IoT Security: User awareness

**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

INTERESTED TO LEARN MORE? CHECK OUT OUR STUDIES!
European Union Agency for Network and Information Security
https://www.enisa.europa.eu/iot

**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.
- For battery-powered, smart devices providing alternate/emergency charging methods.

**How to operate a smart home device securely**
- Change default passwords of Wi-Fi networks and use robust encryption (e.g., WPA2).
- Change default passwords of device.
- Disable or protect remote access to IoT devices when not needed.
- Use wired connection instead of wireless where possible.
- Modify the privacy and security settings of the device to your needs.
- Disable features that are not being used.
- Use devices on separate router network where possible.
- Ensure that an outage (for example due to jamming or a network failure) does not result in a insecure 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.
USER ACCOUNT
or data management
Remote device management
and interaction

SMART APPLIANCES
- Smart locks
- Smart smoke detectors
- Smart thermostats
- Smart light bulbs
- Security alarms
- Surveillance IP cameras

MOBILE APPLICATIONS
- Local device management and interaction
- Remote device management and interaction
- Internet of Things ecosystem

DEVICE VENDORS AND SERVICE PROVIDERS
- Advanced metering infrastructure
- Home area networks
- High speed networks
- LP-WAN PAN

END-TO-END INTEGRATION OF DEVICES IN TO THE HOME AREA NETWORK
- Minimum reliability
- Infrastructure
- Trust relationships
- Access control
- Cryptography
- Secure data protection, authentication, authorization, self-protection

SECURITY ALARMS
- Gateways for security
- Segregation with the AMI
- Operational security and maintenance
- Vulnerability survey
- Security updates
- Remote interfaces protection
- Security management system for support infrastructure
- Control of user data
- Secure backup and/or deletion of data

MOBILE APPLICATIONS
- User account or data management
- Secure device management and interaction

HIGH CAPACITY DEVICES
- Network attached storage
- Broadband routers / home gateways / smart hubs
- Audio / Visual systems (smart TV, TV set-top boxes...)

SMART HOME DEVICES AND SERVICES
- Security of the development process
- Design phase
- Development phase
- Testing phase
- Security functions for hardware and/or software
- Secure data protection
- Cryptography
- Secure data protection, authentication, authorization, self-protection

SECURITY FUNCTIONS FOR HARDWARE AND SOFTWARE
- Security of the development process
- Design phase
- Development phase
- Testing phase
- Security functions for hardware and/or software
- Secure data protection
- Cryptography
- Secure data protection, authentication, authorization, self-protection

END-TO-END SECURITY FOR SMART HOME DEVICES AND SERVICES
- Protection of data exchanges
- Gateway for security
- Segregation with the AMI
- Operational security and maintenance
- Vulnerability survey
- Security updates
- Remote interfaces protection
- Security management system for support infrastructure
- Control of user data
- Secure backup and/or deletion of data

INTEGRATION OF DEVICES INTO THE HOME AREA NETWORK
- Minimum reliability
- Infrastructure
- Trust relationships
- Access control
- Cryptography
- Secure data protection, authentication, authorization, self-protection

SECURITY ALARMS
- Gateways for security
- Segregation with the AMI
- Operational security and maintenance
- Vulnerability survey
- Security updates
- Remote interfaces protection
- Security management system for support infrastructure
- Control of user data
- Secure backup and/or deletion of data

END-TO-END SECURITY FOR SMART HOME DEVICES AND SERVICES
- Protection of data exchanges
- Gateway for security
- Segregation with the AMI
- Operational security and maintenance
- Vulnerability survey
- Security updates
- Remote interfaces protection
- Security management system for support infrastructure
- Control of user data
- Secure backup and/or deletion of data

GOOD PRACTICES FOR SECURING IOT
- IoT connectivity
- Advanced metering infrastructure
- Smart home gateway or hub
- Device security
- User accounts
- Data security
- Network security
- Gateway for security
- Segregation with the AMI
- Operational security and maintenance
- Vulnerability survey
- Security updates
- Remote interfaces protection
- Security management system for support infrastructure
- Control of user data
- Secure backup and/or deletion of data

INTEGRATION OF DEVICES INTO THE HOME AREA NETWORK
- Minimum reliability
- Infrastructure
- Trust relationships
- Access control
- Cryptography
- Secure data protection, authentication, authorization, self-protection

SECURITY ALARMS
- Gateways for security
- Segregation with the AMI
- Operational security and maintenance
- Vulnerability survey
- Security updates
- Remote interfaces protection
- Security management system for support infrastructure
- Control of user data
- Secure backup and/or deletion of data

END-TO-END SECURITY FOR SMART HOME DEVICES AND SERVICES
- Protection of data exchanges
- Gateway for security
- Segregation with the AMI
- Operational security and maintenance
- Vulnerability survey
- Security updates
- Remote interfaces protection
- Security management system for support infrastructure
- Control of user data
- Secure backup and/or deletion of data

GOOD PRACTICES FOR SECURING IOT
- IoT connectivity
- Advanced metering infrastructure
- Smart home gateway or hub
- Device security
- User accounts
- Data security
- Network security
- Gateway for security
- Segregation with the AMI
- Operational security and maintenance
- Vulnerability survey
- Security updates
- Remote interfaces protection
- Security management system for support infrastructure
- Control of user data
- Secure backup and/or deletion of data