CONNECTSMART!

Smart products can enhance our lives, but there can also be risks.

More and more people are purchasing smart products for their home that connect to the Internet. These connected devices can bring huge benefits, including greater efficiency, convenience, and insight, as well as the ability to monitor things remotely. However, alongside the benefits, there can be risks.

Check out our tips on how to connect smart!

SEARCH for potential security and privacy issues before buying

Search the product online for reviews or news articles that identify security or privacy issues. Check whether you can make your device more secure by changing the password and adjusting the privacy settings. Confirm if the device receives regular software updates so any security vulnerabilities can be fixed.

MAKE strong, unique passwords for each device

Generic default passwords can be easily identified and allow attackers to gain access. Set strong, unique passwords for each device, service and your home router. The longer the password the better; mix upper and lower case letters, numbers, and special characters to increase the strength.

ADJUST settings for maximum security and privacy

Many devices and services come with minimal security protection by default and collect significant amounts of important information about you – so change your settings for greater security and privacy. Also plan to reset your device regularly. If attackers do access your device, malicious code is often stored in memory and a reset will clear it. If you become aware of an incident that may affect your device, visit the manufacturer's website or contact the retailer where you bought it for information on what to do next.

REGULARLY update software

If the device or app has an auto-update feature, turn it on. Find out how to check for software updates for each device and do it once a month. Most companies will release updates when they patch security vulnerabilities. Also accept updates for the apps on your mobile phone that control your device.

TURN OFF features you don't need and device when not in use

Lots of features on your device can continue to monitor you even when you don't expect or need them to. To avoid this, disable cameras, microphones, or location tracking apps when you are not actively using them. And, if you are not using the device, turn it off.

CONSUMERS INTERNATIONAL

Internet Society