RESEARCH ARTICLE

PUBLIC WI-FI: RISKS, PRIVACY CONCERNS, AND PRACTICAL PROTECTIONS

Anuradha Singh

Department of Computer Science,

Pillai College of Arts, Commerce & Science, New Panvel

Corresponding author E-mail: anuradhasingh@mes.ac.in

DOI: https://doi.org/10.5281/zenodo.18054993

Abstract:

Public wireless networks (public Wi-Fi) offer convenience and digital inclusion but also expose users, providers, and third parties to a broad range of technical, privacy, legal, and social risks. This paper reviews the technical foundations of public Wi-Fi, catalogues principal attack vectors and privacy threats, summarizes relevant standards and high-profile vulnerabilities, examines user behavior and provider responsibilities, and proposes layered mitigation strategies for individuals, organizations, and policymakers. The analysis draws on security guidance and studies from established authorities and recent research to present practical, evidence-based recommendations that balance usability and protection. Key findings include (1) most meaningful risk to end users comes from weak or absent link encryption, rogue hotspots, and application-level vulnerabilities; (2) technical fixes (WPA3, certificate validation, secure DNS, VPNs) reduce—but do not eliminate—risk; (3) human behavior (auto-connect settings, credential reuse) remains a major factor; and (4) a combination of technical controls, user education, and policy measures is necessary to make public Wi-Fi safer and equitable.

Keywords: Public Wi Fi, Privacy Threats, Mitigation Strategies.

1. Introduction:

Public Wi-Fi is ubiquitous: cafés, airports, libraries, hotels, city centers, and transportation hubs commonly offer wireless Internet access as a free or low-cost service. For many users—students, travelers, low-income households—such networks are essential for accessing information, education, employment, and public services. Yet the same openness that makes public Wi-Fi valuable also creates an attack surface for passive eavesdropping, active interception, malware distribution, and privacy abuse. Understanding these risks, their technical mechanisms, and how to mitigate them is crucial for individuals, enterprises that offer public access, and regulators shaping digital inclusion policy.

This paper is structured as follows: Section 2 explains how public Wi-Fi works and the baseline security provided by Wi-Fi standards. Section 3 surveys major attack techniques and privacy threats associated with public hotspots. Section 4 reviews notable vulnerabilities and guidance from authorities.

Section 5 discusses user behavior and socio-economic aspects. Section 6 presents layered mitigation strategies (device configuration, network architecture, application design, and policy). Section 7 offers recommendations for stakeholders and Section 8 concludes.

2. Technical Foundations of Public Wi-Fi

To analyze risk, we must first summarize how public Wi-Fi operates in practical deployments.

2.1 Basic Architecture

A public Wi-Fi hotspot typically consists of an access point (AP) bridging wireless clients to a local network and onward to the Internet via a NAT/gateway. Clients associate with the AP at the link layer (802.11), then obtain network configuration via DHCP and connect to services over TCP/IP and higher-level protocols (HTTP, HTTPS, SMTP, etc.). Many venues deploy a captive portal—a web page that forces user interaction (such as login, acceptance of terms, or payment) before granting full Internet access.

2.2 Link-Layer Security: WPA Variants

Wi-Fi Protected Access (WPA) replaces the insecure WEP and evolved through WPA, WPA2, and WPA3. Enterprise deployments use 802.1X/EAP for per-user authentication; simpler public hotspots often use WPA2-PSK or operate as open networks with no link encryption. While WPA2 and WPA3 provide strong confidentiality when correctly configured, many hotspots are misconfigured or intentionally left open for convenience, exposing traffic to observation or manipulation.

2.3 Application-Layer Protections

Even on untrusted networks, well-designed applications can protect user data via end-to-end encryption (HTTPS/TLS) and secure authentication. Therefore, the risk to user data depends on both link-layer protections and whether applications encrypt traffic. When applications do not enforce encryption or when users ignore certificate warnings, attackers can intercept or alter data despite higher-level protections (OWASP Foundation, 2021).

Authoritative testing guidance and catalogues of Wi-Fi testing procedures and vulnerabilities exist to assist security practitioners; these resources summarize the testing methodology and common vulnerabilities in Wi-Fi systems.

