Private WiFi®

PRIVATE WiFi^{TM}

AOL Support

Briefing Guide

Published May 2012

1. Introduction

The PRIVATE WiFi Team is looking forward to working with AOL Customer Support to help your customers understand and use PRIVATE WiFi.

We have prepared this briefing guide to give you some background on the risks your customers are facing each time they use a wifi hotspot, in a hotel, airport, park or coffee shop, and how PRIVATE WiFi protects them.

If you have any questions, please feel free to contact us at support@privatewifi.com.

2. Understanding Wifi Insecurity

The information in this section describes wifi networks and the risks inherent to them. It also discusses what VPNs are and how PRIVATE WiFi protects users.

What is Wifi?

Wifi is a wireless networking technology that is used around the world. A wireless network uses radio waves, just like cell phones, televisions and radios do. In a wifi network, computers with wifi network cards connect wirelessly to a wireless access point or "router." The router is connected to the Internet via a cable or DSL modem. Any user within 300 feet or so of the access point can then connect to the Internet. Wifi networks can either be open, where anyone can access them, or closed, where users need a password to access them.

An area that has public wireless access is called a public wifi hotspot. If you've been in an airport, coffee shop, library or hotel recently, chances are good that you've been right in the middle of a public wifi hotspot. There are roughly 750,000 wifi hotspots around the world.

Why Wifi Hotspots Are Vulnerable

Most people assume that using a wifi hotspot at a hotel, airport, or coffee shop is as safe as logging into their network at home or at the office. But the risks of using wifi networks are exponentially greater than those experienced at home or in an enterprise setting.

For example, while sharing folders, printers, desktops, and other services can be useful at home or in the office, doing so is inappropriate at a wifi hotspot, where hackers can access this information.

It is literally impossible to tell the safe networks from the bad ones. Wifi eavesdropping is possible everywhere. Because of this, the Terms and Conditions of all wifi hotspots have warnings such as these:

> **AT&T WiFi** (Starbucks, McDonalds, Barnes & Noble): If you have VPN, AT&T recommends that you connect through it for optimum security. If you do not typically use a VPN ... be aware that your surfing activities may be monitored in a public hotspot. It is advisable not to access any secure site such as on-line banking sites, portfolio management or other web sites supporting your personal data. Email access may be at risk as well.

T-Mobile: Wireless systems use radio channels to transmit voice and data communications over a complex network. Privacy cannot be guaranteed …. We strongly encourage and support certain customer-provided security solutions, such as virtual private networks, encryption and personal firewalls.

Guest Tek (Westin, Copley Square, Boston): Guest-Tek advises against using Wi-Fi unless your computer is equipped with a Virtual Private Network client to provide adequate encryption.

Wifi Hotspot Risks

Users of public wifi hotspots face numerous risks, including identity theft, data loss, and privacy intrusions.

The following is a list of different types of hacks that can occur in public wifi hotspots:

- **Sniffers:** Software sniffers allow eavesdroppers to passively intercept data sent between a user's web browser and web servers on the Internet. This is the easiest and most basic kind of attack. Any email, web search or file a user transfers between computers or open from network locations on an unsecured network can be captured by hackers.

- **Sidejacking:** Sidejacking is a method where an attacker uses packet sniffing to steal a session cookie from a website a user just visited. These cookies often contain usernames and passwords and are generally sent back to the user unencrypted. Anyone listening can steal this log-in information and then use it to break into the user's Facebook or gmail account.
- **Evil Twin/Honeypot Attack:** This is a rogue wifi access point that appears to be a legitimate one, but actually has been set up by a hacker to eavesdrop on wireless communications. An evil twin is the wireless version of the "phishing" scam: an attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. When a victim connects, the hacker can launch man-in-the-middle attacks, listening in on all internet traffic, or just ask for credit card information in the standard pay-for-access deal.
- **ARP Spoofing:** Address Resolution Protocol (ARP) spoofing is a technique used to attack a wireless network. ARP spoofing allows an attacker to sniff traffic on a LAN and modify or stop the traffic altogether. Any traffic meant for the victim's IP address is mistakenly sent to the attacker instead. The attacker could then forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack).

