

Systems and Software

Evil Twin Wifi Hotspots

Overview

Are public hotspots safe?

Fake Wifi Hotspots can trick a surfer into revealing their confidential information. These hotspots are called Evil Twins.

Details

Fake hotspots can be as simple as a laptop in a backpack. The laptop is configured as an access point and given the service name of a legitimate service like “T-Mobile Hotspot”. Unsuspecting surfers connect to the fake hotspot and enter their credit card details in the same way as they would on a legitimate hotspot. Guess who now has their credit card details...?

More complicated fake hotspots can have a real connection to the internet. The unsuspecting surfer may go to their bank to pay a bill, eBay to check on a bid they have made etc. In all cases their confidential information is being skimmed.

The fake hotspot can also have applications that copy data off the surfers’ hard disk.

What can the surfer do?

The fundamental problem is when a surfer is in a public place there is no way for them to tell the difference.

Check the URL address on the browser. Is it https or just the unprotected http? Is there a padlock symbol? This only helps with hotspots that are displaying fake web pages. Hotspots that are really connected to the internet are much harder to spot.

It is safer to scan for hotspots and make a manual selection, than allowing automatic connections. This may help spot subtle differences. It would be unusual to have two T-Mobile hotspots in a small coffee shop.

Installing a firewall will help prevent anyone from accessing files on laptops and PDAs.

The safest advice is to only do banking when at home. A wired connection to Broadband is the safest, but even home hotspots will be more secure than a public one.