EMAIL SECURITY
EMERGENCY RESPONSE GUIDE
Has someone hacked your email account or pretended to be you?

If someone gains unauthorised access to, or impersonates your email account, they can intercept or gain access to your private communications, or send emails pretending to be you. With access to your email account, a cybercriminal can commit fraud, or blackmail you by stealing your financial or other sensitive information. If someone is impersonating you, they can convince others to click on malicious links, open malware attachments, steal sensitive information or steal their money.

This guide will help you through a series of steps detailing simple ways you can limit the damage caused by an email compromise. The ACSC has designed this guide to cover both the situation where someone has compromised your email account directly, and when someone is impersonating you or your business. Some of these steps may not be applicable to every situation, consider your circumstances to determine whether you should complete the relevant step(s).

**STEP 1: Report to authorities**

- Report the incident to the ACSC through ReportCyber

**STEP 2: Check account security**

- If a hacker has gained unauthorised access to your email account, secure your account by completing some simple security checks.

**STEP 3: Notify contacts and relevant third parties**

- Alert your clients, colleagues, and other contacts so they can be aware of suspicious emails. Certain businesses have mandatory reporting obligations with regards to customer data breaches.

**STEP 4: Send a takedown request**

- If someone is impersonating you with a similar domain name, contact the registrar of the malicious domain and send a request to take the domain down.

**STEP 5: Contact the email provider**

- If someone is using an email service such as Gmail or Outlook.com to impersonate you, you can report this to the provider as abuse.

**STEP 6: Protect yourself**

- We recommend reading the ACSC Email Security – Prevention and Protection guide to help avoid this happening again in the future.

**A CASE STUDY: Saffron Conveyancing**

Follow the fictional story of the Saffron Conveyancing small business and the steps they took when they fell victim to an email impersonation attack.
Introduction

What’s happening?

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.

We understand an email attack may have you feeling pressured, panicked, or stressed. Keep calm and follow this guide to stop the attack and limit the damage.

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.

Do these steps now

Follow these steps to take simple, immediate actions to reduce the impact of an email attack and what’s important to you: your money, business, data, and reputation.

Step 1

Report to Authorities

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

Your report goes directly to the relevant police jurisdiction. By reporting early, you ensure the best chance of a positive outcome. It doesn’t matter if you have incomplete information as you can update police on any further actions you take.

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.

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 as proof of a police report being submitted (e.g. for 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 as the situation progresses.

---

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report to the ACSC on ReportCyber</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report to any involved banking/financial institution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(if money has been lost or transferred)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 to identify any intruders, regain control over your account, and help prevent you from getting hacked in the future.

When checking your account security, you should do the following:

1. Change your password/passphrase
2. Update your account recovery details
3. Sign out of all other sessions
4. Enable multi-factor authentication
5. Check account mail settings (including mailbox rules)
6. Check third party application access
7. Check login activity
8. Check your email folders, devices and other accounts

Need further assistance?

For more detailed information on how to check your account security, read the ACSC’s Step-by-Step Guide: Check Account Security for Gmail and Check Account Security for Outlook, available at cyber.gov.au.

Notify contacts and relevant third parties

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

You can use the below template to email your contacts and make them aware of suspicious activity.

To our contacts,
We have recently identified that <insert your organisation’s name> has been a target of fraudulent cybercriminal activity. We became aware on <insert incident date(s)>, that a malicious actor sent emails to our contacts impersonating our business and our staff. These emails may have related to invoices, requests for large transfers, or to change banking details for payments. The emails were sent by the following email address: <insert hacked or impersonated email address>.

If you received an email from <insert your organisation’s name> that matches this description, please ignore the email’s content and send it to us for further investigation. You may want to check with your bank whether any payments were made to the fake invoice or the fraudulent bank details.

We encourage all of our contacts to remain vigilant and pay close attention to any suspicious emails. The cybercriminal may be copying our email signatures, our names, and our email addresses. If you receive an email from <insert your organisation’s name> and are not sure if it’s legitimate, please contact us for confirmation using a phone number you know to be correct.

Sincerely,
<Insert your organisation’s name>.

As you make progress in responding to your hacked email account, you may wish to consider updating your contacts about any significant progress made regarding the incident. 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: www.oaic.gov.au.

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 to identify any intruders, regain control over your account, and help prevent you from getting hacked in the future.

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check the security on your email account(s).</td>
<td>☐</td>
<td>___ / ___ / ___</td>
</tr>
</tbody>
</table>

Record the date and time that you undertook any action so you can keep police informed about the situation.

Refer to the Office of the Australian Information Commissioner and seek legal support regarding mandatory reporting obligations: www.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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify your contacts (customers, colleagues, family and friends, suppliers, etc) to alert them to any suspicious activity.</td>
<td>☐</td>
<td>___ / ___ / ___</td>
</tr>
</tbody>
</table>

Record the date and time that you undertook any action so you can keep police informed about the situation.
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 spelling or the name of the business (in the bit after the @ sign of the email address). The use of a fraudulent domain name which 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.

Who you can contact

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 for further advice.

You can also contact the registrar of the malicious domain name and request they take the domain down. Domain registrars are businesses authorised to register domain names on behalf of a customer. Find the registrar’s contact details, so you know where to send the takedown request. You can find this information by doing a whois lookup of the domain name used to impersonate you. You can perform a whois lookup for .au domains at whois.auda.org.au and for international domains at lookup.icann.org.

