**Under embargo until 9am CET, February 22, 2016**

**Press release**

# Avast Wi-Fi Hack Experiment Demonstrates "Reckless" Behavior of Mobile World Congress Attendees

*Thousands of smartphone users unknowingly connected to Avast's bogus Wi-Fi hotspot at one of the world's largest tech conferences and exposed their browsing activities*

**Mobile World Congress — Barcelona, Spain, February 22, 2016 –** Avast Software, maker of the world's most trusted mobile and PC security, today revealed results of a Wi-Fi hack experiment conducted at the Barcelona Airport the weekend before the start of Mobile World Congress to demonstrate how at risk people really are on public WiFi. The experiment, performed by Avast's security researchers, revealed that thousands of trade show visitors threw caution to the wind when looking for a public Wi-Fi connection, risking being spied on and hacked by cybercriminals.

For the experiment, Avast researchers set up Wi-Fi networks next to the Mobile World Congress registration booth at the Barcelona Airport. The Wi-Fi network names were "Starbucks", "Airport_Free_Wifi_AENA" and "MWC Free WiFi" — Wi-Fi names (SSIDs) that are either commonplace or that look like they were set up for the congress visitors. With mobile devices often set to connect to known SSIDs automatically, users occasionally overlook the networks they are connecting to. While convenient for many, this feature bears the risk of being spied on by cybercriminals who set up a false Wi-Fi network with a common SSID. Moreover, with any Wi-Fi network that does not request a password, the Web traffic can be visible to anyone. To mitigate these risks, simple Wi-Fi monitoring tools are available for free online.

In just 4 hours, Avast gathered more than 8 million data packets and learned the following about the Mobile World Congress visitors:

- 50.1 percent had an Apple device, 43.4 percent had an Android device, 6.5 percent had an Window Phone device
- 61.7 percent searched information on Google or checked their emails on Gmail
- 14.9 percent visited Yahoo
- 2 percent visited Spotify
- 52.3 percent have the Facebook app installed, 2.4 percent have the Twitter app installed
- From 63.5 percent Avast could see the identity of the device and user

"Many individuals recognize that surfing over open Wi-Fi isn't secure. However, some of these same people aren't aware that their device might automatically connect to a Wi-Fi network unless they adjust their settings," said Gagan Singh, president of mobile at Avast. "With most Mobile World Congress visitors traveling from abroad, it's not surprising to see that many opt to connect to free Wi-Fi in order to save money, instead of using data roaming services. When taking this route, people should utilize a VPN service that anonymizes their data while connecting to public hotspots to ensure that their connection is secure."

Avast SecureLine VPN for Android and iOS devices encrypts connections on unsecured public Wi-Fi and allows users to browse anonymously. The app also lets users choose the server location they would like to connect with, enabling users to access content from their home country that may otherwise be restricted by geo-location.

At Mobile Wold Congress in Barcelona, in Hall 8.1 (App Planet), Booth no. H65, visitors can step into a hacker's shoes and see what data is visible over an unencrypted Wi-Fi network. At the show, Avast is featuring Avast SecureLine VPN, which is available on Google Play and in the Apple App Store.

**About Avast**

Avast Software (www.avast.com), maker of the most trusted mobile and PC security in the world, protects 230 million people and businesses with its security applications. In business for over 25 years, Avast is one of the pioneers in the computer security business, with a portfolio that includes free antivirus for PC, Mac, and Android, to premium suites and services for both consumers and business. In addition to being top-ranked by consumers on popular download portals worldwide, Avast is certified by, among others, VB100, AV-Comparatives, AV-Test, OPSWAT, ICSA Labs, and West Coast Labs.

# # #