



Aware *and* Safe

BE AWARE. STAY SAFE.

SAFE IN THE AGE OF AI

The Smart Home Guide to AI Security



FREE SAMPLE · CHAPTER 1

Your Home Is a Computer Now

From “The Smart Home Guide to AI Security” — read the full first chapter free.

Your Home Is a Computer Now

Walk through your home and count what's connected. The obvious ones first: phones, laptops, tablets, the TV. Now the quiet ones: the speaker on the kitchen counter. The doorbell. The thermostat. The door lock you open with your phone. The lightbulbs with an app. The printer. The game console. The baby monitor. The robot vacuum.

Most people land somewhere between ten and thirty connected devices. Did you expect that number? Almost nobody does. We bought them one at a time, each feeling like a small upgrade, and never stopped to add them up.

Here's the part that matters: every one of those devices is a small computer. It has a processor and memory. It runs software. It connects to your Wi-Fi, and through your Wi-Fi to the internet. That means every one of them is something that can, in principle, be reached, tricked, or taken over from outside your home.

What "smart" actually means

When a company calls a device "smart," it usually means three things:

It has sensors. A microphone, a camera, a motion detector, a thermometer — something that observes you or your home.

It has a network connection. Wi-Fi, usually. It talks to your router, and through it to the manufacturer's servers on the internet.

It has an account. You signed in somewhere — an app, a website — to make it work. That account, with your email and password, is now tied to a microphone in your kitchen.

None of this is evil. It's how the convenience works: the speaker needs to hear you to answer, the camera needs the internet to show you the front door while you're at work, the thermostat needs your schedule to save energy. But each capability is also an opening. A microphone that hears you can, if mishandled or hacked, let someone else hear you. A camera that watches your porch can, if poorly secured, let someone else watch your porch. An account that controls your door lock is worth protecting like the key it replaced.

The attack surface, in plain English

Security people use the phrase "attack surface" to mean "all the ways in." Your home's attack surface used to be doors and windows. Now it includes:

- Every smart device and the app that controls it
- Your Wi-Fi router — the single box everything connects through
- The accounts tied to those devices (each with a password worth stealing)
- The companies' servers where your recordings, videos, and routines are stored

You don't need to memorize this list. You just need the mental shift: **your home is a small network now, and networks need the same common-sense care as physical homes.** You lock doors. You don't leave keys under the mat. The digital equivalents — strong unique passwords, updated software, a secured router — are the subject of this book.

Why a lightbulb can be a security problem

This is the question everyone asks, and it's a good one. Who cares about hacking a lightbulb?

Nobody wants your lightbulb. They want what it's connected to. Every device on your Wi-Fi can, in the wrong circumstances, become a stepping stone to the rest of your network — the laptop with your banking, the phone with your photos. Criminals have repeatedly taken over thousands of small, boring devices (cameras, routers, even lightbulbs) and linked them into networks that attack bigger targets. Your lightbulb doesn't need to contain secrets to be useful to someone — it just needs to be reachable and unguarded.

There's a second reason: some "boring" devices aren't boring at all. A smart TV has a microphone. A robot vacuum builds a map of your home's interior. A smart speaker hears everything within earshot. The device's job description tells you what it can observe — and anything it can observe is worth protecting.

One evening, device by device

To make the attack surface concrete, follow one ordinary evening through the eyes of your network.

6:00 p.m. You get home. Your phone rejoins the Wi-Fi — the router notes it, as always. The smart lock logs the unlock. The thermostat, which has been saving energy all day, starts warming the house because your phone's location told it you were on your way.

6:30 p.m. In the kitchen, you ask the speaker to play the news. It records your request, sends the audio to a company server, and streams the answer back. Your partner asks it to add milk to the shopping list — another recording, another server trip.

7:15 p.m. The doorbell rings. It's a package. The doorbell camera records the courier, uploads the clip to the cloud, and pings your phone. You watch the 20-second video from the couch.

8:00 p.m. The kids are gaming online — the console is chatting with game servers. Someone starts the robot vacuum, which spends the next hour building a detailed map of your floor plan and, on some models, uploading it.

10:30 p.m. The TV streams a movie. The baby monitor watches the nursery. The smart lock auto-locks at 11, per the schedule you set.

Nothing about this evening felt technological. It felt like home. But count the computers that participated: phone, lock, thermostat, speaker (twice), doorbell, console, vacuum, TV, baby monitor — plus the router orchestrating all of it, and the half-dozen company servers that received audio, video, location, and maps along the way.

Every one of those connections is useful. Every one is also a relationship — between you and a company, between your home

and the internet — that deserves the small amount of care this book describes.

Start with an inventory

You can't secure what you don't know you have. So the first habit — the foundation everything else builds on — is a simple list.

This week, walk through your home and write down every connected device. Phone, laptop, TV, speaker, doorbell, camera, thermostat, lock, bulbs, printer, console, vacuum, monitor, anything with an app. Note which ones have cameras or microphones — star those.

You don't need fancy software. A note on your phone works. What matters is that the list exists, because every later chapter refers back to it: which devices need password changes, which need muting rules, which should move to a separate network.

Most people are surprised twice: first by how long the list is, and later — when something goes wrong — by how glad they are to have it.

LINE TO REMEMBER

Your home is a network now — and you can't protect what you haven't counted.

Ears in the Walls

The smart speaker is the most intimate computer most people own. It sits in the kitchen, the bedroom, the living room. It hears arguments and apologies, business calls and bedtime stories. And unlike your phone — which you carry, lock, and think of as private — the speaker just sits there, always on, always listening for its name.

Let's be precise about what that means, what's myth, and what actually protects you.

What your speaker actually hears

Smart speakers listen in two stages. The first stage happens entirely inside the device: a small, simple piece of software listens for the wake word — "Alexa," "Hey Google," whatever you set. Until it hears that word, nothing is recorded and nothing leaves your home. The device is, in a real sense, deaf to meaning; it's just pattern-matching a sound.

The second stage starts when the wake word is detected. Then the speaker records what you say next and sends that audio to the company's servers, where powerful software figures out what you asked and how to respond. That recording — your voice, your words — now exists on someone else's computer.

Two honest complications:

Enjoyed this chapter?

This was Chapter 1 of *The Smart Home Guide to AI Security*, part of the *Safe in the Age of AI* series by Aware and Safe. The complete handbook includes every chapter, all the checklists, and the companion resources — available now in the edition that suits you.

Ebook + Audiobook Bundle

\$8.99

Everything together — the best value.

<https://awareandsafe.com/safe-in-the-age-of-ai/smart-home-guide/#formats>

Ebook

\$6.99

Premium PDF — read on any device.

<https://awareandsafe.com/safe-in-the-age-of-ai/smart-home-guide/#formats>

Audiobook

\$4.99

Full MP3 narration + companion PDF.