**Are the Free Wi-Fi Kiosks on New York Streets Safe?**

**Tech Tip**

**By J. D. BIERSDORFER**

**AUG. 26, 2016**

LinkNYC kiosks, which offer free Wi-Fi connections, web browsing and battery charging, are beginning to sprout up on the sidewalks of New York City.

Q. Are those LinkNYC Wi-Fi things on the street safe to use? Will the city (or anybody else) collect personal information about me?

A. The LinkNYC kiosks that began to supplant aging pay phones on the sidewalks around New York City this year can also make calls — but they do so in a very 21st-century manner. Passers-by can make free phone calls to anywhere in the United States through the Vonage service on each kiosk, using the small display screen, microphone and keypad on the front of each unit. (For privacy and volume control, users can also plug in their own headphones.)

Each of the slender vertical LinkNYC towers also provides a fast, free Wi-Fi connection for mobile devices and laptops. The display screen offers free web browsing, and each Link station has USB ports for charging phone and tablet batteries. For emergencies, each tower has a red 911 button, too.

As explained in the privacy section of the LinkNYC website, when you first use one of the kiosks, you need to supply an email address to be informed of updates or changes to the service. Each unit collects anonymous aggregated data to study for system use and diagnostics — as well as to influence the large color advertising screens on the sides of the kiosk that subsidize the service.

Using any public wireless network or computer terminal brings a risk of compromised security, and the New York Civil Liberties Union has previously expressed concern about data privacy with the LinkNYC units. However, the kiosks do have certain precautions built in.

For example, there is a standard open network called “LinkNYC Free Wi-Fi” that relies on your web browser’s security to encrypt data between your device and the hot spot. But this type of network is less secure than others.

The kiosks also include a “LinkNYC Private” network for those with the hardware to handle it. This is an encrypted network connection between the towers and the devices that support the Hotspot 2.0 technology — at this point, mainly Apple iPhones and iPads released in the last three years or so and running at least iOS 7.

For further security measures, the USB ports on the LinkNYC towers can be used only for charging devices but not for transferring data (including malicious software that may be lurking). The LinkNYC’s web browser has a content filter designed to help screen out malware, although the software has not been particularly successful yet in blocking adult-oriented sites from public use. And in case you forget to log out of a webpage, the kiosk will automatically log you out after 30 seconds of inactivity.

Even with all the safeguards in place, it is a good idea to treat the LinkNYC kiosks as you would any public network anywhere in the world. Do not log in to sites that store your financial information, do not enter your credit card number into any web forms and stay aware of others on the street who may be playing close attention to your online activity.