How to connect to the District of Columbia WIFI/HotSpot

**CREATION DATE:** March 12, 2020

This guide is designed to assist workers with accessing and/or utilizing the District’s Hot Spot as well as other WIFI connections when you are away from the agencies secure WIFI network.

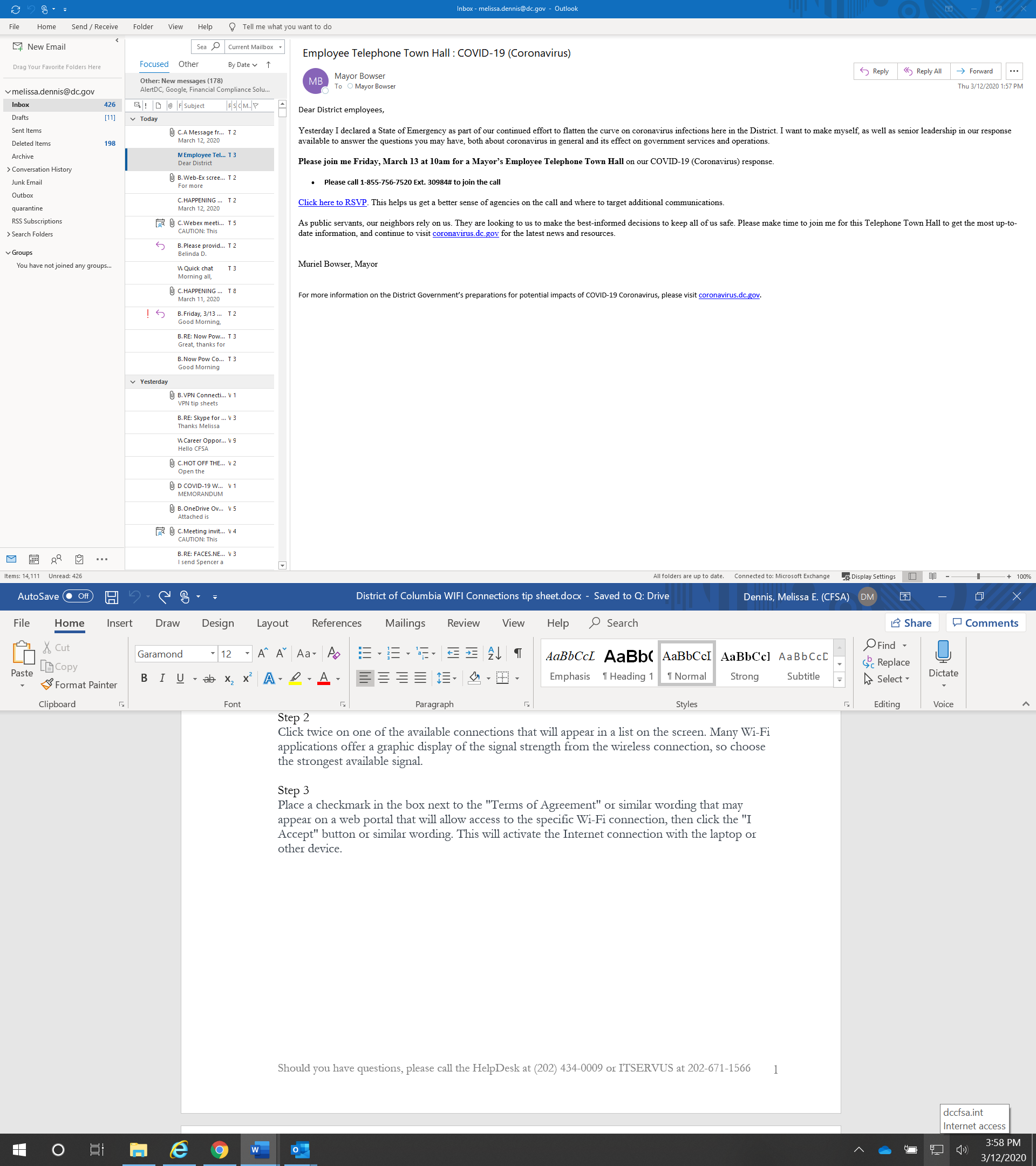
A 'hotspot' is a site where anyone with a computer or other device with Wi-Fi capability can come and browse the Internet for free using the District’s wireless network.

OCTO has installed hotspots in every Ward to provide convenient, citywide Wi-Fi Internet access for all. OCTO created a simple mapping application that displays all the wi-fi hotspots and information about each hotspot site. <https://octo.dc.gov/node/710032>.

