Depending on the industry in which your clients operate, uncontrolled internet usage doesn’t just risk introducing malware to the network. It can also cause regulatory compliance issues and damage their reputation.

PUBLIC WIFI RISKS

1. Xirrus. “Rolling the Dice with public Wi-Fi.” (October 2016)
4. ZDnet.com. “Hackers are Using Hotel Wi-Fi to Spy on Guests, Steal Data.” (July 2017)
5. Latesthackingnews.com. “Connecting to Airport WiFi is Safe, Right?” (December 2017)
6. CSOonline.com. “Healthcare Experiences Twice the Number of Cyber Attacks as Other Industries.” (March 2018)

Whether people are at the coffee shop, hotel, airport, or doctor’s office, public WiFi is a growing part of everyday life. For more information about securing your clients public WiFi, visit webroot.com/DNSPGuestWiFi

SO WHAT CAN MSPS DO to protect their clients’ public WiFi from hacking and other threats?

1. Teach clients about bandwidth and content filtering rules.
2. Ask clients to provide a proof of purchase for all their hotspots. (The better-training is required, the better your clients will train their users.)
3. Ask clients to perform an annual scan of their wireless networks. (This can be done using a third-party service.)
4. Add DNS-layer protection to your portfolio.
5. Help clients create a separate network-enabled SSID and wireless isolation.
6. Add a user agreement.
7. Help clients position their WiFi access points wisely.

For more information about securing your clients public WiFi, visit webroot.com/DNSPGuestWiFi

PROTECTING YOUR CLIENTS' HOTSPOTS

Public WiFi is a growing part of everyday life. The more restrictions, the better—but it’s important to enforce them wisely. You don’t want your clients’ users to complain about slow connections, but you also don’t want those users accessing malicious, illegal, unwanted, or bandwidth-draining content, like torrent sites. (And who wants their internet service turned off due to inappropriate downloads?)

Add DNS-layer protection to your portfolio. The DNS connection is involved in every aspect of internet usage, but it’s highly vulnerable to cyberattacks. By adding DNS-layer protection, you can prevent cybercriminals from tracking your clients’ users, learning where they go online, stealing access credentials, and using that information to gain access to your clients’ networks.

Help clients create a separate network-enabled SSID and wireless isolation. With a service set identifier that’s separate from your clients’ internal network, you give their guests WiFi access without giving them free reign to access the private corporate network and important company information. You can also help clients enable wireless isolation to prevent devices from accessing to each other through the hotspot.

Add a user agreement. Although your clients should take measures to ensure the security of any users who access their guest WiFi, there’s only so much they can do. They shouldn’t be held responsible if users engage in high-risk or illegal online behaviors using their hotspot. A user agreement can help paint a user in a responsible way that says your clients cannot be held liable for the actions of their guests.

Help clients position their WiFi access points wisely. Clients should place their WiFi points in a way that is most effective for the needs of their business. The best location might be different depending on where you live and how your clients’ users use their WiFi.

More for more information about securing your clients public WiFi, visit webroot.com/DNSPGuestWiFi