IoT security: ten failures that lead to real breaches, and how to avoid them

26 October 2026 · 6 min read · blogs.iictp.org/iot-security-best-practices

Connected devices are hard to secure: they are numerous, long-lived, physically exposed and often hard to update. These are common failures and the habits that prevent them.

TL;DR The short version

- IoT devices are hard to secure because they are numerous, long-lived, physically exposed and hard to update.
- Design out failures such as default passwords and unsigned or impossible firmware updates.
- Give each device a unique identity, sign and verify firmware, and follow ETSI EN 303 645 and the OWASP IoT guidance.

Read online, listen to it, or change the text size: https://blogs.iictp.org/iot-security-best-practices

Ten failures to design out

1. Default or shared passwords.
2. No way to update firmware, or updates that are not signed.
3. Services left open that the device does not need.
4. Unencrypted communication.
5. Secrets and keys stored in plain text on the device.
6. No device identity, so a fake device can join.
7. Flat networks where one compromised device reaches everything.
8. No logging or alerting from the fleet.
9. No plan for end of life, so old devices stay online unpatched.
10. Security treated as a launch task rather than a lifecycle one.

What to do instead

- Give every device a unique identity and credentials.
- Sign firmware and verify it at boot.
- Segment networks and allow only what is needed.
- Encrypt data in transit and at rest.
- Monitor the fleet and be ready to revoke a device.

Standards to read

ETSI EN 303 645 and the OWASP IoT guidance set out baseline practices for consumer and general IoT.

> Related credential: IoT & Embedded Systems Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. ETSI EN 303 645. Cyber Security for Consumer Internet of Things. etsi.org.
2. OWASP. Internet of Things Project. owasp.org/www-project-internet-of-things/.

Published by IICTP, an independent technical credential body, on 26 October 2026. The current version of this post is at https://blogs.iictp.org/iot-security-best-practices. More guides: blogs.iictp.org.