Using a Bluetooth Scanner to Search for Hidden Trackers

What are Bluetooth trackers?

Bluetooth trackers are small devices that can send precise location information to the person who owns the device. These devices can be useful to help people find everyday objects that are lost, such as keys or wallets. However, because they are small (often the size of a deck of playing cards or smaller), easy to hide, and give precise location, these devices can be misused for stalking. Examples of trackers include AirTags, Tile, and Chipolo devices.

How can I find a bluetooth tracker?

Method 1: Manual Search

One method for finding trackers is to manually search for them in common places. These include:

- Vehicles (wheel wells, license plates, under the carriage, under the hood)
- Purses,
- Backpacks, or
- Clothing items.

They may be hidden within the linings, pockets, or upholstery of these items.

The most recent versions of iPhones or Androids should automatically notify you about an Apple-branded tracker (an AirTag) that has been moving with you while separated from its owner. However, these notifications may not detect trackers that move with you for a short period of time, such as an AirTaig on a vehicle driven for a short distance.

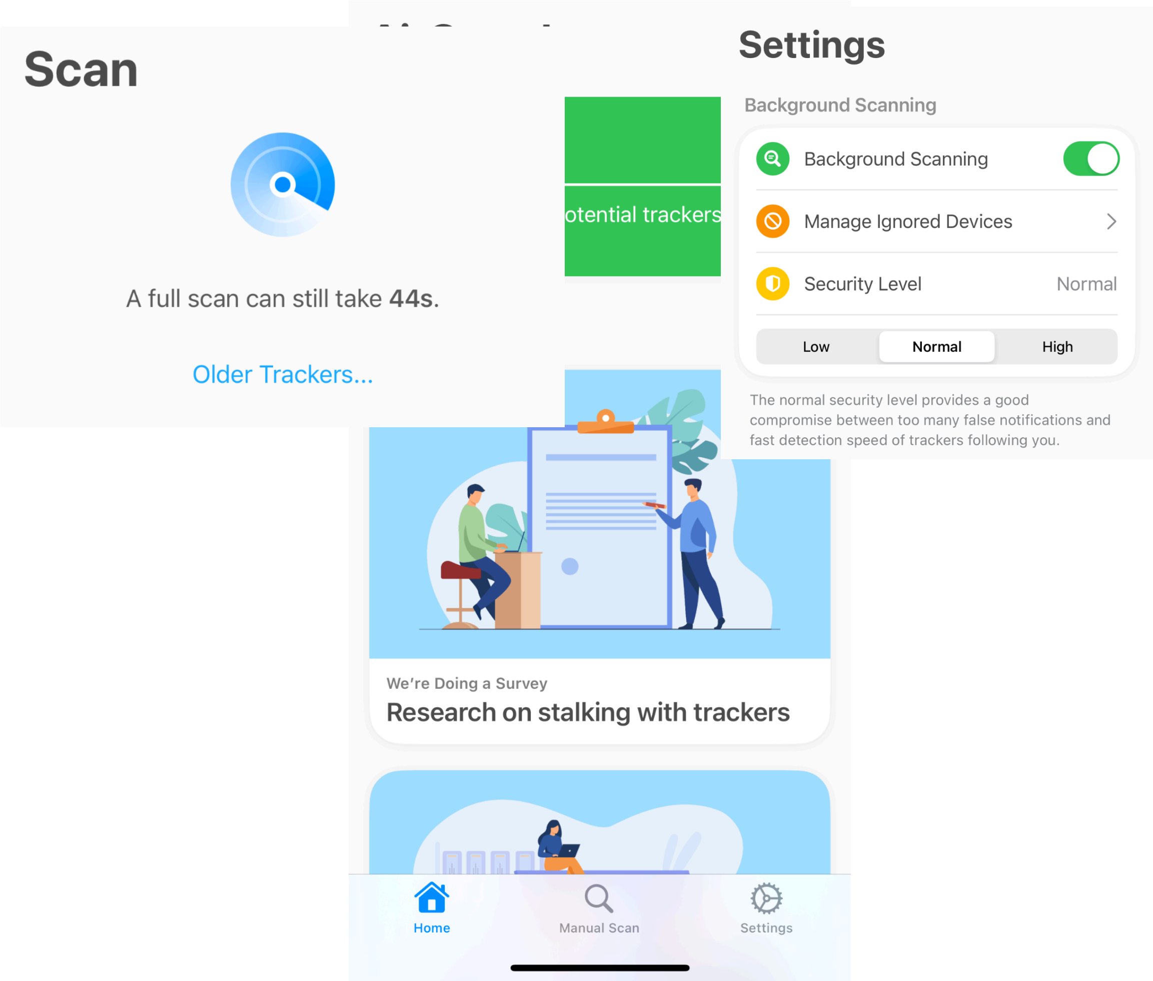
This guide will give step-by-step instructions and tips for using an app to help scan for trackers. While there are many apps that can scan for Bluetooth devices, we recommend using AirGuard which scans specifically for popular brands of Bluetooth trackers, or nRF Connect which detects any Bluetooth devices, including non-tracking devices such as headphones or smartwatches. We explain both apps below.

