WEBROOT
Smarter Cybersecurity™

WIFI HOTSPOTS: A GROWING OPPORTUNITY FOR MSPS

WiFi hotspots are a part of everyday life. We expect to be connected while at home, at work, and on the go. But many organizations unwittingly put themselves and their customers at risk with poorly secured hotspots or by neglecting security obligations. While these behaviors are cause for concern, they also open up new opportunities for managed service providers (MSPs) to sell security services, such as DNS protection and content filtering, to their customers. This not only gives clients peace of mind, but also delivers more complete network visibility, which is a must-have in today's cybersecurity landscape.

"Over half (55%) of users worldwide wouldn't think twice about sharing information or doing something in exchange for a strong WiFi signal."[1]

REDUCE WIFI HOTSPOT THREATS WITH DNS PROTECTION

Unsecured WiFi hotspots increase risk for organizations of all sizes. Whether corporate-owned devices are traveling between business, home, and public networks; employees are using personal devices at the office; or guests are accessing the internet via public WiFi in your clients' buildings, endpoint security alone isn't enough to keep users safe. By integrating DNS-layer protection into your clients' defenses, you not only enable greater network visibility, but also drastically increase the overall cybersecurity posture of their business and users.

ENSURE CYBER SAFETY WITH CONTENT FILTERING

Regulations such as PCI, GDPR, HIPAA, and others, coupled with security and safety concerns, make DNS content filtering an absolute necessity in reducing the risks from malicious data exfiltration. What's more, organizations that want to offer convenient public WiFi to their customers or guests must adhere to industry- and location-specific compliance requirements, or else face stiff fines.

[1]Statista. "Risks online adults worldwide are willing to take for free Wi-Fi 2017." (June 2017)

By adding DNS-layer web filtering for WiFi hotspots, you can:

- Stop users from accessing potentially harmful websites that host malware or dangerous content
- Help clients achieve regulatory compliance by blocking adult or undesirable web content
- Enforce policies by blocking sites that violate internal regulations
- Block illegal user activities and content
- Stop undesirable and illegal content flagged by the Internet Watch Foundation (IWF)

"83 percent of users connect to WiFi at hotels, 72 percent log on at cafes, and 64 percent use airport hotspots."[2]

BOOST COST SAVINGS WITH IMPROVED BANDWIDTH

Slow internet speed and website delivery is irritating to customers and can cost your clients money. Providing content filtering services that block high bandwidth websites and ensure critical processes have priority can improve site speed and reduce bandwidth usage. As a result, your clients may not need to upgrade systems as often to keep up with bandwidth demand, which can result in dramatic cost savings.

WEBROOT SOLUTIONS FOR WIFI HOTSPOTS

As the #1 endpoint security provider to the world's top MSPs, Webroot offers your clients first-rate, proactive protection against threats across endpoints, servers, mobile devices, and corporate and public networks. Webroot SecureAnywhere® DNS Protection for Guest WiFi is an easy, straightforward way to secure guest/public WiFi connections, enforce acceptable web access policies on guest devices, gain visibility, and block up to 90% of malware before has the chance to damage your clients' business or reputation. Built with MSPs in mind, Webroot solutions offer single-pane-of-glass management across your clients' install bases. MSPs can easily deploy and manage SecureAnywhere® Business Endpoint Protection and DNS Protection from one convenient location, saving both time and money.

To learn more about Webroot SecureAnywhere suite, visit webroot.com.

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.

World Headquarters
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

Webroot EMEA
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

Webroot APAC
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900

[2]Xirrus. "Rolling the Dice with public Wi-Fi." (October 2016)