

IoT Security: User awareness



HOW TO CHOOSE A SMART HOME DEVICE SECURELY

- Verify whether the smart features are really required or whether a normal device would be sufficient
- Be careful when buying used IoT devices, as they could have been tampered with
- Research the vendor's device security measures
- If battery powered, favor devices providing alternate/emergency charging methods

HOW TO OPERATE A SMART HOME DEVICE SECURELY

- Change default password of Wi-Fi networks and use robust encryption (e.g. WPA2)
- Change default password of device
- Disable or protect remote access to IoT devices when not needed
- Use wired connections instead of wireless where possible
- Modify the privacy and security settings of the device to your needs
- Disable features that are not being used
- Install updates when they become available
- Use devices on separate home network when possible
- Ensure that an outage (for example due to jamming or a network failure) does not result in a unsecure state of the installation

HOW TO USE ONLINE SERVICES FOR SMART HOME SECURELY

- Use a password manager
- Use different passwords for different services
- Control data exchange requested by a service



Securing the IoT

ENISA'S EFFORTS ON IoT SECURITY

- Evaluation of threats
- Promotion of security good practices
- Stakeholders engagement
- Awareness raising
- Community expert groups
- Liaison with policy makers

ENISA IoT SECURITY GOOD PRACTICES FOR

- Device vendors
- Service providers
- End-users
- Electronic communication providers

INTERESTED TO LEARN MORE? CHECK OUT OUR STUDIES!

European Union Agency for Network and Information Security
<https://www.enisa.europa.eu/iot>



The EU Cyber Security Agency 

