

AirTags & Bluetooth Trackers

What are Bluetooth trackers?

Bluetooth trackers are small inexpensive gadgets that can be attached to or placed inside property. They are intended as a way to locate lost items – the trackers can make a noise, or be located on a map. They are paired with one or more devices used by their owner – typically a mobile phone, or a tablet.

Many trackers use only Bluetooth and can only be tracked when their user is nearby. They will often give the tracker's last known location – the last time the tracker and its paired device were close together.

Other Bluetooth-only trackers do not need to be in proximity of the paired/original device. Where the tracker is nowhere near its paired/original device, the location of the tracker is relayed by nearby compatible devices – for example, for AirTag, any Apple device using the 'Find My' network.

Some trackers, e.g. the Vodafone Curve, have GPS capability which means they do not need nearby devices to function. These are usually larger with a short battery life.

Can someone be tracked through an Apple AirTag or other Bluetooth tracker?

These devices can be used to stalk people by dropping them into a bag or pocket, or hiding them in or attaching them to a vehicle.

If a victim finds a Bluetooth tracker in or on their property that they do not recognise, they should photograph where it was found (if safe to do so) and contact the police, or Officer in the Case (OIC) in an on-going case.



Victims should try to avoid taking a tracker home with them, or to any location significant to them, especially if it is a location unknown to their stalker.

AirTags (Apple iOS)

How it works

Apple AirTags use any nearby Apple device using Bluetooth and the Find My network to relay their position. Provided they are near such a device they can be constantly tracked by their owner. AirTags can be set to Lost Mode, or remotely disabled by the owner.

How you can tell an unknown AirTag is moving with you

If you use an Apple device the Find My network will notify you that an unknown AirTag is seen moving with you for a period of time, showing the alert "AirTag Found Moving With You". Other devices, such as AirPods or third party devices using Find My will produce similar alerts - see <u>Apple's guidance on unknown AirTags</u> for how these appear.

This notification feature is only present in iOS 14.5 and above and so you should keep all devices updated with the latest iOS.

If one of these messages appear, a stalker could be using an AirTag or other device to track the location of the victim.

An AirTag will also make a beeping sound when it has been out of range of its paired/original device for between 8 and 24 hours. This is useful for users of Apple devices who have turned off Bluetooth and the Find My network, and for users of other (or no) devices. However, it is possible to tamper with the AirTag to disable the audible warning, or to place it so that the sound is muffled or completely muted.

Apple have released an app, Tracker Detect App, for Android users to detect AirTags. This does not alert in the same way as an Apple device - victims would have to manually scan for any AirTags in the area. The Tracker Detect app can be made to



scan for around ten minutes to search for AirTags. Any nearby AirTag can then be made to play a sound to help locate it.

What to do if you find an unknown AirTag

Consult Apple's guidance on what to do if you are alerted that an unknown AirTag or other device is moving with you. Instructions on how to disable an AirTag that you have physically found are under the heading **Get information about or disable an AirTag, Find My network accessory or set of AirPods**.

The instructions show how to find out the serial number of the AirTag, and how to disable it (by removing the battery). The victim of stalking should screenshot or photograph the serial number of the tracker, and note the time and date, as evidence for the police.

Once this has been done, the victim may wish to disable the AirTag. This should be done with caution as the owner of the AirTag will be aware it has been disabled. In a domestic abuse situation where the victim is still living with their abuser it may be better not to disable the AirTag.

The victim should not contact the owner directly if they are concerned for their safety – contact the police if in immediate danger, or the OIC in an ongoing case, and pass on the serial number for them to investigate.

If the stalker realises their tracker has been found, they may report is as lost or disable it from their own account to avoid detection.

No history or location data stored on the AirTag – it is end to end encrypted, so only the owner of the tag can see its location. Anyone else finding an AirTag will not be able to find out where it has been.



Tile trackers

How it works

Tile trackers are used with a dedicated app. The Tile is not routinely tracked by the app, but if it is not near to its paired device the owner can turn on Notify When Found. This will show the tracker's last known location – originally this will be where it was last in contact with its paired device, but will be updated if it is close to another device running the Tile app. Premium, paid use of Tile allows the owner to see where the tracker has been over the last 30 days.

