

Wi-Fi Security Advisor: Overview

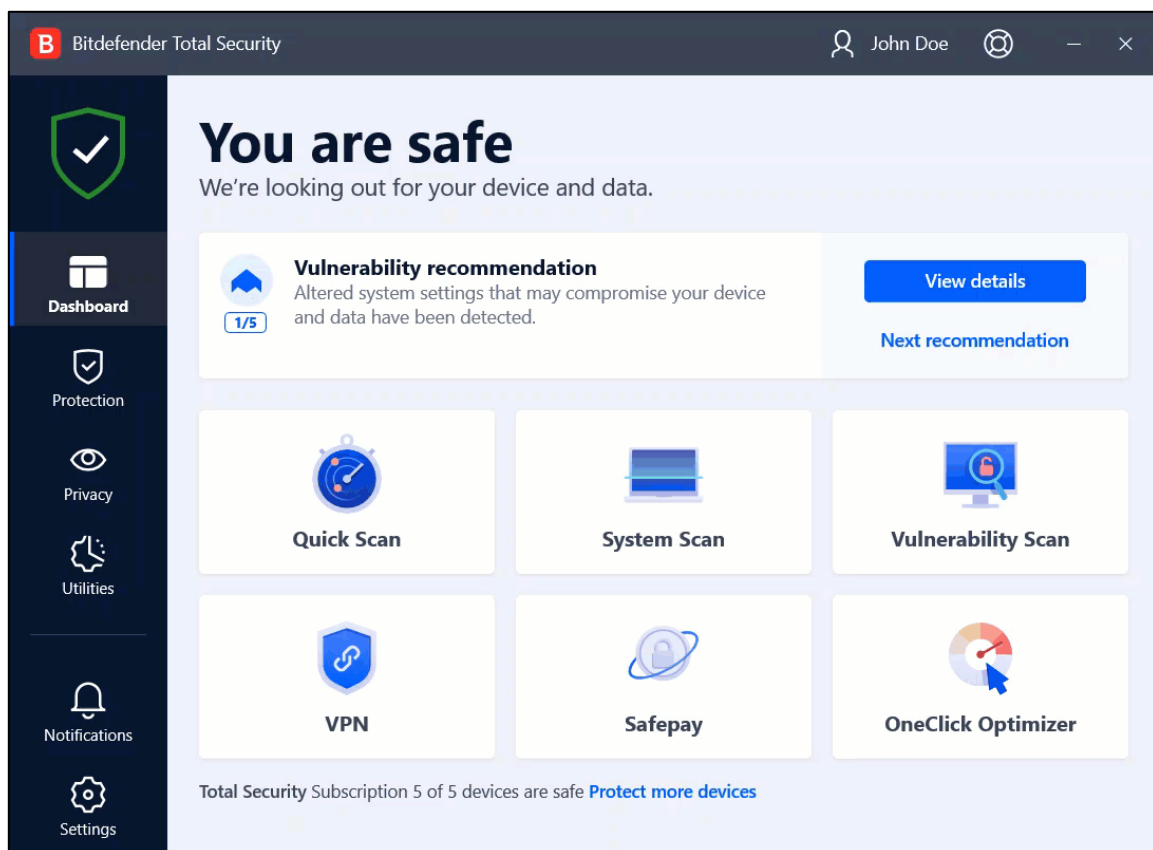
To safeguard you against the perils of unsecured or unencrypted public Wi-Fi, Bitdefender Wi-Fi Security Advisor analyzes how secure a wireless network is, and when necessary, it recommends you use Bitdefender VPN. Bitdefender Wi-Fi Security Advisor monitors the following networks: Home Wi-Fi, Office Wi-Fi, Public Wi-Fi.

While on the go, working in a coffee shop, or waiting at the airport, connecting to a public wireless network for making payments, checking emails or social network accounts can be the fastest solution. But prying eyes trying to hijack your personal data can be there, watching how the information leaks through the network. Personal data means the passwords and usernames you use to get access to your online accounts, such as emails, bank accounts, social media accounts, but also the messages you send. Usually, public wireless networks are more likely to be unsafe since they do not require a password for login, and if they do, the password could be made available to anybody who wants to connect. Moreover, they may be malicious or honeypot networks, representing a target for cybercriminals.

Turning on/off Wi-Fi Security Advisor

To turn on or off the Wi-Fi Security Advisor notifications:

1. Click Protection on the navigation menu on the Bitdefender interface.
2. In the Vulnerability pane, click Open.
3. Go to the Settings window and turn on or off the Wi-Fi Security Advisor switch.



Configuring Home Wi-Fi

To start configuring your home network:

1. Click Protection on the navigation menu on the Bitdefender interface.
2. In the Vulnerability pane, click Open.
3. Go to the Wi-Fi Security Advisor tab and click Home Wi-Fi.
4. In the Home Wi-Fi tab, click SELECT HOME WI-FI. A list of the wireless networks you connected to until now is displayed.
5. Point to your home network, and then click SELECT. If a home network is considered unsecured or unsafe, configuration recommendations to improve its security are displayed.
 - To remove the wireless network, you have set as a home network, click the REMOVE button.
 - To add a new wireless network as home, click Select new Home Wi-Fi network.

Configuring Office Wi-Fi

To start configuring your office network:

1. Click Protection on the navigation menu on the Bitdefender interface.
2. In the VULNERABILITY pane, click Open.
3. Go to the Wi-Fi Security Advisor window, click Office Wi-Fi.
4. In the Office Wi-Fi tab, click SELECT OFFICE WI-FI. A list of the wireless networks you connected to until now is displayed.
5. Point to your office network, and then click SELECT. If an office network is considered unsecured or unsafe, configuration recommendations to improve its security are displayed.
 - To remove the wireless network, you have set as an office network, click REMOVE.
 - To add a new Office wireless network, click Select new office Wi-Fi.

About Public Wi-Fi

While connected to an unsecured or unsafe wireless network, the Public Wi-Fi profile is activated. While running in this profile, Bitdefender will automatically:

- recommend connecting to Bitdefender VPN to secure the network
- enable Advanced Threat Defense
- enable Bitdefender Firewall and apply the following settings to your wireless adapter:
 - Stealth mode – ON
 - Network type – Public
- enable the following options from Online Threat Prevention:
 - Encrypted web scan
 - Fraud protection

- Phishing protection

Checking information about Wi-Fi networks

To check information about the wireless networks you connect to:

1. Click Protection on the navigation menu on the Bitdefender interface.
2. In the Vulnerability pane, click Open.
3. Go to the Wi-Fi Security Advisor tab.
4. Depending on the information you need, select one of the three tabs, Home Wi-Fi, Office Wi-Fi, or Public Wi-Fi.
5. Click the name of the network to learn more. By expanding each network, the following details are displayed:
 - **Secured** – here you can view if the selected network is secured or not. Unencrypted networks can leave the data you use exposed.
 - **Channel/Frequency** – here you can view the channel frequency used by the selected network.
 - **Type of sign in** – here you can view if the selected network is protected using a password or not. It is highly recommended to connect only to networks that have set strong passwords.
 - **Encryption type** – here you can view the encryption type used by the selected network. Some encryption types may not be secure. Therefore, we strongly recommend you check information about the displayed encryption type to be sure that you are protected while surfing the web.
 - **Password strength** – here you can view how strong the password is. Note that the networks that have set weak passwords represent a target to cybercriminals.
 - **Authentication type** – here you can view the authentication type used by the selected network.