Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

EMAIL ATTACKS PREVENTION GUIDE

cyber.gov.au

Protect your business from email fraud and compromise

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**. Criminals can impersonate business representatives by using compromised email accounts, or through other means – like using a domain name that looks similar to a real business. 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 bank account operated by the scammer.

This guide will help protect your business from business email compromise. **Protective measures are simple, cost-effective and immediately beneficial**.

Protective measures can help by:

- preventing your email accounts from being compromised
- making it harder for a cybercriminal to impersonate you
- protecting your business from falling victim to email fraud

Table of Contents

Step 1 - Turn on multi-factor authentication

Having multi-factor authentication increases the security on your email account. Multi-factor authentication means there are two checks in place to prove your identity before you can access your account. For example, you may need to supply an authentication code from an app as well as your password.

It makes it more difficult for someone to access your email account.

For more information, read our advice on multi-factor authentication, available at cyber.gov.au/mfa.

Remember to use a strong passphrase for your email account if you cannot use multi-factor authentication. Find out more at cyber.gov.au/passphrases.

Step 2 - Protect your domain names

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

If your domain name expires, it will become available for anyone to purchase. A criminal could purchase your previous 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.

Remember to renew your domain names, even if you don't use them anymore. This will stop your digital identity from falling into the wrong hands.

Find out when your domain names expire and set a reminder in your calendar to renew them ahead of their expiry.

Step 3 - 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.

Consider registering similar domain names that could be used to confuse your contacts.

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

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**ap**l.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**l**.com p**à**ypal.com

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 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.

Have a discussion with your service provider about adding Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) records to your domain name. If your DNS hosting is with a separate provider, you will need to contact them also.

Step 5 - Protect your privacy

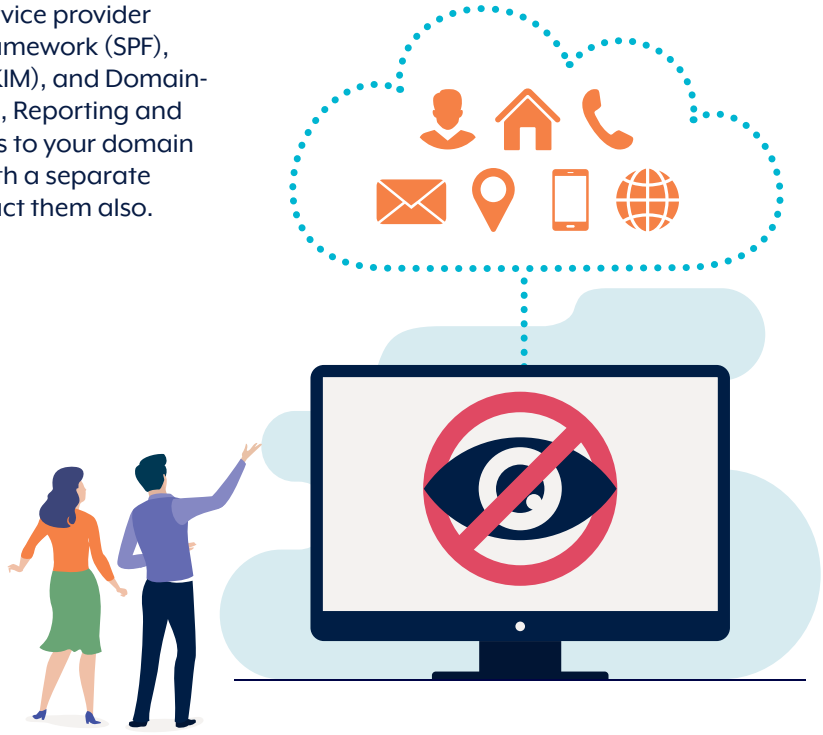
Cybercriminals can learn a lot about someone by doing a simple Google search. This information helps a cybercriminal appear more credible if they pretend to be you in an email.

Be careful posting information online that identifies:

- where you work
- what your position is
- your work email address
- your personal email address

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

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



To find out more, search "**How to Combat Fake Emails**" at cyber.gov.au.

Step 6 - Implement policies and procedures

If a staff member receives an email from a customer, colleague, or supplier with an unusual or unexpected request, they should find out if the email is legitimate before actioning the request. To ensure this, introduce policies and procedures to address security risks and help keep your business secure.

For example:

- Consider introducing an approval process for requests that ask to change payment details or make a large transfer.
- Verify such requests by calling the sender. Call them on a known and verified phone number (not a phone number from the email, as this could be operated by a cybercriminal). Speak with the sender over the phone to verbally confirm the request or change.
- Ensure workers have clear guidance to verify account details and to think critically before actioning unusual requests.

Have a reporting process to report threatening demands for immediate action, pressure for secrecy or requests to circumvent protective business processes.

Step 7 - Training and awareness

The best defence against email scams is training and awareness for your employees, including how to identify scams or phishing attempts. Ensure 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
- unexpected or suspicious links

Incorporate, update and regularly repeat cyber security training and awareness amongst your employees to protect your business from cybercriminals.

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. Stay up to date on cyber security threats and trends by becoming an ACSC Partner.

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** who would like to be kept up to-date with relevant information.

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