**How to Connect to the DC WIFI or a Public WiFi Connection**

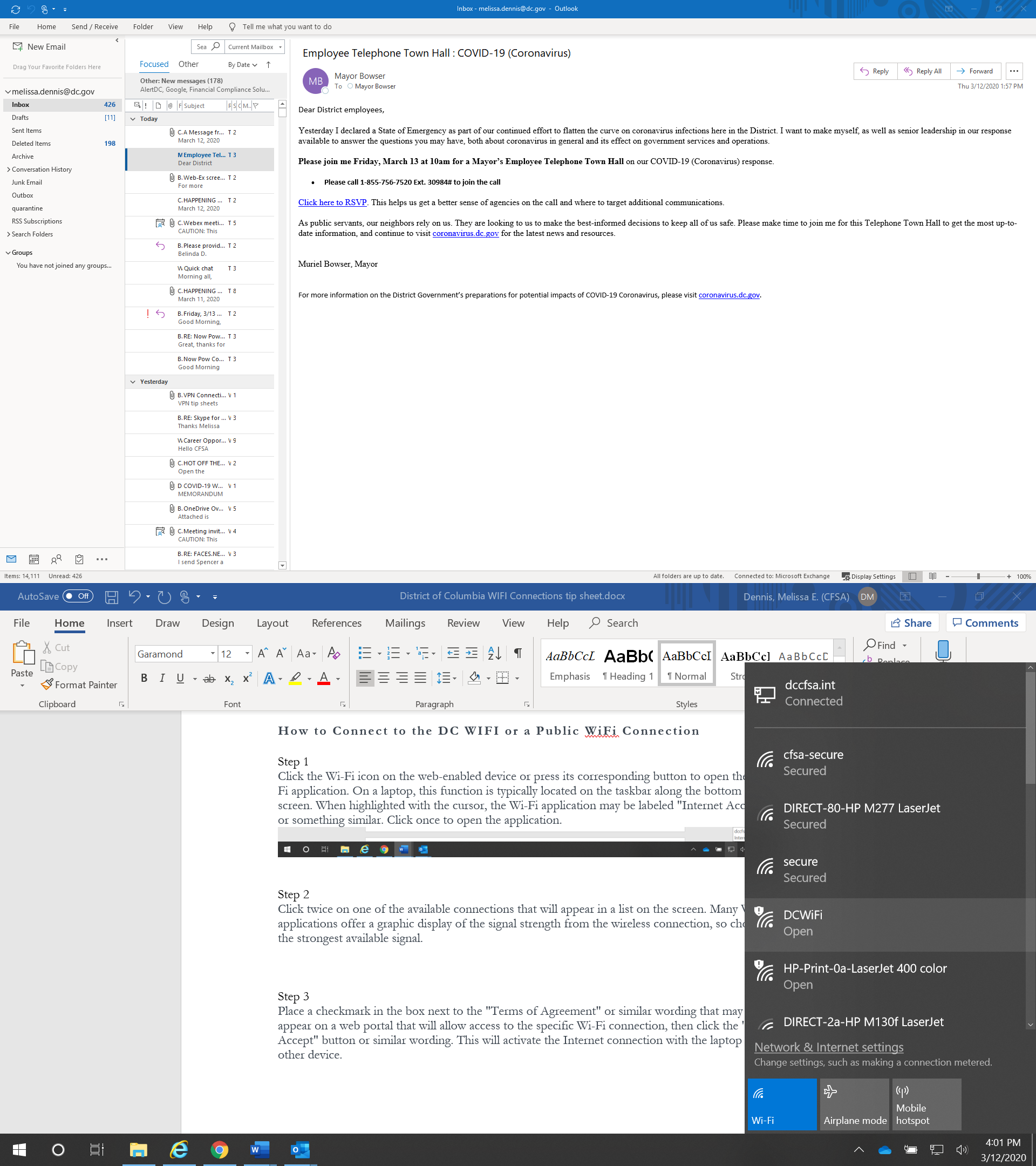
Step 1

Click the Wi-Fi icon on the web-enabled device or press its corresponding button to open the Wi-Fi application. On a laptop, this function is typically located on the taskbar along the bottom of the screen. When highlighted with the cursor, the Wi-Fi application may be labeled "Internet Access" or something similar. Click once to open the application.



