When your coffee maker becomes a cyber weapon

Kristin Burnham, Author of Security Intelligence. Theintelligence.com, October 17, 2025

We are surrounded by smart devices — here's how to ensure they can't be used against you.

Internet-connected devices are everywhere. A sleek coffee maker that syncs with your phone to start brewing before you're out of bed. A smart bulb that sets "romantic mode" on cue. A thermostat that knows you're heading home before you walk in the door.

But then one morning, your coffee maker pings your phone: A firmware update is ready. You pause. *Why does a coffee maker need a firmware update? And what exactly would happen if it didn't get one?*

That small moment of hesitation is justified because every device you connect — no matter how harmless it seems — is another path in for would-be hackers, expanding your potential attack surface.

Smart plugs, light bulbs, thermostats, pet feeders, digital picture frames, even connected washing machines are all Internet-of-things (IoT) devices that barely enter our thoughts after we've set them up. They're quietly multiplying across homes and offices, and most people don't think of them as security risks.

Which is exactly what makes them perfect targets: low attention, low maintenance, and often entirely unaudited.

But these innocuous devices can give attackers visibility into your network, access to other connected systems, or even a route onto your laptop. Worst-case scenario: Your IoT gear could be hijacked and repurposed as part of a botnet that attacks someone else's systems — with your network as the launchpad.

The Internet of (compromised) things

The IoT threat isn't theoretical. Hackers recently broke into the payment and control systems of **smart washing machines** in a Dutch housing complex. The intruder granted free usage to residents and forced management to disable the machines entirely. (A win for laundry day; a loss for network security.) And though it wasn't ransomware or data theft, it was proof of concept — when even a washing machine can be hacked, nothing with a network chip is off-limits.

Which is why it's not surprising that last week a botnet campaign **targeted more than 50 known vulnerabilities** across routers, CCTV systems, DVRs, and various other internet-connected consumer devices. Once infected, those devices became launchpads for denial-of-service attacks, proxy networks, and other malicious campaigns. And if those smart gadgets were sitting in an office or lobby somewhere, suddenly it's not just your coffee maker at risk, it could be entire the company network.

These examples underscore an uncomfortable truth: While you might not consider your smart toaster or pet feeder an obvious entry point for hackers, attackers still love them. They're plentiful, easy to exploit, and rarely monitored. Once compromised, they can expose sensitive data, enable surveillance, or serve as stepping stones to higher-value targets.

What you can do

The good news is that protecting these devices doesn't require a degree in network security — just a few simple habits that make life a lot harder for would-be intruders.

- **Change your credentials.** It sounds obvious, but most IoT hacks start here. Devices often ship with factory passwords like "admin" or "12345." Set a strong, unique password the moment you plug any network-connected device in, and if possible, disable remote access or restrict it to specific IPs.
- **Be aware of updates.** Set a recurring calendar reminder to manually check for firmware updates, or consider enabling automatic updates. One word of caution, however: Though rare, sometimes automatic updates cause problems, as Jeep owners recently experienced.
- **Segment your network.** Don't let IoT devices share the same network as your personal computers or work devices. Create a separate Wi-Fi or virtual local area network (VLAN). (Many modern routers let you spin up an "IoT network" with a few clicks.) That way, even if a device is compromised, it can't pivot elsewhere. For workplaces that use IoT devices like smart thermostats or lightbulbs, this is *especially* important.
- **Disable unnecessary services or ports.** Many gadgets ship with unused or legacy features that quietly widen the attack surface. Things like Universal Plug and Play (which automatically lets devices find and talk to each other on your network), File Transfer Protocol (or FTP, which transfers files without encryption), and Telnet (which allows remote control through an unprotected command line) are often *enabled* by default, but they also create open doors for anyone who knows where to look. If you're not using these functions, turn them off. The smaller your attack surface, the safer you are.
- **Monitor device behavior.** You don't need enterprise-grade tools to stay alert. Check your router's admin page periodically for unknown devices or unusual bandwidth spikes. If your "off" smart plug suddenly starts sending traffic at 2 a.m., something's wrong.
- **Buy from reputable brands.** Before buying your newest IoT device, look for vendors that regularly issue firmware updates, publish security notices, or have a vulnerability disclosure program. A smart light that costs $10 more but receives updates is a better investment than one that's abandoned after launch.

In the connected era, "smart" can also mean "vulnerable." The same features that make life more convenient — voice control, automation, remote access — can also make these devices attractive to hackers.

You don't need to abandon the smart gear you love and that make your home and work life easier. Treat those devices with the same caution you'd give your phone or laptop and update 'em, lock 'em down, and keep an eye on 'em.