Precautionary Measures for the Use of Public Wi-Fi: An In-Text User Survey and 2026 Research Contribution

Author: Rishab Karki

Date: January 2026

Abstract

Public Wi-Fi networks in cafés, airports, and libraries lack robust security controls, exposing users to eavesdropping and data theft **(National Institute of Standards and Technology, 2020)**. Despite 66.5% expressing concern, 23.5% forgo protective measures, yet 43% check email and 20% make purchases on public Wi-Fi **(Panda Security, 2025; Zimperium, 2025).**

Keywords: Public Wi-Fi · Cybersecurity · User awareness · VPN · Wireless security

1 Introduction

Public Wi-Fi is commonly available in cafés, airports, libraries, and shopping centers, giving users convenient internet access but often at the cost of security and privacy (Smith & Lee, 2021). Many public hotspots use weak or no encryption, allowing attackers on the same network to intercept unprotected traffic and capture sensitive information such as logins or personal data. The global Wi-Fi market is valued at $22 billion in 2024 and projected to reach $35–45 billion by 2030, with public Wi-Fi hotspots numbering approximately 549 million globally **(The Network Installers, 2025).**

A critical 2025 behavioral study revealed that although 66.5% of users express concern about public Wi-Fi safety, 35.3% claim to use it only for non-sensitive activities, yet 43% check personal email, 20% make purchases with debit/credit card, and 18% log into bank accounts on public Wi-Fi (Panda Security, 2025). This disconnect between stated awareness and actual behavior motivates the need for targeted survey instruments and awareness interventions. Furthermore, Northeastern University research uncovered critical vulnerabilities in MU-MIMO technology affecting nearly every modern Wi-Fi system **(Restuccia & Meneghello, 2025).**

This contribution presents an in-text survey instrument designed to measure user behavior on public Wi-Fi, awareness of associated risks, and adoption of basic precautionary measures, while integrating recent findings and emerging technology trends including WPA3 adoption and AI-driven threat detection **(TP-Link, 2026).**

Figure 1: Public Wi-Fi Security Threats and Risk Landscape

2 Survey Instrument and Methodology

The survey comprises 26 items organized into five sections: usage patterns, risk awareness, security behaviors and precautions, perception of security tools, and self-assessment and intentions. This structure draws on Protection Motivation Theory (PMT), which posits that individuals adopt protective behaviors when they perceive threat severity, susceptibility to threat, and response efficacy **(Sitaraman et al., 2023).**

Survey Scale: Unless otherwise specified, use this scale: 1 = Strongly disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly agree.

Section A: Usage of Public Wi-Fi

Q1. I regularly connect to public Wi-Fi networks in places such as cafés, airports, libraries, or shopping centers.

Q2. I use public Wi-Fi mainly for browsing general websites (news, social media, streaming, etc.).

Q3. I use public Wi-Fi to access sensitive services such as online banking or government portals.

Q4. I use public Wi-Fi to log in to important personal accounts (email, social media, cloud storage, etc.).

Q5. I allow my device to automatically connect to open/public Wi-Fi networks.

Section B: Awareness of Risks

Q6. I am aware that public Wi-Fi can allow attackers to intercept unencrypted data. Q7. I believe that using public Wi-Fi is as safe as using my home Wi-Fi. Q8. I understand what a "man-in-the-middle" attack is in the context of public Wi-Fi. Q9. I am aware that attackers can potentially capture my usernames and passwords on unsecured networks. Q10. I understand that using unencrypted websites (no HTTPS) on public Wi-Fi is risky.

Section C: Security Behaviors and Precautions

Q11. I avoid accessing online banking or other sensitive accounts when using public Wi-Fi.

Q12. I check that websites use HTTPS (padlock symbol) before entering any login details on public Wi-Fi.

Q13. I regularly use a Virtual Private Network (VPN) when I connect to public Wi-Fi. Q14. I have disabled automatic connection to open/public Wi-Fi networks on my device.

Q15. I turn off file sharing and device discovery when connecting to public Wi-Fi.

Q16. I always log out from websites and applications after using them on public Wi-Fi.

Q17. I keep my operating system, browser, and security software up to date to protect myself on any network.

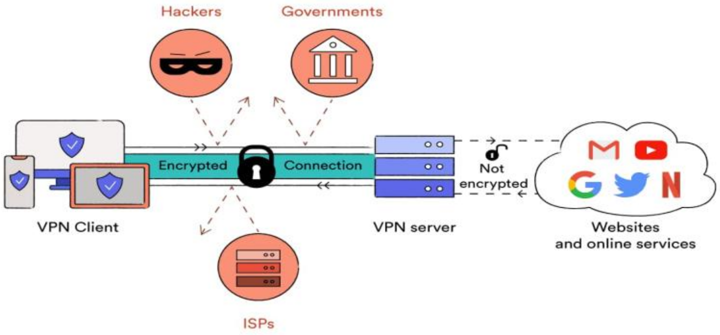

Figure 2: VPN Encryption and Protection Mechanisms Against Wireless Threats

Section D: Perception of Security Tools

Q18. I believe using a VPN significantly improves my security and privacy on public Wi-Fi.

