

4.3 Smart Home and IoT Devices

Core Concepts: Minimize Your Exposure, Protect Your Data

Smart home and other Internet of Things (IoT) devices make life convenient; smart speakers, security cameras, thermostats, door locks, light bulbs, refrigerators, and more. But these devices are often the weakest link in your home network. Many ship with poor default security, rarely get updated, and connect to the internet 24/7.

A compromised smart device can become a gateway for attackers to access your entire network, spy on you through cameras and microphones, or recruit your devices into a botnet (an army of hacked devices used for cyberattacks).

With some basic precautions, you can enjoy the convenience of smart devices without compromising your security.

4.3.1. Understanding IoT Security Risks

What are IoT devices?

Any device that connects to the internet but isn't a traditional computer or phone:

- Smart home: Speakers (Alexa, Google Home), thermostats, light bulbs, plugs
- Security: Cameras, video doorbells, smart locks, alarm systems
- Entertainment: Smart TVs, streaming devices, game consoles
- Appliances: Refrigerators, ovens, washing machines, robot vacuums
- Wearables: Fitness trackers, smartwatches
- Health: Baby monitors, medical devices

Common IoT security problems:

- **Weak default passwords:** Often "admin" or "12345"
- **No security updates:** Many manufacturers abandon support after a couple years
- **Always listening:** Smart speakers and cameras can be compromised for spying

- **Excessive data collection:** Many devices send usage data to manufacturers
- **No encryption:** Some send data unencrypted over your network
- **Unnecessary features:** Open ports, remote access enabled by default

Real-world consequences:

- Hackers streaming from home security cameras
- Smart speakers recording conversations and sending them to strangers
- Compromised devices used in massive DDoS attacks (e.g., Mirai botnet)
- Smart locks unlocked remotely by attackers
- Baby monitors accessed by strangers

You don't need to avoid IoT devices, they're useful and can make life easier. But treat them with appropriate caution. An IoT device is basically a tiny computer, running software, connected to the internet 24/7. Would you leave a computer with default password "admin" connected to the internet? No? Then don't do it with your TV either.

4.3.2. The Basics

- Change all default passwords
- Keep firmware updated
- Disable unnecessary features
- Review device permissions and privacy settings
- Use strong authentication for device apps

Change All Default Passwords

Default passwords are publicly available and attackers scan for devices using them.

For each IoT device:

- Check if it has a default password (look in manual or on device label)
- Log into the device's app or web interface
- Find password/security settings
- Change to a strong, unique password
- Store password in your password manager

Keep Firmware Updated

IoT devices need security updates just like computers. Enable automatic updates where possible.

How to update:

- Open the device's mobile app
- Look for Settings > About > Firmware or Software Update
- Enable automatic updates if available
- If not available, check for updates manually

For devices without apps:

- Check manufacturer's website for updates
- May need to download and install manually

Create a quarterly reminder to check for updates for your IoT devices that don't auto-update.

Disable Unnecessary Features

IoT devices often have features enabled by default that you don't need. Turn them off.

Common features to disable:

- **Remote access:** Unless you need to control devices away from home
- **Cloud recording:** For cameras, use local storage if you can
- **Voice purchasing:** On smart speakers (someone could order without your permission)
- **Always-on microphones:** If you don't use voice commands
- **Usage analytics:** Data sharing with manufacturer

How to find these:

- Device app > Settings > Privacy or Security
- Look through all settings
- Default to "off" or "disabled" for things you don't actively use

Review Device Permissions and Privacy Settings

IoT device apps request permissions on your phone. Review and restrict them.

Check app permissions:

- Phone Settings > Apps > [IoT Device App] > Permissions
- Ask yourself: "Does my smart bulb app really need my location?"
- Deny unnecessary permissions

Common unnecessary permissions:

- Smart bulb app requesting location (unless for automation)
- Thermostat app wanting microphone access
- Any device requesting contacts

Use Strong Authentication for Device Apps

The apps that control your IoT devices should have strong passwords and MFA.

For each device manufacturer account:

- Create unique, strong password (use password manager)
- Enable two-factor authentication if available
- Use different email for IoT accounts vs banking/primary email

See the Authentication section for detailed password and MFA guidance.

