General IoT and Smart Home Devices Security Tips

Compiled by the Clinic to End Tech Abuse

Last Updated: June 9, 2022

Who is this guide for?
Anyone who would like to strengthen the security and privacy of their Internet of Things (IoT) and Smart Home devices. It is especially for anyone who is concerned that an abusive person may be secretly monitoring them.

What does this guide cover?

Aspects to take into account

- We strongly recommend that you talk to a domestic violence or other appropriate organization to make plans for your safety if you are worried about violence or threats.
- We have marked changes that could be visible to an abuser with this sign:

Be careful!

This action could be visible to abuser

- All images included in this guide are for educational purposes only

What are IoT and Smart Home devices?

IoT devices: Internet of Things (IoT) devices can connect to the Internet, gather information from you, and make this information available from any device. IoT devices include wearables (e.g., fitness trackers), air quality sensors, and medical devices that track vital signs.

Image taken from https://www.findlayallhazards.com/blog/the-dangers-of-industrial-entropy-2/

Smart Home devices: they are IoT devices specifically used in homes. Examples include smart speakers (e.g., Google Home), smart doorbells (e.g., Amazon Ring), and smart thermostats. Devices like Amazon Echo and Google Home are set up with an account so that the owner of the device can administer its settings from a mobile app. The image on the left corresponds to the Amazon Echo smart speaker and the image on the right corresponds to a Ring smart doorbell:

Images obtained from https://www.pexels.com/photo/black-amazon-echo-on-table-977296 and https://www.amazon.com/Ring-Doorbell-Activated-Installation-Condition/dp/B08PCRN5YT

What is a Wi-Fi router?

It is the home device that connects your smartphones, tablets, smart speakers, video game consoles, etc. to the Internet.

Image taken from https://commons.wikimedia.org/wiki/File:TP-Link_WR841ND_WiFi_router_transparent.png

Usually, home devices are wirelessly connected to home Wi-Fi routers. However, devices could also be connected to it via an Ethernet cable:

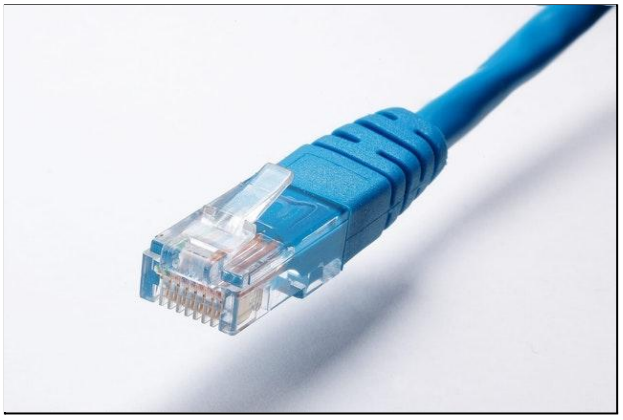


Image taken from https://www.pexels.com/photo/cable-connection-connector-cord-415043/

Many Smart Home devices need a Wi-Fi connection to work. Thus, it is common that they have a wireless connection with home Wi-Fi routers.

Common Smart Home devices

Smart Home devices range from smart speakers to home security cameras. The following website has an interactive tool that can help you identify common Smart Home devices and the data they can gather from you:

https://refugetechsafety.org/hometech

Image taken from https://refugetechsafety.org/hometech

Risks raised by Smart Home devices

Smart Home devices could be misused to monitor and harass people in many ways. For example:

- Smart cameras could be used by an abuser to know if the house is empty or if there are visitors
- An abuser could change the thermostat settings remotely (i.e., outside the home) to make the person currently located in the home feel uncomfortable
- Smart speakers could be used to record conversations

To address these risks and more, it is important to (1) identify the smart home devices in your home, (2) strengthen the security settings of the account associated with devices like smart speakers, and (3) get to know features these devices have to further protect you from, for example, unwanted location tracking. More information about this will be presented in the following sections.

