Cybercrime Prevention Flyer

CPF 0004-2022-CID361-9H 8 February 2022

Bluetooth Tracking Devices

With a Bluetooth tracking device, tracker, or tag and a mobile device or computer, it is easy to locate misplaced items such as a set of keys, a wallet, a purse, or even keep track of a child playing outside with friends. As convenient as the trackers are to have and use for the average consumer, criminals have found nefarious means for these devices.

What exactly is a Bluetooth tracker?

A Bluetooth tracker is a small device powered by a battery similar to a vehicle key fob battery. The tracker, slightly smaller than a half-dollar but can vary in size, sends a signal via Bluetooth to a linked mobile device or computer with the location of the tracker. The distance the tracker can transmit the signal depends on the manufacturer of the tracker, but some trackers, when out of range of the linked device, can continue to send a signal by connecting to and using the connection of other nearby Bluetooth-enabled devices.

Some examples of the trackers are the Apple AirTag and the Samsung Galaxy SmartTag; however, other widely used Bluetooth trackers are the Chipolo, Cube, and the Tile Mate, Pro, Slim, and Sticker.

Criminal Use of Bluetooth Trackers

Criminals are placing Bluetooth trackers in vehicles they want to steal, people they want to stalk, or people they want to track for some other suspicious activity. Bluetooth trackers, easily concealed, have been discovered behind license plates, between and underneath car seats, and in personal items carried by unsuspecting victims.

In two recent reports, a man claimed an AirTag was identified on a newly purchased vehicle and in another incident a women in Philadelphia claimed she was being tracked by someone with a tracker device. In both instances, the individuals had received notifications on their phones that an unknown device was connected and that their location could be identified by the owner of the device.

Security and Protection

Bluetooth trackers are small and can be nearly impossible to locate, but you can take measures to protect yourself.

Report a crime to U.S. Army Criminal Investigation Division

Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

- Pay attention to your surroundings, and inspect your belongings regularly.
- Do not leave belongings unattended in public places.
- Keep pockets, purses, and backpacks secured by ensuring they are closed.
- Keep your vehicle locked and in a well-lit area while not in use.
- If you park in your garage while at home, keep the garage door closed.
- Apple iPhones will notify a user if an unknown device is tracking. Android devices will not, but Apple recently released a Tracker Detect application for Android devices.
- If you find a tracker that does not belong to you and is connected to a mobile device in your possession, disable the Bluetooth connection on your device and notify law enforcement. There is no legitimate reason for anyone other than yourself to secretly place a tracker in your car or among your belongings.

DoD Memorandum on Geolocation Devices

Per a 2018 DoD Memorandum, the use of geolocation capable devices, applications, and services poses a risk to the DoD. Personnel are prohibited from using geolocation features and functionality on both non-government and government-issued devices while in locations designated as operational areas.

Additional Resources

How to Protect Yourself Against AirTag and Tile Stalking

New Jersey Cyber Security and Communications Integration Cell – The Nefarious Use of Bluetooth Tracking Devices

AirTag Stalking Attacks Are on the Rise. Here's How To Protect Yourself.

Are You Being Stalked? What to Do When You See an "AirTag Found Moving With You" Alert

Apple AirTags and Your Safety

To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to: Subscribe CPF