Anthony Hertel

IT 104-009

September 4, 2025

Public Wi■Fi Vulnerabilities and Firewall Protections

Introduction

Public Wi■Fi is available almost everywhere, which makes it easy to check email, homework, or even banking while away from home. Convenience does not mean safety, though. Open or poorly secured hotspots can expose passwords, messages, and financial details to attackers who share the same network (Tamez Cavazos, 2016).

Potential Benefits

Public Wi■Fi still offers real value. Free access helps students and workers stay productive in places like airports, cafés, and libraries. It also supports people who do not have reliable home internet, reducing barriers to basic online services (Express Computer, 2016).

Legal and Ethical Issues

Risks on shared networks can lead to legal or ethical problems. Users may unintentionally share copyrighted material, visit restricted sites, or spread malware over a public network. Providers also have responsibilities: post clear terms of use, apply basic protections, and warn customers about threats such as fake access points (Allen, 2025).

Security and Social Concerns

Attackers sometimes create “evil twin” hotspots or use man■in■the■middle techniques to intercept traffic on open Wi■Fi (NPR, 2010). Good habits help: prefer HTTPS, enable a reputable VPN, and keep a host firewall turned on to block unsolicited connections (AI■Driven Firewall Log Analysis, 2025). These steps reduce exposure even when a network itself is not trustworthy.

Future Research

Ongoing work is exploring AI■assisted monitoring, stronger encryption, and easier■to■use privacy tools so average users can stay safe by default (Tikanmäki et al., 2025). Education also matters: simple checklists in schools and public spaces can remind people to avoid sensitive logins and to verify network names with staff.

Conclusion

Public Wi■Fi is convenient and useful, but the risks are real. With a few practical steps—verify the network, use HTTPS and a VPN, and keep your firewall enabled—people can enjoy free connectivity while protecting their personal information (Tamez Cavazos, 2016; Allen, 2025).

References

Allen, J. (2025). The cybersecurity risks of mobile lawyering. GPSolo, 42(3), 52–57.

AI■Driven Firewall Log Analysis: Enhancing Threat Detection with Deep Learning Techniques. (2025). International Journal of Advanced Computer Science and Applications, 16(7).

Express Computer. (2016). Use public Wi■Fi? How to stop people snooping while you surf in public Wi■Fi service.

NPR. (2010). The Zombie Network: Beware “Free Public Wi■Fi”.

Tamez Cavazos, F. J. (2016). Free Wi■Fi: Is it safe? EDUCAUSE Review (Online).

Tikanmäki, I., Blek, T., Niskakangas, J., & Varamäki, K. (2025). Enhancing cybersecurity in healthcare.