4.3.3. Better Protection

- Research before you buy
- Put IoT devices on guest network
- Use physical controls for cameras and microphones
- Review smart speaker voice history

Research Security Before Purchasing

Not all IoT devices are created equal. Buy from manufacturers with good security track records.

Before buying, check:

- Does it receive regular firmware updates?
- How long does manufacturer support it?
- Does it require account creation or work locally?
- Does it support WPA3 WiFi encryption?
- Are there known security issues? (search "[device name] security vulnerability")
- What data does it collect and where does it go?

Good signs:

- Manufacturer offers multi-year support commitment
- Automatic firmware updates
- Local control option (doesn't require internet)
- End-to-end encryption for data

- Two-factor authentication support

Red flags:

- Unknown or generic Chinese manufacturer
- No firmware updates in 6+ months
- Must have cloud account to function
- Vague privacy policy
- Price seems too good to be true

Put IoT Devices on Your Guest Network

IoT devices shouldn't have access to your computers and phones. Use your guest network to isolate them.

Why this matters:

- Compromised smart bulb can't access your laptop
- Hacked security camera can't see your file shares
- Infected smart TV stays contained

What to do:

- Set up guest network on your router (see Home WiFi section)
- Connect IoT devices to guest network instead of main network
- Keep computers, phones, tablets on main network

Exception: Devices that need to communicate with your phone/computer (like Chromecast, AirPlay, or printer) may need to be on the main network. This is a tradeoff where you weigh convenience against security for each device.

Use Physical Controls for Cameras and Microphones

Cameras and microphones in IoT devices can be compromised. Use physical controls.

For cameras:

- Focus on entry points (doors, windows) not living spaces
- For smart displays, use the physical camera cover if available
- Tell guests if cameras are present
- Use motion-activated recording instead of continuous
- Store locally instead of cloud when possible

- Set auto-delete for old footage (30 days is reasonable)
- Enable encryption if available

For microphones:

- Many smart speakers have physical mute buttons; use them when you want privacy
- Consider where you place always-listening devices

Review Smart Speaker Voice History

Smart speakers record your voice commands. Review and delete this history regularly.

Amazon Alexa:

- Alexa app > More > Settings > Alexa Privacy
- Review Voice History > Filter by date
- Delete recordings or enable auto-delete

Google Home:

- Google Home app > Settings > Google Assistant > Your data
- Review and delete activity
- Enable auto-delete for activity older than 3-18 months

Apple HomePod:

- Apple doesn't store Siri recordings by default
- Check opt-in settings: Settings > Siri & Search > Siri & Dictation History

4.3.4. Extra Credit

- Use local control instead of cloud
- Use VLAN for advanced network segmentation

Use Local Control Instead of Cloud

Devices that work locally don't require internet and can't be compromised through manufacturer's cloud.

Local control options:

- Home Assistant - Open-source home automation platform

- Hubitat - Local smart home hub
- Devices with Zigbee or Z-Wave (don't require manufacturer cloud)

Benefits:

- Works even if internet is down
- No dependency on manufacturer's servers
- Devices still work if company goes out of business
- More privacy, data stays in your home

Tradeoff: More complex to set up and requires ongoing maintenance. Only recommended for technically comfortable users.

Use VLANs for Advanced Network Segmentation

VLANs provide the strongest isolation between IoT devices and your trusted devices.

VLAN segmentation example:

- VLAN 10: Trusted devices (computers, phones)
- VLAN 20: IoT devices (smart bulbs, thermostats)
- VLAN 30: Security cameras (complete isolation)
- VLAN 40: Guest network

Firewall rules:

- IoT devices can access internet but not trusted devices
- Trusted devices can initiate connections to IoT (for control)
- Security cameras can't initiate any connections

Requirements:

- Managed router/firewall (OPNSense, UniFi, etc.)
- Managed network switch (if using wired devices)
- Technical knowledge to configure VLANs and firewall rules

See the Home WiFi section for more on VLANs, of TheDen Home Network Guide.

Revision #1

Created 2026-07-12 21:51:58 UTC by Chris Landis

Updated 2026-07-12 21:53:25 UTC by Chris Landis