Method 2: Download the AirGuard app

Airguard is an app developed by researchers specifically designed for finding Bluetooth trackers. It scans for the most common brands of trackers. At the time of writing, it scans for AirTags, Tiles, SmartTags, and Chipolo devices. AirGuard is available for both **Android and iPhone.**

To use AirGuard, download it from either the iPhone AppStore of the Google PlayStore, and give it permission to use both your device's Bluetooth and Location.

When you open the app, it will look similar to the image below (although it may look different on newer versions or Android). It will tell you whether it has detected any suspicious trackers moving with you over the past 14 days. There are also options called **Manual Scan** and **Settings.**



Scan

A full scan can still take **44s**.

Settings

Background Scanning: on

Security Level: Normal

The normal security level provides a good compromise between too many false notifications and fast detection speed of trackers following you.

We're Doing a Survey

Research on stalking with trackers

Manual Scan Selecting manual will make the app perform a manual scan for Bluetooth trackers currently in your nearby vicinity. It will scan for **all** trackers, not just trackers that have been moving with you.

Settings The settings options will allow you to toggle on and off background scanning. When background scanning is enabled, AirGuard will stay active even when you exit the app, and constantly search for trackers. If it detects a tracker that is moving with you, it will sned you a notification.

You may also ignore all devices of a certain type by selecting "Manage Ignored Devices" and selecting which brands of trackers to detect.

Finally, you can choose how sensitive the app is to potentially suspicious trackers by selecting from **Low, Medium, and High**. A high sensitivity will alert you of trackers moving with you for only a short period of time, but it may lead to more false positives.

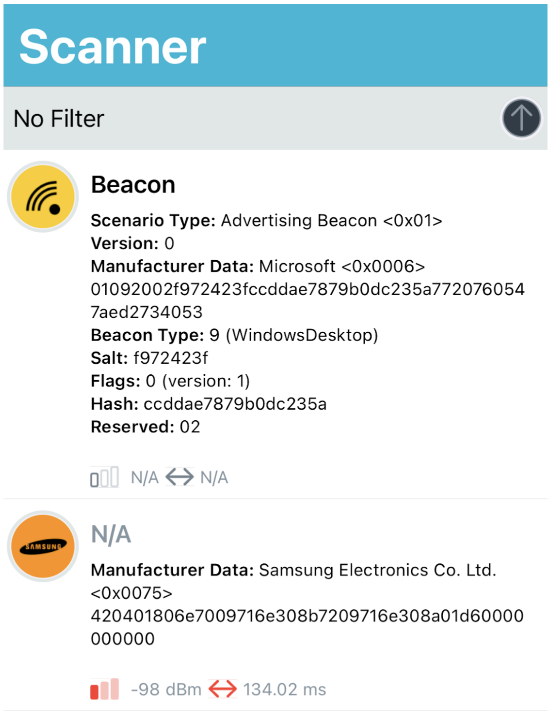
Method 3: Download the NRFConnect App

AirGuard is designed specifically for searching for Bluetooth trackers, and detects the most common and most effective brands of trackers. However, other brands of trackers may not be detected by AirGuard. An alternative to AirGuard that is to use an app that scans for all Bluetooth devices, even ones that are not trackers. This method is more comprehensive, but less user-friendly, because this method detects all Bluetooth devices which can include keyboards, headphones, speakers, and smartwatches. Below are some tips for using one of these apps, NRFConnect, to search for potential trackers.

