CHECKLIST · SCAMS & SECURITY

# Data breaches hitting hundreds of thousands of Australians are rising

Published 27 October 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/oaic-data-breach-statistics-january-june-2026/

- [ ] **Read the whole breach notice.** It should say which of your details were involved and what the organisation recommends you do.
- [ ] **Change your email password if your contact details were taken.** Use a strong password you haven't used anywhere else, and turn on multi-factor authentication.
- [ ] **Call back on a number you look up yourself.** If someone rings claiming to be from a company or agency, hang up and call the number on its official website.
- [ ] **Contact your bank directly if financial details were involved.** Type its web address into your browser rather than clicking a link, and change your online banking password and PIN.
- [ ] **Contact the issuing agency if an ID document was involved.** Ask the agency that issued your driver licence, Medicare card or passport what to do next.
- [ ] **Keep a record of every step you take.** Note dates, who you spoke to and what you changed, in case you're harmed later.
- [ ] **Business owners: list the personal information you hold.** Delete what you no longer need, as the Privacy Commissioner recommends.
- [ ] **Business owners: check whether the breach scheme covers you.** Annual turnover over $3 million, running a private health service, or handling tax file numbers can all bring you in.



General information only, not legal, tax or financial advice. Check the full story and its sources before acting.