Thefts via public Wi-Fi are grounds for warning

March 9 2014, by Nancy Owano

Public park in Brooklyn, NY has free Wi-Fi from a local corporation. Credit: Jim.henderson/Wikipedia.

(Phys.org) —If you are basking in the convenience of doing an online bank transfer at a coffee house while spooning the cream off a designer

special, consider the tradeoff, which is placing your personal data at risk. Also consider yourself warned by none other than a high-level officer at Europol. Free Wi-Fi hotspots pose data risks. That was the warning recently voiced by cybercrime officer Troels Oerting, head of the cybercrime center at Europol. He spoke to the BBC. He noted a growing number of attacks being carried out via public Wi-Fi. Europol, the European Union's laws enforcement agency, is assisting several member states who had seen attacks carried out on networks.

Oerting spoke of WiFi misuse on the rise, for purposes of stealing information, identity or passwords, and money from users making use of the Internet while sitting in places featuring public or insecure Wi-Fi connections. The attackers were not using novel techniques, he said, Their approaches were already known in the ways they trick people into connecting to a hotspot that superficially resembles those seen in cafes, pubs, restaurants and other public spaces. The approach is in the "Evil Twin" mode where once the victim connects a smart mobile device or laptop, the eavesdropping begins.

Late last year, European Parliament switched off its public Wi-Fi system after discovery of a man-in-the-middle attack (thieves attempting to insert themselves between users and a hotspot to get the data passing between the two points). The attackers went after data on communications between smartphones and public WiFi. Staff were advised to change their passwords and avoid unknown public WiFi in other locales such as train stations or airports.

Many people are connecting to the Internet while on the go including those taking advantage of WiFi connections in the form of free public access points. Advice to avoid working with sensitive information over public Wi-Fi hot spots appears frequently, yet security experts find that many users do not recognize the risks.

Kaspersky Lab last year found that 34% of those surveyed stated they do not take any additional security measures when they connect to public hot spots. Another 14% reported that they were not concerned about using open access points when using services that process personal financial data, such as online stores, online banking services, and e-payment systems. Only 13% of mobile device users surveyed said they asked about the encryption standards used before connecting to hot spots with their devices.

More information: via BBC

© 2014 Phys.org

Citation: Thefts via public Wi-Fi are grounds for warning (2014, March 9) retrieved 28 April 2024 from https://techxplore.com/news/2014-03-thefts-wi-fi-grounds.html