SOPHOS

Hot Tips for Securing Your Wi-Fi Network

By **James Lyne**, Director of Technology Strategy

Whether you're a home user, small business or enterprise it's important to make sure you secure your wireless network. And sadly, many people still don't. There are plenty of resources available to help you do this and best practices you can adapt to your organization's size. Here are the 11 top tips we recommend you consider.

1. Use strong encryption

Enable Wi-Fi protected access (WPA) and ideally WPA2. This provides much stronger encryption for securing your communications than WEP, which hackers can easily crack. You can see an example of this in our video.

2. Create a strong password

Even WPA2 can be cracked by the bad guys if you don't use a secure password. You can see in our video how a simple password can be cracked in a short space of time. Check out our guide to creating easy-to-remember but hard-to-crack passwords. You won't have to type your password very often, but it could prevent criminals from watching what you do online. Remember too that cybercriminals can use cloud services to aid password cracking, so even a seemingly secure but shorter password may not be safe.

3. Consider your authentication strategy

If you are using WPA2-PSK, your employees, friends or family will all be using the same password, and may unintentionally share it with others. Remember that any of them can see your network traffic. If an employee leaves the company, they may retain your network key—allowing them to later decrypt your traffic or access the network. For larger organizations, consider using a certificate-based authentication mechanism or RADIUS so that each user has their own managed credentials. That way they avoid accidentally sharing access to your network. There are many strong authentication deployment modes available for you to use in a good enterprise wireless solution.

4. Change the name of your network

It's a little known fact that the network SSID (such as “Home” or “Free Public Wi-Fi”) is actually part of the security for encrypted networks.* Using a default name can make it easy for attackers to guess your password quickly. Try to use a unique name, but also make sure not to give too much information away, as it may tempt attackers to target you.

5. Consider SSID hiding carefully

SSID hiding is a feature which hides your network name from the list that people in the area can see on their computers or mobile devices. This means a user has to manually configure the network name and password. SSID hiding reduces temptation from casual attackers, so it’s a useful feature. However, be aware that within a few seconds any attacker with basic knowledge will reveal this wireless network name. It is a very light defense that you shouldn't rely on. Make sure you combine it with strong encryption and a good password.

6. Beware of device authorization lists

MAC address filtering prevents devices that aren’t on an authorized list of allowed hardware devices from using your network. This feature is often presumed by administrators to be a strong defense. Unfortunately, these MAC addresses are easily forged by attackers. Having to manually authorize these addresses within your organization can also be a significant administrative burden. It’s a good practice to follow the principle of "defense-in-depth." However, we recommend not using MAC address filtering. Instead, focus your efforts on strong passwords and encryption.

* The handshake authentication includes the network name as part of the calculation. There are tools to generate pre-calculated lists and readily available lists that use common SSIDs. Changing the SSID makes the cracking effort much slower for an attacker as they have to re-compute against the SSID name.

7. Manage the names of networks you've previously used

By default, most devices will remember networks you have previously connected to. For example, if you used a hotel's wireless connection, your device will likely remember its name and search for that network wherever you travel. Attackers' wireless scanning tools will identify your laptop or mobile device and see that it has previously connected to a network with this name, even if it's not presently in range. This may not seem like a significant issue, but wireless network names may give away key information such as the business you work for, hotels or sites you have visited, or—in extreme cases—your address (we've seen networks named after street addresses). Remember to remove such profiles after use if they give away sensitive information.

8. Protect yourself on open networks

If you connect to an open hotspot such as those commonly provided by hotels, you need to take additional steps to be sure your traffic isn't visible to hackers. Make use of a strong VPN to encrypt all of your traffic over the wireless network. You should also check the hotspot is legitimate when providing credit card details or login information, as sometimes cybercriminals set up fake hotspots.

9. Practice defense-in-depth

Network security is only one layer of a good security strategy. You should follow best practices for endpoint protection, patching and web security. With the right security practices you can keep yourself secure even if your wireless network is compromised, reducing the odds of a hacker getting away with your data.

10. Manage visitors and restrict traffic

If you are a business that needs to provide guest or consultant access, consider offering a separate network with restrictions on what guests can access. A hotspot registration portal can be an easy way to restrict access without a lot of administrative effort. Wireless solutions should enable you to easily deploy such networks, allowing visitors only access to the Internet and keeping them away from corporate services.

11. Manage your wireless access points

Make sure that your wireless access points (particularly those of branch offices and other locations) use the correct security configuration. Many enterprises may have secure wireless at headquarters, but then have weak access point configuration at branch offices. These can act as a back door to the enterprise, undermining your security efforts. Policy management and remote logging are therefore a priority to make sure security is consistent across your environment.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

A Sophos Article 08.12v1.dNA

SOPHOS