Guide to safer hotspot operation

Hotspot operators have diverse requirements of their service. This guide gives you advice on how to easily and securely deploy a Wi-Fi hotspot. Take advantage of LANCOM Systems' many years of expertise to make ideal use of your bandwidth and to know that your data and that of your customers are managed securely.

Technical tips

a) Professional hotspot solution

A professional hotspot solution for Wi-Fi guest access featuring web-based user authentication comes with the LANCOM Public Spot Option or a cloud-managed hotspot via the LANCOM Management Cloud. This gives you the assurance that only guests who are in possession of a (time or volume limited) ticket/voucher can access the guest network using the appropriate credentials.

b) Separate subnets (guests, administration, and service)

Give each subnet for management, guests and service a separate SSID, e.g. for the guest network, the management network, the restaurant network, etc. At the same time, be careful not to set up too many subnets, as this can affect the efficiency of the overall network. Current standards require all of the SSIDs to be encrypted with WPA2 or WPA3, with the exception of the guest network: This is generally unencrypted, since guest authentication is performed via a web-based interface. Consequently, only guests with access credentials are able to log in. It is important that you also separate the subnets at the network level. There are a number of options for doing this. Your IT system vendor can advise you on this matter and implement network separation (find LANCOM partners).

c) No communication between clients on the guest SSID

On the guest SSID, you should prevent the clients (tablets, smartphones, laptops) from communicating with one another. There is no need for end devices to communicate with one another within a guest network that is only intended to provide Internet access. On the contrary, this represents a security risk if guests have inadvertently set up shared directories on their devices. LANCOM access points provide this feature.

d) Restrict web access

Please note that you should inform your guests about restricted access to Internet content in your Terms and Conditions (see “More tips”).

- Port blocks: We recommend that some ports should be blocked, such as those used by the peer-to-peer connections that are often used by illegal

file-sharing networks. The best option is to block the ports by means of the firewall integrated into the central network component (e.g. the router). In practice, a “Deny - All” strategy is advisable: Block all ports and only open those required for the services you want to allow: For example, port 80 for surfing, port 53 for DNS, port 443 for HTTPS (secure web sites), ports 110, 143, 465, 993 and 995 for e-mail, and port 500 and 4500 for VPN applications. Visit our Knowledge Base for specific help with further questions.

- Content Filter: We recommend using a web content filter that allows you to block inappropriate Internet content. This software allows you to block access to certain web page categories, such as “Violence” and “Pornography”.
- Firewall: The increasing number of cyberattacks is a threat to the security and availability of your data and that of your guests. A suitable firewall solution ensures that your sensitive data is protected against attacks both from within the network (e.g. from the guest network) and from the outside. Be sure to secure this data against unwanted access and cyberattacks with an effective and trustworthy security architecture “Made in Germany”, because: For non-EU providers of security technology, it is impossible for them to simultaneously comply with legislation in their home countries and in Europe. Their customers thus risk access from the outside and data leakage.

More tips

a) Information about the Internet connection

Make it clear that your role as the service provider is limited to providing passive Internet access (Wi-Fi hotspot) to third parties: You should register this Internet access with your provider using your business name. For a hotel this would be, for example, “Hotel Exemplary, owner: John Doe” instead of just entering your first and last names.

b) General terms and conditions for hotspot use

Firstly: There is no requirement for you to display your general terms and conditions in the registration mask! Instead you have an opportunity to present your company to your guest or customer on their end devices, and also to set out the framework for using the hotspot. Before your guests and customers can use your hotspot, make sure that they accept your terms and conditions, which should comply with current GDPR guidelines.

In particular, your guests should agree that they shall not upload any copyrighted material such as music, films and images to or from the Internet, or otherwise violate applicable law. It’s easy to do: In the login mask for the hotspot, you oblige your guests and customers to confirm the terms and conditions with a click of the mouse. Talk to your IT system vendors about the technical implementation.

c) No data is disclosed to third parties

In the terms and conditions, point out to the guest that under no circumstances should they pass on their credentials for Wi-Fi guest access to third parties. This

does not apply to group tickets that you buy with the LANCOM Public Spot option or the LANCOM Management Cloud, e.g. for conferences on your premises. In this case, all conference participants conveniently get the same access code to the guest network. Make sure here that these group tickets are only valid for the duration of the event. The uncontrolled use of your hotspot has a direct impact on your customers and guests, as significantly more bandwidth is taken up.

d) Data storage

Basically, you should only record the data of your customers that is required for the technical processing and billing of the Wi-Fi hotspot*.

Basic data: Basic data includes information such as name, address, date of birth, bank details if applicable, and technical data of the connection (fixed IP addresses). We recommend that you save your customers' basic data for a certain period of time so that you can contact them if necessary. To do this, obtain the customer's consent when they agree to your terms and conditions.

With regard to the discussion on data retention, you as a hotspot operator have no obligations: The law only affects telecommunications providers, not the provider of Wi-Fi access.

e) Port blocks / Content Filter

In your terms and conditions, inform your guest if you restrict Internet access in any way. If you block ports, e.g. for peer-to-peer or VPN connections and/or a web content filter (LANCOM Content Filter) to block targeted websites, be sure to explicitly inform your guests about this before they use the hotspot.

If you have any further questions, please do not hesitate to contact us:
LANCOM Systems GmbH, Office Sales Team, tel.: +49 (0) 2405/499 36-333.

* This information refers to the legal situation in the Federal Republic of Germany. For other countries, please inform yourself about the respective applicable legal situation.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de
www.lancom-systems.com