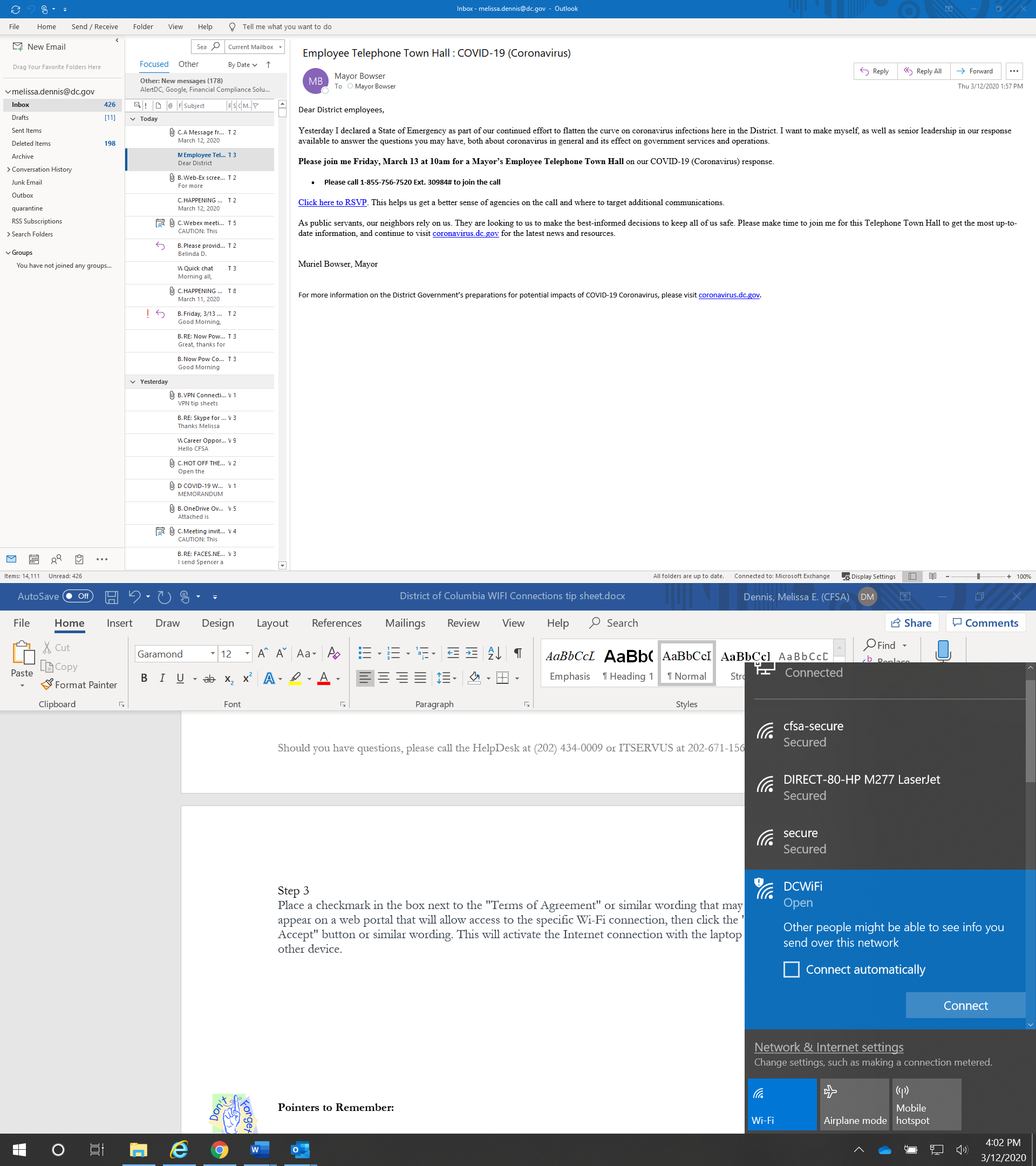
Step 2

Click twice on one of the available connections that will appear in a list on the screen. Many Wi-Fi applications offer a graphic display of the signal strength from the wireless connection, so choose the strongest available signal.



Step 3

Place a checkmark in the box next to the "Terms of Agreement" or similar wording that may appear on a web portal that will allow access to the specific Wi-Fi connection, then click the "I Accept" button or similar wording. This will activate the Internet connection with the laptop or other device.



**Pointers to Remember:**

j0104746

**Do** connect to secured public networks whenever possible. In the event that you’re unable to connect to a secured network, using an unsecured network would be permissible if the connection requires some sort of login or registration.

**Don't** access personal bank accounts, or sensitive personal data, on unsecured public networks. Even secured networks can be risky. Use your best judgment if you must access these accounts on public Wi-Fi.

**Don't** leave your laptop, tablet, or smartphone unattended in a public place. Even if you’re working on a secure Wi-Fi network, that won’t stop someone from taking your property or sneaking a peek at your device.

**Don't** shop online when using public Wi-Fi. Sure, shopping doesn’t seem like it involves sensitive data, but making purchases online requires personal information that could include bank account and retailer login credentials. Shopping isn’t something you want to do on an unsecured Wi-Fi network.

**Do** turn off automatic connectivity. Most smartphones, laptops, and tablets have automatic connectivity settings, which allow you to seamlessly connect from one hotspot to the next. This is a convenient feature, but it can also connect your devices to networks you ordinarily would not use. Keep these settings turned off, especially when you’re traveling to unfamiliar places.

**Do** monitor your Bluetooth connectivity. Bluetooth in the home is an amazing feature on many smart devices. However, leaving Bluetooth on while in public places can pose a huge risk to your cybersecurity. Bluetooth connectivity allows various devices to communicate with each other, and a hacker can look for open Bluetooth signals to gain access to your devices. Keep this function on your phone and other devices locked.