OTA
Online Trust Alliance

SMART DEVICE PURCHASE & SETUP CHECKLIST

Maximizing Security & Privacy of Connected Devices

SECURITY

□ Before purchase, confirm your ability to return the device for a refund if upon set up you find the security and/or privacy practices do not meet your personal requirements. If you cannot opt out of sharing data with third parties or are not provided the option of opting in, consider alternative products.

□ Before purchase review device’s warranty and support policies and verify that security and software patches are provided for the life of the product, beyond that of the warranty offered by the manufacturer.

□ Register your device providing your contact information and primary email address to the manufacturer to help ensure you receive security updates and related notifications to help maximize your security and privacy.

□ Verify your device is updated and patched directly from the manufacturer. Confirm the device is fully updated at setup and configured to install new updates whenever available. If possible enable automatic updates. After installing updates, verify your personalization, privacy and security settings have not been changed or modified.

□ Use a unique user name and password which does not identify your family or the brand/model of the device and change them frequently. This can reduce the threat of your device being maliciously targeted by hackers.

□ When downloading apps to your device, install them directly from the manufacturer's official site where possible and carefully review any requested permissions such as location tracking, use of the camera and microphone.

□ When browsing sites with your connected device, exercise the same caution you would with your personal computer or smart phone.

□ Turn off and unplug your device(s) if you are gone for extended periods of time to reduce the risk of your device being hacked, being susceptible to power surges and save on energy use.

□ If possible, connect your device directly through a wired connection. If your home router has a guest network, use it to isolate your device(s) from other networks.

□ Disable or protect remote access to your connected device(s) when not needed to reduce the risk of hacking.

□ Any device that connects to the Internet should be guarded by a firewall to help prevent unauthorized access. Use a router-based firewall and turn on any built-in firewall settings your device might have.

□ Document all of the smart devices and applications you use. List the company URL, passwords, contact email and phone numbers. Password protect the document or use a password “vault” mobile application.

PRIVACY

□ If you are selling your connected device, reset the device to factory settings and/or clear any saved data. If you are purchasing or using a previously owned or opened device, be sure it has been reset to factory settings (including ad identifiers, parental controls and privacy settings) before use, then secure it with a new password.

□ Review the privacy practices of connected devices you own or are considering buying, including data collection and sharing policies with third parties. Reset permissions to reflect your preferences (for example – data collection and sharing, camera and microphone settings and other functions). If your settings cannot be modified, consider the “reset to factory settings” option to force a clean setup.

□ To maximize your privacy, disable any camera and microphone when not actively/intentionally using them. Consider removing the camera, flipping it to face the wall or covering the camera lens to prevent accidental or unauthorized use. Doing so means the camera will only capture a black image or the wall.

□ Create user profiles with unique settings for children’s use of the device.

For updates visit - https://otalliance.org/SmartHome