MISA
London Region Professional Network

PRIVACY CHALLENGE

Public WiFi

"Nowadays, I'm feeling that my personal information is travelling more than I am!"

"Public Wi-Fi systems such as those found on airplanes, in cafés or at malls are completely insecure and anyone using them should think of everything they type as being broadcast to a billboard in Times Square"
That was the reaction from security professionals when a USA Today journalist was hacked while he used the Gogo onboard WiFi network to email his editor during a flight. Lucky for him, the hacker saw that he was writing a story about the US FBI/Apple standoff over gaining access to the iPhone via back doors into their products and he told the journalist what he had done after the plane landed. He wanted to impress upon him how important the story he was writing is because it's about everyone's privacy. A less conscientious hacker may not have been so kind, especially if the journalist was accessing something more sensitive. (Read the Story)

Did You Know?

When you have to click through a screen that sometimes asks you for information (e.g., room # in a hotel) and click "I agree" after seeing terms of service, you are using what is called a "captive portal". It is not any more secure than an open connection. Captive portals help organizations harvest emails for marketing campaigns, or collect social media information to sell to third parties, essentially, trading user privacy for network access. Captive portals cause those authentication certificate errors you see when you go to a secure (https) site because the secure site detects interception from the captive portal.

Resources

- Learn how to make your mobile phone a secure Wi-Fi hotspot.
- See more tips on staying safe on public Wi-Fi networks.

Challenge: Get informed! Service providers are usually pretty explicit about what they offer and what personal information they collect from you. The problem is that most people don't read it. Take a look at Starbucks' Privacy Statement for an eye-opening glimpse.

Things to Know

• • •

1. The safest way to use public Wi-Fi is to simply not use it.

2. The next safest way to use public Wi-Fi is to connect via a Virtual Private Network (VPN).

3. No matter how secure it seems, your computer is vulnerable to hackers because you have no idea who is in charge of that router or who has access to it and all the data that passes through it.

4. File sharing (e.g., iCloud, Dropbox, Google Drive) while on public Wi-Fi can expose all of the files you are sharing with your team to everyone on the public network.

5. An attacker can set up a shared folder filled with malicious files that appears in your list of shared folders. You might open it out of curiosity and release malware onto your computer.

6. Be aware of fake Wi-Fi hotspots made to look like legitimate hotel, café and airport hotspots and designed to fool you into connecting in order to steal your information.