3. Threats and Attack Vectors

Public Wi-Fi faces a wide range of attacks. Below, we classify and describe the principal vectors.

3.1 Passive Eavesdropping (Sniffing)

On open or weakly protected networks, attackers can passively capture wireless frames and extract unencrypted application data. Historically, many websites and services sent sensitive content without TLS; while adoption of HTTPS has reduced exposure, some services still leak information or partially encrypt sessions. The ability to sniff traffic enables the harvesting of credentials, session cookies, and personal information when those items are transmitted unencrypted.

3.2 Man-in-the-Middle (MITM) Attacks and Rogue Hotspots

Active MitM attacks on Wi-Fi take several forms. An “evil twin” or rogue hotspot impersonates a legitimate AP (often by using a familiar SSID) and entices victims to connect. Once connected, the

attacker mediates traffic and can intercept credentials, inject malicious content, or perform SSL stripping if clients accept downgraded or invalid certificates. Techniques such as ARP spoofing/poisoning or DNS spoofing accomplish similar goals when the attacker is already on the same network.

3.3 Side-Jacking and Session Hijacking

Even when credentials are submitted over HTTPS, attackers may capture session cookies transmitted over insecure channels or exploit applications that do not mark cookies as secure/HTTP Only. enabling session reuse (side-jacking). This can allow attackers to impersonate users on web services that rely on cookie-based sessions.

3.4 Malware Distribution and Network-Level Push Attacks

Compromised or malicious hotspots can attempt to push malware or malicious redirects to connected devices (for example, via captive portal injection or malicious advertising). On devices with outdated software or weak configuration, these vectors can lead to compromise.

3.5 Protocol and Implementation Weaknesses

Bugs in protocols and implementations can introduce vulnerabilities. The KRACK (Key Reinstallation Attack) research demonstrated that weaknesses in the WPA2 handshake could be exploited to decrypt traffic in some circumstances, underscoring that even widely deployed standards can harbor bugs requiring vendor patches. Proper patching and firmware updates are therefore critical (Wired, 2017).

3.6 Tracking and Privacy Erosion

Beyond active attacks, public Wi-Fi can be used for passive tracking. APs, or third-party analytics services tied to hotspots, can log device MAC addresses, probe requests, connection times, and browsing patterns to build profiles of users or to track movement across venues. While MAC randomization on modern devices helps, many deployments still gather identifying metadata for legitimate analytics or monetization, sometimes without clear user consent.

3.7 Supply-Chain and Infrastructure Compromise

If the hotspot infrastructure is compromised—either the APs themselves or the upstream gateway—attackers can capture or modify traffic for many clients. Similarly, poorly segmented provider infrastructure risks exposing backend management interfaces.

4. Evidence From Authorities and Studies

Several consumer protection and security organizations have published guidance and study findings that illuminate the scale and nature of public Wi-Fi risks.

The U.S. Federal Trade Commission (FTC) provides consumer guidance on how to know whether information is safe on public Wi-Fi and recommends cautious behavior when using hotspots, pointing out that unencrypted sites and services leave data exposed. The FTC's consumer guidance helps users understand which actions reduce exposure.

The Electronic Frontier Foundation (EFF) offers practical privacy preservation materials (Surveillance Self-Defense) for protecting device privacy in hostile network environments; the EFF emphasizes end-to-end encryption, use of Tor, and privacy-respecting tools for users concerned about surveillance (Electronic Frontier Foundation, 2024).

Security research and case studies repeatedly identify the same set of attacks (evil twin, MitM, side-jacking) as practical under real-world conditions. Peer-reviewed and industry papers document vulnerability patterns in free public Wi-Fi and evaluate mitigation effectiveness—concluding that no single measure eliminates all risk and that layered defense is required (Shinde, 2022).

Regulatory bodies and standard-setting organizations (including FCC reports and working groups) have commented on Wi-Fi security, particularly when hotspot lending and community Wi-Fi initiatives intersect with public policy objectives (e.g., digital inclusion). Policymakers sometimes grapple with tradeoffs between promoting access and ensuring safety/oversight of public connectivity. Recent policy actions have even affected funding for hotspot lending programs, demonstrating that broadband access policy and security considerations interact in consequential ways (AP News, 2023).

5. User Behavior and Socio-Economic Considerations

5.1 Why Users Take Risks

Users frequently connect to public Wi-Fi out of convenience, cost avoidance (mobile data), or lack of alternatives. In many cases, users are unaware of specific threats, underestimate risk, or accept tradeoffs to get online quickly. Behavioral studies and surveys show that despite growing awareness campaigns, users continue to engage in risky behaviors such as auto-connecting to known SSIDs, ignoring certificate warnings, reusing passwords, and performing sensitive transactions (banking, shopping) on public networks.

5.2 Digital Inclusion and Equity Tradeoffs

Public Wi-Fi plays a critical role in bridging the digital divide. For low-income individuals and communities, removing or overly restricting public Wi-Fi can exacerbate inequities. Therefore, security measures must be designed to preserve access while protecting users—this requires affordable, privacy-preserving designs, clear consent mechanisms, and education.

5.3 Venue Responsibilities and Business Models

Venues offering Wi-Fi balance costs, user experience, legal liability, and data monetization. Some operators monetize through analytics, advertisements, or captive-portal data capture. These models raise privacy concerns when personal data is collected or shared without robust notice and consent. Transparency and minimal data collection are important principles for preserving trust.

6. Mitigation: Layered Defenses

No single technique fully eliminates the risks of public Wi-Fi. Effective protection relies on layered measures across device configuration, application behavior, network architecture, and policy. Below, we propose practical, implementable measures for each stakeholder.

6.1 For Individual Users (End-User Controls)

6.1.1 Prefer Cellular or Personal Hotspot When Possible

Mobile network connections (cellular data) generally present a smaller risk profile than untrusted Wi-Fi; using a phone's personal hotspot to tether laptop/tablet traffic is often safer.

6.1.2 Disable Automatic Connections

Turn off "auto-connect" to open Wi-Fi networks and remove known SSIDs that are no longer needed. Confirm network names with venue staff before connecting.

6.1.3 Use End-to-End Encryption: HTTPS/TLS and Secure Apps

Only use websites and services that enforce HTTPS/TLS. Modern browsers show padlock indicators; do not ignore certificate warnings. Prefer apps that implement certificate pinning or robust TLS validation.

6.1.4 Use a Reputable VPN

A well-configured, trusted virtual private network (VPN) creates an encrypted tunnel between the device and a trusted endpoint, protecting traffic from local eavesdroppers. Note: VPNs do not protect against compromised endpoints or malicious captive portals that themselves ask users to share credentials.

6.1.5 Keep Devices and Apps Patched

Apply OS and application updates promptly to remediate known vulnerabilities (e.g., KRACK mitigations). Avoid using vulnerable or unmaintained devices on public networks.

6.1.6 Limit Sensitive Operations

Where possible, avoid sensitive transactions (banking, entering passwords) on untrusted networks. If necessary, use multi-factor authentication and one-time passwords to reduce credential theft.

6.1.7 Use Endpoint Protection and Firewalls

Enable device firewalls, disable file and printer sharing on public networks, and employ endpoint anti-malware solutions.

6.1.8 Harden Privacy Settings

Enable MAC address randomization (most modern OSes do this by default when scanning and sometimes when connecting), disable unnecessary background services, and minimize device broadcasting.

6.1.9 Verify Captive Portals

When required to use a captive portal, verify the correct URL and communicate only the minimum required data to gain access.

EFF's Surveillance Self-Defense resources outline many of these user-level practices and tools for privacy protection (Electronic Frontier Foundation, 2024).

6.2 For Hotspot Operators and Venues

6.2.1 Encrypt the Local Link and Segment Networks

Where feasible, deploy WPA2-Enterprise or WPA3 configurations that avoid a shared PSK. At minimum, segment guest traffic from operational/management networks, apply client isolation (AP isolation) to prevent lateral attacks, and ensure the gateway enforces strong TLS for captive portal interactions.

6.2.2 Use Secure Captive Portal Design

Design captive portals to use HTTPS, minimize data collection, provide clear privacy notices, and not request sensitive credentials (banking passwords, social security numbers). If social login is used, prefer OAuth flows that do not expose full credentials to the venue.

6.2.3 Monitor and Patch Infrastructure

Keep AP firmware and management consoles updated, disable unused management interfaces, change default credentials, and employ network monitoring to detect rogue APs or anomalous traffic.

6.2.4 Provide Safe Defaults and User Education

Offer guidance, signage, or an informational splash page recommending best practices (e.g., use VPN) and avoid asking users for unnecessary personal data. If analytics are collected, provide opt-in and anonymization.

6.2.5 Privacy-Respecting Analytics

When gathering network usage metrics, minimize retention, anonymize identifiers, and provide transparent policies and opt-out mechanisms.

6.3 For Application and Service Developers

6.3.1 Enforce HTTPS and Secure Cookies

All web services should enforce HTTPS via HSTS, use secure cookie flags, and avoid transmitting sensitive tokens over plain HTTP. Certificate pinning (with careful update mechanisms) can reduce MitM risk.

6.3.2 Implement Robust Session Management

Design sessions to expire appropriately, bind sessions to device attributes where practical, and use short-lived tokens plus multi-factor authentication for sensitive actions.

6.3.3 Protect Mobile Apps

Mobile applications should validate TLS properly, avoid insecure storage of credentials, and offer logout or remote-wipe capabilities.

6.4 For Policymakers and Regulators

6.4.1 Promote Safe Public Wi-Fi Programs with Standards

Public subsidy programs that expand Wi-Fi access (e.g., libraries, schools) should require baseline security and privacy standards—segmentation, secure captive portals, and minimal data retention—to balance inclusion and safety.

6.4.2 Encourage Vendor Accountability and Disclosure

Regulators can require transparent disclosure about data collected by hotspot providers and enforce privacy notices and opt-in models.

6.4.3 Fund Digital-Literacy Programs

Invest in outreach and education so users understand risks and protective behaviors. The FCC and other agencies have engaged in discussions about hotspot lending and connectivity programs—demonstrating that policy decisions materially affect both access and the security posture of community Wi-Fi offerings. Recent regulatory changes affecting funding for hotspot programs show that security and policy are tightly coupled (AP News, 2023).

7. Case Studies and Notable Incidents

7.1 KRACK: Protocol-Level Lesson

The KRACK vulnerability highlighted that even widely adopted standards (WPA2) can contain subtle implementation or protocol flaws that allow key reinstallation and decryption of some traffic. The

research led to vendor patches and reinforced the need for coordinated disclosure and prompt firmware updates. The episode demonstrated two lessons: (1) rely on multiple layers of security (TLS in addition to WPA), and (2) vendors and operators must have patch management plans (WIRED, 2017).

7.2 Rogue Hotspot Social Engineering

Security researchers and incident reports frequently describe attackers creating malicious "free Wi-Fi" SSIDs similar to a café or airport network. Users connect, are presented with a captive portal or are transparently proxied, and attackers harvest credentials or push malware. These incidents emphasize the need for awareness and checking network names with staff.

7.3 Policy Tensions in Public Hotspot Programs

Changes in funding or rules for library hotspot lending and school bus connectivity illustrate the tension between expanding access and maintaining oversight when public funds are used. Policy reversals have affected the availability of safe, managed hotspot solutions for vulnerable populations—showing that security cannot be decoupled from broader social policy (AP News, 2023).

8. Evaluation of Mitigation Effectiveness

Mitigation strategies vary in their cost, usability impact, and effectiveness. Below is a brief evaluation:

- **VPNs**: Highly effective against local MitM and eavesdropping when the VPN is trustworthy. Limitations: does not prevent phishing sites or malicious captive portals that capture credentials before VPN startup; depends on user adoption and trustworthy provider behavior.
- **WPA3 / WPA2-Enterprise**: Very effective for link encryption when available; limitations include legacy device support and operator complexity.
- **HTTPS/TLS**: Essential for application-level protection; effectiveness depends on proper implementation and certificate trust (users ignoring warnings undermines TLS).
- **Device hardening (patching, firewall)**: Reduces attack surface but requires user discipline and management in heterogeneous device contexts.
- **User education**: Important but often insufficient alone—users may understand warnings but still prioritize convenience.
- **Policy & regulation**: Effective at scale for setting minimum standards; enforcement and funding are necessary for practical outcomes.

  A layered approach—combining technical controls with education and policy—produces the best balance of protection and usability.

9. A Set of Practical, Prioritized Recommendations

Below are prioritized, actionable steps arranged by stakeholder.

For Individual Users (Priority Order)

1. Use a VPN for public Wi-Fi sessions that carry sensitive data.
2. Ensure system and app updates are applied.
3. Disable automatic Wi-Fi connections and verify SSIDs.
4. Use HTTPS sites and avoid entering passwords on pages with certificate warnings.
5. Enable MAC randomization and device firewalls.

For Venue Operators

1. Use secure captive portals (HTTPS), segment guest traffic, and enable client isolation.
2. Keep AP firmware updated and disable unnecessary management services.
3. Publish a clear privacy notice and minimize analytics collection/retention.
4. Provide visible tips to users about safe usage (e.g., signage recommending VPN use).

For App Developers and Service Operators

1. Enforce HTTPS with HSTS; avoid mixed content.
2. Use secure session and cookie practices; implement multi-factor authentication for sensitive services.
3. Implement certificate pinning where feasible with robust update strategies.

For Policymakers and Public Program Designers

1. Fund secure hotspot lending programs with mandatory minimum security/privacy standards.
2. Support digital-literacy campaigns in parallel with access initiatives.
3. Encourage open, privacy-preserving models for public Wi-Fi analytics.

10. Future Directions and Research Gaps

While the broad contours of public Wi-Fi risk are well understood, several areas need further work:

- **Measurement of real-world attacks**: Longitudinal studies quantifying how often public Wi-Fi leads to credential theft or device compromise would inform cost-benefit analyses for policy.
- **Usable security for captive portals**: Design research on captive portals that are secure, privacy-respecting, and easy for operators to deploy—reducing incentive to keep insecure defaults.
- **Privacy-preserving analytics**: Technical solutions enabling venues to collect useful metrics without persistent identifiers deserve wider deployment and standardization.
- **Inclusive secure infrastructure models**: Publicly funded models that provide secure access (managed hotspots, vetted VPNs) for underserved communities warrant piloting and evaluation.

Conclusion:

Public Wi-Fi is a powerful enabler of connectivity and inclusion, but it carries inherent technical and privacy risks. No single technology or policy eliminates those risks; instead, a layered approach that combines device-level protections (VPNs, TLS enforcement, patching), network operator best practices (encryption, segmentation, secure captive portals), application security, user education, and thoughtful policy is necessary. Policymakers must balance digital inclusion goals with minimum security and privacy standards to protect vulnerable populations while preserving access. Finally, ongoing research, measurement, and vendor accountability are essential to adapt defenses to evolving threats.

References:

1. Electronic Frontier Foundation. (2024). *Surveillance self-defense: Tips, tools, and how-tos for safer online communications*. Electronic Frontier Foundation. https://www.eff.org/issues/surveillance-self-defense
2. Federal Communications Commission. (2022). *Public Wi-Fi access, hotspot lending programs, and broadband policy initiatives*. Federal Communications Commission. https://www.fcc.gov

3. Federal Trade Commission. (2023). *Are public Wi-Fi networks safe? What you need to know*. Consumer Advice, Federal Trade Commission. https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe
4. OWASP Foundation. (2021). *Wi-Fi security testing guide*. Open Web Application Security Project (OWASP). https://owasp.org
5. Shinde, D. V. (2022). *Study of public Wi-Fi security challenges and solutions*. *International Research Journal of Humanities and Interdisciplinary Studies (IRJHIS)*. https://irjhis.com/paper/IRJHISIC2203054.pdf
6. Vanhoef, M., & Piessens, F. (2017). *Key reinstallation attacks: Forcing nonce reuse in WPA2*. *Proceedings of the 2017 ACM Conference on Computer and Communications Security (CCS)*. https://www.wired.com
7. WIRED. (2017). *KRACK WPA2 vulnerability: Protocol weaknesses, impacts, and remediation*. *WIRED Magazine*. https://www.wired.com
8. Associated Press. (2023). *FCC funding and policy changes affecting public Wi-Fi and hotspot lending programs*. *AP News*. https://apnews.com