CHECKLIST

5 STEPS FOR PROTECTING YOUR BUSINESS’ PUBLIC WiFi

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—not to mention your business and reputation—from hacking, viruses and malware, spying, and other WiFi threats.

Plus, depending on your industry, you may be subject to compliance regulations that require you to secure any public or guest WiFi networks.

Here are 5 easy steps to protect your business’ public WiFi and the customers and guests who use it.

□

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 malicious hackers from viewing browser histories, gaining access credentials, redirecting searches to malicious pages, and other cybercriminal activities. You can also enforce content filtering to ensure regulatory compliance (see Step 5 below).

□

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 your private corporate network and important company information.

□

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.

□

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.

□

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 to access malicious or unwanted sites. (And who wants to spend extra money on unused bandwidth?)