- **“Free Public WiFi” Rogue Networks:** “Free Public WiFi” networks are ad-hoc networks advertising “free” Internet connectivity. Once a user connects to a viral network, all of his or her shared folders may be accessible to every other laptop connected to the networks. A hacker can then easily access confidential data on the user’s hard drive. These viral networks can be used as bait by an Evil Twin. “Free Public WiFi” networks turn up in many airports.
- **Man-in-the-middle Attacks:** Any device that lies between a user and a server can execute man-in-the-middle attacks, which intercept and modify data exchanged between two systems. To the user, the man-in-the-middle appears to be a legitimate server, and to the server, the man-in-the-middle appears to be a legitimate client. In a wireless LAN, these attacks can be launched by an Evil Twin.

3. Benefits of Using PRIVATE WiFi

As we have seen above, the risks of using wifi hotspots are varied and real. For individuals, that can mean credit card losses and, ultimately identity theft. For professionals, it can mean the loss of business secrets and breach of client confidentiality.

Anyone who uses wifi regularly, whether in a hotel, airport, public park or a coffee shop, should have access to a VPN such as PRIVATE WiFi. It is the only way to protect all of the risks shown above.

How PRIVATE WiFi Protects

When a user activates PRIVATE WiFi, it quickly builds an encrypted tunnel through their Internet connection from wherever they are to one of our secure Internet gateways. All Internet data between them and PRIVATE WiFi is encrypted from that point on.

Data passes through this tunnel, protected from anyone who tries to intercept it. Even if the data is intercepted, it is hopelessly scrambled and useless to anyone without the key to decrypt it.

PRIVATE WiFi uses industry standard 128-bit encryption. It’s the same technology used by banks and credit card companies, but we use it to secure everything our users send and receive, including all website traffic, emails, attachments, and IMs.

Private WiFi is a VPN

VPN stands for Virtual Private Network. A VPN is a computer network that uses a public telecommunication infrastructure such as the Internet to provide remote offices or individual users secure access to their organization's network.

Most large companies have a VPN which is supported by their IT departments to protect corporate communications. PRIVATE WiFi provides the same capability for individuals, business travelers, and small and medium sized enterprises.

How PRIVATE WiFi Affects IP Addresses

PRIVATE WiFi assigns a temporary and random private IP address to each user. This private IP address cannot be traced by anyone through our server nor can anyone find the user’s real IP address or location.

PRIVATE WiFi and Blocked Websites

Since PRIVATE WiFi masks a user’s IP address, our users are able to access websites to which they may not normally have access.

For example, some sites such as Netflix and Hulu are only accessible within the U.S. If someone in Europe has our software, they can activate PRIVATE WiFi and choose one of our U.S.-based servers. By doing so, websites such as Netflix and Hulu will assume they are in the U.S., and will allow them access.

Private WiFi®

4. Private WiFi Marketing

Below is our marketing message that you can use when talking to customers.

Why do you need a secure wifi connection? Because most wifi signals are unencrypted.

Anything you send or receive in open, public hotspots like hotels, airports, coffee shops, and parks can be intercepted. Your passwords, pictures, private data, and personal stuff are all vulnerable. Your identity can literally be stolen out of the thin air. Firewalls or antivirus software can't stop it, but PRIVATE WiFi can. PRIVATE WiFi encrypts everything you send and receive, so no one else sees anything. It's a layer of privacy and anonymity that no other technology can provide.

Key Features

- **Sophisticated Technology:** PRIVATE WiFi is a Virtual Private Network (VPN) that uses the same proven encryption technology trusted by financial institutions and government agencies.

- **Total Anonymity:** PRIVATE WiFi automatically reroutes your data through an encrypted server in another location. Not only will your Internet activity be anonymous, no government, advertiser, website, malware, hacker, or identity thief will be able to track your real location. Your actual location and IP address is never disclosed.

