Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

EMAIL ATTACKS
PREVENTION GUIDE

cyber.gov.au

Table of contents

Protect your business from email fraud and compromise.

This guide will help protect your business from an email security incident. Use this table of contents as a checklist as you work through the steps in this guide.

Let’s get started

Introduction

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. This could result in fraud, with cybercriminals intercepting financial transactions such as invoices (often referred to as business email compromise). Cybercriminals could also use your email account to convince others to click on malicious links, open malware attachments, or share sensitive information.

Preventative and protective measures are simple, cost effective and immediately beneficial.

Why do I need to protect myself from email attacks?

Email is a common target for cybercriminal activity. If someone gains unauthorised access to your email account, they now have access to your private communications. A cybercriminal could steal your sensitive information, or even commit fraud and send emails pretending to be you.

A common email attack is **business email compromise.** Business email compromise is when criminals use email to abuse trust in business processes to scam organisations out of money or goods. Criminals can impersonate business representatives using similar names, domains and/or fraudulent logos as a legitimate organisation or by using compromised email accounts and pretending to be a trusted co-worker.

Why would a cybercriminal hack or impersonate me?

Aside from stealing your information or damaging your reputation, the goal of these attacks is usually to scam your contacts into sending funds to a fraudulent bank account that is operated by the scammer. The ACSC Annual Cyber Threat Report 2020-21 puts self-reported losses for business email compromise at $81.45 million for the 2020-21 financial year. In the same period, business email compromise made up nearly 7% of all cybercrime reports made to the ACSC.

Account hacking and email impersonation are common delivery methods for cybercriminals to send fake invoices, fraudulent bank details, phishing emails, or malicious attachments. These activities can capture sensitive information and infect you and your customers' devices.

Email attacks are very common, as it can be difficult for the recipient to detect scam emails. This is especially difficult when they are tricked into thinking it was sent from someone they know and trust.

What can I do?

This guide will step you through simple ways you can limit the damage caused by an email attack. Whether that attack is hacking your email account or impersonating you by another method, the ACSC has you covered.

If you are currently experiencing **AN EMAIL ATTACK** or other cyber security incident, contact the Australian Cyber Security Centre 24/7 Cyber Security Hotline:

1300 CYBER1 (1300 292 371) or asd.assist@defence.gov.au

You can also refer to the ***ACSC's Email Attacks – Emergency Response Guide***, available at **cyber.gov.au**

Step 1

Turn on multi-factor authentication

Multi-factor authentication (MFA) typically requires a combination of something a user knows (PIN, password/passphrase) and something a user has (smartcard, physical token) or something a user is (fingerprint or other biometric).

MFA makes it harder for cybercriminals to gain initial access to your email accounts, services and information by making them jump through more security hoops and additional authentication layers. This means the cybercriminal will have to spend more time, effort, and resources to get into your account before any attack can begin.

For more information on MFA, visit **cyber.gov.au/mfa.**

Action	Completed	Date and Time
Turn on multi-factor authentication on all services, devices, software applications and third party websites storing your data.	○	____/____/____ ___ : ___ am/pm

In cases where MFA is not available, a unique strong passphrase can often be the only barrier between adversaries and your valuable information and accounts. Passphrases use four or more random words as your password, and are most effective when they are long, unpredictable and unique.

Find more information on creating strong passphrases at **cyber.gov.au/passphrases**.

Protect your domain names

A domain name is a string of characters, often words, that identities you or your business to other people using the Internet. This is the text that typically comes after the "@" symbol in an email address.

The most common uses of a domain name are for websites and email – for example, instead of sending email from cinnabarhomes@gmail.com, a business owner can send from an address such as blaine@cinnabarhomes.com.au.

If your domain name expires, it will become available for anyone to purchase. A criminal could purchase this domain name and use it to impersonate you or your business by setting up an email address and contacting your customers.

