

# PROTECTING YOUR CLIENTS

# WiFi



## HOTSPOTS

Public WiFi is a growing part of everyday life.

Whether people are at the coffee shop, hotel, airport, or doctor's office, public WiFi is rapidly becoming a standard offering for businesses of all types.

When your clients provide public WiFi, they have an obligation to protect users. But uncontrolled internet usage brings high risk.

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

Illegal torrent sites and apps

Unwanted or inappropriate content

Bandwidth Drains

And much more



72%

of users connect to public WiFi at cafés<sup>1</sup>

80%

of people say WiFi is the most important amenity at hotels<sup>2</sup>

### THE SECRET MENU ITEM YOU DON'T WANT

The public WiFi at a café was hijacked<sup>2</sup> to use cafe-goers' laptop CPU power to mine cryptocurrency.

### THE WORST KIND OF ROOM SERVICE

The DarkHotel group has been active for over a decade. They target business travelers using WiFi in luxury hotels<sup>4</sup> to deliver malware, spy on guests, and steal data.

64%

of travelers use airport hotspots<sup>1</sup>

### THE MILE HIGH SPY CLUB

It took a white hat hacker <30 mins to clone the WiFi at a major airport<sup>5</sup> using his phone as a hotspot. Right away, he had willing users ready to hand over their credit card details for a so-called "premium" connection. (Thank goodness he's one of the good guys.)

### AND WHEN IT COMES TO DOCTORS' OFFICES...

Healthcare experiences

**2X**

AS MANY CYBERATTACKS as other industries.<sup>6</sup>



## 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.

When it comes to protecting your clients' networks, the more restrictions, the better—but it's important to enforce them wisely. You don't want their 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?)

2

#### 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 selling DNS Protection for Guest WiFi to your clients, you can prevent cybercriminals from viewing their (and their users') browser histories, gaining access credentials, redirecting searches to malicious pages, and much more. You can also help clients enforce content filtering to ensure regulatory compliance and maintain bandwidth.

3

#### Help clients create a separate internet-enabled SSID and enforce 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.

4

#### 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. Help clients set up a user agreement so that any WiFi users must accept official Terms of Use before they can hop on the hotspot. This shifts legal liability for the results of risky behavior onto the users, where it belongs, rather than your clients.

5

#### Help clients position their WiFi access points wisely.

Clients shouldn't place access points next to a wall or other obstructions that can limit the signal. At the same time, they shouldn't put them right out in the open where someone could physically tamper with them.



For more information about securing your clients public WiFi, visit [webroot.com/DNSPGuestWiFi](http://webroot.com/DNSPGuestWiFi)

<sup>1</sup>Xirrus. "Rolling the Dice with public Wi-Fi." (October 2016)  
<sup>2</sup>Motherboard.vice.com. "Starbucks Wi-Fi Hijacked Peoples Laptops to Mine Cryptocurrency." (December 2017)  
<sup>3</sup>Statista.com. "Statista Hotels Survey." (May 2017)  
<sup>4</sup>ZDnet.com. "Hackers are Using Hotel Wi-Fi to Spy on Guests, Steal Data." (July 2017)  
<sup>5</sup>Latesthackingnews.com. "Connecting to Airport WiFi is Safe, Right?" (December 2017)  
<sup>6</sup>CSOnline.com. "Healthcare Experiences Twice the Number of Cyber Attacks as Other Industries." (March 2018)