ABS Australian Business Startup

A free guide from Australian Business Startup

Scam Watch: the scams targeting new Australian businesses (2026)

What each scam looks like, the red flags, and what to do, plus a quick checklist and where to report and get help.

Why this guide exists

The moment you get an ABN, register a business name or put your details on a public register, you show up on a lot of lists. Most of the mail that follows is harmless. Some of it isn't.

Scammers like new businesses because you're busy, you're still learning which bills are real, and you might not know yet what a genuine government letter looks like. This guide covers the scams that come up again and again in our group and in official warnings, so you can spot them quickly and get on with your day.

To give you a sense of scale: the National Anti-Scam Centre's *Targeting Scams* report for 2025 (published March 2026) recorded $2.18 billion in combined reported scam losses across Australia. Payment redirection scams, which hit businesses hard, were the second-biggest category by losses at $166.8 million (Source: Scamwatch / National Anti-Scam Centre, *Targeting Scams* report, 2025 data).

You don't need to be paranoid. You just need a few habits. The most important one shows up in nearly every section below:

> **Stop. Check. Then act.** Never use the phone number, link or QR code in a message you weren't expecting. Look up the organisation yourself, or log in to your account directly.

1 Fake ABN, ASIC and business-name renewal "invoices"

How it looks: A letter or email titled something like "Business Name Renewal" or "Company Review", with a reference number, a due date, a QR code and sometimes a "pay early" discount. It uses your real details, pulled from public registers.

Some of these are outright scams. Others come from private companies offering to renew on your behalf, often for much more than the official fee. ASIC has warned that these notices can look like an invoice even though you don't have to pay them.

Red flags:

- Anything asking you to pay to "renew" or "maintain" your ABN. Applying for an ABN through the Australian Business Register (abr.gov.au) is free, and there's no renewal fee.
- A business-name renewal that isn't due yet, or a fee much higher than ASIC's published fee.
- A sender that isn't ASIC. ASIC says its emails come from addresses ending in **@asic.gov.au**, and business-name renewal reminders come from **ASIC.Transaction.No-reply@asic.gov.au**.
- Fine print saying "this is not an invoice" or "this is an offer of services".

What to do: Search your business name on ASIC's register or log in to ASIC Connect to check your actual renewal date. Renew directly with ASIC, or through an agent you've already chosen. If a message claims to be from ASIC and you're unsure, contact ASIC directly through asic.gov.au.

2 ATO impersonation calls, texts and emails

How it looks: A call or robocall saying you owe tax and face arrest or a fine. A text saying you're owed a refund. An email asking you to "verify your details" on a myGov-style page.

Red flags:

- Threats, urgency, or demands to pay by gift card, crypto or a bank transfer to a personal account.
- A link or QR code in an unexpected message. The ATO says it won't send unsolicited SMS or emails containing links or QR codes, or asking you to share personal information through them.
- A caller who won't let you hang up and call back.

What to do: Don't respond. Hang up and call the ATO's scam line on **1800 008 540** (8 am to 6 pm AEST, Monday to Friday) to verify or report. The ATO app also has a "Verify a call" feature. Forward scam emails to **ReportScams@ato.gov.au**. If you've paid money or shared personal details, call the ATO straight away.

3 Invoice and payment-redirection fraud (business email compromise)

How it looks: An email that seems to come from a supplier, your bookkeeper or even a customer: "We've changed banks, please use these new details for this invoice." Sometimes the scammer has actually got into a real email account and is replying inside a genuine thread.

Red flags:

- Any change to bank details, especially by email alone.
- Pressure to pay today, or a request to keep it quiet.
- A sender address that's one character off (for example, *supp1ier.com.au*).

What to do: Make it a rule: **bank detail changes get confirmed by phone, using a number you already have**, not the one in the email. Turn on multi-factor authentication (MFA) on your email. If you've paid a fraudulent account, call your bank immediately. Speed matters for any chance of recovering money. Then report through ReportCyber.

