Live, MSN), Gmail, or another third party email provider like ProtonMail. By using valid vendors, spoofed email addresses can bypass anti-spam or anti-phishing filters as they are not coming from forged email addresses.

If you are a victim of display name spoofing, you may be able to send an abuse report to the email service provider as abuse. They will conduct an investigation and may take action where appropriate.

You can report fraudulent email usage to the relevant email service provider:

- For Outlook, Hotmail, Live or MSN, forward the email as an attachment to abuse@outlook.com
- For Gmail, submit an abuse report at support.google.com/mail/contact/abuse
- For other email providers, refer to their websites for abuse reporting methods.

Step 6 - Protect yourself from future email cyber attacks

We have information to help you prevent a future attack:

Read through our **Email Attacks Prevention Guide** available at cyber.gov.au/emailsecurity.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre