# Top Eleven Threats to Your Wireless Network

As the use of Wi-Fi increases, so does the vulnerability to both opportunistic and targeted attacks. Bad actors can range from cyber vandals to sophisticated cyber criminals with commercial, political, or social motivations. Organizations that fail to properly secure their wireless networks expose their customers, partners, and internal users to a number of risks:

## 1 Wi-Fi Password Cracking

Wireless access points that still use older security protocols, like WEP, make for easy targets because passwords are notoriously easy to crack.

## 2 Rogue Hotspots

Nothing physically prevents a cyber criminal from enabling a foreign access point near your hotspot with a matching SSID, which invites customers to log in. Users that fall victim to the Rogue AP are susceptible to a malicious code injection that often goes unnoticed.

## 3 Planting Malware

Customers who join a guest wireless network are susceptible to unknowingly walking out with unwanted malware, delivered from bad-intentioned neighboring users. A common tactic used by hackers is to plant a backdoor on the network, which allows them to return at a later date to steal sensitive information.

## 4 Eavesdropping

Guests run the risk of having their private communications detected, or packet sniffed, by nosey cyber snoops while on an unprotected wireless network.

## 5 Data Theft

Joining a wireless network puts users at risk of losing private documents that may contain highly sensitive information to cyber thieves who opportunistically intercept data being sent through the network.

## 6 Inappropriate and Illegal Usage

Businesses offering guest Wi-Fi risk playing host to a wide variety of illegal and potentially harmful communication. Adult or extremist content can be offensive to neighboring users, and illegal downloads of protected media leave the business susceptible to copyright infringement lawsuits.

## 7 Bad Neighbors

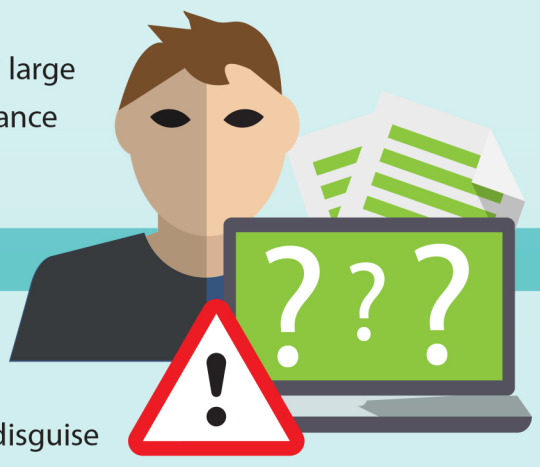
As the number of wireless users on the network grows, so does the risk of a pre-infected client entering the network. Mobile attacks, such as Android's Stagefright, can spread from guest to guest, even if victim zero is oblivious to the outbreak.

## 8 Man in the Middle Attack (MiM)

Mundane communication over Wi-Fi can lead to a breach when a villainous actor secretly intercepts and alters legitimate conversations.

## 9 Wireless DoS

Attackers can cause a standstill in Wi-Fi access by intentionally sending large amounts of traffic to legitimate access points, which disables the appliance from legitimate use.



## 10 Masquerading Attacks

Cyber criminals set on breaching Wi-Fi security commonly attempt to disguise their devices as legitimate or known devices by spoofing MAC addresses.

## 11 Misconfigured AP

Deploying access points without following Wi-Fi security best practices can lead to inadvertent misconfigurations, which often leads to a security risk.

Enabling Wi-Fi is easy, security is the challenge. Every WatchGuard product is built with consideration for the Secure Wireless environment.

Learn more: **ccbtechnology.com/watchguard-wifi-cloud**

WatchGuard®

© 2016 WatchGuard Technologies, Inc. All rights reserved. WGCE66887_090916