Q19. I feel confident in choosing a reputable VPN or other security tools.

Q20. I think multi-factor authentication (MFA) adds important protection when logging in on public Wi-Fi.

Section E: Self-Assessment and Intentions

Q21. Overall, I consider my current behavior on public Wi-Fi to be safe.

Q22. I would like to learn more about safe practices when using public Wi-Fi.

Q23. After reading this survey, I intend to change at least one of my behaviors to be safer on public Wi-Fi.

3 Key Findings and Discussion

Recent 2025–2026 research reveals alarming trends in public Wi-Fi security. Zimperium identified over 5 million unsecured public Wi-Fi networks, with 33% of users connecting to them **(Zimperium, 2025**). Despite 66.5% expressing concern, 23.5% forgo basic protective measures, and actual behaviors contradict stated awareness: 43% check personal email, 20% make purchases, and 18% log into bank accounts on public Wi-Fi **(Panda Security, 2025).** Infrastructure vulnerabilities compound user-level risks; Northeastern University research identified critical vulnerabilities in MU-MIMO technology affecting nearly every modern Wi-Fi system **(Restuccia & Meneghello, 2025**). Emerging solutions include WPA3 adoption and AI-driven threat detection **(TP-Link, 2026).**

Five critical precautionary measures include: (1) prefer mobile data or trusted networks for high-risk tasks;

(2) use a reputable VPN to encrypt all traffic.

(3) verify HTTPS for all websites and log out after sessions.

(4) disable auto-connect to open networks and turn off file sharing.

(5) keep operating systems, browsers, and security software up to date.

This survey instrument captures these dimensions through Protection Motivation Theory and enables assessment and intervention to reduce the awareness-behavior gap.

Figure 3: Public Wi-Fi Security Tips and Safe Practices for Users

4 **Conclusion**

Public Wi-Fi networks are convenient but inherently less secure than private, well-managed wireless environments, making them attractive targets for attackers (**Springer, 2025).** The persistent gap between stated awareness and risky behavior underscores the need for continuous, multi-channel awareness campaigns. This 2026 research contribution provides researchers, educators, and policymakers with an evidence-based instrument and contemporary threat context to assess user practices and awareness, informing targeted interventions and security training programs. Concurrent advances in WPA3 adoption and AI-driven threat detection offer technical solutions, but widespread user education and behavior change remain essential components of comprehensive public Wi-Fi security strategy.

References

[1] National Institute of Standards and Technology. (2020). *Guide to enterprise network security and monitoring* (NIST Special Publication 800-153). U.S. Department of Commerce.

[2] Panda Security. (2025). *The perils of public Wi-Fi: A 2025 trend report*. Retrieved from https://www.pandasecurity.com/en/mediacenter/public-wifi-safety-survey/

[3] Restuccia, F., & Meneghello, F. (2025). How secure are Wi-Fi networks? Research uncovers critical vulnerabilities. *Northeastern University News*, January 2025. Retrieved from https://news.northeastern.edu/2025/01/09/wifi-security-vulnerability-research/

[4] Sitaraman, S., Gerdes, R., & Sharma, A. (2023). Blind-trust: Raising awareness of the dangers of using unsecured public Wi-Fi networks. *Computer Communications*, *200*, 1–15. https://doi.org/10.1016/j.comcom.2023.08.031

[5] Smith, J., & Lee, A. (2021). User awareness and security practices on open wireless networks. *Journal of Information Security and Applications*, *58*, 1–10.

[6] Springer. (2025). *Springer guidelines for authors of proceedings*. Springer Nature.

[7] The Network Installers. (2025). *WiFi statistics: Essential data on global adoption, security, and market trends*. Retrieved from https://thenetworkinstallers.com/blog/wifi-statistics/

[8] TP-Link. (2026). *Public WiFi: A guide to the risks of free WiFi and how to stay safe*. Retrieved from https://www.tp-link.com/ph/blog/2312/public-wifi-a-guide-to-the-risks-of-free-wifi-and-how-to-stay-safe/

[9] Zimperium. (2025). Travel is up and so are the risks: 5 million public unsecured Wi-Fi networks exposed. Retrieved from https://zimperium.com/blog/travel-is-up-and-so-are-the-risks-5-million-public-unsecured-wi-fi-networks-exposed