

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to find an unwanted AirTag or Bluetooth tracker nearby

<https://cyberguardlab.com/blog/unwanted-airtag-bluetooth-tracker>

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.

CYBERGUARDLAB · GUIDE

How to find an unwanted AirTag or Bluetooth tracker nearby

TRACKER ALERT

AirTag Found Moving

Play Sound, Find Nearby, then disable the tracker.

With You

Play Sound · Find Nearby

Disable — don't just mute BT

Locate the physical tag

NFC serial + Instructions

Android: Tracker Detect

An unwanted AirTag or Bluetooth tracker alert means a Find My-compatible item (or another industry-spec tracker) may be traveling with you while separated from its owner-so someone else could see its location. This guide is about finding and handling that unknown tracker on iPhone, iPad, or Android. It is not about locking a lost phone, changing smart-home defaults, or "hacking" someone else's AirTag.

What an unwanted-tracker alert actually means

Apple and Google built cross-platform unwanted-tracking alerts so phones can warn you when a tracker moves with you over time. On Apple devices you may see alerts such as AirTag Found Moving With You, AirPods Detected, "Product Name" Found Moving With You, or Unknown Accessory Detected. Separated AirTags (and some accessories) can also play a sound when moved. A borrowed Family Sharing item can trigger an alert too-so the first job is to locate the device, not panic.

Paid link

Norton 360 | See the Norton first-year offer



Norton 360

From \$39.99

first year - 30-day refund

See the offer

[See the Norton first-year offer](https://cyberguardlab.com/norton)

Offer page: <https://cyberguardlab.com/norton>

Turn on tracking notifications (iPhone / iPad)

- * Update to a supported OS (Apple: Tracking Notifications from iOS/iPadOS 14.5+; compatible non-Apple Bluetooth trackers need iOS/iPadOS 17.5+).
- * Settings -> Privacy & Security -> Location Services -> On; under System Services, keep the location-related options Apple lists for tracking alerts enabled.
- * Settings -> Bluetooth -> On.
- * Settings -> Notifications -> Tracking Notifications -> Allow Notifications.
- * Turn Airplane Mode off-alerts will not arrive in Airplane Mode.

Steps when you get an alert or hear a sound

- * Tap the alert -> Continue -> Play Sound. Listen and replay if needed.
- * If available on a supported iPhone with Ultra Wideband, tap Find Nearby and follow Precision Finding until you locate the item.
- * Search belongings you rarely check: jacket pockets, bag outer pockets, under a car seat or bumper area, luggage tags.
- * If you cannot find it and feel unsafe, go to a safe public place and contact local law enforcement. Do not rely on turning off Bluetooth or Location Services on your phone-that does not stop the tracker's owner from seeing its location.
- * When you find an AirTag, hold the top of an NFC-capable phone near the white side until a notification appears; note the serial number and partial owner contact, and screenshot for records.
- * Tap Instructions to Disable and follow on-screen steps so the owner stops getting live location updates.

iPhone vs Android: how you scan

Platform | Built-in alerts | Manual check

iPhone / iPad | Find My unwanted-tracking notifications (when Bluetooth + Location + Tracking Notifications are on) | Find

My -> Items -> review unknown items detected with you; Play Sound / Find Nearby from the alert

Android 6.0+ | Google unwanted-tracking detection for AirTags / Find My-compatible trackers | System scan for unknown trackers, or Google Play Tracker Detect (scan ~10+ minutes, then play sound if found)

If you feel your safety is at risk

- * Prioritize getting to a safe public place over "fixing" tech settings.
- * Keep the physical tracker and screenshots of serial / owner digits for police.
- * Law enforcement can request information from Apple related to an unlawfully used AirTag or Find My accessory-provide the device and serial when asked.
- * Tell a trusted person where you are; avoid confronting someone you suspect planted the tracker alone.

FAQ

Could this just be a borrowed AirTag or AirPods?

Yes. Family Sharing or a friend's forgotten tag/buds can trigger alerts. Still locate the item; you can mute alerts for a Family Sharing item if Apple offers that option on the notification.

I turned off Bluetooth on my phone. Am I safe?

No. Disabling Bluetooth, Location Services, or Find My on your device does not stop the tracker's owner from seeing its location. You must disable the tracker itself using Apple's Instructions to Disable (or the equivalent for a compatible non-Apple tracker).

Does Microsoft Defender or buying new antivirus find AirTags?

No. Unwanted trackers are found with OS tracker alerts / Tracker Detect / NFC, not antivirus. Antivirus still helps if a phishing page later tries to steal accounts on the same phone or PC-buy nothing required; Microsoft Defender is valid on Windows.

Android only-what should I install?

Use the system unknown-tracker features when available, or Apple's Tracker Detect app from Google Play for Find My-network AirTags and compatible tags.

Related reading on CyberGuardLab?

See lost phone lock steps and smart-home default passwords-different problems than a hidden tracker.

If you still want a paid suite

Finding an unwanted tracker does not require paid antivirus. Use OS alerts, Tracker Detect, and NFC disable steps-buy nothing if that is enough. Optional PC/phone malware hygiene after any related phishing: Norton (paid link), Bitdefender (paid link), TotalAV (paid link), McAfee (paid link), Avast (paid link).

Extra caution

If an alert appears after a date, ride-share, or workplace conflict, treat safety first. Locating and disabling the tracker is the tech fix; documenting serial numbers for law enforcement is the safety path.

Sources

- * Apple: Unwanted tracking alert steps
- * Apple: Detect unwanted trackers (Personal Safety)

Also read

- * Lost phone: lock Apple and Google accounts
- * Change smart-home default passwords
- * Is Microsoft Defender enough?
- * Android Private DNS setup
- * Home security camera hygiene

* Clicked a phishing link: first hour