Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

January 8th, 2024
CS-01-24

NAMEDROP, AIRDROP AND BLE IDENTIFIED RISKS

OVERVIEW:

The MC3 and other law enforcement agencies have seen files, notes, texts, images, and other data being shared or 'dropped' unintentionally between users and peers. This feature on mobile devices is used to help share information, including contact information, between users in a more convenient way. This feature was built to help share information, it has also been used to share inappropriate images or other malicious software.

Apple devices that support AirDrop use Bluetooth Low Energy (BLE) and other WiFi technology to share data between devices. This feature is on by default, but only available for sharing with Contacts Only. This feature can be changed to share information with everyone/anyone, or it can be completely turned off. Android devices have a similar feature.

NameDrop is another feature where devices share contact information such as phone number and email addresses. For this feature to function, both devices must be in proximity with one another (within centimeters), AirDrop and Bluetooth must also be active, and you must activate a button on the screen to share your information. With the iOS update 17, this feature was enabled by default.

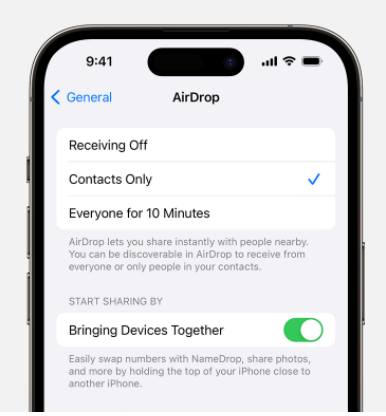
BLE and Bluetooth signals along with the transmission of data has also been more prevalent. BLE connectivity is being used to communicate with other devices, accessories, streaming music and audio, file sharing, connectivity to vehicles, and other capable devices. When this feature is turned on, the signal is broadcasted and visible or discoverable by other devices nearby. In most instances, the devices must be connected and paired. However, in older devices or devices with older versions of BLE technology, they can be vulnerable to man-in the-middle (MITM) attacks, eavesdropping, and BLE disruptive type attacks. The disruptive attack in some cases can crash mobile devices, rendering them unresponsive, and a restart of the device is required.

ADDRESSING THE ISSUE:

To best protect yourself from receiving un-intentional data or other files, it is recommended to simply turn off AirDrop or limit Airdrop to Contacts Only. If a user is notified that someone wants to share or AirDrop data with another user and the sender is unknown, it is recommended that the transaction NOT be allowed or authorized.

For the NameDrop feature, the user can simply turn off this feature or limit the feature so that the device can only receive this data from another device. The user of the device must still unlock the device to receive the data. Further, it is recommended that the owner of the device

change or be aware that the image or ‘poster’ on their device is, or can be, exchanged when sharing contact information with another device.



To turn off the NameDrop feature, in the setting application, search for ‘bringing devices together’ and turn it off. Further, this is the same location where the user can turn off the AirDrop feature or change it.

BLE and Bluetooth signals are required for some of the features to function properly. An option can be to disable or turn off Bluetooth connections. If this is done, the user should turn off Bluetooth from the settings application, not just in the notification center of the device. Further, updating to the latest software version of the devices can help alleviate some of the disruptive attacks. Upon turning off the Bluetooth function, the device connection would not be displayed.