1.Give your router a smart name.

You don’t have to stick with the default name provided by the manufacturer as it could potentially identify the make or model. HakTrap suggests a unique name not associated with your or your address or any other personal identifiers.

2. Use a strong encryption method for Wi-Fi.

In your router settings, it’s a good idea to use a strong encryption method, like WPA2, when you set up Wi-Fi network access. This will help keep your network and communications secure.

3. Set up a guest network.

Keep your Wi-Fi account private. Visitors, friends and relatives can log into a separate network that doesn’t tie into your IoT devices. Keep your private network quarantined.

4. Change default usernames and passwords.

Cybercriminals probably already know the default passwords that come with many IoT products. That makes it easy for them to access your IoT devices and, potentially, the information on them. Are you considering a device that doesn’t allow you to change the default password? Then consider a different one.

5. Use strong, unique passwords for Wi-Fi networks and device accounts.

Avoid common words or passwords that are easy to guess, such as “password” or “123456.” Instead, use unique, complex passwords made up of letters, numbers, and symbols. You might also consider a password manager to up your security game.

6. Check the setting for your devices.

Your IoT devices might come with default privacy and security settings. You might want to consider changing them, as some default settings could benefit the manufacturer more than they benefit you.

7. Disable features you may not need.

IoT devices come with a variety of services such as remote access, often enabled by default.

If you don’t need it, be sure to disable it.

8. Keep your software up to date.

When your smart phone manufacturer sends you a software update, don’t put off installing it. It might be a patch for a security flaw. Mobile security is important, since you may connect to your smart home through mobile devices. Your IoT device makers also may sent you updates — or you might have to visit their websites to check for them. Be sure to download updates and apply them to your device to help stay safe.

9. Audit the IoT devices already on your home network.

It could be time to upgrade that old security camera. Take time to check if newer models might offer stronger security.

10. Do the two-step.

We’re talking authentication. Two-factor authentication — such as a one-time code sent to your cellphone — can keep the bad guys out of your accounts. If your smart-device apps offer two-factor authentication, or 2FA, use it.

11. Install HakTrap or a device like it.

There are many devices on the market at different price points that fits most consumers needs. Do your research and select the solution that matches your desired level of protection and budget.