

Print it, fill in the contacts, and keep a copy where you can find it if systems are down.

Organisation: · Last updated:

Key contacts (fill in NOW, not during an incident)

Role	Name	Phone
Incident lead	<input type="text"/>	<input type="text"/>
IT support / MSP	<input type="text"/>	<input type="text"/>
Bank (fraud line)	<input type="text"/>	<input type="text"/>
Cyber insurer + policy #	<input type="text"/>	<input type="text"/>
Australian Cyber Security Hotline	—	1300 292 371 (24/7)

First hour

1. **Don't panic, don't pay.** Ransom demands and scam "fees" are negotiable-by-ignoring; get advice first.
2. **Contain.** Disconnect affected devices from the network/Wi-Fi. Don't turn them off (evidence lives in memory).
3. **Change passwords** for affected accounts from a *clean* device — email first, then banking, then admin accounts.
4. **Call your bank** immediately if money was sent or bank details were changed on an invoice.
5. **Write down what happened** while it's fresh: what was clicked, when, on what device, what you saw.

First day

6. **Call your IT support/MSP** and your **cyber insurer** (they often have their own response team — call before spending money).
7. **Report it:** ReportCyber at cyber.gov.au (and Scamwatch for scams). If money is involved, this can help recovery.
8. **Check email rules.** Attackers add hidden forwarding rules — check email settings for rules you didn't

create.

9. **Brief your team.** Tell staff what happened in plain terms and what to watch for (follow-up scams impersonating you are common).

First week

10. **Assess what data was exposed.** Personal information involved? You may have obligations under the Notifiable Data Breaches scheme — see [oaic.gov.au](https://www.oaic.gov.au).
11. **Tell affected people** honestly and early if their data was involved.
12. **Close the hole.** Patch, enable MFA everywhere, remove unused accounts.
13. **Debrief without blame.** What made this possible? What nearly stopped it? Fix the system, not the person.