Australian Government
Department of Industry, Science, Energy and Resources

Be COVID Fraud Aware

Scammers target small business because they recognise that owners are busy and usually have limited resources to keep their systems safe. This risk has increased as a result of the COVID-19 pandemic.

The latest COVID-19 scams are designed to take advantage of the changes to our daily life – including loss of jobs and financial vulnerability, fear of infection and the shortage of particular goods and services.

This guide is intended to highlight some of the common scams to be aware of, and show you where to get further information and assistance.

Common scams to look out for

Phishing

Phishing is when scammers **impersonate** a **government department or trusted business** to obtain your personal, business or financial information**.** Phishing can lure you into providing those details, or prompt you to **click on links or attachments that download software that steals this information, or even damages your device**.

For example, look out for emails, SMS texts, instant messages and social media posts:

- With links claiming to have important updates about the latest COVID-19 safety measures, or claiming to have information on the location of possible COVID-19 cases in your area.
- Pretending that you or your employees have been in a COVID affected area and asking for personal information.
- Offering to help you access a government 'benefit' or 'subsidy'.
- Pretending to assess you or your employees' eligibility for the vaccine, or placing you on a fake waitlist.

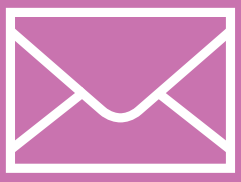
Fake charities

Scammers may **pose as charities** collecting money for people affected by COVID-19. They can either pretend to be a well-known charity, or create their own charity name. Often, they pick a name that sounds close to a real charity, and set up fake websites that look similar to those run by the real charity.

Business email compromise

Scammers may **pretend to be a supplier or employee** (including by compromising their email account or using their company logo and branding) to request payment or change bank details.

For example, they may pose as a supplier and use COVID-19 as an excuse to request that you send your usual account payments to a different bank account.



Supply scams

Supply scams use **fake websites** and **social media pages** to sell you products related to COVID-19 that you never receive, such as hand sanitisers, gloves or surgical masks. They may also offer to sell non-existent products that claim to prevent or cure COVID-19.

As the COVID-19 vaccine rolls out in Australia, scammers may ask you to **pay for a vaccine, or get early access to a vaccine**, for you or your employees. Be aware that COVID-19 vaccines are **voluntary, free and available** to all people living in Australia. You cannot pay to get early access. Also be aware that scammers may try to sell fake COVID-19 vaccine certificates and related documents.

How can you protect your business?

Some things to keep in mind:

- Genuine emails about online government or businesses services will not include links to sign in pages, or ask for your personal information, account details, PIN or passwords.
- If you are unsure if the email, call or SMS you have received is genuine, **do not click any links or open any attachments**, and contact the organisation using contact details that you've found yourself (e.g. using a search engine like Google).
- If you are unsure about a change to a supplier or employee's bank account details, call them to confirm even if an explanation is provided by email.
- Genuine charities will likely be registered. You can check this using the Australian Charities and Not-for-Profits Commission website.
- Make sure your business computers have up-to-date security software.
- Train your staff to be on the lookout for scams or anything unusual.

Protecting your customers

The **Office of the Australian Information Commissioner** has tips on how to protect the personal information provided to you by your customers and a guide to securing personal information (which includes examples for businesses).

To reduce the risk of someone impersonating your business:

- Advise your customers that you will never contact them to ask for their customer login or payment card information.
- Monitor who is mentioning your business name online using a tool like Google Alerts.
- Create strong passwords for your business accounts and update passwords when there are staffing changes.

What if you are scammed or want to report a scam?

You can report any scams to SCAMwatch.

If you have sent money or banking details to a scammer, contact your bank immediately. You are also encouraged to contact your local police, or report it to ReportCyber if the contact has taken place online.

If a scammer is impersonating your business:

- Consider if the matter should be reported to ReportCyber.
- Warn your customers about the scam, and place a notice on your website.
- Report any fake social media accounts to the platform so they can be shut down.
- If any of your email accounts have been compromised, change your password for those account(s).

Where do I get further information?

Remember that the look, feel and content of scams can change daily. Regularly visit the SCAMwatch website run by the **Australian Competition and Consumer Commission** to find further information on how to protect your business, and keep up to date on the latest scams.

Other useful sources of information:

- The **Australian Cyber Security Centre** provides advice and information about how to protect your business online. This includes a Small Business Cyber Security Guide and information on Quick Response codes in a COVID-19 environment.
- The **business.gov.au** website contains information on cyber security and your business and tips to identify authentic government grant sources.
- The **Department of Health** regularly updates its website with information on COVID-19, including vaccines. You can also call the COVID-19 hotline on 1800 020 080, or use the Vaccine Clinic Finder (available via the eligibility checker) to find an authorised vaccine clinic near you and make an appointment.
- The **Australian Tax Office** has a range of information on protecting your business, plus easy to read tips on is it a scam?, and how to verify and report a scam.
- The websites of large organisations (such as banks) often have scam alert pages with details of current known scams using their branding.