Although Tiles are popular, they are far less common than Apple devices on the Find My network, so will be rather less effective in tracking either lost property or people.

Newer Tiles have a QR code stamped on the rear of the gadget, which is intended to allow someone finding a Tile to contact its owner. However, completing these details is voluntary for the owner, and not linked to details associated with its paired device, so the owner can easily remain anonymous.

How you can tell an unknown Tile is moving with you

Tiles currently do not have an audible alert like AirTags if they are separated by their owners for extended periods of time. They cannot be scanned for specifically, but may appear in a scan for general Bluetooth devices (see **Other trackers** below).

What to do if you find an unknown Tile

The Tile Pro (the new rectangular version, and earlier square version) have batteries which can be removed to stop the device from tracking. Other Tiles can be tightly wrapped in aluminium foil to dampen any Bluetooth signal, which would allow the victim to take it to the police to report, without the owner being aware. The victim should try to avoid taking the Tile home with them, especially if they are unable to disable it.



Other trackers

There are numerous other trackers on the market, which may be associated with a brand of phone (Galaxy Smart Tag), a mobile network (Vodafone Curve), branded (Chipolo), or generic (there are numerous cheap, unbranded trackers available on eBay and Amazon).

If a victim finds any kind of unknown tracker on they should photograph where it was found (if safe to do so) and contact the police, or Officer in the Case (OIC) in an ongoing case.

For branded trackers, it may be useful for the victim to search for it online to find out about its capabilities and whether it can be disabled. For example, the Vodafone Curve is a GPS tracker (as well as Bluetooth) so does not rely on nearby devices to pinpoint its location. This makes it much more effective as a long-distance tracker than most Bluetooth devices, and also means it's considerably larger with a short battery life.

How to find other trackers

A victim can look for Bluetooth devices in the area by using either the Bluetooth settings on their phone, or by downloading a dedicated Bluetooth device scanning app from the App Store or Google Play. However, these scanners will pick up any active Bluetooth device in the area – there may be many such devices, often not labelled with helpful or accurate names. Not all scanners are equally accurate or comprehensive – some may miss devices entirely.



Example trackers

This shows a selection of popular trackers available at the time of writing. Some of these are available in different colours, and older versions of e.g. Tile come in a wide range of colours and designs. Other trackers, branded and unbranded, are available.

Galaxy Smart Tag



Size: 39.1mm square by 10.4mm deep

Weight: 13g

Battery life: Up to 300 days (removeable/replaceable)

Apple AirTag



Size: 31.9mm diameter by 8.0mm deep

Weight: 11g

Battery life: Over a year (removeable/replaceable)

Tile



Pro:

Size: 58mm x 32mm by 7.5mm deep

Weight: 14g

Battery life: Up to one year (removeable/replaceable)





Mate:

Size: 37.8mm square by 7.1mm deep

Weight: 8g

Battery life: Up to 3 years (non-removeable/replaceable)

Note: There are multiple Tile models, including older versions in a number of colours and designs: <u>Tile Models</u>

Chipolo



Size: 37.9mm diameter by 6mm deep

Weight: 8g

Battery life: Up to 2 years (removeable/replaceable)

Vodafone Curve



Size: 42.1mm diameter by 16.4mm deep

Weight: 30g

Battery life: Up to 7 days (rechargeable)

Note: Battery life is shorter when the Curve is being

actively tracked.



Other and unbranded trackers



These vary in size, weight, battery type and life. Very cheap Bluetooth only trackers tend to be around keyfob size and often take C2302 batteries, while some are rechargeable. Small GPS trackers requiring their own SIM card are also available.

All URLs

How you can tell an unknown AirTag is moving with you

https://support.apple.com/en-gb/HT212227

What to do if you find an unknown AirTag

https://support.apple.com/en-gb/HT212227

Example trackers

https://tileteam.zendesk.com/hc/en-us/articles/229572348-Tile-Models