Give smart devices their own Wi-Fi.

Cameras, TVs, speakers and smart plugs are often the weakest link at home. Keep them apart from your computers and phones, and keep visitors off your main network too.

THE PROBLEM

Weak by design

Many gadgets ship with default passwords and rarely get security updates.

One flat network

If one gadget is hacked, the attacker can reach your laptop, phone and files.

Unknown visitors

Guests' phones and laptops may carry malware you can't check.

WHAT TO DO

1. **Make a separate network.** Put smart devices on an IoT or guest Wi-Fi, and visitors on a guest Wi-Fi, with a strong passphrase and client isolation switched on.
2. **Change the default password** on every device and on your router, and use a unique one each time.
3. **Update and trim.** Turn on automatic updates, switch off features you don't use (remote access, microphones, UPnP) and register devices only when needed.
4. **Retire the unsupported.** If a device no longer gets updates, replace it. Before buying, check how long the maker will support it.

WE RECOMMEND

Start with your router's guest Wi-Fi

Most modems have one. It's free and takes ten minutes. For proper separation of trusted, smart-device and guest networks, we install and set up **UniFi** gateways and Wi-Fi, which create separate networks with firewall rules between them.

apcsc.com.au

Scan for ACSC smart device advice

Sources: Australian Cyber Security Centre (cyber.gov.au) – Smart devices and Internet of Things guidance · CISA (cisa.gov) – Securing Your Home Network and Secure Our World: Update Software · NIST – Cybersecurity for IoT Program (nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program).

APCSC is an independent business and is not affiliated with the Australian Government or the Australian Cyber Security Centre.

ABN 13 262 392 536 · © 2026