TORONTO

REPORT FOR ACTION

Status of iOS AirDrop Functionality on City devices

Date: November 5, 2024
To: General Government Committee
From: Chief Information Security Officer and Chief Technology Officer
Wards: All

SUMMARY

This report provides an update to the General Government Committee on the City's decision to continue disabling the AirDrop functionality. This report was requested by the General Government Committee in September 2024.

RECOMMENDATIONS

The Chief Information Security Officer and Chief Technology Officer recommend that:

1. General Government Committee receive this report for information.

FINANCIAL IMPACT

There is no financial impact resulting from the adoption of this report. The Chief Financial Officer and Treasurer has reviewed this report and agrees with the financial impact information.

DECISION HISTORY

At the September 24, 2024 meeting, the General Government Committee requested the Chief Technology Officer and Chief Information Security Officer to report back to the Committee on November 20, 2024 with an update on the iOS AirDrop functionality for Members of Council.
Agenda Item 2024.GG16.16

COMMENTS

Apple AirDrop is a feature within Apple's iPhone, iPad, and laptop operating systems (iOS, iPadOS and MacOS) that enables users to wirelessly share and receive photos, documents, links, and other data with other Apple devices nearby. It uses both Bluetooth and Wi-Fi to create a peer-to-peer connection between devices in close proximity, without the need for internet connectivity.

In 2019, a cyber security flaw with AirDrop was uncovered and widely reported in the media that could expose the personal information of AirDrop senders and receivers. Apple's system relies on "hashing", an encryption method to scramble personal information on devices. When AirDrop is turned on, the device automatically scans for nearby AirDrop enabled devices, sharing this scrambled information to create a connection. Cyber attackers can exploit this process by intercepting and unscrambling contact information, such as personal email addresses and phone numbers, resulting in privacy breaches and unauthorized access to sensitive information. In response to this cyber security vulnerability, the City of Toronto banned the use of AirDrop across all City-issued Apple devices in 2019.

Apple has periodically released updates to AirDrop, including adding the "Contacts Only" setting in 2014, allowing users to restrict sharing to only known contacts, versus the default "Everyone" setting, which allows for sharing to all nearby Apple devices. This "Contacts Only" setting can still pose cyber and privacy risks for users who frequently use their Apple devices for business and regularly add new contacts, as they may unintentionally expose themselves to malicious actors attempting to share harmful documents. In 2022, Apple introduced a time limit on the default "Everyone" setting, allowing users to be visible to any nearby Apple device via AirDrop for only 10 minutes before reverting back to "Contacts Only" (applicable for iPhone and iPad, not Apple laptops/desktops). While these updates help reduce exposure, they do not eliminate the possibility of receiving malicious files or being targeted by phishing attempts.

A cyber risk assessment conducted by City staff in September 2024 confirmed that the same risks persist. At the time of writing this report, the City had corresponded with Apple and no timeline had been provided for a permanent fix. Should Apple issue further updates to address the vulnerability, the City will evaluate the validity of each update upon release.

CONTACT

Andree Noel, Deputy Chief Information Security Officer, Office of the CISO, 437-243-9347, Andree.Noel@toronto.ca

Mladen Subara, Director, Operation Support Services, Technology Services Division, 437-223-5892, Mladen.Subara@toronto.ca

SIGNATURE

Maneesh Agnihotri
Chief Information Security Officer

Sonia Brar
Chief Technology Officer