Your customers or contacts may recognise your domain name and believe you are still operating that email address, when in fact they are really corresponding with a cybercriminal. The cybercriminal could abuse this trust to add authenticity to their criminal activity.

If you had any accounts or services attached to that older domain name (e.g. Microsoft 365), a criminal could also capture password reset emails for those accounts and use them to gain further control of your information and online identity.

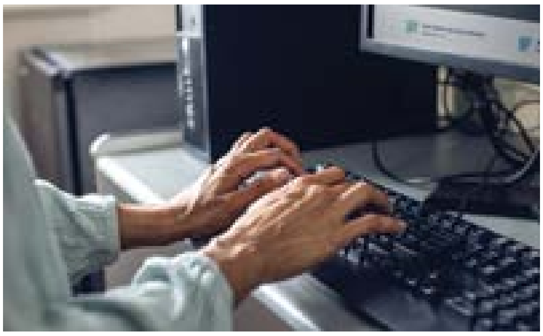
Remember to renew your domain names, even if you don't use them anymore.

The time and money spent renewing a domain name is minimal. However, if a business fails to do this, the domain name can easily end up on a 'dropped domains' website for others to register, which could be used to impersonate you or your business.

Action	Completed	Date and Time
Find out when your domain names expire, and set a reminder in your calendar to renew them ahead of their expiry.	○	____ /____ /____ ___ : ___ am/pm

If you have let any old domain names expire, make it a priority to repurchase them – before someone else does.

Register additional domain names



A common fraud method cybercriminals use is to register a domain name which looks very similar to your business name. At a glance, email addresses made through fraudulent domain names may look similar enough to your own that your contacts may not realise they are not emailing the real you.

Using paypal.com as an example, here are some common lookalike domain name tricks that a cybercriminal might use to try and confuse someone.

Legitimate domain name	paypal.com
Remove letters	pypal.com
Add letters	payp**p**al.com
Add additional words	paypal**online**.com
Use a different domain extension	paypal.**net**, **paypal.au**
Rearrange letters	pay**apl**.com
Add a hyphen	pay-pal.com
Add www to the start of the domain name	**www**paypal.com
Rearrange parts of the domain name	paypal-**au**.com
Replace letters with similar characters (e.g. numbers, capital letters or symbols)	paypa**1**.com paypa**I**.com p**à**ypal.com

To help prevent this attack, consider registering similar domains to your own that could be used to mislead someone.

Action	Completed	Date and Time
Register similar domain names that could be used to mislead someone.	○	____/____/____ ____ : ____ am/pm

Step 4

Set up email authentication measures

If you have your own business domain which you use for emailing, setting up email authentication protocols on your domain may help to prevent email spoofing attacks. This is where a cybercriminal sends an email pretending that it's from your email address, without ever having to hack your email account.

Email spoofing is like sending a letter and forging who it was written by. Anyone can write a return address on an envelope; it doesn't mean that's where it's truly from.

Email spoofing occurs when someone forges the "From:" field of an email to say that it was sent from an email address other than their own.

If someone tries to spoof your email address, setting up email authentication protocols will identify that those emails are not legitimate. These protocols help prevent spoofed emails from making it to their destination – they will normally go either to the recipient's spam folder, or won't be delivered at all.

Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) are all email authentication protocols which may be used to strengthen email security and mitigate the risk of cybercriminals spoofing your email addresses.

Action	Completed	Date and Time
Have a discussion with your service provider about adding SPF, DKIM, and DMARC records to your domain name. If your DNS hosting is with a separate provider, you will need to contact them also.	○	____ /____ /____ ___ : ___ am/pm

To find out more, read the ACSC's ***How to Combat Fake Emails*** guidance on **cyber.gov.au.**

Step 5

Protect your privacy

Cybercriminals can learn a lot about someone by doing a simple Google search. This information helps a cybercriminal appear more credible if they pretend to be you in an email.

