The terms ‘connected devices’ and ‘Internet of Things’ (or IoT) refer to devices that are connected to the internet, such as smartwatches, voice assistants, smart home devices like smart meters, and many more. As we steadily adopt smart devices into our lives, we shouldn’t forget to keep them secure and our data protected. But how can we preserve them from security threats?

Follow these eight crucial steps:

1. Give your router a name
   Don’t stick with the name the manufacturer gave it as it may identify the make or model.

2. Use a strong encryption method for Wi-Fi
   Use a strong encryption method like WPA2 as this will keep your network secure.

3. Set up a guest network
   Visitors, friends and relatives should log into your router using a separate network that doesn’t tie into your primary one. This is to ensure a virus doesn’t spread to your primary network, should they use a compromised or malware-infected device.

4. Change your connected devices’ default usernames & passwords
   Unique, strong passwords containing a combination of letters, numbers and special characters make it harder for hackers to access your data.

5. Disable features you may not need
   Connected devices come with a variety of services such as remote access, which are often enabled by default. So, if you don’t need it, be sure to disable it.

6. Avoid public Wi-Fi networks
   Public Wi-Fi networks that do not ask you to provide a password are NOT secure. So in case you need to use them for your mobile devices, make sure you use a VPN.

7. Keep your software up to date & install anti-virus software
   Your smart device makers may send you updates. Or you may have to visit their official websites to check for them. Be sure to carefully download (beware of malicious downloads) and apply regular updates as these may offer critical patches to security holes.

8. Use multi-factor authentication
   This requires a combination of two or more validation methods to access a device, making it impossible to breach by hackers.

https://justaskthales.com/