1) Download an app that can scan for Bluetooth devices. We recommend **nRF Connect,** and this guide is based off that.
    a. For Android devices, the app can be downloaded from the PlayStore (link to app).
    b. For iPhones, the app can be downloaded from the App Store (link to app).

2) When you open the app, you will most likely see many devices around you. This is normal, especially if you live in an apartment building. The app will detect many devices, including laptops, phones, speakers, headphones, and even devices used for public

infrastructure.



Beacon

Scenario Type: Advertising Beacon <0x01>
Version: 0
Manufacturer Data: Microsoft <0x0006>
01092002f972423fccddae7879b0dc235a772076054
7aed2734053
Beacon Type: 9 (WindowsDesktop)
Salt: f972423f
Flags: 0 (version: 1)
Hash: ccddae7879b0dc235a
Reserved: 02

N/A ↔ N/A

N/A

Manufacturer Data: Samsung Electronics Co. Ltd.
<0x0075>
420401806e7009716e308b7209716e308a01d60000
000000

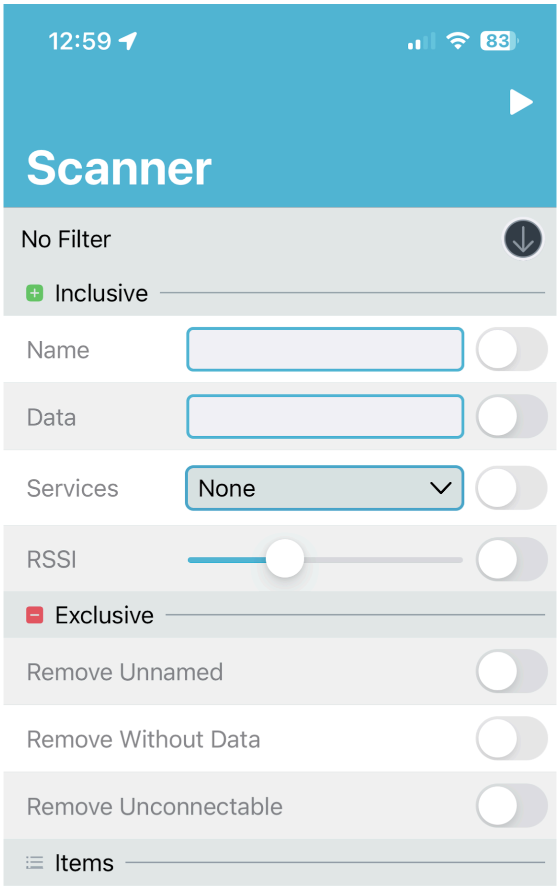
-98 dBm ↔ 134.02 ms

It will look like this:

3) To help hone in on potential trackers, select the **Filters** option. All Bluetooth devices have a signal strength. Typically, the stronger the signal, the closer the Bluetooth device is to your phone. By filtering for devices sending a **strong** signal to your phone, the app will show only nearby devices.

To do this, tap on the grey “No Filter” bar, which opens a menu:

4) From here, select the toggle that says **RSSI** with a slider bar. RSSI allows you to filter by signal strength. The interface will now tell you how many devices it is filtering (see below). In the below example, it is now only showing 4 out of the 257 devices it found. These are the devices with the strongest signal, usually the closest.