Protecting your identity online can go a long way in reducing the chances of being impersonated. Be careful posting information online that identifies where you work, what your position is, or your work email address, as these details can be used to impersonate you. The more information a cybercriminal can discover from public sources, the more convincing a potential scam can be.

Joel regularly posts about his consulting company on his personal Facebook account, and recently mentioned finishing up a contract with Devon Corp. When he sent an invoice for the last portion of the work, his contact at Devon Corp said that they had already paid and showed a copy of the payment, which went to a different bank account that he did not recognise.

Avoid having your email addresses (both personal and business) publicly listed on the internet.

If your email address can be found on various websites or forums, it may become a target for impersonation.

Action	Completed	Date and Time
Review your social media accounts and online presence to see if there is any sensitive information online that could be used to impersonate or spoof you or your business.	○	____/____/____ ___ : ___ am/pm
Visit ACSC on cyber.gov.au for up to date advice and security tips for social media and networking applications	○	____/____/____ ___ : ___ am/pm

For more information about how to manage your information online, visit the Office of the Australian Information Commissioner at **oaic.gov.au**.

Step 6

Implement policies and procedures

Your staff are the last line of defence against fraudulent email attacks.

If a staff member receives an email from a customer, colleague, or supplier with an unusual or unexpected request, they should determine if the email is legitimate before actioning the request.

If a link in an email looks legitimate, open a web browser window and type the address in manually rather than clicking on a link which may be compromised.

Consider introducing an approval process for requests that ask to change payment details or make a large transfer. You should verify any such requests by calling the sender using a known, verified number (not a number from the email). Speak with the sender over the phone to verbally confirm the request or change.

Ensure workers have clear guidance to verify account details, to think critically before actioning unusual requests, and have a reporting process to report threatening demands for immediate action, pressure for secrecy or requests to circumvent protective business processes.

Create a good cyber security culture by rewarding and recognising employees who report potential threats, and encourage regular cyber security discussions to increase awareness across your organisation.

Action	Completed	Date and Time
Introduce policies and procedures into your business to address security risks.	○	____ /____ /____ ___ : ___ am/pm

Step 7

Training and awareness

The best defence against email scams is training and awareness for your employees, including how to identify scams and protect your business from cybercriminals. Ensure that your staff know to always be cautious of emails with the following:

- **Requests for money, especially if urgent or overdue**
- **Bank account changes**
- **Attachments, especially from unknown or suspicious email addresses**
- **Requests to check or confirm login details.**

Teach your employees the value of good cyber hygiene – don't reuse passwords or passphrases on different accounts, and think before clicking on links or sharing information online.

Make sure that your staff are aware of any new policies or processes that you have implemented in Step 6 (page 8).

Action	Completed	Date and Time
Incorporate, update and regularly repeat cyber security training and awareness amongst your employees.	○	____/____/____ ___ : ___ am/pm

For more information about identifying phishing attacks and other good cyber security practices, visit **cyber.gov.au.**

Step 8

Remain vigilant and informed

While it is one thing to have built up your defences to protect your information, it is best to remain on the lookout for evolving cyber threats and trends which could impact you at any time.

