PROTECTING PUBLIC WiFi HOTSPOTS

Public WiFi is a growing part of everyday life.

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

When you provide public WiFi for your customers, you have an obligation to protect them. But uncontrolled web usage brings high risk.

Depending on the industry in which you operate, uncontrolled web usage doesn't just risk introducing malware to the network. It can also cause regulatory compliance issues and damage your reputation with customers.

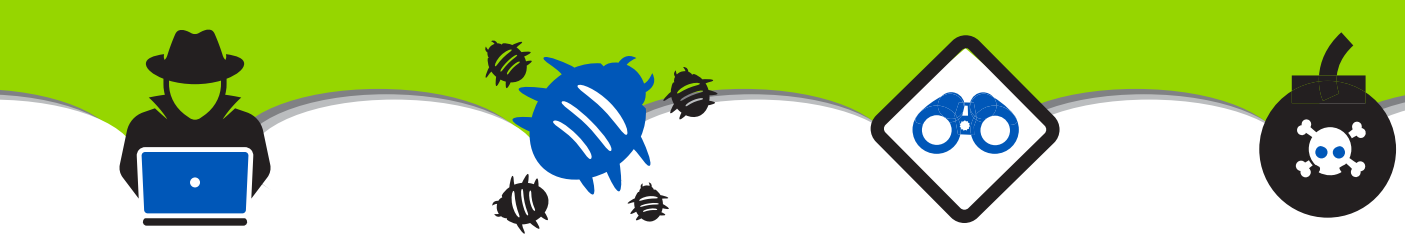
PUBLIC WiFi IS AT RISK FROM

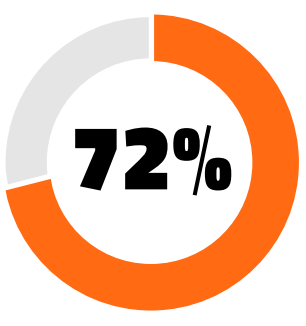
Man-in-the-middle attacks

Malware distribution

Snooping and sniffing

And much more





of users connect to public WiFi at cafés[1]

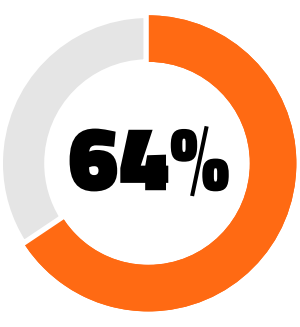
of people say WiFi is the most important amenity at hotels[3]

THE SECRET MENU ITEM YOU DON'T WANT

The public WiFi at a café was hijacked[2] to use cafegoers' 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[4] to deliver malware, spy on guests, and steal data.



of travelers use airport hotspots[1]

THE MILE HIGH SPY CLUB

It took a white hat hacker <30 mins to clone the WiFi at a major airport[5] using his phone as a hotspot. Right away, he had willing customers 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.[6]

SO WHAT CAN BUSINESSES DO

to protect their public WiFi, their customers, and their reputations from hacking and other threats?

1 Implement DNS-layer Protection

The DNS connection is involved in every aspect of internet usage, but it's highly vulnerable to cyberattacks. By adding DNS protection for your guest WiFi, you can prevent cybercriminals from viewing browser histories, gaining access credentials, redirecting searches to malicious pages, and much more. You can also enforce content filtering to ensure regulatory compliance.

2 Create a separate internet-enabled SSID.

With a service set identifier that's separate from your internal network, you give guests WiFi access without giving them free reign to access to your private corporate network and important company information.

3 Use strong network encryption and change.

WiFi Protected Access II (WPA2) is the preferred protocol and provides unique encryption keys for each wireless client that connects to it. And you already know how important it is to regularly change your passwords—the same holds true for your WiFi.

4 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. At the same time, don't put it right out in the open where someone could physically tamper with it.

5 Provide the right bandwidth and apply 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. You don't want guests to complain about slow connections, but you also don't want them accessing malicious or unwanted sites. (And who wants to spend extra money on unused bandwidth?)

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

[1] Xirrus. "Rolling the Dice with public Wi-Fi." (October 2016)
[2] Motherboard.vice.com. "Starbucks Wi-Fi Hijacked Peoples Laptops to Mine Cryptocurrency." (December 2017)
[3] Statista.com. "Statista Hotels Survey." (May 2017)
[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)

WEBROOT® Smarter Cybersecurity™