

The Light Bulb That Gave Away the Keys

Why retired smart devices and controllers need a secure goodbye

A story that could be yours *(illustrative scenario)*

Your facilities team upgrades the office lighting and replaces an aging thermostat and building controller. The old units go into a recycling bin, or get sold as a "lot" online. A stranger buys the box for a few dollars.

At a kitchen table, with an inexpensive USB adapter and free software, they copy each device's memory and search it. Out comes your Wi-Fi password, a login for a cloud service, and clues about how your network is laid out. They never set foot in your building. **The equipment you threw away handed them the keys.**

This has already happened

- **Smart bulbs.** A researcher opened a LIFX Mini bulb, copied its memory, and found the owner's Wi-Fi password in plain text, plus a private key used to connect to the vendor's cloud. LIFX says it fixed the issues in late 2018.¹
- **Used smart devices.** A Rapid7 researcher reports that over five years, more than 30% of the used IoT devices he bought on eBay still held data such as account passwords and Wi-Fi keys.² In a later test, 4 of 10 secondhand Amazon Echos still held the owners' Wi-Fi name and password, and he has bought whole batches of devices still configured for an operating business.³
- **Hospital equipment.** Of 13 infusion pumps bought on the secondary market, 8 still held Wi-Fi passwords and one held Windows network (Active Directory) login data.⁴
- **Business network gear.** ESET bought 18 used enterprise routers. Nine were left fully intact; each contained VPN or other network credentials or hashed admin passwords, and enough detail to identify the former owner.⁵

The same risk applies to building-automation and industrial controllers (PLCs), which keep network settings and passwords in memory.

How AI makes it worse

What once took an expert days now takes far less. AI tools can help an attacker identify an unfamiliar device, explain its firmware, sift a memory dump for passwords, and repeat the process across a whole pallet of equipment. The same tools then help turn what was found (company names, network names, vendor accounts) into convincing, tailored phishing or a path deeper into the network.

This is already happening. Google's threat intelligence team found state-backed hackers using its Gemini AI to research target organizations, study vulnerabilities (including IoT bugs), and write phishing content. Its conclusion: AI lets attackers "*move faster and at higher volume,*" and serves less-skilled actors as "*a learning and productivity tool.*"⁶

Four takeaways

1 A factory reset is a start, not proof.

Resets can be skipped or fail on "dead" devices. Verify the wipe, or physically destroy the memory.

2 Change passwords before devices leave.

Rotate Wi-Fi keys, service accounts, cloud logins, and VPN keys tied to retired equipment.

3 Use certified data destruction.

Choose an IT asset disposition (ITAD) partner that sanitizes to recognized standards (e.g., NIST SP 800-88) and gives you serial-level certificates.

4 Know what you own.

Inventory smart lighting, thermostats, cameras, controllers, and PLCs, and include them in every decommissioning plan.

WHAT'S YOUR MISSION? Cadre6 helps organizations build simple, cradle-to-grave processes for connected devices, from installation to secure retirement. Tell us what you're retiring and what's at stake: hello@cadre6.com

Sources

1. LimitedResults, "Pwn the LIFX Mini white," Jan. 2019 (limitedresults.com); Tom's Guide, "LIFX Smart Bulbs May Reveal Your Wi-Fi Password," Jan. 30, 2019, incl. LIFX statement.
2. D. Heiland, Rapid7, "Privacy, Security, and Connected Devices: Key Takeaways from CES 2024," Jan. 18, 2024.
3. D. Heiland, Rapid7, "Out With the Old, In With the New: Securely Disposing of Smart Devices," Jan. 6, 2025.
4. D. Heiland & C. McGuire, Rapid7 research report on secondhand medical infusion pumps, 2023 (rapid7.com/info/medical-devices-report).
5. ESET Research, white paper and press release on used enterprise routers, Apr. 18, 2023; WIRED, "Used Routers Often Come Loaded With Corporate Secrets," Apr. 2023.
6. Google Threat Intelligence Group, "Adversarial Misuse of Generative AI," Jan. 29, 2025.