Identifying devices connected to your Wi-Fi network

Many Smart Home devices need to connect to a Wi-Fi network for them to work. Consider installing an app like **Fing**, whose free version will allow you to scan your Wi-Fi network to identify the devices connected to it:

- Android app: https://play.google.com/store/apps/details?id=com.overlook.android.fing
- Apple/iOS app: https://apps.apple.com/us/app/fing-network-scanner

Fing will show you the devices' names, as well as more technical details like their IP and MAC addresses.

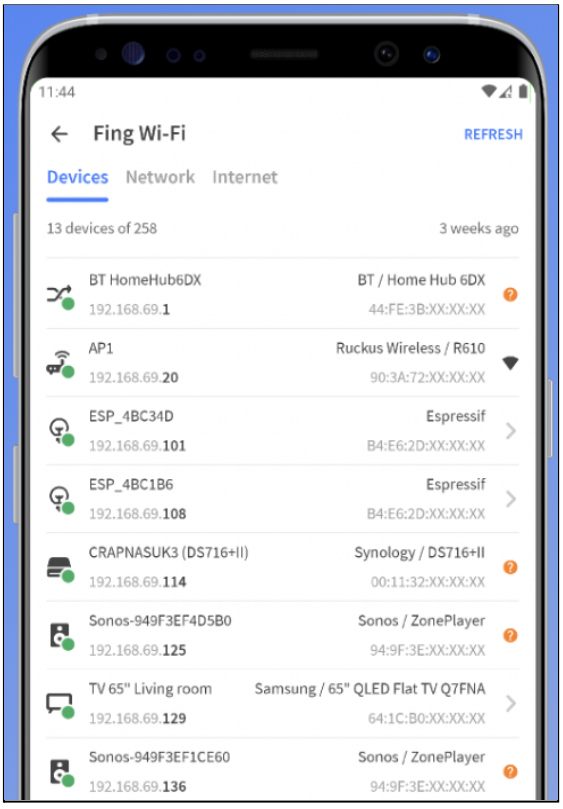


Image taken from https://play.google.com/store/apps/details?id=com.overlook.android.fing

What to do if an unknown device is connected to your Wi-Fi network

If you do not recognize a device connected to your Wi-Fi network, consider the following:

Could it be a device you use whose details are not shown?

Some information about devices is not shown by apps like Fing. In other cases, the shown device name or icon is generic. Thus, we encourage you to think about whether the “unknown device” could be a device you regularly use.

If you thought about this and still think the connected device does not belong to you, you could:

Change your Wi-Fi password

Be careful!

This action could be visible to abuser

Important: Keep in mind that if you change your Wi-Fi password, you would have to connect all your devices to your Wi-Fi network again.

You can change your Wi-Fi password via the app of your Internet service provider (e.g., the Xfinity app if your Internet service provider is Xfinity).

Another alternative to change your Wi-Fi password is for you to access your home Wi-Fi router’s administrator website. In order to access it, open a web browser (e.g., Google Chrome, Firefox, or Safari). In the URL field, enter the following options (the numbers as well as the dots, e.g. *192.168.0.1)* one by one and hit enter until one of the options displays a website:

- **Option 1:** 192.168.0.1
- **Option 2:** 192.168.1.1
- **Option 3:** 192.168.2.1
- **Option 4:** 10.0.1.1
- **Option 5:** 10.0.0.1
- **Option 6:** 10.10.1.1

The website that appears is your home Wi-Fi router's administrator website. In some cases, before seeing the website, you will see a window asking for a username and password. Usually, this information is printed on a sticker pasted on one of the sides of the home Wi-Fi router. This is an example Wi-Fi router administrator website (the website you see might look different depending on your internet service provider):