- **Simple to Use:** PRIVATE WiFi is security you don't have to think about. It automatically activates itself every time you connect to the Internet, and runs invisibly in the background while you browse the web or write an email. A small icon in computer's System Tray (PC) or Menu Bar (Mac) shows you that it's working.

- **Real-Time Data:** PRIVATE WiFi's status screen gives you real-time information about your communications.

- **Dedicated Support:** PRIVATE WiFi is committed to extraordinary customer service. Real help from a real person is always available via email.

PRIVATE WiFi Video

Please watch our video which describes the risks of wifi hotspots and how PRIVATE WiFi protects: http://youtu.be/sTq2wZw8__4.

Encourage your customers to watch it as well – it's the best way we have come up with to help them understand why they need PRIVATE WiFi.

5. Frequently Asked Questions

Below are answers to commonly asked questions regarding PRIVATE WiFi, public wifi networks, and VPNs.

Does a VPN do the same thing as antivirus software and firewalls?

A VPN is different from antivirus software or a firewall.

Antivirus software protects a computer from any external threats, such as malware, computer viruses, worms, and Trojan horses.

A firewall is a device or set of devices which block unauthorized access to a computer system while permitting authorized communications.

A VPN prevents data from being intercepted by hackers by encrypting it when it is sent over the Internet. It might be the most important security component for any computer user who uses a public wifi network.

To be completed protected, a user really needs all three.

Does PRIVATE WiFi only work if the user is accessing a public wifi network?

PRIVATE WiFi is set up to automatically activate whenever the user is accessing an unencrypted wifi network.

Users can override this default setting to use it at all times, but if they are accessing a WPA encrypted network, PRIVATE WiFi's protection is redundant.

Can a user use PRIVATE WiFi outside of the U.S.?

PRIVATE WiFi can be used anywhere around the world, whether the user in inside or outside of the U.S.

Is PRIVATE WiFi available for tablets and smartphones?

We are currently developing software that can be used on both tablets and smartphones.

Private WiFi®

6. Technical Appendix

The following is technical information about PRIVATE WiFi.

PRIVATE WiFi’s Underlying Technology

PRIVATE WiFi uses OpenVPN. OpenVPN is open source software that uses VPN techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. OpenVPN is a widely-used technology, and is considered highly secure and efficient.

Server Information

We have many servers located throughout the U.S., Canada, Europe, and Asia. Most of these locations contain server “clusters”, which means that several servers are available to effectively handle the traffic. We have a very sophisticated server selection algorithm that takes both current load and distance into account, and automatically assigns users to the server that will provide the best service. However, users can override the automatic server selection if they wish to connect to any other server in our network.

VPNs vs. HTTPS/SSL

Secure websites contain “https” in their URL and have a small lock symbol next to them. SSL, or Secure Sockets Layer, is the technology behind HTTPS. SSL creates an encrypted link between a website and the user’s browser which, in theory, ensures that all data passed between them remains private.

Many websites use SSL to provide a secure connection, including Facebook, Twitter, online retailers, banks, and so on. SSL is usually the only protection websites use to prevent passwords, credit card information and other sensitive data from being intercepted by hackers.

The problem with SSL is that it’s simply not secure. Up to as many as 90% of websites that use SSL are vulnerable to specific attacks that have been developed over the past few years, and few websites have implemented the necessary changes to block these kinds of attacks.

One of the more well-known attacks is known as BEAST. BEAST (Browser Exploit Against SSL/TLS) was a program developed by researchers last year that also exposes SSL vulnerability. This program allows hackers to access encrypted data that websites use to grant access to restricted user accounts, such as PayPal login information.

There are many other SSL vulnerabilities. For instance, SSL implementation is spotty; some websites use it all the time, but some only use it during the login process. This is problem because users can still get hacked after logging into a website. Also, SSL relies on a system of easy-to-forge certificates. A hacker could set up a website using a fake certificate that looks exactly like PayPal and empty out a user's account.

SSL gives users a false sense of security and few users are aware that they are vulnerable to attacks when using supposedly secure websites. The only way for users to be completely safe is to use a VPN whenever they are accessing a public wifi network.