How concerned should you be about AirTags?

January 30 2023, by Sophie Cox

AirTag. Credit: Wikimedia Commons. Image licensed under Creative Commons Attribution-Share Alike 4.0 International. Creator: KKPCW

I didn't even know what an AirTag was until I attended a cybersecurity talk by Nick Tripp, senior manager of Duke's IT Security Office, but according to Tripp, AirTag technology is "something that the entire Duke community probably needs to be aware of."

An AirTag is a small tracking device that can connect to any nearby Apple device using Bluetooth. AirTags were released by Apple in April 2021 and are designed to help users keep track of items like keys and luggage. Tripp himself has one attached to his keys. If he loses them, he can open the "Find My" app on his phone (installed by default on Apple devices), and if anyone else with an Apple device has been near his keys since he lost them, the Bluetooth technology will let him see where his keys were when the Apple device user passed them—or took them.

According to Tripp, AirTags have two distinct advantages over earlier tracking devices. First, they use technology that lets the "Find My" app provide "precise location tracking"—within an inch of the AirTag's location. Second, because AirTags use the existing Apple network, "every iPhone and iPad in the world becomes a listening device."

You can probably guess where this is going. Unfortunately, the very features that make AirTags so useful for finding lost or stolen items also make them susceptible to abuse. There are numerous reports of AirTags being used to stalk people. Tripp has seen that problem on Duke's campus, too. He gives the example of someone going to a bar and later finding an AirTag in their bag or jacket without knowing who put it there.

The IT Security Office at Duke sees about 2–3 suspected cyberstalking incidents per month, with 1–2 confirmed each year. Cyberstalking, Tripp emphasizes, isn't confined to the internet. It "straddles the internet and the real world." Not all of the cyberstalking reports Duke deals with involve tracking devices, but "the availability of low-cost tracking

technology" is a concern. In the wrong hands, AirTags can enable dangerous stalking behavior.

As part of his IT security work, and with his wife's permission, Tripp dropped an AirTag into his wife's bag to better understand the potential for nefarious use of AirTags by attackers. Concerningly, he found that he was able to track her movement using the app on his phone—not constantly, but about every five minutes, and if a criminal is trying to stalk someone, knowing their location every five minutes is more than enough.

Fortunately, Apple has created certain safety features to help prevent the malicious use of AirTags. For instance, if someone has been near the same AirTag for several hours (such as Tripp's wife while there was an AirTag in her bag), they'll get a pop-up notification on their phone after a random period of time between eight and twenty-four hours warning them that "Your current location can be seen by the owner of this AirTag."

Also, an AirTag will start making a particular sound if it has been away from its owner for eight to twenty-four hours. (It will emit a different sound if the owner of the AirTag is nearby and actively trying to find their lost item using their app.)

Finally, each AirTag broadcasts a certain Bluetooth signal, a "public key," associated with the AirTag's "private key." To help thwart potential hackers, that public key changes every eight to twenty-four hours. (Are you wondering yet what's special about the eight-to-twenty-four hour time period? Tripp says it's meant to be "frequently enough that Apple can give some privacy to the owner of that AirTag" but "infrequently enough that they can establish a pattern of malicious activity.")

But despite these safety features, a highly motivated criminal could get

around them. Tripp and his team built a "DIY Stealth AirTag" in an attempt to anticipate what measures criminals might take to deactivate or counteract Apple's built-in security features. (Except when he's presenting to other IT professionals, Tripp makes a point of not revealing the exact process his team used to make their Stealth AirTag. He wants to inform the public about the potential dangers of tracking technology while avoiding giving would-be criminals any ideas.)

Tripp's wife again volunteered to be tracked, this time with a DIY Stealth AirTag that Tripp placed in her car. He found that the modified AirTag effectively and silently tracked his wife's car. Unlike the original AirTag, their stealthy version could create a map of everywhere his wife had driven, complete with red markers showing the date, time, and coordinates of each location. An AirTag that has been modified by a skilled hacker could let attackers see "not just where a potential victim is going but when they go there and how often."

"The AirTag cat is out of the bag, so to speak," Tripp says. He believes Apple should update their AirTag design to make the safety features harder to circumvent. Nonetheless, "it is far more likely that someone will experience abuse of a retail AirTag" than one modified by a hacker to be stealthier. So how can you protect yourself? Tripp has several suggestions.

1. Know the AirTag beep indicating that an AirTag without its owner is nearby, potentially in your belongings.
2. If you have an iPhone, watch for AirTag alerts. If you receive a notification warning you about a nearby AirTag, don't ignore it.
3. If you have an Android, Tripp recommends installing the "Tracker Detect" app from Apple because unlike iPhone users, Android users don't get automatic pop-up notifications if an AirTag has been near them for several hours. The "Tracker Detect" Android app isn't a perfect solution—you still won't get

automatic notifications; you'll have to manually open the app to check for nearby trackers. But Tripp still considers it worthwhile.

4. For iPhone users, make sure you have tracking notifications configured in the "Find My" app. You can go into the app and click "Me," then "Customize Tracking Notifications." Make sure the app has permission to send you notifications.
5. Know how to identify an AirTag if you find one. If you find an AirTag that isn't yours, and you have an iPhone, go into the "Find My" app, click "Items," and then swipe up until you see the "Identify Found Item" option. That tool lets you scan the AirTag by holding it near your phone. It will then show the AirTag's serial number and the last four digits of the owner's phone number, which can be useful for the police. "If I found one," Tripp says, "I think it's worth making a police report."

It's worth noting that owning an AirTag does not put you at higher risk of stalking or other malicious behavior. The concern, whether or not you personally use AirTags, is that attackers can buy AirTags themselves and use them maliciously. Choosing to use AirTags to keep track of important items, meanwhile, won't hurt you and may be worth considering, especially if you travel often or are prone to misplacing things. Not all news about AirTags is bad. They've helped people recover lost items, from luggage and wallets to photography gear and an electric scooter.

"I actually think this technology is extremely useful," Tripp says. It's the potential for abuse by attackers that's the problem.

Provided by Duke Research Blog