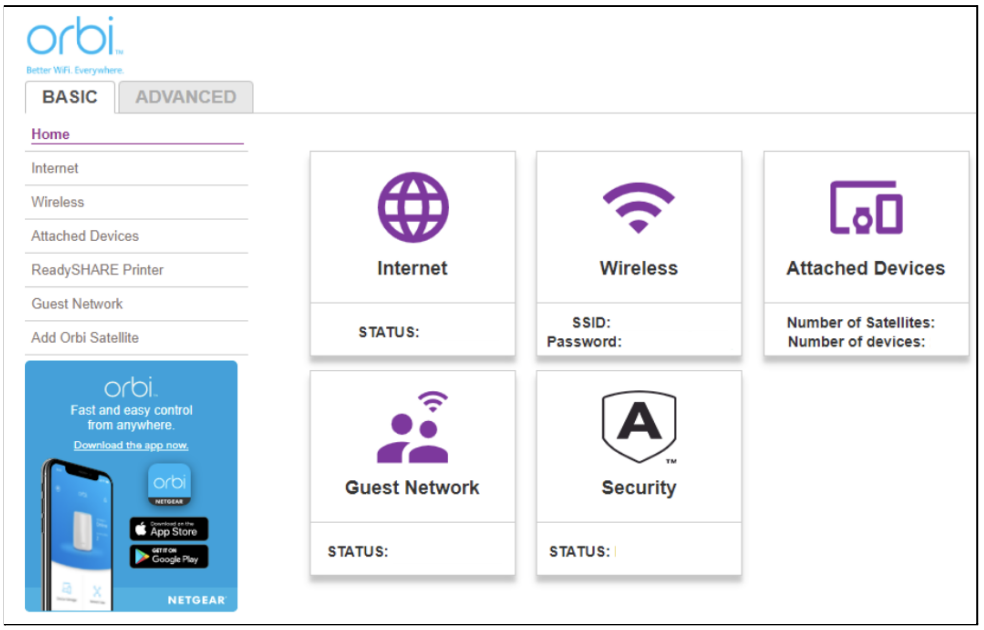


Image taken from https://www.pcmag.com/how-to/how-to-access-your-wi-fi-routers-settings

In the home Wi-Fi router administrator website, you can change your Wi-Fi password. Make sure to set up a new password the person you are concerned about cannot guess.

If you need further assistance, we encourage you to contact your internet service provider. They could assist you to change your Wi-Fi password.

Identifying IoT devices in your surroundings

You may install an app like **IoT Assistant** to help you find IoT devices in your surroundings. This app was developed by researchers at Carnegie Mellon University and it will show you a map of the area you are currently located at with flags of multiple colors that represent devices that gather different data from people nearby (e.g., a police security camera could be tracking visual data in a public space).

Important: You may see a lot of flags depending on the area you are located. These devices can be owned by universities, local authorities or other entities and used for benign purposes (e.g., to monitor the air quality in a park). Many flags are not necessarily cause for alarm.

IoT Assistant
Carnegie Mellon University Labs

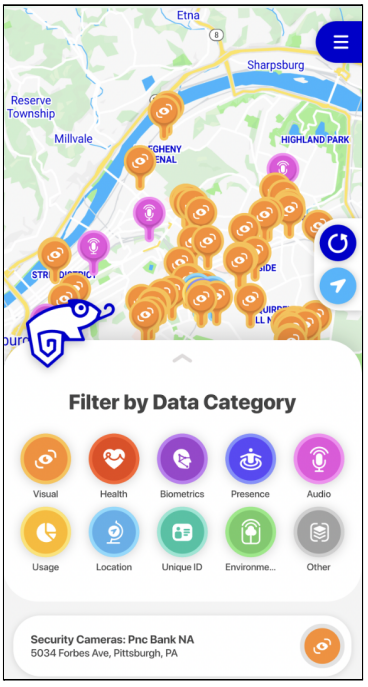


Image taken from https://play.google.com/store/apps/details?id=io.iotprivacy.iotassistant

- Android app: https://play.google.com/store/apps/details?id=io.iotprivacy.iotassistant
- Apple/iOS app: https://apps.apple.com/us/app/iot-assistant/id1491361441

How to be informed about unwanted location trackers (e.g., Apple AirTags and Tile trackers)

Location trackers like Apple AirTags or Tile trackers are marketed to help people find lost devices. The image on the left is an Apple AirTag and the image on the right is one Tile tracker:

Images taken from https://www.apple.com/airtag/ and https://www.thetileapp.com/en-us/store/tiles/pro

Tile trackers can vary in size and the way they look (e.g., companies allow users to add an emoji or a text on one of the tracker sides and buy cases/covers for them):

