CHECKLIST · SCAMS & SECURITY

Hackers are defrosting supermarket freezers. Is yours online?

Published 6 November 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/commercial-refrigeration-hacking-warning/

- [ ] **Ask your refrigeration technician how they connect.** Find out whether your fridge, freezer or cool room controller can be reached from the internet, and through which app, web page or remote-access tool.
- [ ] **Take controllers off the open internet.** If remote access is needed, have your IT provider put it behind a firewall or other edge device that's kept up to date.
- [ ] **Change default passwords on every controller and monitoring app.** Use strong, unique passwords, and turn on multi-factor authentication where it's offered.
- [ ] **Ask for firmware updates.** Have your technician confirm each controller is on the maker's latest version. Danfoss AK-SM 8xxA system managers need version 4.3.1 or later.
- [ ] **Replace unsupported equipment.** Ask which controllers no longer get security updates from the maker, and budget to replace them.
- [ ] **Keep controllers on their own network.** Ask your IT provider to separate refrigeration systems from office computers and guest Wi-Fi.
- [ ] **Set temperature alarms.** Agree safe upper and lower limits for each unit, and make sure an alert reaches a named person when a reading drifts.
- [ ] **Report anything odd to the ACSC.** Call 1300 CYBER1 (1300 292 371) if temperatures or settings change without explanation.

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