

## Evil Twins FAQ

### What is an “Evil Twin”?

An Evil Twin, sometimes referred to as Wiphishing, is a potential security threat to users of Wi-Fi, predominantly in public hotspots. A hacker sets up what is called a “rogue access point” which mimics the characteristics of the network to which users expect to connect. Users unknowingly connect to the rogue access point and the hacker’s network instead of the intended network.

The Evil Twin hijacks data, such as passwords, account information, credit card information, etc., and then connects the user to the Internet as intended. A sophisticated evil twin can even control what Web site appears when the Internet is accessed, often mimicking the intended starting Web site, for the purposes of capturing the user’s private information.

To date, there have been no reported large-scale incidences of Evil Twin attacks, but most network administrators have been aware of this theoretical threat for some years. Recent media coverage of Evil Twin threats has directed consumer attention to the matter, making users concerned about the problem and how they can protect themselves.

The Wi-Fi Alliance recommends that users of wireless networks exercise the same level of caution they’ve learned to use to avoid scams in the wired world. End users should change their passwords regularly, not respond to questionable e-mails, and look for secure connections. As Wi-Fi continues to grow in reach and popularity, consumers need to make some new simple security precautions a habit, like connecting through a provider that uses encryption with a list of trusted hotspots, using a VPN, and always enabling security within a home network. Also, users should make it a point to look for products that are Wi-Fi CERTIFIED for WPA™ (Wi-Fi Protected Access) or WPA2™ security.

### Who is affected?

Users of Wi-Fi in public hotspots should be aware of the threat posed by an “evil twin”. An evil twin can capture sensitive data, even through instant messaging.

### How likely is this type of attack?

In reality, the likelihood of attack is low but users should be cautious and use some fairly simple security precautions to avoid becoming a victim.

### How can Wi-Fi users protect themselves from Evil Twin threats?

There are a number of other steps you can take to reduce your risk.

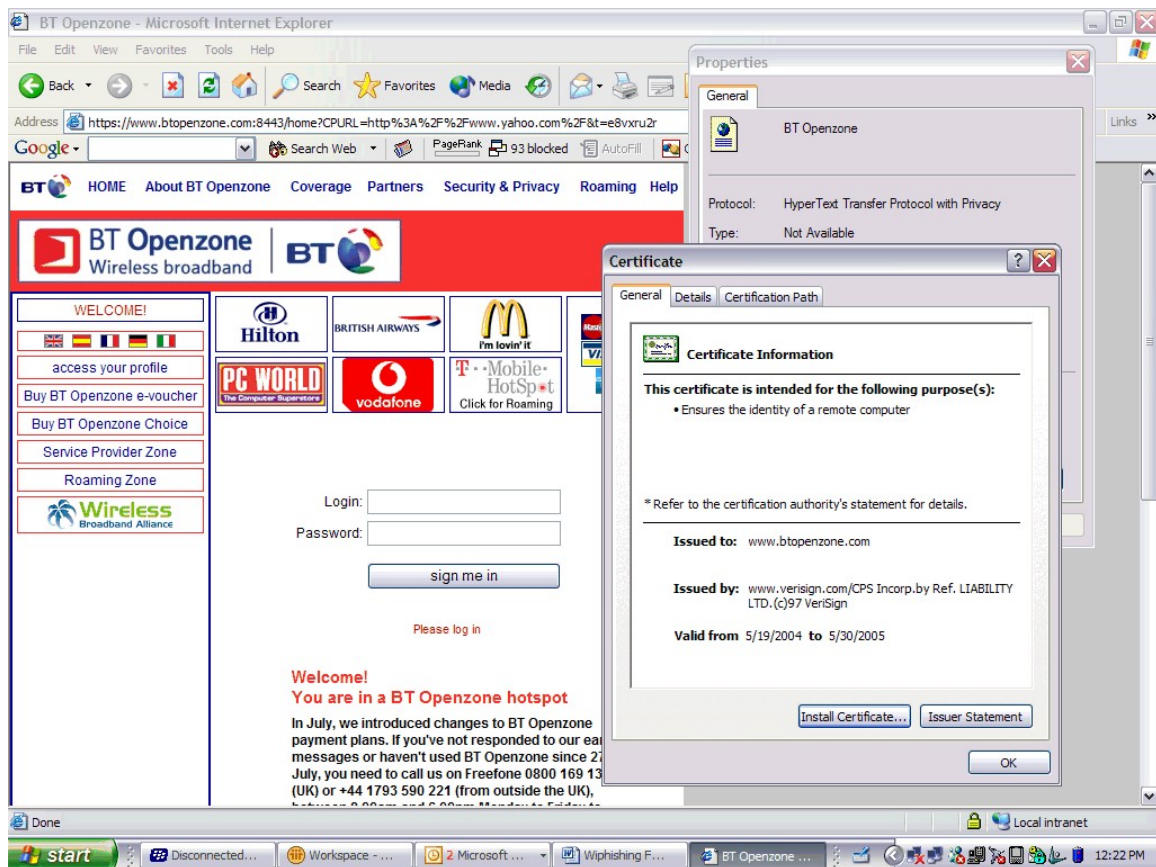
#### At home, users should do all of the following:

- Only buy products that are Wi-Fi CERTIFIED™ for WPA or WPA2 security – look for the Wi-Fi CERTIFIED logo or find certified products online at [www.wi-fi.org](http://www.wi-fi.org)
- Always enable WPA or WPA2 security for your home network. Having WPA or WPA2 in the product is not enough. The security keys must be configured on the access point/router and each client device. Security is off by default in most products. Note that using WEP security is not sufficient.

- Re-name the home network to something unique, instead of the default name. This will prevent you from inadvertently connecting to a rogue access point which is broadcasting a seemingly-familiar network name.

**At Wi-Fi Hotspots, be sure to take at least one of these measures:**

- Only log-in to known hotspots using an SSL (https) connection. Your browser will typically show a lock icon at the bottom of the login page when you have a secure SSL connection. To be certain of the secure connection, check the digital certificate on the login page. You can do this in Internet Explorer by selecting File: Properties: Certificates. This will show the name on the digital certificate as backed by the Certificate Authority. These are very difficult to forge. A sample certificate is pictured below:



- Use the VPN tool provided by an employer. If the employer does not provide a VPN, users can download a commercially-available VPN based on the IETF's IPsec framework – there are a number of these available online. If you cannot make a successful VPN connection, there is a chance you've connected to a rogue network. You should disable your Wi-Fi card and inform your company's IT staff, as well as the hotspot operator.
- Connect through a hotspot service provider that provides a list of trusted hotspots and a smart software client that encrypts your user information before sending it over the Internet.

- Look for hotspots employing WPA security, which has mechanisms to ensure that the network to which users connect is authentic. If your hotspot provider doesn't offer WPA security, ask them if they plan on introducing WPA-protected services soon.
- Disable your laptop's Wi-Fi card unless you are planning to use it

**For more information:**

The Wi-Fi Alliance has produced a whitepaper entitled "WPA Deployment Guidelines for Public Access Wi-Fi Networks" to address establishment of strong security measures in hotspot locations. It is available for download at [www.wi-fi.org](http://www.wi-fi.org), under White Papers, or via [this link](#).