4 Fake domain-name renewal notices

How it looks: An invoice to "renew" your domain from a company you've never dealt with. Or it's for a name that's slightly different, like *.net.au* instead of *.com.au*, or a foreign extension. Some claim "another company wants your name" unless you pay now.

auDA, which administers .au domains, has also warned about phishing emails from people posing as auDA staff asking you to click a link to "verify" your registration.

Red flags: A provider that isn't your registrar, a domain name that doesn't exactly match yours, urgency, or a link to "verify" your licence.

What to do: Log in to your existing registrar to check your renewal date. Ignore offers for names you don't want. If you're unsure about an email claiming to be from auDA, contact auDA directly through auda.org.au and report it to Scamwatch.

5 Trade mark and IP Australia lookalike invoices

How it looks: Soon after you apply for a trade mark (your application is public), you get official-looking letters or emails. They might offer to add your mark to an "international register", ask you to renew years early, or demand a fee "payable to WIPO" by overseas bank transfer.

Red flags:

- Names that sound official but aren't IP Australia.
- "This is optional" buried in small print.
- Renewal requests years before your renewal is due.
- A sender address that doesn't end in **@ipaustralia.gov.au**.
- Payment to an overseas account.

What to do: IP Australia says genuine notices and invoices go to your IP Australia Online Services account. Check there, or search Australian Trade Mark Search, before paying anything. Listings on unofficial "registers" don't give you any legal protection.

6 Directory and listing scams

How it looks: A call: "Just confirming your listing details for this year's directory." Later an invoice arrives for an ad or listing you never agreed to, sometimes with a recording of you saying "yes". Or a form to "update your free listing" with a hefty annual fee in the fine print.

Red flags: Unsolicited calls to "confirm" something you never ordered. Vague directory names. Forms you're asked to sign and return. Threats of debt collection.

What to do: Don't confirm details or say "yes" on unsolicited calls. Check whether anyone in your business actually ordered it. You generally don't have to pay for goods or services you didn't agree to. If you're being pressured, contact your state or territory fair trading or consumer affairs agency, and report it to Scamwatch.

7 Fake buyers, fake suppliers and overpayment scams

How it looks: A "buyer" places a large order and then "accidentally" overpays, asking you to refund the difference before their payment bounces. Or on a marketplace, a buyer sends a fake "payment received" email or asks you to pay a fee to "release" funds. On the supply side, a too-cheap wholesaler takes a deposit and disappears.

Red flags: Overpayments. Rushed refunds. Payment confirmations that arrive by email rather than showing in your actual account. Couriers they insist on arranging. Suppliers who only accept crypto, gift cards or transfers to a personal account.

What to do: Only treat money as received once it has cleared in your own bank or platform account. Never refund an "overpayment" until it has cleared. Check new suppliers through the ABN Lookup (abr.business.gov.au), reviews and a phone call, and start with a small order.

8 "Your Facebook Page will be disabled" phishing

How it looks: A message, comment or email that claims to be from "Meta Support" or "Page Policy Team". It says your Page breaches copyright or community standards and will be removed unless you "appeal" through a link. The link leads to a fake login page that steals your password and two-factor code.

Red flags: Pages with names like "Meta Business Support" that have few followers. Links to non-Meta websites. Deadlines like "24 hours". Requests for your password or login code.

What to do: Don't click. Check for real warnings from inside Facebook itself, using your account or Page settings and notifications. Turn on two-factor authentication and review who has admin access to your Page. If you've entered your details, change your password straight away, then use Facebook's official account-recovery tools.

9 Fake grants and "guaranteed funding"

How it looks: A call, ad or email saying your business qualifies for a government grant. All you need to do is pay an "application", "processing" or "release" fee, or hand over your myGov or bank login.

Red flags: Upfront fees. Guaranteed approval. Requests for logins. Websites that don't end in .gov.au but use government logos.