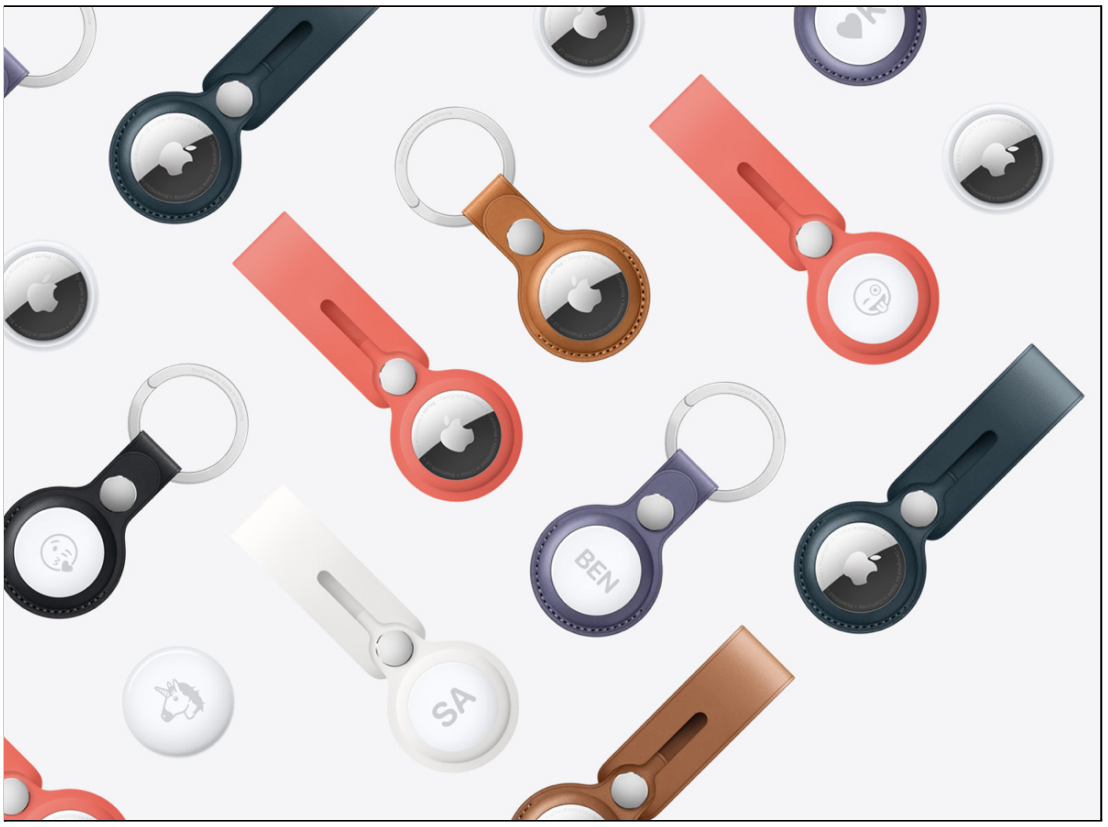


Image taken from https://www.apple.com/airtag/

Location trackers could be repurposed to track people's whereabouts.

Protecting yourself from unwanted location tracking (Apple AirTags)

If you have an iPhone (Apple phone)
First, make sure that:

1. Your iPhone's software is up to date (Settings > General > Software Update)
2. **Location Services** is on (Settings > Privacy > Location Services)
3. **Find My iPhone** is on (Settings > Privacy > Location Services > System Services)
4. **Significant Locations** is on (Settings > Privacy > Location Services > System Services)
5. **Bluetooth** is on (Settings > Bluetooth)
6. Tracking Notifications is on (Find My app > Me)
7. **Airplane mode** is off

If the above conditions are met, then your iPhone will show you a notification if it detects an unknown Apple AirTag moving with you. The notification will look like this:

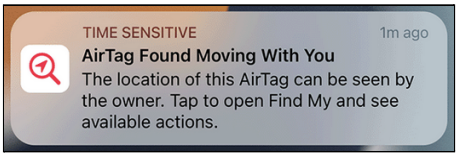


Image taken from https://support.apple.com/en-us/HT212227

If you tap on the notification, you will see a map and various options:

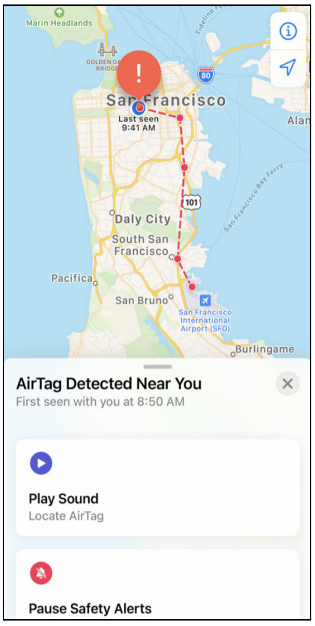


Image taken from https://www.apple.com/airtag/

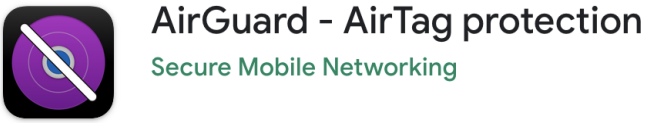
The map will show you the trajectory along which the Apple AirTag has been moving with you. Additionally, below the map you can tap on **Play Sound** so that the Apple AirTag emits a sound for you to locate it. If you scroll down, you will see an option to obtain more information about the AirTag.

Also, we recommend you to check your iPhone, specifically go to **Settings** > **Your name** > scroll down and check if an Apple AirTag appears on the list of devices connected to your iCloud account.

If you have an Android phone (e.g., a Samsung, LG, Google phone, etc.)
Install an app titled **Tracker Detect** that can inform you about an unknown Apple AirTag moving with you:

- Android app: https://play.google.com/store/apps/details?id=com.apple.trackerdetect

Alternatively, install **AirGuard**, a free Android app developed by security researchers in Germany:



- Android app: https://play.google.com/store/apps/details?id=de.seemoo.at_tracking_detection.release

This video summarizes the actions you can take if you receive an “AirTag Found Moving With You” notification: https://www.youtube.com/watch?v=mGh7-IuPRR4

Be careful!

This action could be visible to abuser

Important: the person you are concerned about can immediately realize that the AirTag stopped reporting location data (e.g., if you remove its battery). We encourage you to do safety planning with a support worker if you are concerned this might cause an escalation of abuse.

More information about what you could do if you receive a notification informing you about an Apple AirTag moving with you is available here:
https://support.apple.com/en-us/HT212227

Protecting yourself from unwanted location tracking (Tile trackers)

Install the **Tile** app and use the Scan and Secure feature to look for trackers in your surroundings.

Tile
Tile Inc.

- Android app: https://play.google.com/store/apps/details?id=com.thetileapp.tile
- Apple/iOS app: https://apps.apple.com/us/app/tile-find-lost-keys-phone/id664939913

Be careful!

This action could be visible to abuser

Important: we encourage you to do safety planning with a support worker if you are concerned about escalation of abuse.

General privacy and security tips

1. **Change default passwords**

Be careful!

This action could be visible to abuser

Most IoT devices and Wi-Fi routers come with default usernames and passwords. It is very important for you to change them to set up stronger passwords that are difficult to guess or find online by anyone. This website can help you test password strengths: https://password.kaspersky.com/

2. **Keep your devices up to date**

Software updates often contain important changes to improve the security of your devices to mitigate new forms of risks. When connected to the Internet, many devices automatically look for software updates. However, you can manually check for updates via your Smartphone or apps' settings.

3. **Install apps that help you detect security problems (e.g., antivirus apps)**

Be careful!

This action could be visible to abuser

Examples of apps that can help you detect security problems in your devices include iVerify available in Apple App Store, and antivirus apps available in Google Play, like AVG, Avast, McAfee, Malwarebytes, Kaspersky, Norton 360, and ESET. Antivirus apps can also be installed on other devices (e.g., Windows computers).