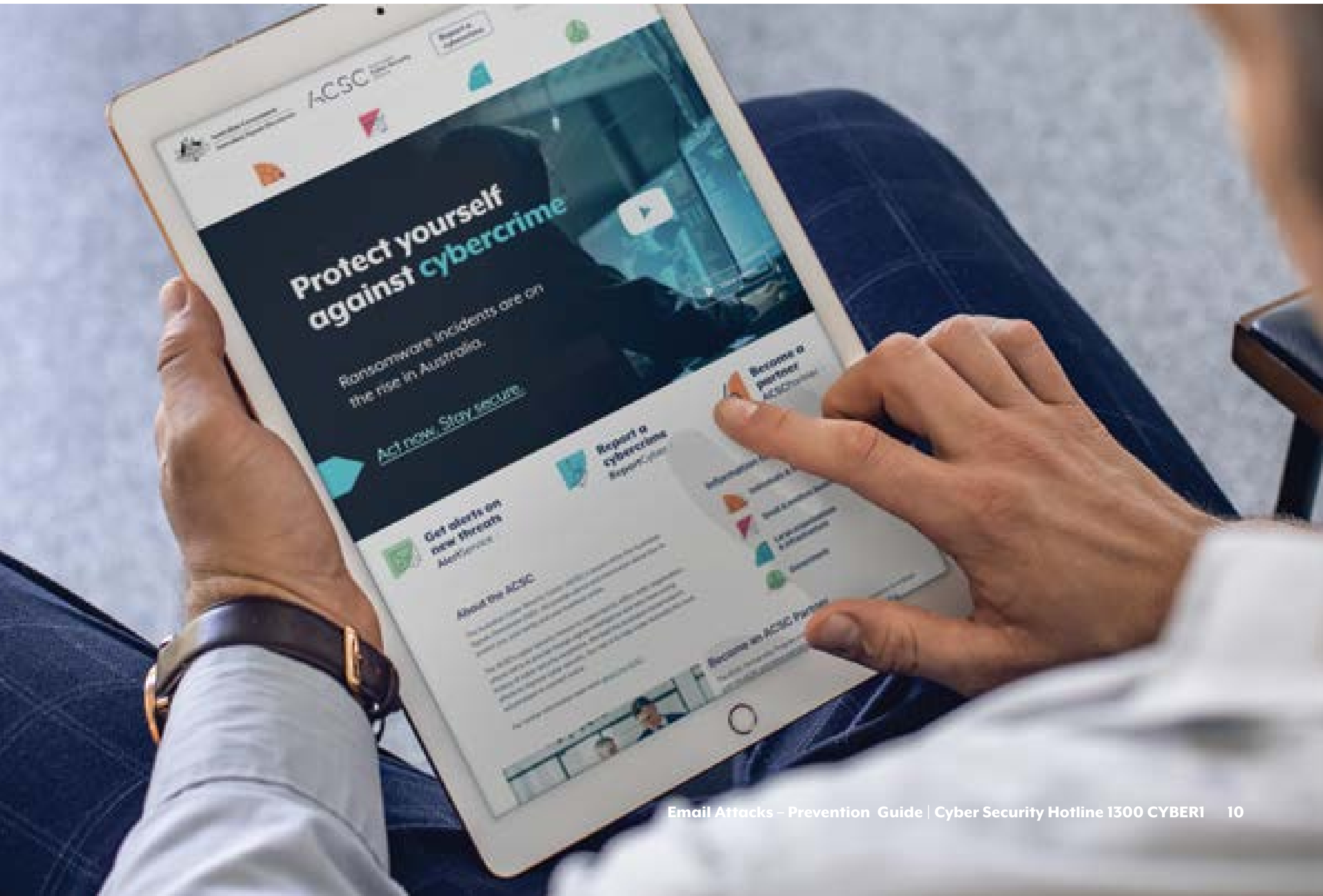
Consider becoming a partner of the ACSC, which will give you access to timely information to assist in keeping your systems and networks safe.

The ACSC Partnership Program enables a wide range of organisations to engage with the ACSC and fellow partners, drawing on collective understanding, experience, skills and capability to lift cyber resilience across the Australian economy.

We have three streams of partners:

- **Network Partners** – for organisations with responsibility for networks, experts in cyber security such as academics and not-for-profit institutions.
- **Business partners** – for businesses, large or small, that would like to be kept up to date with relevant cyber security information for their businesses.
- **Home partners** – for individuals and families that would like to be kept up to date with relevant information.

To learn more, visit **cyber.gov.au**.


ACSC
Protect yourself against cybercrime
Ransomware incidents are on the rise in Australia.
Act now. Stay secure.
Get alerts on new threats
Report a cybercrime
Become a partner
About the ACSC
Become an ACSC Partner

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

Use of the Coat of Arms

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