# **IoT Security: User awareness**

- Be careful when buying used IoT devices, as they could have been tampered with

- Modify the privacy and security settings of the device to your needs
- 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

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









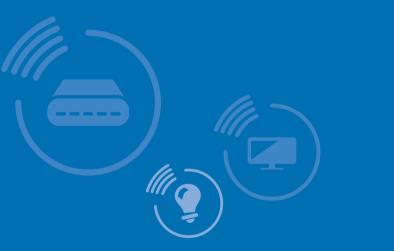
## **HOW TO CHOOSE A SMART HOME DEVICE SECURELY**

- Verify whether the smart features are really required or whether a normal device would be sufficient
- 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
- Disable features that are not being used

#### **HOW TO USE ONLINE SERVICES FOR SMART HOME SECURELY**



## INTERESTED TO LEARN MORE? CHECK OUT OUR STUDIES!

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



# 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

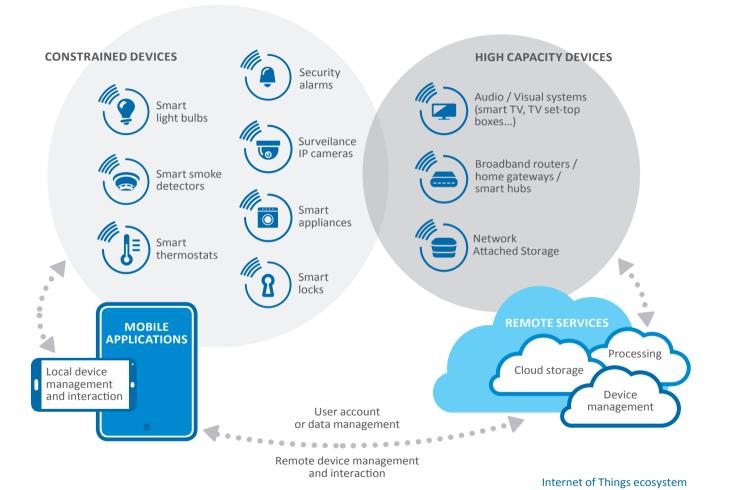
#### **ENISA IOT SECURITY GOOD PRACTICES FOR**

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









**DEVICE VENDORS AND SERVICE PROVIDERS** 

\*\*

# DEVELOPMENT OF SMART HOME DEVICES AND SERVICES

Security of the development process

- Design phase
- ✓ Development phase
- ✓ Testing phase

Security functions for hardware and software

- ✓ Security Audit
- Communication protection
- ✓ Cryptography
- ✓ User data protection
- ✓ Identification, authentication, authorisation
- **✓** Self-protection

END-USERS | ELECTRONIC COMMUNICATION PROVIDERS



# INTEGRATION OF DEVICES INTO THE HOME AREA NETWORK

Minimum reliability

- ✓ Hardware
- ✓ Software

#### Trust relationships

- ✓ Trust infrastructure
- ✓ Secure pairing✓ Check security assumptions
  - assumptions
- Network security

  ✓ Gateway for security
- ✓ Network segragation



#### USAGE UNTIL END-OF-LIFE

## Protection of data exchanges ✓ Ensure access rights

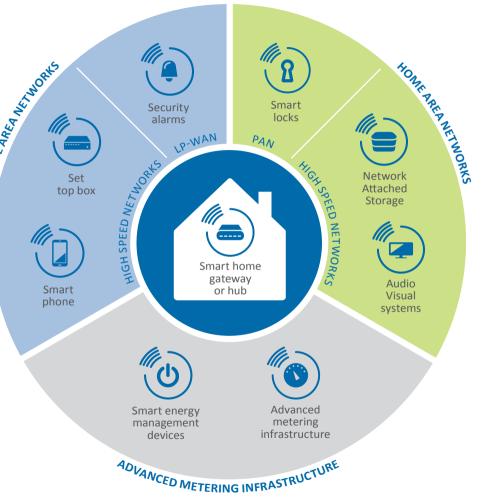
- ✓ Gateway for security
- Segregation with the AMI

#### Operational security and maintenance

- ✓ Vulnerability survey
- ✓ Security updates
- ✓ Remote interfaces protection✓ Security management system
- Security management system for support infrastructure

## Control of user data

Secure backup and/or deletion of data



Good practices for securing IoT

IoT connectivity