WEBROOT
Smarter Cybersecurity™

SMB Best Practices for WiFi Hotspots

Easy, Effective Tips for Securing your WiFi Hotspots

Overview

WiFi hotspots are a growing part of everyday life. The average consumer expects to be connected while at home, at work, or on the go. However, many organizations unwittingly put themselves and their customers at risk with poorly secured WiFi hotspots or by neglecting legal security obligations.

This is particularly true for small- to medium-sized (SMBs) who want to offer a free WiFi service, but do not want to put their business in harm's way or spend a lot of money. For businesses looking to reduce costs while protecting their WiFi connection, follow these guidelines:

1 Create an internet-enabled service set identifier (SSID) separate from your internal network.

This way, you can provide a separate network and password for guests without giving them uncontrolled access to your private corporate network that contains important company information.

2 Configure your router's settings to use strong network encryption.

WiFi Protected Access II (WPA2) is the preferred protocol and provides unique encryption keys for each wireless client that connects to it.

3 Position your WiFi access points wisely.

You never want to place an access point next to a wall or other obstructions that can limit the signal. Additionally, you don't want to put it in too public of a place where people could tamper with it.

4 Provide the appropriate amount of bandwidth for your internet users.

You don't want your guests to complain about slow connection speeds, but you also don't want to spend extra money on unused bandwidth.

5 Implement strict content filtering rules.

When it comes to protecting your network and business data, the more restrictions, the better—but it's important to enforce them wisely.

6 Change your password periodically.

You know how important it is to regularly change your passwords. The same holds true for your WiFi network.

Overall, one of the best solutions SMBs can use to secure public/guest WiFi is DNS protection. This is because the DNS connection is involved in every aspect of internet usage, but it's highly vulnerable to cyberattacks. Once it's compromised, cybercriminals may be able to view browser history, gain access to login information, redirect searches to malicious pages, and much more.

Additionally, regulations such as PCI, GDPR, HIPAA, and others, coupled with security and safety concerns, make web content filtering an absolute necessity. By adding DNS-layer content filtering for WiFi hotspots, organizations can block users from accessing potentially harmful websites that host malware or dangerous content. As a result, SMBs can achieve regulatory compliance and stop undesirable and illegal content flagged by the Internet Watch Foundation (IWF).

Slow internet speed and website delivery is irritating to customers and can cost organizations money. As mentioned above, blocking undesirable traffic such as media streaming and other unwanted or malicious content at the domain layer allows organizations to drastically improve network bandwidth.

Content filtering services also ensure critical processes have priority, and can improve site speed and reduce bandwidth usage. As a result, organizations may not need to upgrade systems as often to keep up with bandwidth demand, which can result in more cost savings.

Learn more about Webroot SecureAnywhere® DNS Protection for Guest WiFi here.

About Webroot

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.