12:59

83

Scanner

No Filter

Inclusive

Name

Data

Services None

RSSI

Exclusive

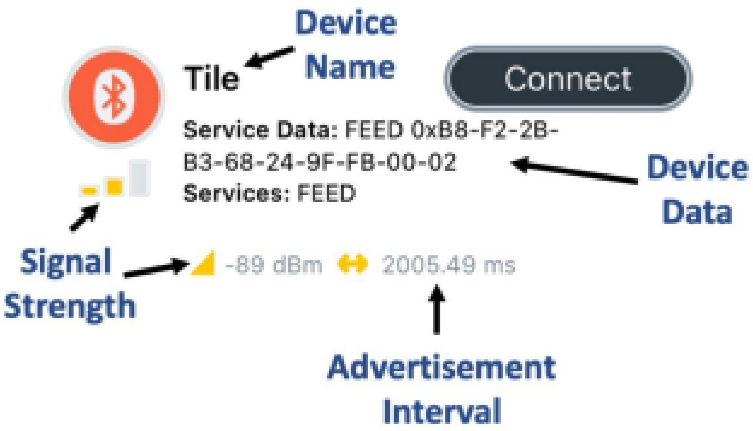
Remove Unnamed

Remove Without Data

Remove Unconnectable

Items

Drag the slider to adjust the sensitivity. Setting it to around -60 dBm should help initially. Dragging the slider left makes it less sensitive (only show devices with a **strong** signal), and dragging the slider right makes it more sensitive (show devices even with a **weak** signal). You can play with the setting to see how many devices show up.

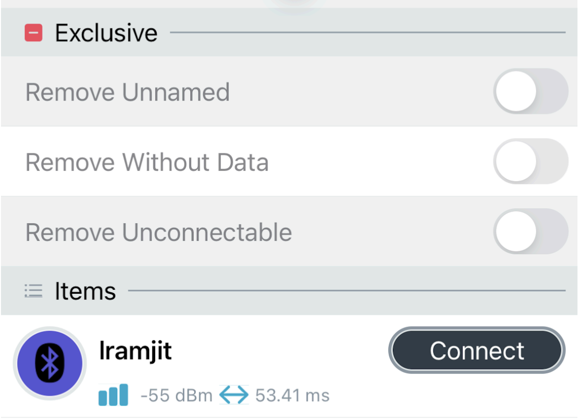

Tile

Service Data: FEED 0xB8-F2-2B-B3-68-24-9F-FB-00-02

Services: FEED

-89 dBm 2005.49 ms

Figure 1: Example Bluetooth device shown in the nRF connect app.


Exclusive

Remove Unnamed ○

Remove Without Data ○

Remove Unconnectable ○

Items

Iramjit

-55 dBm 53.41 ms

5) The app unfortunately can only give a limited amount of information about the types of devices it finds, such as the *device name* and *service data* (a way for the system to identify a device) The below example (credited to Maggie Delano's guide), explains what each piece of information means. Some devices will share their name, such as in the example of a Tile device above. Others will not. This depends on the device, not the app.

You can check for devices that you know are in the area, such as your own electronic devices, and try moving them farther away to help identify unknown devices with a strong signal.

What to do if you suspect that a tracker is being used to stalk you

If you are worried about a Bluetooth tracker in your clothes, bag or in a car, try to remove everything from your pockets, the bag, or the car. Leave your electronic devices other than your phone in a safe place, as they will likely have a Bluetooth signal picked up by the app. This will minimize the number of potentially benign Bluetooth devices detected by the app.

Then **try driving the car or walking to different locations to see if the signal remains strong wherever you go.** If the signal remains strong (remember strong signal means nearby) then there may be a tracker that is still traveling with you.

Cars themselves may show up as Bluetooth devices if your car is Bluetooth-enabled, but keeping track of how many devices are moving with your car can help clue you in.

What to do if you find a device

Keep in mind that if you find a device on something that you do not own (e.g. a vehicle that is registered to another person), it may not be legal to remove or disable the device.

Disabling the device

WARNING: The person who placed the device will be able to see that the device has been disabled and will be able to view the last location which may put you in danger. Please contact law enforcement or a local domestic violence agency for resources if you are concerned for your safety.

You can disable the device by prying apart the plastic casing and removing the battery. Another alternative is to mail the device to another location, or dispose of it in a public waste area.

Finding out who placed the device

You can inspect the tracking device looking for a few things: the manufacturer name, the device type (there may not be one), and a serial number or UPC code (usually inside a compartment/near the battery). Then go to the manufacturer's website and look for "illegal stalking" or "help"--this should give you an email address to contact. Even if the tracking device doesn't have an app for remote access, the company should still be able to trace it by the serial number. A civil subpoena or a criminal investigation request from law enforcement directed to the manufacturer should be able to elicit significant information about the device.

Outside of legal options, you can try a few things to help learn more about the device. You can try downloading the app and attempt to register the device as if it's new, and see if the app tells you anything, such as account recovery information. You can also try calling customer support and simply asking for who its registered to—you can just say "Oh, someone set up this device and we can't remember who it was. Can you tell us the name on the account?" They should say no, but often they won't.