CICADA | RESOURCES

LESSON 01 OF 03 · 6 MIN · WORKING KNOWLEDGE

Wi-Fi and the router nobody checks

Three changes that close a very common door: guest network, router hygiene, and segmenting the risky devices.

Separate the guests

A guest network keeps visitors, personal phones and smart devices away from the systems that hold business data. Most business routers support one; some call it a VLAN. Turn off client-to-client access if you can, and use a password you're happy to change.

If your router can't separate networks, it may be time to replace it. A business-grade router is cheaper than a single incident.

Router hygiene

- Change the default admin password and store it in the password manager.
- Turn off remote administration from the internet unless you specifically need it.
- Use WPA2 or WPA3; never run an open network for business.
- Update firmware, automatically if available, otherwise quarterly.
- Change the default Wi-Fi password that came on the box.

Segment the dumb stuff

Payment terminals, cameras, printers and smart devices often run old software and don't need to talk to payroll. Put them on their own network. At minimum, don't let them share a flat network with customer and financial data.

If staff work from home, require the VPN or zero-trust access for business systems. Home router security isn't something you control.

THE BOX IN THE CUPBOARD

The router is a computer with an admin login and firmware. If nobody has logged into it since installation, it deserves an hour of attention.

Key takeaways

- ✓ A guest network keeps unknown devices away from business systems.
- ✓ Change the router admin password and disable remote admin.
- ✓ Keep firmware current.
- ✓ Segment payment, camera and smart devices where possible.