

Why does my Coffee Smell like Data?

Coffee isn't the only aroma in the air at a coffee shop with wireless internet access. With the right software a laptop can "smell" or "sniff" (in IT lingo) your data from a distance. A person "sniffing" the data can see everything going in and out of your computer if it is not properly secured. Almost no public access point will be properly secured, so it is essential that you be selective about what you do online when using a public wireless network.



Randy Abrams

In order to help keep your data private there are security mechanisms called WEP, WPA, and WPA2. From a practical perspective they are like putting a lock on a door that has a window in it. This means you still must be selective about how and where you surf using wireless devices.

The simplest rule of thumb is that if the website does not start with `https://` then do not enter anything you wouldn't want someone else to see. Most websites start with `http://`, but the ones that start with `https://` are what we call SSL, or secure sites. The data sent to and from your computer to an `https` site is well encrypted, so an attacker cannot read it.

If you can use a VPN (Virtual Private Network), it is an attractive option for keeping your data private. In most cases VPNs are used by companies and you must check with your administrator to see if all data is sent through the VPN or just data to and from the company network. There are options for individuals to set up and use VPNs, but they do require some technical knowledge to properly choose and use.

Physical security and privacy are issues in public places. Make sure nobody is watching you, or pointing a cell phone camera at you, when you type in information such as user names and passwords. If you work on confidential information, consider a privacy filter. Privacy filters prevent a person sitting next to you from being able to read your screen.

Wireless at a hotel is exactly the same as wireless at a coffee shop, airport, or any public place. In fact, the only difference between public access points and home or hotel room wireless is that you probably do not have to worry about an unknown person looking over your shoulder. The data on a home wireless set up can still be sniffed.

To make it as simple as possible, remember that if the website does not start with `HTTPS://`, whatever you send and receive is public knowledge on a wireless network!

Feel free to send questions or comments to askeset@eset.com



Randy Abrams is Director of Technical Education for ESET

AskESET@eset.com

www.eset.com

610 West Ash Street, Suite 1900

San Diego, CA 92101 • 866.496-ESET

ESET paid for this space and is solely responsible for its content.