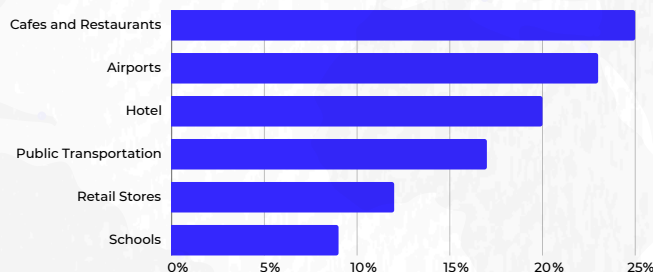


# PROTECT GUEST WI-FI USERS FROM CYBER ATTACKS

Your guests expect public Wi-Fi, and they expect a secure experience. **By adding protective DNS to your public Wi-Fi offering, you not only prevent your guests from harm, but you protect your organization as well.**

*Most common places to have information compromised via public Wi-Fi (source: Forbes, 2023)*



## PROVIDING PUBLIC WI-FI BRINGS BENEFITS AND THREATS

Offering public Wi-Fi can drive customer loyalty, result in shoppers spending more, create a competitive edge, or improve user satisfaction. However, guest Wi-Fi can expose customers to various threats on your network, including malware distribution, botnets, phishing scams, and more. Additionally, your brand could be at risk if inappropriate content is accessed in your store, hospital, school, or workplace.

## PROTECTING RETAIL USERS

One large US-based retailer deployed DNSFilter to thousands of stores in only 28 days. As end users step into their stores, they are unable to access sites on public Wi-Fi based on the retailer's preferences. This proactive approach not only enhances customer satisfaction but also safeguards the brand's image and reputation. By using DNSFilter, thanks to its world's fastest Dual-Anycast network, users experience fast, reliable Internet connectivity and are protected from malicious threats and phishing attacks. This proactive stance on providing safe, reliable public Wi-Fi networks not only prioritizes customer well-being but also underscores the retailer's commitment to providing a safe and enjoyable shopping environment.

## SECURING HOSPITALITY

Hacking groups like DarkHotel have been active since 2007, often targeting traveling business executives via phishing campaigns and C2 to gain access to critical systems. Providing public Wi-Fi is table stakes for the modern hospitality industry, and ensuring the protection of guests using Wi-Fi is imperative. As crucial as cybersecurity may be, DNSFilter also plays a pivotal role in aiding organizations by blocking CSAM (child sexual abuse material) and other harmful content, particularly important in areas vulnerable to human trafficking, such as hotels. DNSFilter is a partner of We Protect Global Alliance, Internet Watch Foundation (IWF), and Project Arachnid.

## SHIELDING EDUCATION


Providing safe and secure public Wi-Fi in educational settings is crucial for fostering a safe and effective learning environment. By defending against cyber threats like malware and phishing attacks, secure Wi-Fi supports uninterrupted online learning and protects educational resources. Moreover, it empowers educators to leverage technology for innovative teaching methods, enhancing the overall learning experience. Adopting DNSFilter underscores the institution's commitment to student safety and academic excellence, while also creating an easier path toward CIPA compliance.

## ABOUT DNSFilter

DNSFilter is protective DNS delivered in a variety of ways, including via access points to protect end users of public Wi-Fi. DNSFilter makes it easy to block unwanted DNS traffic, from cyber threats to unsavory content. With 70% of attacks using Domain Name System (DNS), DNSFilter provides the world's fastest protective DNS powered by machine learning that uniquely identifies 61% more threats than competitors on an average of ten days earlier, including zero-day attacks. Over 35 million monthly users trust DNSFilter to protect them from phishing, malware, and advanced cyber threats.

### GET IN TOUCH

 [dnsfilter.com](https://dnsfilter.com)

 (877) 331-2412

 [sales@dnsfilter.com](mailto:sales@dnsfilter.com)