

## Client eBrief



<https://mevansbookkeeping.wixsite.com/website>

TEL: 0481 555 023

ABN: 51 140 069 827



## ATO Lodgement Dates

These dates are from the ATO website and do not account for possible extensions.

You remain responsible for ensuring that the necessary information is with us in time.

See [ATO Due dates by month](#) to check monthly lodgment and payment dates.

### **BAS/IAS Monthly Lodgements**

Final dates for lodgements and payments:

November Activity Statement  
21 December 2021

December Activity Statement  
21 January 2021

### **BAS Quarterly Lodgements**

Final dates for lodgements and payments:

**2nd Quarter 2022 Financial Year:**  
**December Quarter 2022 (incl. PAYGI)**  
28 February, 2022

**3rd Quarter 2022 Financial Year:**  
**March Quarter 2022 (incl. PAYGI)**  
28 April, 2022

When a due date falls on a Saturday, Sunday, or Public Holiday\*, you can lodge or pay on the next business day.

\*A day that is a public holiday for the whole of any state or territory in Australia.

Due date for super guarantee contributions:

**2nd Quarter 2022 Financial Year:**  
October to December 2022 – contributions must be **in the fund** by 28 January, 2022

**3rd Quarter 2022 Financial Year:**  
January to March 2022 – contributions must be **in the fund** by 28 April, 2022

Late payments of superannuation are **not** tax deductible. If your business has overdue superannuation guarantee payments and you are unsure of how to proceed, please contact us to discuss.

## The Fair Work Ombudsman has a New Website

The [Fair Work Ombudsman's website](#) assists employers and employees to find information about the various stages of employment.

Now with a new design and structure it will be easier for employers and employees to access information and advice on any type of device and in most languages. The improved search function will support finding information easier.

The Fair Work Ombudsman's new page has the same content and functionality of most tools, and the resources remain unchanged, including their [Pay and Conditions Tool](#).

### Updated Structure

The Fair Work Ombudsman have re-organised some of their information and resources into clearer, simpler pathways to help employers and employees find the information they need quicker.

The [Pay](#), [Leave](#) and [Ending Employment](#) sections won't change significantly, with 'Pay' being re-labelled to 'Pay & Wages'. They are also re-organising existing information to create two new sections:

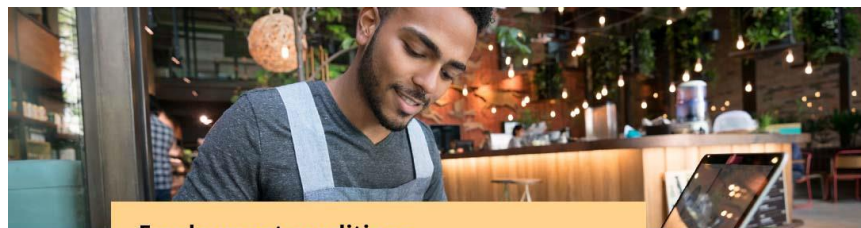
### Starting Employment



This new section will bring together information and resources for employers and employees before or at the start of the employment relationship. It will include information about:

- Hiring employees
- Before starting employment
- Probation
- Types of employees (for example, full-time, part-time, casual, shift workers)
- Unpaid work (for example, work experience, trials, and student placements).

## Employment Conditions



**Employment conditions**

Designed for people looking for information about employment conditions for current employees, this section will bring together information on topics such as:

- Awards and agreements
- Hours of work (including breaks, rosters and RDOs)
- Public holidays
- Flexible working arrangements
- Discrimination, bullying and harassment
- Workers compensation
- Industrial action and union membership
- Performance in the workplace.

For more information see: [Home](#) | [Fair Work Ombudsman](#)



## Cyber Security & Protecting Your Business

A cyber security incident that impacts a small business can be devastating. Unfortunately, those at the Australian Cyber Security Centre (ACSC) see the impact of cyber security incidents each and every day, on individuals, large companies, and small businesses.

As part of a larger Government agenda we all need to play a small part in the national objective of protection against cybercrime, ACSC are reaching out to small/medium business to assist with the basic foundations and techniques to protect small business against critical cyber related attacks.

### During the 2020-21 Financial Year the ACSC Observed

- Over **67,500** cybercrime reports, an increase of nearly **13%** from the previous financial year.

- Self-reported losses from cybercrime total more than **\$33 billion**.
- Approximately **one quarter** of reported cyber security incidents affected entities associated with Australia's critical infrastructure.
- Over **1,500** cybercrime reports per month of malicious cyber activity related to the coronavirus pandemic (approximately 4 per day).
- More than **75%** of pandemic-related cybercrime reports involved Australians losing money or personal information.
- Nearly **500** ransomware cybercrime reports, an increase of nearly **15%** from the previous financial year.
- Fraud, online shopping scams and online banking scams were the top reported cybercrime types.
- An increase in the average severity and impact of reported cyber security incidents, with nearly half categorised as 'substantial'.

**Source:** [ACSC Annual Cyber Threat Report 2020-21 | Cyber.gov.au](#)

## What are the Most Common Cyber Threats

### The Fake Invoice Scam or Phishing

Let's start with arguably the most popular phishing template out there - the fake invoice technique. Phishing emails are used by cybercriminals and are created to look like official messages, mimicking phrasing, and logos from well-known organisations. Phishing emails ask for a variety of personal information, passwords, and credentials, leading to compromised digital systems.

Like many phishing attacks, this scam relies on fear and urgency, pressuring an end user to submit a payment for goods or services they've never even ordered or received. Time pressure emails are high risk so be aware and if in doubt verify details through a known contact. You need to know you are dealing with a legitimate authority. The Accounting and Bookkeeping community are the obvious targets for this sort of attack. Invoice fraud is quite common and can bypass security systems.

To verify if an email or message is legitimate, find a source you can trust! Visit the official website or call the advertised phone number. Do not use the contact details provided in the email or message, as these could be fraudulent also.

### Business Email Compromise

Business email compromise is a type of email cybercrime scam in which an attacker targets a business to defraud the company. Business email compromise is a large and growing problem that targets organisations of all sizes across every industry around the world. These scams have cost businesses billions of dollars in potential losses.

Email account compromise, or email account takeover, is a related threat that is increasing in an era of cloud-based infrastructure. These scams are difficult to detect and prevent. They leave businesses vulnerable to attacks, potentially leading to identity theft and compromising systems with businesses experiencing significant financial loss as well as compromised access to business and loss of personal information.

### Ransomware

Ransomware attacks are typically conducted via malicious, but legitimate looking email links or attachments. A ransomware attack is a form of malware attack in which an attacker seizes the user's data, folders, or entire device until a 'ransom' fee is paid. Ransomware attack exploits the open security vulnerabilities by infecting a PC or a network with a phishing attack, or malicious websites. Ransomware are legitimate looking links but the link, when opened locks the organisations files until a ransom fee is paid. The ACSC advise is not to pay but to seek ACSC advice if this happens to your business.

## How Cyber Mature is Your Business?

**Use the Assessment Tool and Find Out! See:** [Cyber Security Assessment Tool | Cyber.gov.au](#)

Disclaimer: All or any advice contained in this newsletter is of a general nature only and may not apply to your individual business circumstances. For specific advice relating to your specific situation, please contact your accountant or contact me for further discussion.

**Evans Bookkeeping Services**

Tel: 0481 555 023

Email: [evans.bookkeeping@outlook.com](mailto:evans.bookkeeping@outlook.com)

This newsletter is produced by the Institute of Certified Bookkeepers and distributed by members.

