

Shit, We've Actually Been Hacked!

Your 8-step Emergency Action Card. Print it, fill in your numbers, stick it on the wall.

Stay calm. Act in order. Don't go it alone.

1. **BREATHE.** Panic makes it worse. Take 10 slow breaths. Clear thinking now saves hours later.
2. **CONTAIN — disconnect, don't delete.** Note or photograph any on-screen message, then disconnect Wi-Fi, Ethernet and Bluetooth. Do not wipe or reset the device. If ransomware is visibly spreading, turn it off; otherwise follow your IT provider's instructions.
3. **CALL your IT provider / MSP now.** Phone, don't email (email may be compromised). Tell them what you saw, when, and which system.
4. **REPORT to the ACSC.** cyber.gov.au/report or 1300 CYBER1 (1300 292 371). IDCARE (1800 595 170) helps with identity-related incidents.
5. **NOTIFY your insurer.** Call the breach hotline immediately and follow your policy's instructions. Your insurer may require approval before outside responders are engaged or costs incurred.
6. **PROTECT — secure affected accounts with your IT provider.** Using a clean device, reset affected credentials, sign out active sessions and check MFA.
7. **DOCUMENT everything.** Times, what you saw, who you called. Screenshots and timestamps while it's fresh.
8. **RECOVER & REVIEW.** Restore from clean backups with your IT provider. Once stable, hold a short review: what happened, what we'd do differently, update this plan.

Money moved? If this is invoice fraud or a wrong transfer, call your bank's fraud line FIRST — it's often more urgent than reporting to the ACSC.

Fill these in now — a blank sheet is not an emergency sheet

IT provider / MSP: _____

Emergency phone: _____

Bank fraud line: _____

Cyber insurer: _____

Policy #: _____

Breach hotline: _____

Who decides during an incident: _____

Where the backups are / who can access: _____