What to do: Look up genuine grants yourself using the free **Grants and programs finder** at business.gov.au. business.gov.au says you shouldn't pay for government grant information. Never share your myGov or banking credentials with anyone.

10 SEO, website and lead-gen cold pitches

How it looks: "I noticed your website isn't ranking on Google", "We guarantee page-one results", or "We'll send you 50 qualified leads a week". Plenty of genuine agencies cold-pitch. The problem is the ones that take a deposit and vanish, lock you into long contracts, or quietly register your domain or Google Business Profile in their own name.

Red flags: Guaranteed rankings. Anonymous Gmail addresses. No ABN or physical address. Pressure to pay a big deposit upfront. Reluctance to put deliverables in writing.

What to do: Check their ABN, get a written scope and contract, and ask for references you can actually call. Keep ownership of your domain, website, ad accounts and Google Business Profile in your name. Give contractors access, not ownership.

11 Recruitment and fake job scams using business pages

How it looks: This one comes in two forms. Scammers may create fake job ads using *your* business name to harvest applicants' ID documents or money. Or job seekers who contact you might be targeted by "recruiters" pretending to be you. Separately, you might get "task-based" job offers yourself, where you're paid small amounts at first and then asked to deposit money.

Red flags: Job offers conducted entirely over WhatsApp or Telegram. Requests for ID documents before an interview. Applicants asking you about a job you never advertised. Any "job" where you pay to earn.

What to do: If someone is impersonating your business, report the fake profile or ad to the platform. Warn your followers with a post. Report it to Scamwatch. Advertise jobs only through channels you control, and say publicly that you'll never ask applicants for payment.

Your quick Scam Watch checklist

- [ ] I never pay from a link, QR code or phone number in an unexpected message.
- [ ] I check renewals by logging in directly (ASIC Connect, my domain registrar, IP Australia Online Services).
- [ ] I know my ABN is free and doesn't need renewing.
- [ ] Bank detail changes are confirmed by phone, using a number I already have.
- [ ] MFA is on for my email, banking, accounting software and social media.
- [ ] I keep my domain, website and ad accounts in my own name.
- [ ] Money only counts as received when it has cleared in my account.
- [ ] I don't say "yes" or confirm details on unsolicited calls.
- [ ] My team knows they can always pause and check, with no blame.
- [ ] I know who to call if something goes wrong (see below).

Where to report and get help

Who	What for	How
Your bank	Do this first if money has left your account	Use the number on the back of your card or on the bank's official website
Scamwatch (National Anti-Scam Centre, run by the ACCC)	Reporting any scam, even if you didn't lose money	scamwatch.gov.au
ReportCyber (Australian Cyber Security Centre)	Cybercrime, such as hacked email, business email compromise or ransomware	cyber.gov.au/report, or the 24/7 hotline 1300 CYBER1 (1300 292 371)
ATO	Verifying or reporting ATO impersonation	1800 008 540 (8 am to 6 pm AEST, Monday to Friday); forward emails to ReportScams@ato.gov.au
ASIC	Scams impersonating ASIC; checking a company before you deal with it	asic.gov.au (see "Scams impersonating ASIC"); Moneysmart's Investor Alert List at moneysmart.gov.au
IDCARE	Free identity and cyber support, including a small business service	idcare.org; individuals 1800 595 160; small businesses 1800 595 170

If your identity documents have been exposed, IDCARE can help you work out what to do next. If you've lost money, contact your bank first, then report the scam.

Disclaimer: This guide is general information only and isn't legal, financial or tax advice. Scams change quickly, so always check the latest guidance from the official sources listed above, and talk to a qualified professional about your own situation. Contact details and figures were checked in October 2026.

© 2026 Enviga Pty Ltd (ABN 43 115 695 568). Australian Business Startup is run by Enviga Pty Ltd.
australianbusinessstartup.com.au