What can you do

Look for the Registrar Name in the whois lookup results. This is the company who manages the domain name. 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, you can use the following template to send a takedown request:

Template: Takedown Request for Spoofed Domains

To the abuse team at <registrar company name>: <Y our organisation’s name> would like to lodge an official abuse complaint against the following domain name which operates in your jurisdiction:

- Lookalike domain name:

We believe this domain name was registered in bad faith. It is confusingly similar to our domain name (<your organisation’s domain name>) and has been used to impersonate our business and scam our clients/customers/contacts.

- Description of scam or fraudulent activity, including screenshots where possible:

Open source information shows that <registrar company name> is the current registrar of <lookalike domain name>. We request you take down the offending domain name as soon as possible.

- Delete this paragraph, unless the lookalike domain name used your details for the Registrant, Registrant ID (ABN), and/or Registrant Name: We have also noticed that the offending domain name uses our organisation’s details for the (Registrant/Registrant ID/Registrant Name) field(s). Please advise what identification or details we can provide in order to claim this domain name and have it taken down or transferred.

Thank you for your assistance. Should you require additional information, please feel free to contact us.

- Insert your organisation’s name>

<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find out who manages the domain name by doing a whois lookup at whois.auda.org.au for .au domains, and lookup.icann.org for international domains.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify the Registrar Abuse Contact Email from the whois results, or from the registrar’s website.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send a takedown request to the registrar abuse contact email.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Record the date and time that you undertake any action so you can keep police informed about the situation.
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.

For example, an email may appear to be from “Saffron Conveyancing” but the email address is “sdfjfdafs@gmail.com”.

Success of these attacks rely on whether or not your contacts recognise the email address matches the displayed name. This is trickier to do so on smart phones, where some email applications don’t show the sender’s email address – only their display name.

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.

For spoofed emails using Outlook, Hotmail, Live or MSN, you can forward the email as an attachment to abuse@outlook.com.

If someone is using a Gmail address to impersonate you, submit an abuse report at support.google.com/mail/contact/abuse.

For other email providers, refer to their website for abuse reporting methods.

Step 6

Protect yourself

WHAT NEXT?

Now that you have responded to your current email attack (as best you can), we recommend reading the ACSC Email Security – Prevention and Protection guide to help avoid this happening again.

Available at cyber.gov.au.

The Australian Cyber Security Centre (ACSC) is here to help make Australia the most secure place to connect online. The ACSC, as part of the Australian Signals Directorate (ASD) provides cyber security advice, assistance and operational responses to prevent, detect and remediate cyber threats to Australia.
Saffron Conveyancing

Sabrina works as a receptionist for a small conveyancing business called “Saffron Conveyancing”. The business is owned by Gary, who employs four staff members (including Sabrina) and leases a small office space in the city.

Saffron Conveyancing has five email accounts – one for each staff member (e.g. gary@saffronconveyancing.com.au), and a generic reception@saffronconveyancing.com.au account that is managed by Sabrina. This reception account receives customer enquiries and is the main point of contact for the business.

While Gary was away on annual leave, he sent an email to the reception email address advising that he had just changed banks. The email included the new bank account details and asked if it could be updated for the next pay cycle, which was in a few days’ time.

Sabrina provided the new details to her colleague who was responsible for payroll and asked them to update Gary’s banking details as soon as possible.

The Cyber Security Incident

A week later, Gary had returned to work and asked his staff why his payslip hadn’t been sent out. When they realised Gary was the only one who hadn’t been paid, the staff member responsible for payroll mentioned that it might be an issue with his new bank.

This took Gary by surprise as he didn’t have a new bank. Sabrina showed him the email, which Gary had no recollection of. On closer inspection Sabrina noticed a spelling error in the email address:

Legitimate email address: gary@saffronconveyancing.com.au
Impersonated email address: gary@saffronconveya.cn.com.au

Gary immediately contacted Saffron Conveyancing’s bank but it was too late, the funds had already been transferred to the fraudulent account.

Applying Cyber Security First Aid

Sabrina outlined the situation, and submitted a report to the police through ReportCyber on cyber.gov.au (page 2). She included the steps they had taken so far, as well as a plan for other actions they were about to take.

All staff members reviewed the security settings on their email accounts (page 3) in case a cybercriminal had gained access and was spying on their emails.

Saffron Conveyancing then notified all of their clients and contacts (page 4) that a malicious actor was impersonating their business. They advised that the malicious actor may be targeting the contacts with financial scams and warned everyone to be aware of suspicious emails that appear to be from Saffron Conveyancing.

They looked up the registrar of the fraudulent saffronconveya.cn.com.au domain name and sent them a takedown request (page 5 and 6) to shut down the domain.

Finally, they also sent an official complaint to auDA (page 5). They explained how this fraudulent domain name was a deceptive misspelling of their legitimate domain name and was in breach of auDA’s policies.

Outcome

Following the incident, Gary decided to introduce a new policy for his business. Whenever someone receives an email request to change bank details for staff or clients, they must ring the sender of the email using a phone number they know to be correct to confirm that the request is legitimate.

Additionally, Gary sought advice from the ACSC’s Small Business Cyber Security Guide and rolled out cyber security awareness training to his employees.

While the money they had already lost could not be recovered, the malicious saffronconveyacning.com.au domain name was successfully shut down before further harm could be done. After notifying everybody about the impersonation, a few contacts advised that they had received suspicious emails, but since then there were no additional reports.

Thanks to Saffron Conveyancing’s quick actions, there were no further victims of this cybercrime.
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.

Copyright

© Commonwealth of Australia 2021.

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).
For more information, or to report a cyber security incident, contact us:

[cyber.gov.au](http://cyber.gov.au)  |  1300 CYBER1 (1300 292 371)